**Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
Національна бібліотека України імені В. І. Вернадського**

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 12 (грудень)

Київ – 2022

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2022.– №12 (грудень) . – 414 с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова, С.Дорогих. Дизайн обкладинки С.Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

ЗМІСТ

«Україна реформує професійну освіту в галузі кібербезпеки. Зокрема, Держспецзв'язку та USAID вже впроваджують перші шість нових стандартів.

Реформа ґрунтується на створенні в Україні мережі незалежних кваліфікаційних центрів, повідомили у Держспецзв'язку. Нові центри поліпшуватимуть можливості професійного зростання та підтвердження кваліфікації наявних на ринку фахівців.

Торік до державного класифікатора професій додали 17 професій, що стосуються кіберзахисту та інформаційної безпеки. Зараз розробили перші шість професійних стандартів для таких професій:

- Розробник систем захисту інформації
- Адміністратор мереж і систем
- Фахівець сфери захисту інформації
- Аналітик з безпеки інформаційно-телекомунікаційних систем
- Фахівець з питань безпеки
- Інструктор-методист з інформаційної безпеки та кібербезпеки.

Від наступного року в Україні мають з’явитися незалежні кваліфікаційні центри. У них фахівці, які здобули освіту, зможуть підтвердити відповідність своїх знань, навичок та компетенцій посадам, на які претендують. Затверджені стандарти допоможуть роботодавцям створювати плани кар’єрного розвитку для своїх працівників, кажуть у відомстві». ***(Руслан Сорока. В Україні реформують сферу кібербезпеки та впроваджують шість нових стандартів // Speka.Media (https://speka.media/v-ukrayini-reformuyut-sferu-kiberbezpeki-ta-vvodyat-sist-novix-standartiv-9e033v). 30.11.2022).***

***

«Хотів би наразі проговорити кілька кібербезпекових ризиків, про які потрібно пам'ятати кожному та кожній. Особливо про них треба пам'ятати під

час війни, адже росія агресивно використовує кіберметоди для досягнення своїх цілей. Нам не варто бути наївними в цьому питанні — це точно.

Остерігайтесь фішингу

Кількість фішингових посилань, які блукають зараз інтернетом, просто захмарна. Це — спроба алгоритмічного зламу тисяч акаунтів одночасно, тобто в промислових масштабах. Що зараз шукають багато українців та українок? Роботу. А тому тобі можуть кинути на пошту підбірку вакансій із фішинговими лінками, а ти й купишся. Громадяни, не клікайте бозна на що, що падає вам у пошту! Не відкривайте файли, з приводу яких маєте підозри. Мисліть критично.

Правильно поводьтеся у соцмережах

З самого початку війни до мене в Інстаграмі додаються акаунти з напівоголеними жінками, а деякі з них пропонують переписку. Ці акаунти хочуть взаємодіяти. Очевидно ж, що це — кіберзагроза. У Фейсбуці мене таргетують сайти знайомств з жінками та різноманітні лінії підтримки для невпевнених в собі, розчарованих чоловіків. Дивно. Я — дуже впевнений в собі, успішний чоловік. Жодних приводів для потрапляння в аудиторію ось такого таргетингу я ніколи не давав. Нічого такого не гуглив. Значить, це фішинг. Будьте обережні й ви.

Не встановлюйте підозрілі мобільні додатки

В жодному разі не завантажуйте собі на телефон мобільні додатки невідомого походження. Зокрема, в сегменті криптовалют та операцій з ними. Тут купа діяльності російських кіберслужб, а також банального фінансового шахрайства. Хочете завести собі криптогаманець — зверніться до фахівця, проконсультуйтесь. А якщо такої змоги нема, завантажуйте додатки лише з фірмового магазину додатків (Google Play чи AppStore) або офіційного сайту гаманця (якщо мова йде про комп'ютер). Ці поради стосуються всіх додатків та комп'ютерних програм загалом, а не тільки криптогаманців.

Регулярно оновлюйтесь

Неодмінно оновлюйте операційну систему на комп'ютері та телефоні, щойно вам пропонується така опція. Це дуже важливо. Технологічні розробники дбають про нас під час війни, знаючи, що росія веде проти українців кібервійну. Навіщо це

робити? В кожному оновленні закриваються вразливості, що були у попередніх версіях, тож актуальна версія ОС завжди більш захищена за попередні.

Ігноруйте незнайомців

Не вступайте в довірливу розмову, переписку з незнайомцями в мережі. Ігноруйте зайві запити на переписку від незнайомих людей. Обов'язково передайте цю пораду своїм дітям. Шахрайства та російської агентурної роботи зараз дуже багато, особливо в інтернеті, в соцмережах.

Не користуйтесь підозрілими сайтами

Уважно обирайте, з якими веб-сайтами ви взаємодієте в інтернеті. Уникайте тих сайтів, де в якості банерної реклами пропонується зіграти у віртуальне казино, відвідати порносайт чи ще щось подібне. Якщо можливо, не дозволяйте сайту обмінюватися з вами cookies, особливо якщо це невідомий для вас сайт.

Також не купуйте, не здійснюйте оплату за товари на веб-сайтах, що є для вас маловідомими. Вас можуть просто розвести, кинути на гроші. Фінансових шахрайських схем зараз чимало. Злочинці можуть обладнати шахрайську схему навіть на відомому майданчику електронної комерції, тому там теж будьте обережні.

Не лишайте компромат на себе

Не робіть в інтернеті нічого такого, що змушувало би вас щоразу очищувати історію веб-перегляду, адже якщо вас зламають, вона може потрапити в руки зловмисників. Історія веб-перегляду в браузері також відіграє певну захисну роль, тому коли вона порожня, ви потрапляєте в цілу низку неприємних ситуацій: всі сайти заново починають пропонувати обмінятися вам файлами cookies, а браузер втрачає можливість попередити вас, що ви робите в інтернеті щось не те.

Якщо вам все ж таки треба пошукати щось потенційно компрометуюче (тут кожен визначає сам для себе, що саме), користуйтесь приватними вікнами в браузерах. Їх використання не залишає ніяких слідів в історії веб-переглядача.

Слідкуйте за станом пристрою

Не забувайте тримати певну кількість вільної пам'яті на телефоні та комп'ютері. Вам можуть штучно забити пам'ять, щоб ви працювали в інтернеті

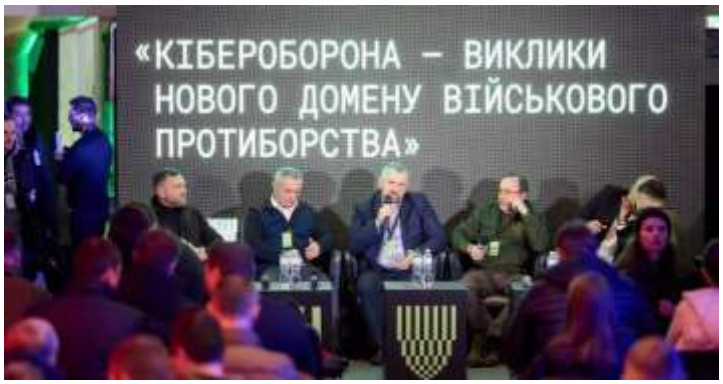
повільніше. Зокрема, Telegram зберігає гігантську кількість кешу, котрий регулярно слід очищувати або виставити в настройках програми автоочищення через задані періоди часу. Також мала кількість пам'яті загалом погано впливає на роботу пристрою: він може почати працювати повільніше, а деякі програми можуть взагалі не запускатися.

Якщо у вас є можливість, оновіть свою техніку. Бути на зв'язку під час війни — вкрай важливо. Тому якщо ваш телефон то працює, то не працює, подумайте над купівлею нового. Але це, звісно, якщо у вас є гроші.

Якщо зайвих коштів немає, спробуйте скинути пристрій до заводських налаштувань. Так, вам доведеться заново встановлювати усі додатки та настроювати телефон, але ця процедура іноді допомагає розв'язати проблеми з частими зависаннями та непрацездатністю апарату». ***(Іван Верстюк. Подбайте про кібербезпеку: вісім порад на час війни // Speka.Media (https://speka.media/dbajete-pro-kiberbezpeku-10-porad-na-cas-viini-pn1r4v). 30.11.2022).***

***

«У Києві відбувся National Defence Hackathon 2022*, у межах якого провели кілька панельних дискусій, де представники державного і приватного секторів обговорювали питання взаємодії кіберзахисту, протидії дезінформації та ІТ-галузі. Особливу увагу приділили правовому статусу кіберволонтерів.



Необхідно якнайшвидше ухвалити закон про створення та функціонування у системі Міноборони кібервійськ

В Україні є кілька інституцій, які займаються кіберобороною: від військової розвідки, Сил спеціальних операцій, Командування військ зв'язку і кібербезпеки до хактивістів і волонтерів, що проводять акції з власної ініціативи.

Завдання — убезпечити людей

У Міноборони під активною кібероборoною мають на увазі дії, спрямовані на те, щоб добути важливу для супротивника інформацію, зрозуміти, на які точки можна надавити, щоб вивести з ладу ті чи інші об'єкти. Полем діяльності стає інтернет і приєднані до нього мережі — банки, об'єкти зв'язку та енергетики.

Але є проблема: ця діяльність юридично слабо регламентована. Тому заступник міністра оборони Олег Гайдук упевнений, що учасники таких акцій мають отримати офіційний статус, щоб надалі уникнути проблем із законом.

«Той, хто чинить активні дії стосовно, наприклад, енергетичного сектору (росії), хай він і пов'язаний із військовими, у мирний час підпадає під кримінальну відповідальність, під час воєнного стану це може вважатися військовим злочином, — каже Гайдук. — Якщо сьогодні цим питанням не перейнятися, то через 5-10 років це може стати неприємною несподіванкою. Думаю, що разом із законодавцями ми маємо це обговорити і знайти інструменти, щоб убезпечити наших людей, які будуть цим займатися».

Керівник служби з питань інформаційної та кібербезпеки апарату РНБО України — секретар НКЦК Наталія Ткачук зазначила, що в України є потужна армія кіберволонтерів, професійні спеціалісти держсектору та підтримка від бізнесу. І зараз важливо напрацювати чітке, прозоре та ефективне законодавче поле, яке стане основою дієвої системи кібероборони.

«Необхідно якнайшвидше ухвалити закон про створення та функціонування у системі Міноборони кібервійськ, який має стати підґрунтям для розбудови спроможностей держави щодо кібероборони, залучення до цієї діяльності кіберволонтерів та створення кіберрезерву. Також у міжнародному праві необхідно

запровадити чіткі критерії, які б визначали межу, після якої має відбутися колективна відповідь членів НАТО на кібератак, — каже Ткачук.

Народний депутат Олександр Федієнко наголошує, що в Україні є закони, які регламентують засади гарантування кібербезпеки і трохи вирішують питання роботи українських фахівців, які захищають нашу державу у кіберпросторі. Але ці законодавчі норми поширюються лише на національний кіберпростір.

«Тобто ми не можемо застосовувати закон щодо кіберзахисту, кібероборони, якщо проводимо активну фазу кібератаки в іншому кіберпросторі, — каже він. — Закон регламентує лише захист наших національних інтересів».

Заступник міністра цифрової трансформації Єгор Дубинський каже, що діяльність ІТ-армії викликає дуже великий інтерес з боку іноземних партнерів.

«Дії нашого ІТ-ком'юніті були таким ж нормальними, як і дії тероборонівців, які 24 лютого взяли до рук зброю. Всі вони захищають свою державу. У жодній країні такого феномену не було», — сказав він.

За словами Дубинського, українське ІТ-ком'юніті мобілізувалося і має значний потенціал, який можна за допомогою Міноборони, Ради національної безпеки і оборони України, Держспецзв'язку та інших відомств спрямувати на напрацювання нових продуктів у сфері кіберзахисту.

Заступник секретаря РНБО України Сергій Демедюк вважає, що кіберпростір є особливою сферою, де звичайні засоби ведення війни застосувати неможливо, а відбувається змагання з ворогом у технологіях і способах передання даних. Тому лише об'єднання зусиль спеціалістів із кібербезпеки державного та приватного секторів дозволить сформувати потужний захист.

Денис Гурський, голова правління і співзасновник SocialBoost, партнера Національного оборонного хакатону — 2022, говорить про важливий внесок кіберспеціалістів. «Повномасштабне вторгнення росії мобілізувало українську tech-спільноту, — каже він. — Ми бачимо, як сотні спеціалістів покинули роботу над власними стартапами та зосередили свої зусилля саме на забезпеченні кіберзахисту держави; наприклад, деякі співробітники SocialBoost-напряму долучилися до цього руху. Вважаємо, партнерство урядових організацій, комерційних компаній та

громадських організацій технологічного напряму має синергетичний ефект у розвитку української кібербезпеки».

«На українських хакерів все це не дуже впливає»

SPEKA поцікавилась у практика — співзасновника «Українського кіберальянсу» Андрія Барановича, чи відчувають хактивісти потребу в такому захисті.

Він каже, що від 2014 року разом із колегами влаштовує акції, спрямовані проти рф. Хактивісти ніколи не приховували, що це справа їхніх рук, у росії проти них неодноразово порушували кримінальні справи.

«За цей час російська федерація жодного разу не намагалася скористатися міжнародним правовим співробітництва з Інтерполом. І я не бачу, як відсутність чи наявність українського закону може вплинути на росію чи міжнародне законодавство, яке від українських законів не залежить, — підкреслює Баранович. — Якщо росіяни захочуть звернутися до Інтерполу, вони це зроблять. Їм, звісно, відмовлять, бо ця справа буде політично вмотивованою».

Представник «Українського кіберальянсу» скептично ставиться до розмов про захист активістів. Він упевнений, що можновладці наслухалися дослідників на кшталт Стефана Соесанто з Університету Цюриха.

«Вони дуже специфічно трактують міжнародне гуманітарне право, не враховують, що ці закони писали для мирного часу, а під час війни діють Laws of Armed Conflict — зовсім інший розділ міжнародного законодавства, — каже Андрій. — Там теж виникають проблеми з усіма цими конвенціями, але насправді на українських хакерів все це не дуже впливає».

Однак співрозмовник Speka вважає, що офіційний статус хактивістам не завадить, тому що це дозволить взаємодіяти з державою у правовому полі.

«Загалом створення кібер- або ІТ-армії — справа вкрай необхідна. У нас є війська зв'язку, є розвідка та контррозвідка, тож має бути і свій кібер, — каже Баранович. — Розмови про це точаться з 2015-2016 років, але відтоді, по суті, нічого не змінилося: держава та волонтери працюють окремо».

*National Defence Hackathon-2022 організувало Міністерство оборони України спільно з Генштабом Збройних сил України, Національним координаційним центром кібербезпеки та Центром протидії дезінформації за підтримки CRDF Global в Україні, Держдепартаменту США, НАТО та Посольства Сполученого Королівства Великої Британії, Північної Ірландії в Україні, ГО SocialBoost. Технологічний партнер: Cyber Unit Technologies». ***(Олексій Батурін. Кібервійсько: влада розмірковує над статусом IT-спільноти, яка захищає Україну в кіберпросторі // Speka.Media (https://speka.media/kiberviisko-vlada-rozmirkovuje-nad-statusom-it-spilnoti-yaka-zaxishhaje-ukrayinu-v-kiberprostori-pjndq9). 05.12.2022).***

***

«Мобільний оператор «Київстар» придбав для «Українського державного центру радіочастот» нове технологічне обладнання на 55 млн гривень. Його будуть використовувати для посилення кіберзахисту України та протидії інформаційним загрозам.

«Сьогодні Україна захищається не лише від прямих військових атак, а й від постійних кіберзагроз. Тому Київстар системно інвестує у відновлення і посилення цифрового захисту країни», — прокоментував подію CEO «Київстар» Олександр Комаров.

Закупівлю обладнання та реалізацію благодійного проєкту здійснював фонд «Київська школа економіки».

«Російське вторгнення обернулось для українців багатьма викликами, які нам ще доведеться подолати. Одним з них є розвиток кібербезпеки, не очевидного, але важливого фактору в сучасній війні», — зазначили директорка фонду Світлана Денисенко.

В «Київстар» зазначили, що раніше компанія вже виділила 300 мільйонів гривень для відновлення цифрової інфраструктури України в рамках програми United24, з яких 150 мільйонів гривень вже переказано на рахунок НБУ.

Раніше SPEKA розповідала, що «Київстар» оголосив про створення нового бізнесу – IT-компанії Kyivstar.Tech, яка стала резидентом Дія.City.» ***(Руслан Сорока. «Київстар» виділив 55 млн гривень для посилення кіберзахисту України // Speka.Media (https://speka.media/kiyivstar-vidiliv-55-mln-griven-dlya-posilennya-kiberzaxistu-ukrayini-v58m1v). 14.12.2022).***

***

«Блокування операторів торкнулося й України. Через це реєстрація українців у Twitter з телефону стала неможливою — при спробі авторизуватися за номером телефону з'ясовується, що коду України немає у списку. Це все, що треба знати про свободу слова від Маска.

У неділю Ілон Маск написав у Twitter розпливчасте попередження: «завтра на ботів чекає сюрприз». У чому полягав сюрприз, він не сказав. Але ц наступні години Twitter заблокував трафік від приблизно 30 операторів мобільного зв'язку по всьому світу, фактично відрізавши доступ до сотень тисяч облікових записів, насамперед в Азіатсько-Тихоокеанському регіоні, включаючи Україну, великі території росії, Індонезії, Індії та Малайзії, повідомляє Platformer.

Коду України немає у списку

Проєкт був частиною спроби Ілона Маска прибрати у Twitter спам. Але замість того, щоб працювати над видаленням окремих правопорушників, компанія виявила мобільні мережі, пов'язані з великими спам-мережами в певних країнах, і заблокувала користувачів, які покладалися на ці мережі, від отримання SMS-повідомлень від Twitter, впливаючи на людей із двофакторною автентифікацією. Потім Twitter повністю заблокував трафік від цих операторів.

Майже одразу почали надходити скарги, оскільки законні користувачі виявили, що не можуть отримати доступ до Twitter.

У Slack інженер Twitter поділився електронним листом від одного провайдера зв'язку, який сказав, що користувачі скаржаться, що Twitter перестав працювати. Компанія швидко розблокувала операторів і повідомила їм, що проблеми з обслуговуванням виникли через «зміни конфігурації маршрутизації».

Цей інцидент підкреслює зростаючу плутанину в Twitter, оскільки компанія намагається виконувати непостійні команди Маска з його постійно зменшуючим набором інженерів. У деяких випадках, як у випадку з телекомунікаційним питанням, компанію звинувачують у внесенні величезних змін без належної перевірки їхніх потенційних наслідків…». ***(Катерина Колонович. Маск хотів забанити ботів: Twitter заблокував трафік українських та близько 30 операторів мобільного зв'язку по всьому світу // Speka.Media (https://speka.media/mask-xotiv-zabaniti-botiv-twitter-zablokuvav-trafik-priblizno-30-operatoriv-mobilnogo-zvyazku-po-vsyomu-svitu-9q6y2v). 13.12.2022).***

***

Правове забезпечення кібербезпеки в Україні

«Президент України Володимир Зеленський підписав Закон 2807-IX (законопроект № 6241) «Про Національну програму інформатизації». Завдяки програмі держоргани зможуть оперативніше комунікувати один з одним і приймати рішення з певних питань, а українці – отримувати держпослуги швидше.

Згідно із Законом, у держуправлінні швидше впроваджуватимуть цифрові технології, що позитивно вплине на результативність та ефективність роботи держорганів.

Закон передбачає створення та функціонування Єдиної інформаційної системи обліку Національної програми інформатизації (ЄІСОНПІ). Вона призначена для формування, контролю, моніторингу, обробки та зберігання

програм, завдань, проєктів і робіт Національної програми інформатизації та матеріалів до них.

Завдяки Національній програмі інформатизації буде можливість вирішити ряд завдань, зокрема:

- забезпечити розвиток інформаційного суспільства;
- застосовувати інформаційні та цифрові технологій у державному управлінні та суспільно-економічних відносинах;
- подолати цифрової нерівність;
- використовувати та розвивати сучасні інформаційні системи, комунікаційні мережі, інформаційні ресурси й інформаційні технології для забезпечення безпеки інформаційної діяльності та кіберзахисту, шляхом побудови, розвитку, інтеграції та;
- інтегрувати Україну у світовий інформаційний простір.
- Закон набуває чинності 1 березня 2023 року». ***(Цифрові технології в держуправлінні: Президент підписав Закон про Національну програму інформатизації // Офіційний веб-сайт Міністерства цифрової трансформації України (https://thedigital.gov.ua/news/tsifrovi-tekhnologii-v-derzhupravlinni-prezident-pidpisav-zakon-pro-natsionalnu-programu-informatizatsii). 26.12.2022).***

***

Кібервійна проти України. Російсько-українська війна

«В Украину доставили оборудование и программное обеспечение, которое позволит лучше подготовиться к новым российским кибератакам.

2 декабря Европейский союз открыл в Киеве лабораторию киберзащиты, которой будут пользоваться Вооруженные силы Украины. Подробности проекта на официальном сайте сообщила Европейская служба внешних действий.

Руководство ЕС воспользовалось Европейским фондом мира, чтобы закупить и отправить в Украину оборудование, программное обеспечение и инструменты защиты, необходимые для открытия кибернетической лаборатории. Она призвана

усилить киберзащиту ВСУ, а именно: своевременно выявлять попытки взлома информационных систем, предотвращать и отражать кибератаки.

Киберлаборатория — это учебная и исследовательская среда, состоящая из нескольких виртуальных и физических компонентов. Представленные в ней технологии позволяет пользователям создавать реалистичную виртуальную среду для симуляции защиты в режиме реального времени. Кроме того, лаборатория станет тренировочной площадкой, где будут готовить новых военных специалистов по кибербезопасности и улучшать навыки уже опытных экспертов. В ЕС уверены, что благодаря этим усилиями украинцы в ближайшем будущем смогут быстрее и эффективнее бороться с хакерами.

«В смоделированной сети представители Вооруженных Сил Украины могут научиться справляться с высоким уровнем стресса, обнаруживая и исследуя уязвимости в различных сетевых системах. Киберлаборатория и улучшенная сетевая безопасность помогают украинским военным развивать навыки выявления, мониторинга и противодействия кибератакам», — отмечается в пресс-релизе…» ***(Евросоюз создал в Украине киберлабораторию для ВСУ: зачем она нужна украинцам // ФОКУС (https://focus.ua/digital/539470-evrosoyuz-sozdal-v-ukraine-kiberlaboratoriyu-dlya-vsu-zachem-ona-nuzhna-ukraincam). 03.12.2022).***

***

«У столиці відбулися другі командно-штабні навчання стратегічного рівня «Національна кіберготовність – 2022». Про це повідомили у Держспецзв'язку.

Захід, який пройшов декілька днів тому, організував Національний координаційний центр кібербезпеки при РНБО за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України».

Участь у навчаннях взяли представники всіх основних систем кібербезпеки України, а також делегати низки міністерств та об'єктів критичної інфраструктури держави. На навчаннях відпрацювали взаємодію відомств під час реагування на кібератаки.

«Набуття управлінцями практичних навичок зі взаємодії та координації, аналізу ситуації та ухвалення рішень надзвичайно важливе для забезпечення кіберстійкості як окремих органів та установ, секторів, так і держави в цілому» – підкреслили у Держспецзв'язку.

Раніше SPEKA розповідала, що 5 грудня набрав чинності закон про уповноважений орган у сфері захисту критичної інфраструктури. Зміни у законі передбачають, що Держспецзв'язку буде уповноваженим органом з питань захисту критичної інфраструктури під час дії воєнного стану, а також протягом 12 місяців після нього». ***(Руслан Сорока. У Києві пройшли навчання з питань кібербезпеки від РНБО та USAID // Speka.Media (https://speka.media/u-kijevi-proisli-navcannya-z-pitan-kiberbezpeki-vid-rnbo-ta-usaid-p0q0yv). 06.12.2022).***

***

«Российские ракеты не могут уничтожить облако», — пояснил министр цифровой трансформации Украины.

ЛАС-ВЕГАС. В феврале прошлого года, когда российские вооруженные силы надвигались на страну, правительство Украины приняло решение перенести терабайты важных правительственных данных в облако, чтобы сохранить интегрированные цифровые услуги для украинцев в условиях ракетных ударов и пулеметных обстрелов.

Amazon Web Services, один из первых партнеров Украины, работала с небольшой группой правительственных чиновников над доставкой трех своих устройств Snowball из Дублина в Украину через Польшу в первые дни российского вторжения. Каждое устройство Snowball — периферийное вычислительное устройство, предназначенное для передачи данных в облако и из него, — способно хранить до 80 терабайт данных в автономном режиме. По словам вице-премьер-министра и министра цифровой трансформации Украины Михаила Федорова, в момент непосредственного начала российской агрессии экстренная миграция в облако оказалась критически важной для непрерывности предоставления государственных услуг в Украине.

«AWS помогла нам в самые первые дни полномасштабного вторжения, — сказал Федоров во вторник, выступая на конференции AWS re:Invent в Лас-Вегасе. «Руководство AWS приняло решение, которое спасло украинское правительство и экономику. Решением по сохранению украинских баз данных и госреестров стала облачная миграция. Что нам больше всего нравится в этом партнерстве с облачными компаниями, так это то, что российские ракеты не могут разрушить облако».

Федоров добавил: «Позвольте мне быть с вами честным. Это бесценно. Государственные реестры и базы данных являются критической информационной инфраструктурой».

Лиам Максвелл, директор AWS по цифровой трансформации правительства, объяснил, что небольшая группа «амазонцев» встретилась с послом в посольстве Украины в первый день российского вторжения, чтобы определить, «что мы могли бы помочь им создать резервную копию, в том числе такие вещи, как регистр народонаселения, владение землей и недвижимостью, записи об уплате налогов, записи об образовании».

«Это заложило основу для создания стратегического шага, чтобы помочь украинскому правительству и защитить их цифровую инфраструктуру», — сказал Максвелл, выступая вместе с Федоровым.

Миграция в облако помогла существующим украинским технологиям оцифровать государственные услуги с помощью приложения для смартфонов под названием «Дия». Несмотря на то, что Украина продолжает защищаться от российских войск как на поле боя, так и в киберпространстве, Федоров сказал, что Украина скоро представит услугу цифровой ипотеки и планирует продолжить оцифровку своего правительства.

«Мы ежедневно сталкиваемся с кибератаками, это кибервойна», — сказал он, добавив, что Россия продолжает угрожать своей энергетической инфраструктуре. «Под атакой находится наша критическая инфраструктура. Но нам удалось защитить [его], и каждую неделю мы запускаем какие-то новые публичные ресурсы. Цифровизация — лучший ответ на этот вызов».

Максвелл возразил, когда журналисты спросили, подвергалась ли сама AWS усилению кибератак со стороны России в отместку за ее помощь Украине.

«У нас была возможность защитить себя, — сказал Максвелл.

Максвелл и Федоров воспользовались конференцией, чтобы подписать меморандум о взаимопонимании, чтобы продолжить свое многообещающее партнерство. AWS — одна из нескольких американских технологических компаний, включая Microsoft и Google, получивших приз мира от президента Украины Владимира Зеленского за их усилия по оказанию помощи нации». ***(Frank Konkel. Ukraine Tech Chief: Cloud Migration 'Saved Ukrainian Government and Economy' // Nextgov (https://www.nextgov.com/cxo-briefing/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/). 01.12.2022).***

***

«У Microsoft розповіли, що взимку росія може посилити свої кібератаки. Країна-терорист таким чином планує тиснути на джерела військової та політичної підтримки України як внутрішньої, так і зовнішньої.

У дописі в блозі генеральний менеджер центру аналізу цифрових загроз Microsoft Клінт Воттс закликав клієнтів підготуватися до нових російських кібератак взимку, пише Bloomberg.

«Недавнє виконання російськими військовими розвідниками атаки в стилі програми-вимагача, відомої як Prestige, у Польщі може бути передвісником подальшого поширення росією кібератак за межі кордонів України», — сказав Воттс.

Воттс також розповів, що, разом з ракетними та безпілотними ударами по цивільній інфраструктурі України, відбулися «додаткові» кібератаки на українські та іноземні ланцюги постачання.

«Ці зусилля мають на меті підірвати політичну підтримку України США, ЄС і НАТО, а також похитнути впевненість і рішучість українських громадян», — резюмував Воттс». ***(Руслан Сорока. Microsoft: росія посилить кібератаки на***

Україну та союзників // Speka.Media (https://speka.media/microsoft-rosiya-posilit-kiberataki-na-ukrayinu-ta-soyuznikiv-pn1xrv). 04.12.2022).

***

«Тем временем российская пропаганда стремится усилить накал народного несогласия по поводу энергетики и инфляции в Европе.

Как мы более подробно сообщаем ниже, после военных потерь России на Украине этой осенью Москва активизировала свой многоаспектный гибридный технологический подход, чтобы оказать давление на источники военной и политической поддержки Киева, как внутри страны, так и за ее пределами. Этот подход включал в себя разрушительные ракетные и кибердары по гражданской инфраструктуре в Украине, кибератаки на украинские, а теперь и зарубежные цепочки поставок, а также операции влияния с использованием кибернетики — направленные на то, чтобы подорвать политическую поддержку Украины со стороны США, ЕС и НАТО и поколебать уверенность и решимость граждан Украины.

В последние месяцы субъекты киберугроз, связанные с российской военной разведкой, предприняли разрушительные атаки против энергетических, водных и других критически важных инфраструктурных сетей в Украине, поскольку ракетные удары отключили подачу электроэнергии и воды гражданскому населению по всей стране. Российские военные операторы также распространили деструктивную киберактивность за пределы Украины на Польшу, критически важный логистический узел, в возможной попытке помешать перемещению оружия и припасов на фронт.

Между тем, российская пропаганда стремится усилить накал народного несогласия по поводу энергетики и инфляции по всей Европе, продвигая отдельные нарративы в Интернете через государственные СМИ и аккаунты в социальных сетях, чтобы подорвать выборных должностных лиц и демократические институты. На сегодняшний день они оказали лишь ограниченное влияние на общественность, но они предвещают то, что может стать тактикой расширения в предстоящую

зиму». ***(Preparing for a Russian Cyber Offensive Against Ukraine This Winter // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/preparing-for-a-russian-cyber-offensive-against-ukraine-this-winter/). 06.12.2022).***

***

«Как мы более подробно сообщаем ниже, после военных потерь России на Украине этой осенью Москва активизировала свой многоаспектный гибридный технологический подход, чтобы оказать давление на источники военной и политической поддержки Киева, как внутри страны, так и за ее пределами. Этот подход включал в себя разрушительные ракетные и кибердудары по гражданской инфраструктуре в Украине, кибератаки на украинские, а теперь и зарубежные цепочки поставок, а также операции влияния с использованием кибернетики — направленные на то, чтобы подорвать политическую поддержку Украины со стороны США, ЕС и НАТО и поколебать уверенность и решимость граждан Украины.

В последние месяцы субъекты киберугроз, связанные с российской военной разведкой, предприняли разрушительные атаки против энергетических, водных и других критически важных инфраструктурных сетей в Украине, поскольку ракетные удары отключили подачу электроэнергии и воды гражданскому населению по всей стране. Российские военные операторы также распространили деструктивную киберактивность за пределы Украины на Польшу, критически важный логистический узел, в возможной попытке помешать перемещению оружия и припасов на фронт.

Между тем, российская пропаганда стремится усилить накал народного несогласия по поводу энергетики и инфляции по всей Европе, продвигая отдельные нарративы в Интернете через государственные СМИ и аккаунты в социальных сетях, чтобы подорвать выборных должностных лиц и демократические институты. На сегодняшний день они оказали лишь ограниченное влияние на общественность, но они предвещают то, что может стать тактикой расширения в предстоящую зиму.

Мы считаем, что эти недавние тенденции предполагают, что мир должен быть готов к нескольким направлениям потенциальной российской атаки в цифровой сфере в течение этой зимы. Во-первых, можно ожидать продолжения кибернаступления России на критически важную инфраструктуру Украины. Мы также должны быть готовы к тому, что недавнее выполнение российской военной разведкой атаки в стиле программы-вымогателя, известной как Prestige, в Польше может быть предвестником дальнейшего распространения кибератак России за пределы Украины. Такие кибероперации могут быть нацелены на те страны и компании, которые этой зимой обеспечивают Украину жизненно важными цепочками поставок помощи и оружия.

Во-вторых, мы также должны быть готовы к тому, что операции по влиянию с помощью кибернетики, нацеленные на Европу, будут проводиться параллельно с действиями по киберугрозам. Россия будет стремиться использовать трещины в народной поддержке Украины, чтобы подорвать коалиции, необходимые для устойчивости Украины, в надежде ослабить гуманитарную и военную помощь, поступающую в регион. Хорошая новость заключается в том, что, имея больше информации, общественность, подкованная в средствах массовой информации, может действовать осознанно и рассудительно, чтобы противостоять этой угрозе.

Вот что мы видим в Microsoft с тех пор, как контрнаступление Украины вынудило российскую армию отступить, как, по нашим прогнозам, российские кибероперации и операции по оказанию влияния могут выглядеть в зимние месяцы, и как мы в Microsoft поможем подготовиться и предотвратить причинение вреда клиентам Microsoft и демократии перед лицом этих нападений.

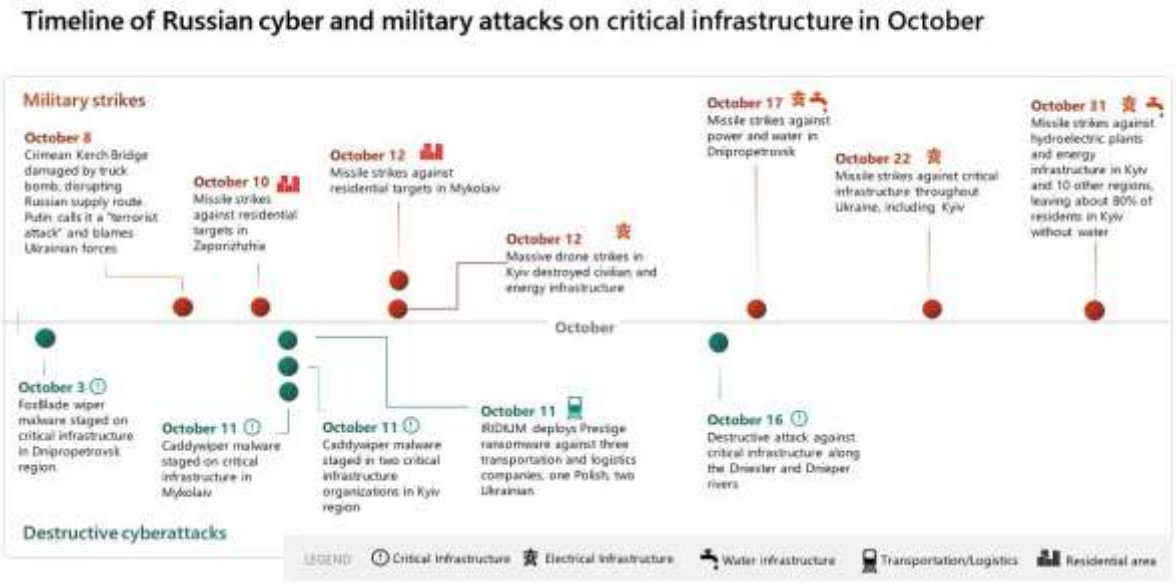
Когда в конце октября Россия отступила с ранее оккупированной территории Украины, Кремль нанес новые удары ракетами и беспилотниками по украинским городам и поддерживающей их энергетической и транспортной инфраструктуре. Ракетные обстрелы отключили электричество более 10 миллионов украинцев и оставили до 80% населения Киева без водопровода. Намерение причинить страдания гражданскому населению Украины было очевидным и фактически признавалось российскими официальными лицами.

Примечательно, что эти недавние ракетные удары сопровождались кибератаками на тех же секторах, совершенными группой угроз, известной в Microsoft под названием IRIDIUM, а в других как Sandworm, связанной с российской военной разведкой, ГРУ. Неоднократные временные, секторальные и географические связи этих кибератак российской военной разведки с соответствующими военными кинетическими атаками указывают на общий набор оперативных приоритетов и дают веские косвенные доказательства того, что усилия скоординированы, что отражено в графиках ниже.

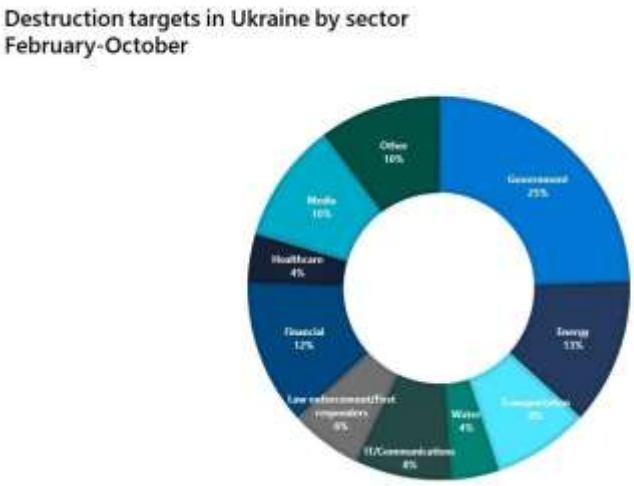
Исследование IRIDIUM, проведенное Microsoft, показывает историю разрушительных атак на критически важную энергетическую инфраструктуру Украины, которая насчитывает почти десятилетие. После аннексии Крыма Россией в 2014 году IRIDIUM начала серию зимних операций против украинских поставщиков электроэнергии, отключив электроэнергию для сотен тысяч граждан в 2015 и 2016 годах. атака, которая нанесла ущерб в размере 10 миллиардов долларов компаниям, включая такие международные фирмы, как Maersk, Merck и Mondelēz, и подчеркивает риск операций этого субъекта для глобальной цифровой экосистемы.

Как мы сообщали ранее, ответственность за волну российских разрушительных кибератак, начавшуюся 23 февраля, и последующие разрушительные атаки на украинские объекты в поддержку военных действий России лежит на IRIDIUM. В октябре количество разрушительных атак IRIDIUM на украинские сети критически важных служб резко возросло после двух месяцев практически полного отсутствия активности вайперов. По мере развития украинского контрнаступления и приближения зимы Microsoft заметила, что IRIDIUM развернула вредоносное ПО Caddywiper и FoxBlade wiper для уничтожения данных из сетей организаций, занимающихся производством электроэнергии, водоснабжением и транспортировкой людей и товаров. Преимущественное внимание было уделено Киевской области, а также южным и центрально-восточным регионам страны, где физический конфликт был наиболее интенсивным.

Кибер- и ракетные удары по транспортным и логистическим компаниям могут помешать транспортировке оружия и припасов. Однако такие обстрелы также могут нарушить прохождение гуманитарной помощи гражданам Украины, усугубляя ущерб от прекращения подачи электроэнергии.



Эта тактика нанесения ударов по гражданской инфраструктуре применяется с самого начала конфликта. Из примерно 50 украинских организаций, которые с февраля 2022 года были атакованы российскими военными операторами с помощью деструктивного вредоносного ПО Wiper, 55% представляли собой организации критической инфраструктуры, в том числе в сфере энергетики, транспорта, водоснабжения, правоохранительных органов, экстренных служб и здравоохранения.



В большинстве случаев злоумышленники развернули вайперы против бизнес-сетей целевых организаций критической инфраструктуры. Однако операционные технологические сети также уязвимы. Например, в апреле компания IRIDIUM попыталась нанести серьезный ущерб производству электроэнергии, атаковав системы промышленного контроля (АСУ ТП) украинского поставщика электроэнергии. Быстрые действия CERT-UA и международных партнеров предотвратили атаку, но высок риск будущих атак АСУ, которые нарушат или разрушат производственные мощности украинской энергетической или водной инфраструктуры.

Российские кибератаки выходят за пределы Украины

Российские кибератаки распространились за пределы Украины в октябре, когда IRIDIUM развернула свою новую программу-вымогатель Prestige против нескольких сетей логистического и транспортного секторов в Польше и Украине. Это была первая связанная с войной кибератака против объектов за пределами Украины после атаки Viasat KA-SAT в начале вторжения.

Мероприятие «Престиж» в октябре может представлять собой взвешенный сдвиг в стратегии кибератак России, отражающий готовность Москвы использовать свое кибероружие против организаций за пределами Украины в поддержку продолжающейся войны. С весны 2022 года Microsoft заметила, что IRIDIUM и предполагаемые российские государственные операторы нацелились на транспортные и логистические организации по всей Украине, вероятные попытки собрать разведданные или сорвать поток военной и гуманитарной помощи через страну. Но эти недавние атаки в Польше предполагают, что спонсируемые российским государством кибератаки могут все чаще использоваться за пределами Украины, чтобы подорвать иностранные цепочки поставок.

Успех IRIDIUM в разрушительной атаке Prestige был ограниченным. Сообщается, что ранние уведомления клиентов и быстрое реагирование, в том числе со стороны группы обнаружения и реагирования Microsoft (DART) и Центра анализа угроз Microsoft (MSTIC), а также с местными службами реагирования на инциденты в Польше, помогли ограничить воздействие атаки менее чем на 20% от одной целевой организации. сеть. Однако, хотя разрушительное воздействие было ограниченным, IRIDIUM почти наверняка собирала разведданные о маршрутах снабжения и логистических операциях, которые могли способствовать будущим атакам.

Возможно, отчасти потому, что в данном случае защитники и ответчики успешно ограничили воздействие, международный протест против этого нового расширения гибридной войны за пределы Украины был приглушен. Тем не менее, эта атака подчеркивает сохраняющийся риск деструктивных кибератак со стороны России на европейские организации, которые напрямую доставляют или доставляют гуманитарную и военную помощь Украине.

Кибероперации по влиянию стремятся разжечь разногласия в реальном мире по всей Европе

Этой зимой европейское население, стремящееся согреться в условиях нехватки энергии и повышенной инфляции, скорее всего, станет мишенью для

попыток России разжечь и потенциально мобилизовать недовольство с помощью операций влияния с помощью киберпространства.

Такие операции предлагают Кремлю более сомнительный, но тем не менее эффективный способ формирования дискурса вокруг конфликта и крупных геополитических событий. Подход России к «активным мерам» предполагает проникновение в электорат противников Кремля при одновременном продвижении кандидатов и официальных лиц, разделяющих предпочитаемые Россией внешнеполитические позиции. С 2014 года Россия стремилась достичь своих целей «силой политики, а не политикой силы» через демократические конкурсы, включая референдум по Brexit 2016 года и выборы в США, Франции и Германии, среди прочих. Россия также использовала политические, экономические и социальные разногласия для мобилизации граждан и даже подстрекательства к насилию внутри демократических государств. Вполне вероятно, что эти инструменты будут развернуты в Европе и во всем мире, чтобы уменьшить поддержку обороны Украины.

У России есть хорошо зарекомендовавшая себя способность влиять на общественное мнение как в США, так и в Европе с помощью операций влияния с помощью киберпространства. В 2016 году Агентство интернет-исследований в Санкт-Петербурге, более известное как российская «ферма троллей», организовало протесты в Техасе и Флориде. Ранее в том же году российские государственные СМИ опубликовали статью о предполагаемом нападении на молодую девушку со стороны мигрантов в Германии (обвинения позже были опровергнуты) и продвигали версию о том, что правительство Германии умышленно скрыло правду. Последовавшая за этим буря в СМИ вызвала серию протестов среди многочисленной русской диаспоры в Германии, которые были возмущены тем, что им говорили о провале немецкой судебной системы.

В 2018 году те же кремлевские тролли, участвовавшие в президентских выборах 2016 года в США, усилили протесты «желтых жилетов» во Франции. Россия не организовывала эти протесты, но ее онлайн-кампании усилили призывы к протесту против правительства президента Эммануэля Макрона, используя смесь

открытых, спонсируемых государством СМИ для продвижения дела, одновременно продвигая хэштег движения #giletsjaunes через скрытые учетные записи в Интернете.

Команда нашего Центра анализа цифровых угроз (DTAC) внимательно отслеживает операции по влиянию с помощью кибербезопасности. Протесты в Европе этой осенью, связанные с энергетикой, инфляцией и войной на Украине в целом, а также их неустанная пропаганда российскими пропагандистскими СМИ, предвещают дополнительные операции, с которыми мы можем столкнуться этой зимой в поддержку целей России, стремясь усилить недовольство европейцев поставками энергоресурсов. ценообразование на энергию и инфляция. Если сбои в энергоснабжении и электроснабжении на Украине приведут к увеличению числа беженцев по всей Европе, российские кибероперации по влиянию могут быть направлены на усиление трений по поводу миграции, чтобы вызвать внутристрановые и межгосударственные конфликты — тема, прослеживающаяся в кампаниях Кремля за последние десятилетие, когда беженцы бежали в Восточную и Центральную Европу во время гражданской войны в Сирии.

В ближайшие месяцы европейские страны, скорее всего, подвергнутся ряду методов воздействия, учитывающих опасения их населения по поводу цен на энергоносители и инфляции в целом. Россия сосредоточила и, вероятно, будет продолжать направлять эти кампании на Германию, страну, имеющую решающее значение для поддержания единства Европы и являющуюся домом для большой русской диаспоры, стремясь подтолкнуть народ и элиту к согласию в пользу Кремля. Тесные связи между прокремлевскими идеологами и крайне правыми в Германии, вероятно, будут использоваться как онлайн, так и офлайн в кампаниях, нацеленных на немецкую аудиторию, с жесткими нарративами о войне на Украине, а также с критикой действий правительства в отношении энергетического кризиса.

Последние количественные анализы подтверждают эти оценки. Лаборатория искусственного интеллекта Microsoft для Good Lab создала Индекс российской пропаганды (RPI) для мониторинга потребления новостей из российских контролируемых и спонсируемых государством новостных агентств и усилителей.

Этот индекс измеряет долю этого пропагандистского потока в общем объеме новостного трафика в Интернете. Индекс RPI в Германии в настоящее время является самым высоким в Западной Европе, более чем в три раза превышающим средний показатель по региону.

Повышенное потребление российской пропаганды в Германии может быть отчасти связано с многолетними инвестициями России в мягкую силу и публичную дипломатию, направленную против страны, где проживает одна из крупнейших русских диаспор в Европе. Целью многих организаций «мягкой силы» является создание связей между людьми и партиями между двумя странами, а несколько спонсируемых государством СМИ базируются в Германии. Большое русскоязычное население Германии, насчитывающее, по оценкам, почти 6 миллионов человек, делает российские операции по оказанию влияния и пропаганду, публикуемую как на русском, так и на немецком, более доступными для немецкой аудитории. Между тем, немецкая политика после окончания холодной войны, когда советские и восточногерманские активные действия осуществлялись синергетически, стремилась к нормализации отношений с Россией, подкрепляемой экономическим сотрудничеством, с не более ярким примером, чем «Северный поток». 2 газопровода. Санкции США против этого проекта, непопулярного как в России, так и в Германии, привлекли к антизападной и пророссийской пропаганде и операциям влияния, особенно на экономические и энергетические темы, более сочувственную аудиторию.

По всей Западной Европе читатели сталкиваются с российской пропагандой как на русскоязычных сайтах, в том числе на сайтах российских государственных СМИ, так и на местных пророссийских сайтах. Потребление сайтов на местных языках в Германии в три раза выше, чем в среднем по Западной Европе, что соответствует высокому уровню потребления российской пропаганды в Германии в целом. В Германии наибольший трафик получают сайты на местных языках: anti-spiegel.ru, uncutnews.ch и немецкоязычное издание Russia Today (RT), de.rt.com. Местные сайты уделяют больше внимания местным проблемам. Анти-Шпигельв частности, основное внимание уделялось использованию нынешнего

экономического климата для продвижения Кремля и очернения Запада. Например, заголовки трех самых читаемых статей за последние четыре месяца:

«То, что США хотят уничтожить экономику Германии, считается теорией заговора и российской пропагандой, но это очевидно».

«Трубопроводы Nord Stream взорваны, а западные СМИ инсценируют, возможно, самую глупую пропагандистскую операцию в истории».

«Меня часто спрашивают, почему я так убежден, что президент России Путин не является частью [Всемирного экономического форума] и его нового мирового порядка. Здесь я хочу ответить на это».

Помимо Германии, многим другим европейским странам, возможно, также придется считаться с совокупным весом российского вмешательства и органического народного недовольства. Ранее в этом году связанная с Россией организация по угрозам SEABORGIUM (которая пересекается с группами угроз, отслеживаемыми как Callisto Group, TA446 и COLDRIVER) нацелилась на Великобританию, используя якобы украденные материалы, чтобы посеять недоверие к британскому правительству, в то время как пророссийские СМИ, такие как Фонд «Современная дипломатия и стратегическая культура», учреждение, управляемое Службой внешней разведки России (СВР), публикует материалы, в которых утверждается, что Великобритания причастна к взрыву моста через Керченский пролив.

Тем временем непрекращающиеся протесты в Чешской Республике способствовали популяризации позиций России по вопросам энергетики и неоднократно освещались в российских государственных и связанных с государством СМИ. Ладислав Врабель — один из организаторов протестного движения «Первая Чехия» — с начала протестов неоднократно появлялся в российских СМИ, таких как Sputnik News, а «ПолитНавигатор» — русскоязычный сайт, который, как сообщается, управляется ФСБ – отправил корреспондента освещать протесты с самого начала. Кроме того, среди общественных деятелей, которые поддерживали демонстрации и выступали на них, есть несколько политиков с длительным и хорошо задокументированным послужным списком

пророссийской деятельности, такой как неофициальные поездки в оккупированный Крым и участие на высоком уровне в финансируемой Кремлем байкерской банде «Ночные волки».

Франция, не так зависящая от российского газа, как ее соседи, возможно, менее уязвима для влияния, связанного с энергетикой. Тем не менее, существует постоянный риск того, что российские агентства будут пытаться вмешиваться во французские дела с помощью недостоверных кампаний в социальных сетях, опираясь на предыдущие усилия и свой успех, распространяя и используя антифранцузские настроения по всей Африке с помощью пропаганды, поддельных аналитических центров и участие на местном уровне, которое указывает на готовность России подорвать лидерство Франции. Наконец, Италия, с ростом стоимости энергии, [36] появляется в качестве дополнительной цели.

Защита цифровой сферы этой зимой: путь вперед

В нашем отчете за июнь 2022 года «Защищая Украину: первые уроки кибервойны» Microsoft предложила методологию борьбы с цифровыми угрозами. Многомерные угрозы требуют многомерной защиты. В Microsoft мы построили наш подход на основе «четырех D» для противодействия злонамеренным киберугрозам и оказания влияния. Всю зиму и весь 2023 год мы будем работать с нашими клиентами и в поддержку демократии, чтобы:

Обнаружить: Коллективно определите с помощью групп Microsoft по анализу угроз тех кибер-актеров, которые могут нанести удар по цепочкам поставок, поддерживающим Украину и энергетическую отрасль, поддерживающих тепло в Европе этой зимой. Мы также оценим кибератаки, чтобы определить, какие из них предназначены для ограничения поддержки и поставок в Украину, а какие могут быть частью более широких операций по взлому и утечке, направленных на подрыв единства поддержки Украины. Что касается клиентов, мы заранее оцениваем и оцениваем потенциальные риски для тех, кто может стать мишенью для России или других государств, представляющих угрозу. В ходе этой оценки уязвимости будут тщательно изучены транспортные, оборонные и энергетические компании, которым Microsoft помогает повысить коллективную скорость обнаружения и

реагирования. Microsoft также продолжит отслеживать и выявлять российские операции влияния с использованием кибербезопасности.

Разрушение: Microsoft Threat Intelligence Center (MSTIC) будет оповещать клиентов и общественность о новых киберметодах, позволяющих всей экосистеме быстро использовать датчики, исправления и средства защиты. Там, где мы сталкиваемся с кампаниями влияния с использованием кибернетики, мы будем придерживаться аналогичной стратегии, освещая операции, направленные на создание сомнений, недоверия или инакомыслия в Украине или среди ее партнеров, стремящихся подорвать поддержку Украины. Наша команда поделится этой информацией с нашими клиентами и общественностью в отношении этих операций и уменьшит их влияние.

Защита: Microsoft усилит коллективную защиту более широкой киберэкосистемы за счет расширения обмена информацией и улучшения технологий для защиты от российских угроз и устранения уязвимостей. Наши команды будут продолжать поддерживать некоммерческие организации, журналистов и ученых как в Украине, так и среди союзников, позволяя этим партнерам расширить свою защиту информационной экосистемы. Например, Microsoft недавно заключила партнерское соглашение с International Media Support (IMS) и Центром стратегических коммуникаций и информационной безопасности в Украине, чтобы улучшить быстрый обмен информацией и реагирование на нее между частным сектором, неправительственными организациями и журналистами в Украине через специальный безопасный коммуникационный центр.

Deter: Microsoft уже более десяти лет занимается обеспечением международных норм для киберпространства. Этой зимой наши команды Digital Diplomacy and Democracy Forward будут работать с пострадавшими клиентами и их представительными правительствами, чтобы добиваться единых действий для защиты цепочек поставок наших клиентов от атак со стороны государства. И мы продолжим наши постоянные усилия по предоставлению действенной информации об угрозах организациям, ставшим жертвами или скомпрометированными российскими субъектами в Украине и в странах, поддерживающих ее оборону.

Наконец, для клиентов Microsoft рекомендует использовать строгую кибергигиену и новейшие технологии обнаружения и реагирования для снижения уязвимости и восстановления после кибератак — список этих конкретных рекомендаций можно найти в недавно выпущенном отчете Microsoft Digital Defense Report (MDDR) 2022.

Украина храбро оборонялась как в сети, так и на земле от безжалостного нападения России. С помощью стран-партнеров, компаний и демократических граждан мы все можем обеспечить защиту украинской и европейской инфраструктуры и устойчивость демократии перед лицом авторитаризма этой зимой». ***(Clint Watts. Preparing for a Russian cyber offensive against Ukraine this winter // Microsoft (https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/). 03.12.2022).***

***

«Россия может нацелиться на операции цепочки поставок и усилить операции влияния

Октябрьская атака с использованием программы-вымогателя российской военной разведкой на транспортную и связанную с ней логистическую отрасль в Польше может свидетельствовать о намерении Кремля продолжить украинское наступление в европейском киберпространстве, предупреждает компьютерный гигант Microsoft.

Россия уже придерживается стратегии цифровой дезинформации в Европе — она особенно эффективна в странах Центральной Европы, включая Германию, и, вероятно, в ближайшие месяцы она усилится, пишет компания в субботнем предупреждении.

«Мир должен быть готов к нескольким направлениям потенциальных российских атак в цифровой сфере в течение этой зимы», — написал Клинт Уоттс, генеральный менеджер Центра анализа цифровых угроз Microsoft.

Ранее этой осенью Microsoft приписала новую кампанию по вымогательству, активную в Украине и Польше, одному и тому же кремлевскому злоумышленнику,

ответственному за вредоносное ПО NotPetya и зимние кибератаки на украинских поставщиков электроэнергии в 2015 и 2016 годах. Связанный с российской военной разведкой ГРУ, злоумышленник чаще всего известен под прозвищем Sandworm, хотя Microsoft отслеживает его как Iridium.

Недавняя активность Sandworm показывает, что она отражает возросшую готовность Москвы наносить удары по критически важной инфраструктуре Украины после военных поражений, вынудивших ее отступить с ранее оккупированной территории. Успехи украинских контрнаступлений сопровождаются всплеском активности вредоносного ПО CaddyWiper и FoxBlade Wiper против организаций, которые в основном обслуживают Киев и занимаются производством электроэнергии, водоснабжением и транспортировкой людей и товаров, сообщает Microsoft.

Развертывание Sandworm программы-вымогателя, которую Microsoft называет «Престиж», против польских целей предполагает готовность нарушить украинскую цепочку поставок, даже когда она достигнет Европы. Престиж имел ограниченный эффект, но злоумышленники «почти наверняка собирали разведданные о маршрутах снабжения и логистических операциях, которые могли облегчить будущие атаки».

Microsoft также оценивает, что более отрицательным способом подорвать европейскую поддержку Украины может быть интенсификация операций по дезинформации, особенно в Германии. Германия занимает первое место среди западноевропейских стран по потреблению российской пропаганды, согласно показателям Microsoft по потреблению новостей из российских контролируемых и спонсируемых государством новостных агентств и усилителей.

Большая русская диаспора в сочетании с многолетней государственной политикой сближения с Москвой создали в Германии сочувствующую аудиторию, открытую для пропаганды, облеченной в риторику об экономике и энергетике.

Германия — не единственная страна, где господствуют российские операции влияния. Microsoft заявляет, что непрекращающиеся протесты в Чешской Республике, призывающие к отставке союзного Украине правоцентристского

правительства, способствовали продвижению позиций России по вопросам энергетики и неоднократно освещались в российских государственных и связанных с государством СМИ». ***(Akshaya Asokan. Microsoft Warns of Growing Russian Digital Threats to Europe // Information Security Media Group, Corp. (https://www.govinfosecurity.com/microsoft-warns-growing-russian-digital-threats-to-europe-a-20631). 05.12.2022).***

***

«Російські окупанти розсилають в Україні небезпечні вірусні листи. Електронні листи розсилаються під виглядом інструкції, як розпізнати дрони-камікадзе Shahed-136.

Про це повідомляє Держспецзв'язку.

Відомо, що першими такі листи отримали фахівці з кібератаки АТ «Укрзалізниця». У темі листа говорилося, як розпізнати дрон-камікадзе. Надходить лист нібито від Державної служби України з надзвичайних ситуацій на адресу morgunov.a@dsns.com.ua. У той же час, доменне ім'я було зареєстровано місяць тому.

«У вкладенні в лист міститься RAR-архів «shahed-136.rar» з PPSX-документом «shahed.ppsx». В результаті його відкриття на пристрій врешті-решт буде завантажено файл «WibuCm32.dll». Він класифікований як шкідлива програма DolphinCape, розроблена з використанням мови програмування Delphi Основний функціонал програми — збір інформації про комп'ютер (ім'я хоста, ім'я користувача, розрядність, версія ОС, значення змінних середовища), запуск EXE/DLL файлів, відображення списку файлів та їх розвантаження, а також створення та ексфільтрація знімків екран», — йдеться у повідомленні Держспецзв'язку.

В організації уточнили, що при розсиланні небезпечних електронних листів хакери часто маскуються під представниками державних органів. Так, у жовтні-листопаді цього року було зафіксовано подібні розсилки начебто від імені

Держспецзв'язку, пресслужби Генштабу ЗСУ, Служби безпеки України та від CERT-UA.

Як уберегти себе від таких листів

бути обережним при відкритті подібних листів чи повідомлень;

звертати увагу на домен — держструктури можуть надсилати лише з доменів gov.ua;

не відкривати та не завантажувати підозрілі файли». ***(Олена Леонова. Окупанти розсилають в Україні небезпечні вірусні листи: деталі // Новини.Live (https://society.novyny.live/okkupanty-rassylaiut-v-ukraine-opasnye-virusnye-pisma-detali-67399.html). 09.12.2022).***

***

«Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, що діє при Держспецзв'язку, попереджає про кібератаку на користувачів системи DELTA.

«DELTA – це створена за стандартами НАТО національна військова система ситуаційної обізнаності, яку використовують Збройні сили України та Сили безпеки та оборони. Зокрема, це програмне забезпечення дозволяє військовим оперативно дізнаватися важливі дані про противника», - наголошується в повідомленні Держспецзв'язку в телеграм-каналі.

Як повідомляють у CERT-UA, 17 грудня Центр інновацій та розвитку оборонних технологій Міністерства оборони України отримав інформацію про поширення повідомлень щодо необхідності оновлення сертифікатів у системі DELTA. Такі повідомлення надходять у месенджерах, а також на електронну пошту. До того ж для розсилки зловмисники використовують скомпрометовану електронну адресу одного із співробітників оборонного відомства.

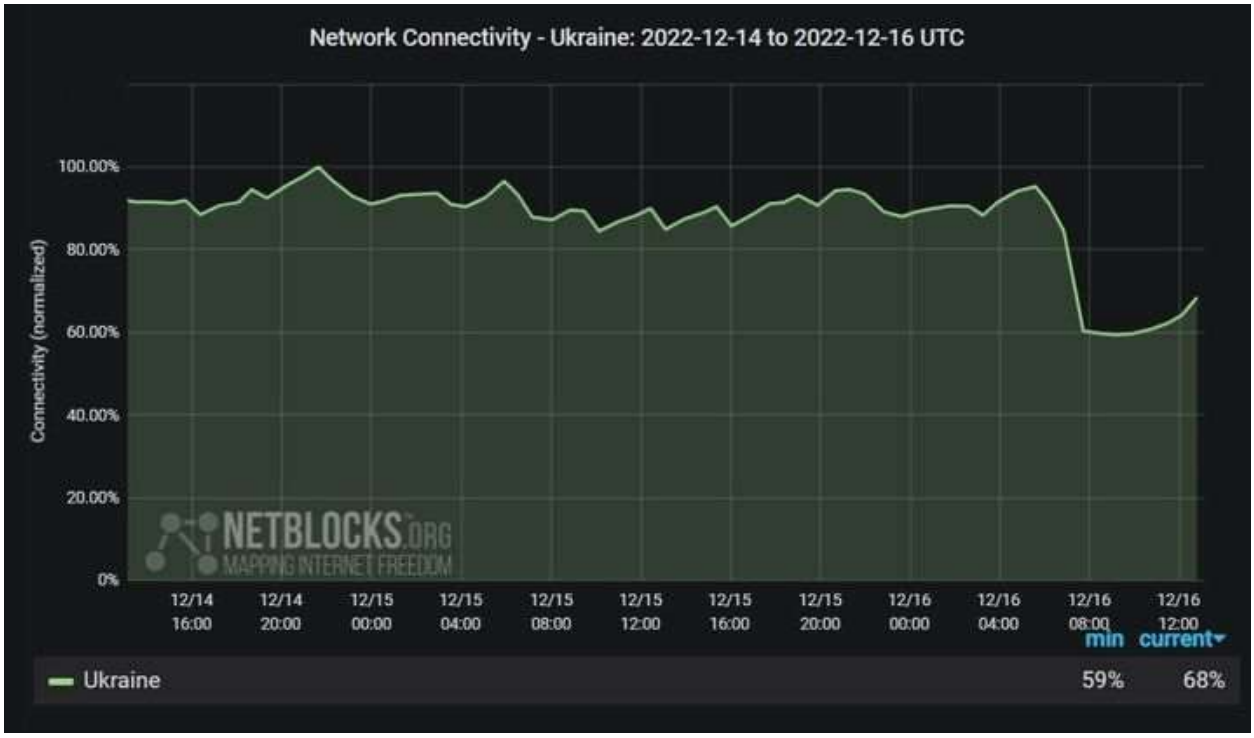
«У повідомленнях містяться вкладення у вигляді PDF-документів, що імітують військові дайджести та мають посилання на шкідливий ZIP-архів. При переході за посиланням у повідомленні на комп'ютері в результаті буде здійснено запуск двох шкідливих програм», - наголошується в повідомленні.

У Держспецзв'язку нагадали, що у грудні було зафіксовано розсилання електронних листів із небезпечним вкладенням нібито від імені ДСНС України – зловмисники використали тему іранських дронів-камікадзе Shahed-136.

Відомство закликає обережно ставитися до будь-яких надходжень. «Навіть якщо, на перший погляд здається, що вони надійшли від представників державних органів, служб, установ. Не відкривайте надіслані вкладення і не переходьте за посиланнями, якщо не впевнені у їхній безпеці», - наголошено в повідомленні». ***(Держспецзв'язку попереджає про нову кібератаку, спрямовану на представників сектору безпеки та оборони // Інтерфакс-Україна (https://interfax.com.ua/news/telecom/879112.html). 18.12.2022).***

***

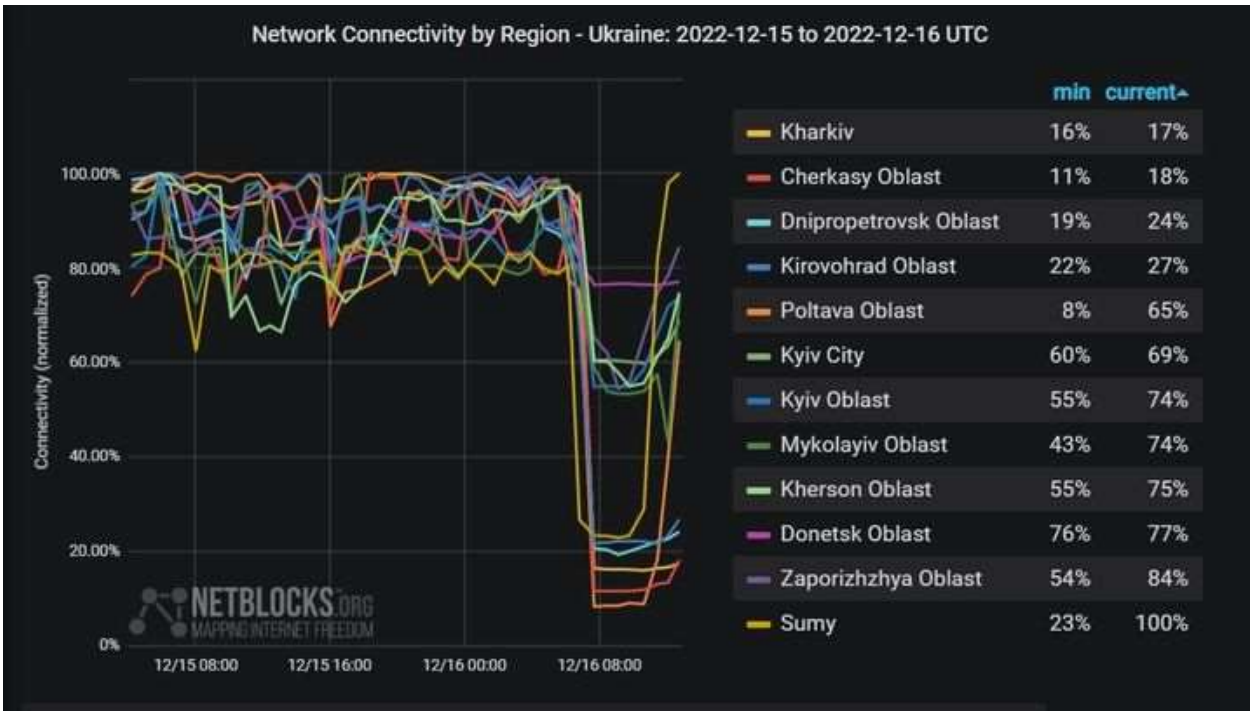
«Організація Netblocks, що стежить за станом всесвітньої мережі в усьому світі, підрахувала рівень падіння інтернет-конекту в Україні після ракетних атак 16 грудня. Натепер він становить 68% від попереднього рівня (але вже почалося відновлення конекту, бо зранку цей показник сягав 59%).



«Мережеві дані свідчать про значне порушення підключення до інтернету в Україні, що відповідає відключенням електроенергії на тлі нових російських

ракетних атак по критичній інфраструктурі», — зазначає Netblocks у своєму Twitter.

У дев'ятьох регіонах, що зазнали зранку обстрілів, найістотніше впали Полтавська й Черкаська області та Харків.



Найбільше падіння, за даними Netblocks, натепер зафіксоване після атак 23 листопада: тоді трафік по Україні впав на 65% — до 35% від попереднього значення». ***(Катерина Венжик. Падіння інтернету в Україні після обстрілів: Netbloks фіксує 68% від попереднього рівня // Speka.Media (https://speka.media/padinnya-internetu-v-ukrayini-pislya-obstriliv-netbloks-fiksuje-68-vid-poperednyogo-rivnya-pjexo9). 14.12.2022).***

***

«Російські хакери атакували сайт та інші сервіси «Львівобленерго». Про це повідомляє пресслужба компанії у Facebook.

«Вночі хакери, які на службі в російських окупантів, атакували сайт та інші ІТ-ресурси «Львівобленерго». Завдяки вчасному попередженню від СБУ та Кіберполіції ІТ-спеціалістам нашої компанії вдалося відбити атаку», — повідомили у компанії.

Наразі вебсайт «Львівобленерго» та інші сервіси можуть працювати з певною затримкою, через додаткові заходи з кіберзахисту.

Раніше стало відомо, що ворог продовжує кібератаку на державні організації України. Хакери використовують тематику іранських дронів-камікадзе Shahed-136 та шкідливу програму DolphinCape». ***(Руслан Сорока. «Львівобленерго» атакували хакери з росії // Speka.Media (https://speka.media/lvivoblenergo-atakuvali-xakeri-z-rosiyi-9e8619). 15.12.2022).***

***

«Київська ІТ-армія складає військовий каталог «Книга катів». Поширення новин про вторгнення серед росіян є ще однією метою діяльності ІТ-волонтерів України.

Члени ІТ-армії України, волонтерської групи комп'ютерників, збирають «Книгу катів» для каталогізації російських солдатів, які вбивають та катують українців, заявив міністр цифрової трасформації Михайло Федоров в інтерв'ю Bloomberg News.

Офіційні особи в Києві раніше повідомили Bloomberg, що вони документують імовірні російські хакерські атаки в рамках плану переслідування російських лідерів у міжнародному суді, «щоб усі зрозуміли, хто заходив в Україну і вбивав українців».

«Сучасні технології допомагають нам ідентифікувати російські військові злочини, як-от розпізнавання обличчя за допомогою штучного інтелекту, який декодує інформацію з публічних камер», — додав він.

Ці дані також допомагають приймати рішення на полі бою. Проте Федоров відмовився сказати конкретно, як хакерство керує прийняттям рішень.

Українська ІТ-армія атакує російські сервіси

ІТ-армія взяла на себе відповідальність за порушення роботи російських сервісів за допомогою кібератак з початку війни.

За словами Федорова, в одному випадку група волонтерів з IT Army «повністю» зламала RuTube, російську відеоплатформу, що належить компанії,

афілійованій з газовим монополістом країни. Це призвело до перебоїв у роботі сайту на тиждень.

«IT Army навіть вдалося зламати бейджі співробітників RuTube, щоб вони не могли потрапити в компанію», — сказав Федоров.

IT-армія намагається донести правдиві новини до росіян

IT-армія також працює над донесенням новин про війну до громадян росії, де контрольовані державою ЗМІ продовжують описувати вторгнення як «операцію сил спеціального призначення».

«Для України дуже важливо доносити правду до росіян, боротися з пропагандою», – сказав Федоров. — Нам потрібно підірвати підтримку президента росії Володимира Путіна та тих, хто підтримує війну».

Зауваження Федорова прозвучали після того, як підозрювані хакери, спонсоровані державою, здійснили серію кібератак на українську інфраструктуру перед наземним вторгненням 24 лютого. За словами Федорова, інциденти були спрямовані на те, щоб паралізувати роботу банків і державних сайтів, і, ймовірно, на їхню підготовку знадобилося від шести місяців до року. Щоб мінімізувати наслідки атаки, український уряд закрив сайти та додаток «Дія».

Український уряд готувався до кібератак місяцями

На той час українські чиновники місяцями готувалися до такої діяльності, сказав Федоров. Члени Альянсу попередили Київ про цифрові загрози для енергетичної інфраструктури, допомагаючи уряду досліджувати вразливі місця, які українці могли б виправити до того, як російські хакери почнуть діяти.

«Ми створили червону команду восени минулого року, а з листопада почали себе сканувати та атакувати, а також почали запроваджувати нові правила кібербезпеки», — додав він.

Ця робота продовжується. За словами Федорова, російські хакери атакували українську енергетичну інфраструктуру, діяльність якої збіглася з ракетними атаками, які мали на меті спричинити відключення електроенергії у країні. «Вони намагалися увійти в мережу», — сказав він, відмовившись надати подробиці з міркувань безпеки». ***(Українські хакери збирають дані про російських військових***

у «Книгу катів» // Internetua (https://internetua.com/ukrayinski-hakeri-zbirauat-dani-pro-rosiiskih-viiskovih-u-knigu-kativ-). 21.12.2022).

***

«З початку року Служба безпеки України нейтралізовано понад 4,5 тис. ворожих кібератак і кіберінцидентів.

Про це повідомив начальник Департаменту кібербезпеки СБУ Ілля Вітюк, інформує Цензор.НЕТ із посиланням на пресцентр СБУ.

«Ми підійшли до 2022 року, маючи позаду 8-річний досвід гібридної війни. Адже війна у кіберпросторі тривала і раніше. На момент вторгнення ми вже були готові до найгірших сценаріїв. А масовані кібератаки, які ми відбили в січні та лютому, стали додатковими "тренуваннями" перед вторгненням», – зазначив Вітюк.

Він підкреслив, що з початком повномасштабної агресії роботи стало набагато більше. Якщо у 2020 році було зафіксовано майже 800 кібератак, у 2021 – 1400, то вже цьогоріч – їхня кількість зросла у понад 3 рази.

«Сьогодні країна-агресор завдає в середньому більше 10 кібератак на добу. Про більшість українське суспільство, на щастя, навіть не знає», – зауважив Вітюк.

Він розповів, що в зоні особливої уваги ворога є енергетика, логістика, військові об’єкти, а також – бази даних органів влади та інформресурси.

«Ми моніторимо ризики і загрози у режимі реального часу 24/7. Більшість хакерів із російських спецслужб, що працюють по нам, знаємо поіменно. Іде робота з їх документування. Після перемоги України на них чекатиме окремий блок засідань міжнародного військового трибуналу», – резюмував очільник Департаменту кібербезпеки СБУ. Джерело: https://censor.net/ua/n3389460». ***(Найбільше кібератак ворога зазнають енергетика, військові об’єкти та бази даних органів влади, - СБУ // Цензор.НЕТ (https://censor.net/ua/news/3389460/nayibilshe_kiberatak_voroga_zaznayut_energetyka_viyiskovi_obyekty_ta_bazy_danyh_organiv_vlady_sbu). 26.12.2022).***

***

«ГО «Платформа прав людини» провела дослідження українського кіберпростору у листопаді та з'ясувала, як кібератаки рф відображається на цифрових правах людини.

«Українська ІТ-армія за минулий місяць паралізувала роботу понад 900 ворожих сайтів, а українські суди за цей же період винесли 6 вироків про притягнення до кримінальної відповідальності громадян за поширення забороненої інформації», — зазначили в ГО.

Загалом, організація встановила, що у листопаді інтернет-користувачі масово піддавалися цифровим атакам. Загалом, з початку війни росія проводила:

Кібератаки на державний сектор – 402 009 разів;

фішингові атаки – їх зафіксували 1 172 572 разів;

поширення дезінформації – нараховано 150 випадків;

шахрайство в мережі – виявлено 5 схем.

Як і в попередні звітні періоди, у листопаді експерти також виявили й систематизували інформацію про блокування вебресурсів, порушення доступу до інтернету, свободи вираження поглядів та доступу до інформації.

Також в листопаді продовжував бути обмеженим доступ до 19 публічних електронних реєстрів.

«Існують сумніви щодо необхідності закриття низки реєстрів і того наскільки такі дії є пропорційними та доцільними для досягнення мети – забезпечення захисту національної безпеки й оборони», — зазначили в ГО «Платформа прав людини». ***(Руслан Сорока. З 24 лютого росія вчинила понад 400 тисяч кібератак на інфраструктуру України // Speka.Media (https://speka.media/z-24-lyutogo-rosiya-vcinila-ponad-400-tisyac-kiberatak-na-infrastrukturu-ukrayini-9q6gkv). 26.12.2022).***

***

«Україна зіткнулася з найбільшим викликом в історії. Її економіка, інфраструктура та логістика під постійними атаками. У цій публікації

поговоримо про те, як змінився бізнес-ландшафт країни і яка в цьому роль технологій.

Збір коштів по всьому світу

Після початку російського вторгнення основним викликом була необхідність зібрати якомога більше грошей по всьому світу.

На жаль, більшість глобальних платіжних систем, як-от Paypal, не працювали в Україні. Це при тому що в Україні поширені безготівкові операції та є зручні й швидкі системи онлайн-банкінгу. Часто українські платіжні мобільні застосунки та системи онлайн-банкінгу кращі за європейські аналоги.

Тож головним викликом було переконати глобальні платіжні системи почати працювати з Україною (чи хоча б з українськими біженцями в Європі), узгодити свою діяльність з місцевим законодавством і уникнути блокувань через операції, пов'язані з окупованими та анексованими територіями.

PayPal та Wise дозволили українцям відкривати облікові записи у цих системах. Український уряд почав тісну співпрацю з Binance та іншими великими криптоплатформами, щоб мати змогу отримувати пожертви у криптовалюті. З'явилися благодійні ініціативи, як-от United24 та інші.

Україна стала цікавою для міжнародних фінансових гравців як отримувач інвестицій та багатьох програм реновації.

Хмарні технології в Україні передусім

Як і в більшості країн світу, в Україні є суворе законодавство щодо зберігання та використання персональних даних. А вся критична інфраструктура має знаходитися всередині країни. На практиці це означає, що державні установи, банки та медичні заклади не можуть використовувати публічні хмарні сервіси на кшталт Microsoft Azure, Amazon AWS чи Google Cloud. Також у більшості випадків українські стандарти та вимоги не синхронізовані з європейськими, що робить додаткові перешкоди у співпраці з іноземним бізнесом.

У той час, коли ваша критична інфраструктура зазнає атак, використання хмарних технологій є гарним рішенням. Не зважаючи на всі потенційні проблеми, що несе використання публічних хмарних сервісів, у порівнянні з локальною

інфраструктурою вони можуть забезпечити надійніше середовище зберігання інформації, що може протидіяти DDoS-атакам та має системи резервного копіювання даних.

Український уряд дозволив використання публічних хмарних сервісів під час дії воєнного стану. Завдяки провідним хмарним провайдерам, критичні галузі економіки, банки, державні органи та урядові організації змогли мігрувати у хмару протягом кількох місяців.

Безумовно, ця ситуація дозволить розвіяти сумніви та побоювання щодо використання публічних хмарних сервісів і призведе до значної перебудови IT-системи країни. Якщо цей процес продовжиться, у України є чудовий шанс побудувати сучасну гібридну IT-інфраструктуру і зберегти 10-20 років, які б пішли на це за звичайних умов.

Занепад «стандартів» соціальних мереж в Україні

Стандарти спільноти таких соціальних мереж, як Facebook чи Instagram не дозволять вам розповісти, що відбувається в Україні. Мова ворожнечі (як один з найпоширеніших випадків їх порушення) також заборонена. Раніше на папері Facebook та Instagram дозволяли користувачам закликати до смерті російських окупантів в Україні, а насправді обмежували чи блокували сторінки українців за розміщення контенту, пов'язаного з війною.

Роками модератори українського контенту працювали з росії і як результат соціальні мережі та інші ресурси на кшталт «Вікіпедії» стали майданчиками для розповсюдження пропаганди та фейкових новин. І свобода слова тут не аргумент, адже працює вона тільки у демократичних країнах.

Очевидно, що наявні засоби модерації контенту застаріли та навіть є шкідливими. Розробка нових стандартів спільноти, а також інструментів для виявлення фейкових новин та профілів є новим соціальним і технологічним викликом.

Водночас соцмережі призвели до появи такого явища, як OSINT (розвідка на основі відкритих джерел). Волонтери та професійні журналісти можуть аналізувати

соціальні мережі та інші відкриті джерела, шукати там інформацію і на її основі проводити розслідування.

Чатботи повсюду

Якщо у вас є хоча б шматочок корисної інформації, українці зроблять на її основі чатбот. Цей інструмент став стандартним для багатьох ситуацій, починаючи з пошуку інформації про відключення електроенергії і закінчуючи повідомленнями в державні органи про підозрілі чи небезпечні предмети.

Telegram став стандартною платформою для чатботів. У порівнянні з іншими меседжерами він простий у використанні, швидкий та по факту найлегший для створення чатботів. Viber, Messenger та WhatsApp не можуть скласти йому достойну конкуренцію. Крім того, як я вже казав, інші платформи не дуже підходять, коли ми говоримо про швидкість і простоту.

Але при цьому Telegram створили у росії, тож ми не маємо 100% впевненості щодо того, хто має доступ до користувацьких даних. Тим не менше, в нашому випадку це безальтернативний вибір попри всі пересторогі.

А де тут штучний інтелект?

ШІ це не те, що може бути розроблено та впроваджено миттєво, тим паче у військовій сфері. Він потребує високоякісних даних, час на навчання, тестування та розгортку. Для нього потрібна глибока інтеграція із наявними бізнес-процесами, військовим ПЗ та політична воля для впровадження. Штучний інтелект дуже чутливий до конкретних вимог та умов. А у нас не було нічого з перерахованого. Чесно кажучи, я не був дуже оптимістичним щодо реальних кейсів використання ШІ. Мабуть, я помилився.

Як результат співпраці між IT-компаніями, ентузіастами ШІ та військовими, з'явилися повідомлення про окремі випадки використання штучного інтелекту. Мова йде про виявлення ракет і військової техніки, розпізнавання обличь російських військових (як інструмент для OSINT), визначення фейкових новин тощо.

Я припускаю, що військовий ШІ стане наступним трендом. Об'єднавши його із індустрією дронів ми отримаємо новий багатомільярдний ринок.

Коротка післямова

Сьогодні я купив каву в місцевій крамничці. У ній не було електрики та інтернету, платіжне обладнання не працювало. Та я зміг розрахуватися безготівково, використавши смартфон як платіжний термінал.

Війна пришвидшує цифрову трансформацію всередині країни, роблячи людей більш гнучкими, освіченими та підготовленими.

На жаль, ціна цього прогресу занадто висока». ***(Олександр Краковецький. Як війна спричинила технологічний зсув для України // Speka.Media (https://speka.media/yak-viina-spricinila-texnologicnii-zsuv-dlya-ukrayini-9q6ewv). 26.12.2022).***

***

Боротьба з кіберзлочинністю в Україні

«Протягом 2022 року українські правоохоронці завершили розслідування понад 600 справ, пов'язаних із криптовалютами — про це повідомив начальник управління оперативно-аналітичного забезпечення та аналізу відкритих джерел департаменту кіберполіції Євген Панченко. У більшості випадків зловмисники використовували цифрові активи для торгівлі нелегальними товарами у даркнеті або ж для відмивання коштів, отриманих злочинним шляхом.

«Криптовалюта дає великі можливості для розвитку економіки, втім, зловмисники також вдало користуються перевагами цього інструменту», — зазначив Панченко.

Глава управління департаменту кіберполіції серед інших взяв участь у семінарі ОБСЄ та UNODC (Управління ООН у боротьбі з наркотиками та злочинністю). Відомства запустили спільний проект, у рамках якого правоохоронці зможуть отримати доступ до необхідних інструментів для фінансового моніторингу та розслідування правопорушень, пов'язаних із цифровими активами.

Нагадаємо — українська кіберполіція заявила про свою готовність підтримати легалізацію криптовалют в Україні. «Наша мета проста — зробити криптообіг в Україні легальним і безпечним, але за принципом «не нашкодь», щоб ринок отримував не регулювання, а стимули для розвитку та конкурентні переваги», — наголосив народний депутат Ярослав Железняк, який брав участь в обговоренні питання…» ***(Українська кіберполіція викрила понад 600 випадків нелегального використання криптовалют // No worries! (https://noworries.news/ukrayinska-kiberpolicziya-vykryla-ponad-600-vypadkiv-nelegalnogo-vykorystannya-kryptovalyut/). 09.12.2022).***

***

«Під час обшуків вилучено понад 100 тисяч SIM-карток, які використовували для реєстрації фейкових акаунтів. Загалом бот-мережі налічували понад півтора мільйона облікових записів у різних соцмережах, поштових сервісах і месенджерах. Ботів реєстрували для поширення фейків і пропаганди, проросійських наративів, виправдання дій окупантів, розповсюдження протиправного контенту.

Профілактичну операцію під умовною назвою «Ботоферма» провели працівники Департаменту кіберполіції спільно з територіальними слідчими підрозділами Нацполіції, органами прокуратури України й у співпраці з операторами стільникового зв’язку.

У результаті викрито протиправну діяльність 31 фігуранта з різних областей України. Правопорушники реєстрували бот-акаунти, з яких розповсюджувалися фейки і протиправний контент. Зокрема, дописи й коментарі містили прокремлівські наративи, виправдання окупації українських територій, пропаганду війни, дискредитували захисників України або представників органів влади.

Також фігуранти за допомогою SIM-карток мобільних операторів рф реєструвалися в онлайн-банкінгу російських фінустанов, надалі здійснюючи грошові перекази на територію країни-окупанта.

Крім цього, припинено діяльність ботоферми, яка функціонувала для розсилки неправдивих повідомлень про мінування об’єктів на території України.

Під час операції кіберполіцейські виявили факт «зараження» мобільних пристроїв громадян шкідливим програмним забезпеченням. Принцип його дії полягав у прихованому віддаленому отриманні перевірочних SMS-повідомлень у процесі реєстрації акаунтів на різних сервісах.

Загалом припинено діяльність 13 ботоферм, що налічували понад 1,5 мільйона фейкових акаунтів.

У співпраці з працівниками Національного центру оперативно-технічного управління мережами телекомунікацій Державної служби спеціального зв'язку та захисту інформації України заблоковано роботу 28 вебресурсів на території нашої країни, які використовували для реєстрації мобільних номерів і подальшого створення бот-мереж.

Проведено 24 обшуки в оселях фігурантів та за місцями розташування ботоферм. За результатами вилучено понад 100 тисяч SIM-карток, зокрема, мобільних операторів рф, понад 100 одиниць комп’ютерної техніки, більше 150 мобільних телефонів та близько 300 GSM-шлюзів. Вилучену техніку направлено на проведення відповідних експертних досліджень.

Відкрито кримінальні провадження за ст. 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих), інформаційно-комунікаційних систем, електронних комунікаційних мереж), ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації), ст. 436 (Пропаганда війни) та ст. 259 (Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності) ККУ. Слідчі дії тривають». ***(Артем Сереженок. Кіберполіція провела загальнонаціональну операцію з припинення діяльності ворожих ботоферм // Internetua (https://internetua.com/kiberpoliciya-provela-zagalnonacionalnu-operaciua-z-pripinennya-diyalnosti-vorojih-botoferm). 21.12.2022).***

***

«Мінцифри співпрацюватиме з найбільшою розвідувальною компанією у світі Recorded Future у сфері кіберзахисту. Про це повідомив міністр цифрової трансформації України Михайло Федоров.

«Підписали меморандум з Recorded Future, який допоможе захистити критичну інфраструктуру в Україні від військової та кіберагресії з боку росії. Також домовилися про спільну роботу над створенням нових продуктів і технологій для захисту критичної інфраструктури, які зможуть використовувати в усьому світі», — розповів Федоров у Telegram.

З початку повномасштабної війни Recorded Future:

- надала розвідувальні дані для захисту критичної інфраструктури України,
- допомогла в розслідуванні воєнних злочинів росіян,
- відкрила доступ до програмної платформи Intelligence Cloud на понад $10 мільйонів.

У межах меморандуму Recorded Future надасть свою розвідувальну платформу, спеціалізованих інженерів та аналітиків розвідки, зазначив Федоров. Зі свого боку Мінцифра надасть власну експертизу та спеціалістів, які співпрацюватимуть з компанією». ***(Руслан Сорока. Мінцифри підписало меморандум про співпрацю у галузі кіберзахисту з Recorded Future // Speka.Media (https://speka.media/mincifra-pidpisala-memorandum-pro-spivpracyu-u-galuzi-kiberzaxistu-z-recorded-future-pkr7x9). 06.12.2022).***

****

«Мінцифра розширює співпрацю з найбільшою розвідувально-аналітичною компанією у світі Recorded Future. Команда підписала Меморандум у сфері захисту критичної інфраструктури в Україні від військової та кіберагресії з боку росії. Також домовилися про спільну роботу над створенням

нових продуктів і технологій для захисту критичної інфраструктури, які зможуть використовувати в усьому світі.

Україна і Recorded Future давно співпрацюють у сфері кібербезпеки. Підписаний меморандум дасть змогу підсилити партнерство та використовувати розвідувальні дані для захисту України у фізичному та кіберпросторі.

«Співпраця з Recorded Future дасть змогу ще ефективніше захищатися від загроз з боку росії. Разом з компанією ми зможемо створювати революційні технологічні продукти для захисту критичної інфраструктури України. Вони будуть корисними в усьому світі», — зазначив Михайло Федоров, Віцепрем'єр-міністр — Міністр цифрової трансформації України.

У межах Меморандуму Recorded Future надасть свою розвідувальну платформу, спеціалізованих інженерів та аналітиків розвідки. Зі свого боку Мінцифра надасть власну експертизу та спеціалістів, які співпрацюватимуть з Recorded Future.

«Україна веде війну від імені вільного світу, що має важливе значення для Заходу. Росія повторює свою безглузду стратегію війни, яку вже застосовувала в Сирії та Чечні, і спрямовує дії на цивільну інфраструктуру. Recorded Future готовий допомогти Україні в обороні за допомогою нашої розвідки. Ми з нетерпінням чекаємо на спільну роботу над цим викликом з командою Міністерства цифрової трансформації України, яка має історію креативних інтернет-рішень», — зазначив Крістофер Альберг, генеральний директор і співзасновник Recorded Future.

З початку повномасштабної війни Recorded Future надала розвідувальні дані для захисту критичної інфраструктури України, допомогла в розслідуванні військових злочинів росіян в Україні, відкрила доступ до програмної платформи Intelligence Cloud на понад $10 мільйонів. Окрім цього, розширила розвідку про загрози щодо російських кібератак». ***(Мінцифра співпрацюватиме з найбільшою розвідувальною компанією у світі Recorded Future у сфері кіберзахисту – підписано Меморандум // Офіційний веб-сайт Міністерства цифрової трансформації України (https://thedigital.gov.ua/news/mintsifra-spivpratsyuvatime-***

z-naybilshoyu-rozviduvalnoyu-kompanieyu-u-sviti-recorded-future-u-sferi-kiberzakhistu-pidpisano-memorandum). 06.12.2022).

***

«Команда Мінцифри підписала меморандум про співпрацю з провідною організацією з кібербезпеки США та Австралії «Інтернет 2.0». Домовилися про співробітництво у сфері кіберзахисту та навчання українських ветеранів навичкам кібербезпеки.

«В Україні розпочав роботу провідний партнер міжнародної Ініціативи протидії кібер-вимагачам (Counter Ransomware Initiative, CRI) "Інтернет 2.0". Початок нашої співпраці – це позитивний сигнал для інших міжнародних компаній і брендів про те, що саме зараз Україна може і має стати потужним партнером у реалізації спільних проєктів», – зазначив заступник Міністра цифрової трансформації Георгій Дубинський.

Україна стала першим у світі партнером «Інтернет 2.0» за межами країн розвідувального альянсу ФВЕЙ (FVEY), до якого входять Австралія, Канада, Нова Зеландія, Велика Британія та США. Згідно з Меморандумом компанія забезпечить навчання українців з кібербезпеки та надаватиме аналітичну підтримку Україні у боротьбі з кібератаками.

«Інтернет 2.0 та Уряд Австралії вважають співробітництво у сфері кібербезпеки з Україною важливим для нашого стратегічного партнерства і для глобального ландшафту кібербезпеки. Ми бачимо себе довгостроковим партнером України як під час війни, так і після неї. Також визнаємо особливий борг, який маємо перед ветеранами України за захист демократії і безпеки всього світу», – зазначив генеральний директор «Інтернет 2.0» Роберт Поттер.

У межах Меморандуму «Інтернет 2.0» надаватиме свої технології та поділиться передовим досвідом для потреб кіберзахисту України. Навчатиме українських ветеранів навичок кібербезпеки та цифрових технологій. Також компанія відкриє офіс в Україні.

«Інтернет 2.0» — це провідна організація з кібербезпеки США та Австралії, місія якої — захищати клієнтів і партнерів від найсучасніших загроз. Основні продукти «Інтернет 2.0» – технологічні рішення з кіберзахисту Cloaking Firewall і Malcore. Підрозділ компанії Advanced Practices надає аналітично-розвідувальні послуги». ***(Посилюємо кіберзахист: Мінцифра підписала Меморандум з міжнародною компанією «Інтернет 2.0» // Офіційний веб-сайт Міністерства цифрової трансформації України (https://thedigital.gov.ua/news/posilyuemo-kiberzakhist-mintsifra-pidpisala-memorandum-z-mizhnarodnoyu-kompanieyu-internet-20). 13.12.2022).***

***

«Год назад в Киев (Украина) прибыла группа из 10 человек из Национальной миссии киберкомандования США.

Майор морской пехоты, руководивший этой группой, перезвонила и сказала: «Мы побудем здесь ненадолго», — сказал генерал армии Пол М. Накасоне, командующий Киберкомандованием США и директор Агентства национальной безопасности/начальник Центральной службы безопасности. Обслуживание.

Накасоне выступил сегодня на форуме Рейгана по национальной обороне в Президентской библиотеке Рональда Рейгана в Сими-Вэлли, Калифорния.

Эта команда выросла с 10 до 39 человек, работая с Украиной над укреплением ее киберзащиты и обеспечением уверенности. По его словам, это окупилось, когда Россия начала свое вторжение.

Урок: присутствие, настойчивость и ценность партнерских отношений — вот что важнее всего, сказал он.

По его словам, Федеральное бюро расследований, Агентство по кибербезопасности и безопасности инфраструктуры, промышленность, научные круги, а также иностранные союзники и партнеры входят в число тех, с кем министерство обороны тесно сотрудничает.

Он упомянул, что ярким примером является партнерство Cybercom с ФБР и CISA для обеспечения безопасных и надежных выборов.

«Мы генерируем действительно хорошие идеи. Мы делимся разведданными и информацией с ФБР и CISA. А затем мы принимаем меры против противников, которые попытаются причинить нам вред», — сказал Накасоне.

По его словам, в прошлом году АНБ опубликовало 24 незасекреченных рекомендации по кибербезопасности относительно того, чего ожидать в плане атак России на такие объекты, как критически важная инфраструктура США.

Фрэнк Кендалл, министр ВВС, который также выступал на панели, сказал о военных киберсистемах: «Если мы вложим в них ресурсы, мы сможем быть достаточно кибербезопасными… Но тактика [врага] будет продолжать развиваться. Со временем мы будем становиться все более изощренными, поскольку мы строим лучшую защиту».

Он добавил, что за последние несколько десятилетий способность Америки защищаться от кибератак значительно улучшилась.

«Вы никогда не будете совершенны, но вы можете быть очень устойчивыми, и вы можете быть в состоянии, когда вы, если вы получите неожиданное нападение, сможете восстановиться», — сказал Кендалл.

По его словам, когда Россия атаковала, Украина не смогла полностью победить киберугрозу, но смогла заблокировать большую часть ее воздействия». ***(David Vergun. Partnering With Ukraine on Cybersecurity Paid Off, Leaders Say // An official website of the United States Government (https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/). 03.12.2022).***

***

«Эксперты призывают их к сотрудничеству, требуют большего от поставщиков, направляют правительство

«Мы занимаемся решением проблем безопасности или мы здесь только для развлечения?»

Так спросил опытный исследователь безопасности Дэниел Катберт в программной речи на конференции Black Hat Europe 2022 в Лондоне в среду.

Вопросы о том, будет ли профессия кибербезопасности коллективным хозяином своей судьбы и как этого добиться, были главной темой конференции Black Hat Europe 2022.

В своем программном выступлении в четверг «Кибербезопасность: следующее поколение» ветеран кибербезопасности Джен Эллис сказала, что либо профессия сама опередит вопрос Катберта, либо сторонние субъекты заставят его задаться. Это связано с тем, что взрывной рост мобильности и устройств Интернета вещей открыл пользователям новые виды вреда: не только виртуальный, но и физический.

«Это меняет ставки и то, как мы думаем о последствиях киберрисков. На самом деле, так важно, чтобы правительства отреагировали», — сказала Эллис, которая регулярно консультирует правительства в различных ролях, в том числе в качестве сопредседателя Ransomware. Целевая группа и советник CyberPeace Institute и Global Cyber Alliance, среди прочих.

Министерство культуры, средств массовой информации и спорта правительства Великобритании в 2018 году опубликовало свод правил для IoT, который содержит 13 основных принципов безопасного проектирования, которые он призвал производителей принять. Законодатели рассматривают возможность сделать их юридическим требованием.

DCMS также изучает вопрос о том, должны ли сертификаты для специалистов по кибербезопасности стать обязательными. На данный момент правительство Великобритании не решило сделать сертификацию обязательным требованием. Эллис сказал, что для того, чтобы это оставалось таким, потребуется участие аудитории и других специалистов по кибербезопасности, добавив, что в их интересах помочь правительству сделать все правильно.

Команда Кибербезопасность

Может ли отрасль коллективно управлять своим будущим? «Мы — индустрия, основанная на выявлении проблем. Мы профессионально циничны. Мы

должны быть такими; в этом нет ничего плохого. На самом деле это отличное качество», — сказал Эллис. «В чем мы не так хороши, так это в совместной работе над поиском решений и согласованием… В контексте этого разговора это означает, что если люди решат, что у нас должна быть обязательная сертификация, она скорее будет передана нам. чем мы, разработавшие его для себя».

Другими словами: по мере того, как общественный риск, связанный с кибербезопасностью, увеличивается, не ожидайте, что старые подходы, решения или подходы будут продолжать применяться — отчасти потому, что все продолжает меняться так быстро, и теперь вовлекается гораздо больше заинтересованных сторон.

Вторя Джеффу Моссу, основателю Black Hat и Def Con, вступившему в среду на открытии конференции, Эллис назвал непрекращающийся рост сложности серьезной проблемой для повышения безопасности (см.: As Complexity Challenges Security, Is Time the Solution?).

Хакерская группа L0pht свидетельствовала перед Конгрессом в 1998 году, что она может отключить Интернет за 30 минут или меньше. Двадцать лет спустя группа снова дала показания, за вычетом 30-минутного заявления. «Но они сказали, что многие из тех же проблем, о которых они говорили 20 лет назад, все еще актуальны», — сказала она. «Они говорили о том, что сложность только возрастает… поверхность атаки увеличивается. Так что тот факт, что мы все еще сталкиваемся с теми же проблемами, является реальной проблемой».

«Справедливо сказать, что мы принадлежим ко второму поколению профессионалов в области кибербезопасности», и то, что сработало для первого поколения, не обязательно поможет следующему, — заявила эксперт по кибербезопасности Джен Эллис из Black Hat Europe 8 декабря 2022 года. (Изображение: Мэтью Дж. Шварц)

В то же время, следующее поколение должно начать брать верх над такими, как L0pht. «Сейчас они находятся в положении, когда они фактически являются бизнес-лидерами», — сказал Эллис. «Некоторые из них работают в правительстве. Некоторые из них уходят на пенсию на с трудом заработанные деньги, которые они заработали благодаря карьере в сфере безопасности».

Эллис сказала, что она не обязательно призывала участников увеличить свою рабочую нагрузку, присоединившись к консультативным советам, чтобы помочь правительству разработать более эффективные руководящие принципы или правила, которые иногда могут способствовать необходимым изменениям. Но она сказала, что один из важных шагов для специалистов по кибербезопасности сегодня — помочь потребителям, в том числе их собственному бизнесу, понять, что они могут влиять на изменения, например, требуя таких вещей, как спецификация программного обеспечения или SBOM, в которой подробно описываются компоненты. программный или аппаратный продукт.

Расширение прав и возможностей покупателей

«Смысл SBOM в том, чтобы сказать крупным покупателям, крупным компаниям: у вас есть право покупать. Вы можете требовать большего от своих поставщиков. Производители, с которыми вы работаете, не должны преднамеренно подвергать вас риску», — сказал Эллис. Конечно, уязвимости будут проникать в разработку программного обеспечения; это сложный процесс. Но когда поставщики решают не заниматься этой проблемой заранее, «это не нормально», — сказала она, и именно тогда потребители такой технологии должны дать отпор и сказать: «Нет, это неприемлемо. Это недостаточно хорошо».

Привлечение поставщиков к ответственности не только предполагает SBOM, но и требует, чтобы поставщики делали больше для повышения безопасности своих продуктов, моделируя угрозы, понимая свои собственные цепочки поставок

и продвигая SaaS-версии своего программного обеспечения, говорит Катберт, который является опытным охотником за ошибками и член нового консультативного совета правительства Великобритании по кибербезопасности.

Отрасли, возможно, предстоит пройти долгий путь, отчасти благодаря всепроникающему инженерному мышлению, которое слишком часто ищет новые инструменты для исправления старых. Катберт вспомнил, как в начале своей карьеры он внедрял брандмауэры для защиты онлайн-сервисов. Но необходимость держать порт 80 открытым облегчила злоумышленникам обход брандмауэров, что привело к внедрению брандмауэров веб-приложений, только для того, чтобы и исследователи, и преступники обходили их с угрожающей скоростью, сказал он.

«Это была большая часть того, как выросло множество инструментов безопасности вокруг вас — рефлекторная реакция на тот факт, что продукт, на который вы хотели положиться, не был надежно разработан, поэтому нам пришлось затем пойти и получить другой продукт … и надеюсь на Бога, что этот продукт сделал свое дело. А затем выступило оскорбительное сообщество и разорвало этот продукт на части», — сказал Катберт. «Вот мы и в 2022 году, и эта проблема все еще существует сегодня».

Лакмусовая бумажка: успех фишинговой атаки

Даже проблемы, которые теоретически должно быть легко остановить, такие как фишинговые атаки, остаются широко распространенными. «Для меня фишинг — это систематическая проблема того, где мы находимся как отрасль, в том смысле, что вы должны иметь возможность щелкнуть что-то, а не получить обратную оболочку для кого-то еще», — сказал он, добавив, что дополнительное обучение не имеет значения. т решение, которое требуется.

Что не помогает, добавил он, так это то, что производители не берут на себя ответственность за то, чтобы сделать больше — например, Microsoft не смогла заблокировать макросы в Office по умолчанию до начала этого года, несмотря на то, что это был главный вектор атаки.

На уровне кода Катберт рекомендует уделять пристальное внимание не только устранению ошибок, но и уменьшению размера базы кода, что оставит

место для меньшего количества ошибок, а также исключению любого кода, которому нельзя доверять. Теория того, как это сделать, хорошо известна. Теперь, по его словам, проблемой остается усыновление». ***(Mathew J. Schwartz. Cybersecurity Pros: Fresh Challenges Face 'Next Generation' // Information Security Media Group, Corp. (https://www.govinfosecurity.com/cybersecurity-pros-fresh-challenges-face-next-generation-a-20654). 08.12.2022).***

***

«Страны Азиатско-Тихоокеанского региона (APAC) быстро переводят национальные законы о защите данных в онлайн, а новый отчет Future of Privacy Forum (FPF) и Asian Business Law Institute (ABLI) способствует переходу от моделей, основанных на согласии, к моделям, основанным на согласии. сосредоточиться на подотчетности обработчиков данных в интересах повышения согласованности между различными юрисдикциями, которые имеют существенно разные правовые системы.

Отчет обнаруживает, продвигает тенденцию к моделям подотчетности в Азиатско-Тихоокеанском регионе

Сказать, что в регионе Азиатско-Тихоокеанского региона действует разнообразный набор законов и нормативно-правовых актов, значит не сказать ничего. Поскольку страны Азиатско-Тихоокеанского региона быстро внедряют законы о защите данных в онлайн, вопрос передачи и защиты персональных данных при их перемещении между этими странами становится важной проблемой.

В настоящее время общим стандартом в регионе является «соблюдение через согласие» или сосредоточение правил на том, что субъект данных решает разрешить. Организации иногда собирают согласие даже сверх того, что требуется местной юрисдикцией, поскольку они считают, что это защищает их базы, когда данные перемещаются между регионами. Как правило, практика получения согласия во всех юрисдикциях ориентирована на крупнейшие и наиболее влиятельные страны региона с самыми надежными законами о защите данных.

Однако в последние годы эта модель столкнулась с проблемами, поскольку защитники конфиденциальности выступили против нее и нашли ухо в ряде влиятельных региональных правительств. Сингапур переработал свои законы о конфиденциальности в 2020 году, Австралия и Новая Зеландия находятся в процессе пересмотра своих давних законов о конфиденциальности, а ряд других стран Азиатско-Тихоокеанского региона (например, Индия и Южная Корея) провели обстоятельные дискуссии на высоком уровне о том, как адекватные модели согласия можно идти вперед.

Однако на данный момент все 14 юрисдикций Азиатско-Тихоокеанского региона признают согласие в качестве правового основания для обработки персональных данных, и это общая черта во всех их правовых системах. Но это только правовая основа для сбора и использования данных для основной цели в 10 из этих юрисдикций. Специальный административный район Гонконг и три страны (Австралия, Новая Зеландия и Япония) допускают согласие в качестве правовой основы только для конкретных перечисленных видов деятельности, которые также различаются в зависимости от страны. И шесть юрисдикций дают лишь ограниченное определение того, что на самом деле влечет за собой «согласие» в рамках своих законов о защите данных.

Таким образом, несмотря на то, что некоторый способ сбора согласия технически соответствует юридическим требованиям в регионе, международная среда передачи данных остается в некотором роде беспорядком. Законы о защите данных каждой страны имеют разное количество условий согласия, и ни одно из них не является общим условием для согласия. Некоторые требуют информированного и добровольного согласия, некоторые нет. И только меньшинство требует письменного или зарегистрированного согласия или того, чтобы оно было «явным» по своему характеру.

Может ли фокус на подотчетности сделать законы о защите данных Азиатско-Тихоокеанского региона совместимыми?

Хотя существует большая разница в том, как структурированы законы о защите данных, в отчете отмечается, что все страны Азиатско-Тихоокеанского

региона разделяют желание гармонизировать свои структуры с целью беспрепятственной международной передачи данных.

Может ли фокус на подотчетности проложить эти дороги? В отчете говорится, что согласие должно быть сохранено в качестве правовой основы для обработки данных в регионе, но в качестве одной из нескольких таких баз. Одной из таких универсальных альтернатив, продвигаемых в отчете, является принцип «законного интереса», который как минимум охватывает ситуации, когда согласие не является уместным или неосуществимым.

Исследование показало, что в большинстве этих юрисдикций потребуется правовая реформа, но в большинстве из них уже действуют действующие правовые структуры, и многого можно было бы добиться, выпустив последовательные и скоординированные руководящие принципы. Ответственность в значительной степени перейдет к обрабатывающей организации, требуя от них демонстрации законного интереса, предусмотренного этими согласованными правилами и руководящими принципами. В отчете в качестве модели предлагается «балансирующий тест» GDPR ЕС, а также четкий список «вариантов использования», основанный на разумных ожиданиях субъектов данных, в которых он используется в качестве правовой основы.

Одна тема, которая еще не затронута в этом обсуждении подотчетности, — это то, как будут выглядеть штрафы, поскольку они сильно различаются в зависимости от страны в Азиатско-Тихоокеанском регионе. Хотя китайское правительство сохраняет почти неограниченный доступ к личным данным в стране, оно также применяет одни из самых суровых в мире наказаний для отечественных предприятий, нарушающих законы о конфиденциальности, недавно наложившие штрафы на таких технологических гигантов, как Alibaba и Didi, на сумму более 1 миллиарда долларов.

Это также поднимает вопрос о доступе правительств к персональным данным и о том, как стандарты единых законов о защите данных могут решить эту проблему, учитывая большое неравенство в том, как эти правительства обрабатывают персональные данные. Хотя ЕС смог организовать общий набор

стандартов, которые Азиатско-Тихоокеанский регион может использовать в качестве модели, он также устанавливает четкие условия для стран, не входящих в блок, которые считаются адекватными партнерами по передаче данных. Камнем преткновения для этой концепции вполне может стать отсутствие подотчетности некоторых правительств, которые могут помочь себе с международными личными данными». ***(Scott Ikeda. As Data Protection Laws Proliferate, APAC Must Shift to Accountability Model, Says FPF and ABLI // CPO Magazine (https://www.cpomagazine.com/data-protection/as-data-protection-laws-proliferate-apac-must-shift-to-accountability-model-says-fpf-and-abli/). 09.12.2022).***

***

«Глобальный опрос рекрутинговой компании Marlin Hawk, в ходе которого было опрошено 470 директоров по информационной безопасности в организациях с более чем 10 000 сотрудников, показал, что почти половина из них (45%) занимают свою текущую должность два года или меньше.

Джеймс Ларкин, управляющий партнер Marlin Hawk, сказал, что этот показатель немного ниже, чем в предыдущем году, когда тот же опрос показал, что 53% директоров по информационной безопасности занимали свои должности менее двух лет.

В целом, исследование показало, что текущий уровень текучести кадров составляет 18% в годовом исчислении. Опрос также показал, что примерно 62% директоров по информационной безопасности были наняты из другой компании по сравнению с 38%, получившими повышение внутри компании.

Однако опрос показал, что только 12% директоров по информационной безопасности подчиняются непосредственно генеральному директору, в то время как остальные подчиняются другим лидерам в области технологий. Также было установлено, что более трети директоров по информационной безопасности (36%), имеющих ученую степень, также получили высшее образование в области делового администрирования или управления, что на 10% меньше, чем в предыдущем году.

Опрос показал, что в общей сложности 61% имеют более высокие степени в другой области STEM.

Наконец, опрос показал, что только 13% респондентов — женщины, и только 20% — небелые.

Ларкин отметил, что роль директора по информационной безопасности продолжает расти, а вместе с ней и уровень стресса, поскольку объем и сложность кибератак продолжают расти. Неясно, влияет ли уровень стресса на текучесть кадров, и если да, то в какой степени, но это одна из немногих должностей, работающих круглосуточно и без выходных, в любой ИТ-организации, добавил Ларкин.

Роль директора по информационной безопасности также стала предметом более пристального внимания после осуждения бывшего директора по информационной безопасности Uber Джо Салливана по обвинению в препятствовании работе. Большинство директоров по информационной безопасности видят свою роль в защите корпорации, но в целом Ларкин отметил, что большинство из них ошиблись бы в сторону прозрачности, когда дело доходит до управления кибербезопасностью.

Одно можно сказать наверняка: директоров по информационной безопасности ценят больше, чем когда-либо. Опрос PwC, в котором приняли участие 722 руководителя высшего звена, показал, что 40 % бизнес-лидеров считают кибербезопасность самым серьезным риском, с которым сталкиваются их организации. Кроме того, 58 % корпоративных директоров заявили, что больше всего выиграют от расширенной отчетности по кибербезопасности и технологиям.

В результате почти половина респондентов (49%) заявили, что увеличивают инвестиции в кибербезопасность и конфиденциальность, а более трех четвертей (79%) заявили, что пересматривают или улучшают управление рисками кибербезопасности.

В результате у директоров по информационной безопасности, как правило, больше доступа к ресурсам, несмотря на нестабильность экономики. Проблема заключается в том, чтобы определить, как лучше всего использовать эти ресурсы с

учетом множества платформ, которые появляются для повышения кибербезопасности. Конечно, учитывая хроническую нехватку талантов в области кибербезопасности, самой большой проблемой может быть просто поиск кого-то, у кого достаточно опыта для управления этими платформами.

Тем временем большая часть обучения директоров по информационной безопасности и других специалистов по кибербезопасности будет продолжаться на работе. Директора по информационной безопасности, в отличие от других должностей уровня С, у которых есть время для более структурированного обучения, не могут позволить себе такой роскоши». ***(Michael Vizard. Survey Reveals Limits of CISOs' Management Experience // Techstrong Group Inc. (https://securityboulevard.com/2022/12/survey-reveals-limits-of-cisos-management-experience/). 13.12.2022).***

***

«Пришло время прогнозов индустрии безопасности на 2023 год. Что ждет специалистов по кибербезопасности и разработчиков в 2023 году? Делать прогнозы для всего, что связано с технологиями и бизнесом, всегда немного сложно, потому что очень многое может измениться очень быстро.

Тем не менее, мы продвигаемся вперед с нашими лучшими предположениями о том, что организации и команды могут ожидать в наступающем году.

Прогноз 1: больше правил безопасности в 2023 году

Защита данных — особенно конфиденциальной личной информации — от вторжений стала одним из основных приоритетов для правительств во всем мире. Поэтому неудивительно, что в ближайшие месяцы, вероятно, будет больше правил конфиденциальности и безопасности данных от государственных органов.

Наряду с этим будет усилено применение передовых методов и стандартов кибербезопасности, которые направлены на то, чтобы подтолкнуть организации к внедрению основных методов обеспечения безопасности как в ИТ, так и в операционных технологиях.

Организации практически любой отрасли должны иметь хороший обзор всех ИТ-активов в своей инфраструктуре, включая различные программные компоненты. Им нужно будет своевременно устранять любые уязвимости, и больше, чем когда-либо, они будут полагаться на автоматизированные инструменты для помощи в управлении уязвимостями.

Прогноз 2: Продолжающийся рост списка материалов для программного обеспечения (SBOM)

Ни для кого не секрет, что киберпреступники используют слабые места в цепочке поставок программного обеспечения для запуска атак, и нет причин сомневаться, что в ближайшие месяцы эта проблема сохранится.

Такие инциденты, как уязвимость Log4Shell, затронувшая огромное количество организаций, сделают внедрение SBOM приоритетной задачей. Эти ресурсы дают организациям эффективный способ отслеживать все компоненты, из которых состоит данное программное обеспечение, помогая им устранять риски, связанные с уязвимостями.

В то же время будут продолжаться усилия по совершенствованию экосистемы SBOM — внедрению в разных секторах, инструментам, стандартизации совместного использования и обмена SBOM и т. д.

Прогноз 3: предпочтение унифицированным платформам

Когда организации решают, какие инструменты кибербезопасности развернуть, ожидайте, что многие будут склоняться к унифицированным платформам, которые удовлетворяют множество потребностей в области безопасности с помощью единой панели управления. Организации должны защищать более сложные среды, чем когда-либо, часто распределенные между несколькими облачными провайдерами, в то время как глобальный дефицит кадров для кибербезопасности сохраняется.

Это, наряду с текущей финансовой неопределенностью, приведет к объединению различных услуг, которые теперь считаются отдельными. Ищите компании, которые внедряют инструменты, которые обеспечивают большую

автоматизацию, чтобы сэкономить время и деньги, а также расставить приоритеты по рискам безопасности.

Прогноз 4: SCA укрепляет свои позиции

Защита цепочки поставок программного обеспечения является приоритетом для многих специалистов по безопасности, и анализ состава программного обеспечения (SCA), обеспечивающий автоматизированный обзор всех компонентов программных приложений, становится все более важным инструментом в управлении рисками цепочки поставок.

Инструменты SCA автоматически сканируют исходный код приложений для создания списка сторонних, открытых и внутренних компонентов, и организации могут использовать эти инструменты для более эффективного управления программными компонентами. Они устраняют необходимость вручную проверять каждый фрагмент кода для идентификации компонентов.

Учитывая недавние проблемы с цепочками поставок, организации начали искать инструменты SCA, которые предоставляют индикаторы операционных рисков, таких как медленное или плохое обслуживание, сомнительная жизнеспособность проекта и множество других факторов, сообщает исследовательская фирма Gartner.

Прогноз 5: больше организаций примут DevSecOps

DevSecOps, расширение модели DevOps для разработки программного обеспечения, которое требует применения мер безопасности на протяжении всего жизненного цикла разработки программного обеспечения, получает все большее распространение в организациях. Это, вероятно, продолжится и в 2023 году, учитывая сохраняющиеся угрозы цепочкам поставок программного обеспечения.

Уязвимости программного обеспечения могут служить отправной точкой для киберпреступников для запуска различных атак, которые могут повлиять на целые цепочки поставок. Одним из наиболее ярких примеров является уязвимость, обнаруженная в Apache Log4j в конце 2021 года, которая позволяет хакерам получить контроль над системами и их данными и подвергает риску миллионы устройств.

Прогноз 6: Автоматизация становится ключом к успеху DevSecOps

Чтобы быть максимально эффективной для групп кибербезопасности и разработчиков, DevSecOps необходимо автоматизировать. Автоматизация сыграет важную роль в превращении DevSecOps в стратегическую инициативу компаний.

Одна из причин, по которой DevSecOps необходимо автоматизировать, заключается в том, что безопасность встроена в процесс и является частью рабочего процесса. Безопасность становится неотъемлемой частью процесса разработки, а не второстепенной задачей.

Другая причина заключается в том, что автоматизация может позволить командам приносить больше пользы, устраняя ручную работу по проверке программного обеспечения на наличие уязвимостей. Это освободит команды для более продуктивной и инновационной деятельности. А автоматизация может уменьшить количество ошибок, возникающих при ручном подходе к управлению уязвимостями программного обеспечения». ***(Here Comes 2023: Rezilion's Security Predictions // Techstrong Group Inc. (https://securityboulevard.com/2022/12/here-comes-2023-rezilions-security-predictions/). 27.12.2022).***

***

«2022 год был годом подъема SBOM. В это время года мы оглядываемся назад на хаос, вызванный взломом, который произошел в 2021 году и ранее. Последствия кибератак SolarWinds и Kaseya продолжались до 2022 года, что наглядно продемонстрировало, насколько уязвима цепочка поставок программного обеспечения.

Уязвимость с открытым исходным кодом Log4j в конце 2021 года еще раз подчеркнула необходимость выявления труднодоступных уязвимостей.

Эти громкие нарушения привели к тому, что Белый дом в прошлом году издал административную директиву, требующую SBOM для третьих сторон для работы с федеральными агентствами, а также сроки и меры безопасности для критически важного использования программного обеспечения. Если вы еще не знакомы с SBOM, это перечень «ингредиентов», используемых в приложении,

включая зависимости зависимостей, библиотеки с открытым исходным кодом и сторонние компоненты.

Программное обеспечение с открытым исходным кодом и цепочка поставок в 2022 году

Неудивительно, что 2022 год принес множество новых уязвимостей в системе безопасности, в то время как многие организации продолжали страдать от последствий активности Log4j. Но даже несмотря на то, что инциденты с SolarWinds и Log4j послужили тревожным сигналом о последствиях воздействия сторонних приложений, репозитории с открытым исходным кодом остаются заманчивыми целями для эксплуатации.

Цифры говорят о многом. Сбои в цепочке поставок программного обеспечения, связанные с компонентами с открытым исходным кодом, увеличились на колоссальные 650% в период с 2020 по 2021 год. Кроме того, в этом году киберпреступность обошлась миру в $7 трлн.

Поэтому, возможно, не случайно, что 77% организаций сообщили о более широком внедрении программного обеспечения с открытым исходным кодом в течение года.

Между тем, Агентство по безопасности инфраструктуры кибербезопасности (CISA) выпустило Обязательную операционную директиву правительства (BOD), направленную на улучшение видимости активов и обнаружение уязвимостей в федеральных сетях. Мандат требует, чтобы агентства выполняли автоматическое обнаружение активов каждые семь дней и выявляли предполагаемые уязвимости в этих активах и сообщали о них каждые 14 дней.

Хотя это прямо не указывает на создание SBOM, его создание необходимо для выполнения мандата.

Доводы в пользу того, чтобы сделать SBOM главным приоритетом в 2023 году

Открытый исходный код теперь вездесущ. Согласно последнему отчету Synopsis Open Security and Risk Analysis, в 2022 году около 97% кодовых баз

содержали открытый исходный код. Понимание и осведомленность о SBOM значительно выросли в 2022 году, и ожидается, что их использование продолжится.

И это должно. Развертывание таких инструментов, как SBOM и анализ состава программного обеспечения (SCA) в SDLC, может помочь предотвратить дальнейший риск Log4j и отслеживать, где используются компоненты с открытым исходным кодом.

Это гарантирует, что все в цепочке поставок получают надежные приложения, созданные на безопасном и надежном коде. Это важно, потому что доверие к приложениям больше не является чем-то само собой разумеющимся, как показано в EO федерального правительства. Даже если ваша организация не ведет дела с федеральным правительством, это лишь вопрос времени, когда SBOM станут обязательными в частном секторе.

Фактически, Gartner прогнозирует, что к 2025 году 60% организаций, разрабатывающих или закупающих программное обеспечение для критической инфраструктуры, будут обязать и стандартизировать SBOM в своей практике разработки программного обеспечения. Это отражает рост менее чем на 20% в 2022 году.

В идеальном мире разработчики проверяют свой код, чтобы убедиться в отсутствии ошибок или ошибок кодирования. Но из-за множества компонентов с открытым исходным кодом, проприетарных и сторонних компонентов, используемых в приложениях, видимость может быть ограничена.

Согласно опросу Linux Foundation, преимущества внедрения SBOM не ограничиваются безопасностью:

51% респондентов заявили, что создание SBOM помогает разработчикам понять зависимости между компонентами в приложении.

49% заявили, что SBOM упрощают мониторинг компонентов на наличие уязвимостей.

44 % сказали, что создание SBOM помогает в управлении соответствием требованиям лицензий OSS.

Так почему бы не сделать все возможное, чтобы снизить риски безопасности ваших продуктов и цепочки поставок. Почему бы не взять страницу из книги федерального правительства и не сделать внедрение SBOM приоритетом в 2023 году.

Как Rezilion может помочь вам сделать 2023 год годом SBOM

Благодаря нашим возможностям Dynamic SBOM, обнаружению, приоритизации и автоматическому исправлению Rezilion упрощает для команд обнаружение, управление и устранение уязвимостей программного обеспечения в режиме реального времени.

С платформой Rezilion вы можете:

Инвентаризируйте все свои программные компоненты с помощью динамической спецификации программного обеспечения (SBOM).

Определите конкретные уязвимости и узнайте, можно ли их использовать в вашей среде.

Отфильтруйте шум из результатов сканирования, чтобы быстро сосредоточиться на том, что важно.

Создавайте интеллектуальные планы исправления, которые позволяют легко устранять сразу несколько проблем». ***(2022 was the year of the SBOM…and 2023 will be, too // Techstrong Group Inc. (https://securityboulevard.com/2022/12/2022-was-the-year-of-the-sbomand-2023-will-be-too/). 28.12.2022).***

***

«Опрос более 6550 специалистов по безопасности показал, что, несмотря на то, что организации продолжают вкладывать значительные средства в кибербезопасность, уверенности в том, что они действительно способны предотвратить атаки, нет.

Опрос, проведенный Ravn Research от имени Ivanti, поставщика платформы управления ИТ-услугами, показал, что 71% респондентов ожидают увеличения своих бюджетов на кибербезопасность на 11% в 2023 году. Только 1% респондентов заявили, что ожидают сокращения бюджетов на кибербезопасность.

Почти 75% также отметили, что они выделяют средства на устранение нарушений безопасности, причем эти ассигнования составляют около 16% от общего бюджета на кибербезопасность.

Эти бюджетные ассигнования последовали за значительным увеличением расходов на кибербезопасность в 2022 году: 97% респондентов сообщили, что их организации готовы к защите от кибератак так же или лучше, чем год назад.

Однако, несмотря на все эти инвестиции, 20% из 1356 руководителей систем безопасности, принявших участие в опросе, заявили, что не поставят и шоколадки на свою способность предотвратить опасные нарушения. Когда респондентов попросили назвать их наиболее насущные угрозы, респонденты ответили, что уязвимости программного обеспечения (89%) и фишинг (88%) занимают первое место.

Опрос также показал, что менее половины (47%) уже определили сторонние системы и компоненты, которые наиболее уязвимы в их цепочке поставок программного обеспечения. Более трети (35%) планировали устранить этот риск в течение следующих 12 месяцев, но только 46% оценили угрозы цепочки поставок как «высокие» или «критические» для 2023 года. Только 42% заявили, что они полностью готовы защитить поставки программного обеспечения. цепи. Целых 98% заявили, что у них есть метод определения приоритетов исправлений.

В целом опрос определил сложность стека технологий (37%) как главную проблему безопасности, за которой следуют 36%, указав на недостаток навыков в области кибербезопасности.

Доктор Сринивас Муккамала, директор по продуктам в Ivanti, сказал, что в кибербезопасности не так много доверия, как должно быть, потому что злоумышленники постоянно адаптируют свою тактику. Он отметил, что команды по кибербезопасности, напротив, не такие гибкие.

На самом деле, многие медленно осознают, что текущие проблемы требуют более ориентированного на данные подхода к кибербезопасности, сказал Муккамала. Напротив, большая часть предыдущих расходов на кибербезопасность была сосредоточена на защите периметров и развертывании платформ управления

информационными событиями безопасности (SIEM) вместо, например, построения модели вместе с необходимыми знаниями в предметной области, необходимыми для определения местоположения наиболее важных данных. Он добавил, что организация должна защищать в режиме, близком к реальному времени.

В целом специалисты по кибербезопасности также могут больше доверять одному типу платформы, чем другому. Например, 69 % сказали, что облако более безопасно, по сравнению с 7 %, которые считают облако менее безопасным. Тем не менее, только 52% заявили, что у них есть полная информация о каждом пользователе, устройстве, приложении и сервисе в своей сети, и только 48% запускают свои инструменты обнаружения активов не реже одного раза в неделю.

Почти половина (45%) также признались, что подозревают, что бывшие сотрудники и подрядчики по-прежнему имеют активный доступ к системам и файлам компании.

Никто точно не знает, что принесет 2023 год с точки зрения угроз кибербезопасности, но хотя кибербезопасность в целом продолжает улучшаться, киберпреступники, которые запускают эти атаки, также будут продолжать разрабатывать дополнительные методы кибератак, чтобы обойти существующие платформы кибербезопасности». ***(Michael Vizard. 2023 Cybersecurity Spending Increases to Combat Evolving Threats // Techstrong Group Inc. (https://securityboulevard.com/2022/12/2023-cybersecurity-spending-increases-to-combat-evolving-threats/). 21.12.2022).***

***

«…2022 году специалистам по безопасности стало сложнее. Но не все так плохо. Аналитика безопасности продолжала развиваться, улучшая обнаружение. Организации начали добиваться успехов в развертывании архитектур с нулевым доверием как для своих периметров, так и для сред идентификации. Бюджеты безопасности не пострадали до конца года, поскольку безопасность, как правило, является одной из последних статей расходов, на которые влияет спад. В конечном

счете, в этом году установилась пара реалий, и чтобы улучшить ситуацию в 2023 году, нам придется с ними справиться.

Никакого сока: в этом году я участвовал в ряде проектов по безопасности облаков и контейнеров с предприятиями. В каждом из них команде безопасности было трудно заставить команды разработчиков и бизнес-лидеров позаботиться о них. Чтобы было ясно, они сказали, что заботятся, но их действия говорили громче. Они не заботятся о безопасности, пока не случится что-то плохое. Затем они с удовольствием бросают охрану под автобус. Мандат на изменения должен исходить от исполнительной власти. Это единственный способ настроить стимулы для защиты данных.

Удостоверения выходят из-под контроля: по мере того, как рабочие нагрузки и данные перемещаются в облако, внедрение эффективной стратегии управления идентификацией и доступом (IAM) в масштабах предприятия становится решающим фактором успеха. Кроме того, сложно модифицировать эффективную структуру аренды и IAM после развертывания рабочих нагрузок, поэтому не нужно тратить много времени на то, чтобы освоить IAM.

AppSec все еще отстает: как бы ни было интересно думать о том, что разработчики создают безопасный код, они не обучены и не заинтересованы в этом. Таким образом, они не делают. Да, вы можете (и должны) встраивать тесты безопасности в пайплайны. Вы должны нажимать (жестко!), чтобы сломать сборки, которые имеют критические ошибки безопасности. Но разработчики были (и будут продолжать) отказываться от ответственности за безопасность приложений, поэтому нам нужно найти золотую середину.

Повышение квалификации. К сожалению, многие компании сокращают штат сотрудников, и тысячи квалифицированных специалистов по безопасности ищут работу. Да, многие из них быстро раскупаются, но не все. Сейчас самое время инвестировать в свои навыки в области безопасности, но слишком многие организации отреагировали на спад, приостановив прием на работу, и не используют спады как возможность повысить свой персонал. Самые сообразительные менеджеры покупают, когда все остальные продают; многие

организации продавали в 2022 году (и продолжат это делать в 2023 году). Если можете, добавьте труднодоступные навыки (например, облачная безопасность и AppSec) прямо сейчас.

Регуляторная неопределенность: из-за продолжающегося судебного разбирательства по поводу конфиденциальности в Европе и нового мандата на разработку программного обеспечения (SBOM) в США по-прежнему трудно понять, что на самом деле означает «соблюдение» и что потребуется для прохождения оценок. Конечно, эффективная программа безопасности должна учитывать большинство требований соответствия, но неопределенность сохранится, поэтому ожидайте некоторой незапланированной работы, когда мы получим ясность в отношении ожиданий…». ***(Mike Rothman. Cybersecurity in 2022: It's Not Getting Easier // Techstrong Group Inc. (https://securityboulevard.com/2022/12/cybersecurity-in-2022-its-not-getting-easier/). 20.12.2022).***

***

«Чат-бот с искусственным интеллектом написал следующую статью об искусственном интеллекте в кибербезопасности. Серьезно. При написании этой статьи никто не пострадал.

Искусственный интеллект (ИИ) и машинное обучение (МО) — это быстро развивающиеся технологии, которые могут значительно повлиять на кибербезопасность. Эти технологии можно использовать для повышения безопасности путем анализа больших объемов данных и выявления шаблонов, которые могут указывать на потенциальную угрозу, что позволяет организациям принимать упреждающие меры для предотвращения атак. Однако они также представляют собой собственный набор проблем, поскольку злоумышленники могут использовать их для автоматизации и масштабирования своих атак. Чтобы полностью понять влияние ИИ и МО на кибербезопасность, важно изучить как преимущества, так и риски этих технологий.

Одним из основных преимуществ ИИ и МО в кибербезопасности является их способность анализировать большие объемы данных и выявлять закономерности, которые могут указывать на потенциальную угрозу. Это позволяет организациям применять упреждающий подход к безопасности, а не просто реагировать на угрозы после их возникновения. Например, AI и ML можно использовать для анализа сетевого трафика в режиме реального времени, выявляя шаблоны, которые могут указывать на потенциальную кибератаку. Это позволяет организациям принимать превентивные меры до того, как атака станет успешной.

Еще одним преимуществом ИИ и МО в кибербезопасности является их способность автоматизировать определенные задачи, такие как обнаружение потенциальных угроз и реагирование на них. Это может помочь снизить нагрузку на специалистов по кибербезопасности и повысить эффективность операций по обеспечению безопасности. Кроме того, AI и ML можно использовать для автоматизации тестирования систем и приложений, помогая выявлять уязвимости, которыми могут воспользоваться злоумышленники.

Однако существуют и значительные риски, связанные с использованием ИИ и МО в кибербезопасности. Одной из основных проблем является возможность использования этих технологий злоумышленниками для автоматизации и масштабирования своих атак. Например, AI и ML можно использовать для автоматизации обнаружения уязвимостей и разработки эксплойтов, позволяя злоумышленникам проводить более изощренные и эффективные атаки. Кроме того, использование ИИ и МО злоумышленниками может затруднить защиту организаций от этих атак, поскольку технологии могут использоваться для обхода традиционных мер безопасности.

Еще одна проблема заключается в том, что ИИ и МО могут быть предвзятыми или ошибочными, что приведет к неправильным или вводящим в заблуждение результатам. Это может быть особенно проблематично в контексте кибербезопасности, поскольку ошибочная система искусственного интеллекта или машинного обучения может не идентифицировать потенциальную угрозу или может неправильно идентифицировать безобидное действие как угрозу. Это может

привести к ложным тревогам или пропущенным угрозам, что может иметь серьезные последствия.

В заключение, ИИ и МО могут сильно повлиять на кибербезопасность как в качестве инструмента повышения безопасности, так и в качестве потенциальной угрозы. Хотя эти технологии предлагают многочисленные преимущества, важно тщательно учитывать риски и принимать соответствующие меры для их снижения. Это включает в себя регулярное обучение сотрудников передовым методам кибербезопасности и инвестирование в необходимые инструменты и технологии для защиты систем и данных». ***(Mark Rasch. A Robot's View of AI in Cybersecurity // Techstrong Group Inc. (https://securityboulevard.com/2022/12/a-robots-view-of-ai-in-cybersecurity/). 20.12.2022).***

***

«Сообщения о кибератаках продолжают появляться в новостях: от атак на компьютерные системы аэропортов до роста числа фишинговых атак в праздничные дни и появления новых групп программ-вымогателей с большими объемами атак. Увеличение количества атак, как по объему, так и по серьезности, означает, что вашей компании нужна максимальная защита — одна программа или система просто не сможет ее защитить.

Многоуровневый подход к вашей кибербезопасности может помочь вам остановить угрозы до того, как они перерастут в атаки.

Причина 1: выявление, использование и прогнозирование слабых мест в системе безопасности и их влияние

Объединяя различные продукты в области кибербезопасности, вы получаете надежную программу, применяя наступательный подход к кибербезопасности, а не реактивный подход. Проверяя операции защиты и безопасности с помощью полной симуляции атаки, вы сразу видите всю картину. Вы увидите, где находятся уязвимости, расставите приоритеты по исправлению, скроете потенциальные сценарии и затраты после атаки, протестируете своих сотрудников, чтобы увидеть, кто может стать жертвой угрозы, и многое другое. Затем вы можете устранить

слабые места до того, как злоумышленники смогут их обнаружить, что может стоить вашей компании сотни тысяч долларов.

Причина 2: позволяет сосредоточиться на реальных угрозах

Имея под рукой информацию, полученную в результате моделирования и тестов, вы можете использовать базу данных Common Vulnerabilities and Exposures, чтобы определить, какие уязвимости представляют реальную угрозу и должны быть устранены в первую очередь, чтобы свести к минимуму ущерб от эксплуатации. Если вы не знаете, как устранить уязвимость, ничего страшного! Именно для этого и нужна база данных — вы можете координировать усилия со специалистами в области ИТ и кибербезопасности, чтобы обеспечить надлежащее устранение уязвимостей.

Избавьтесь от беспорядка и эффективно распределяйте ресурсы. Это чрезвычайно важно для компаний с небольшой или ограниченной ИТ-командой — не тратьте время и деньги на угрозы с низким уровнем риска, когда ваши ресурсы можно было бы лучше использовать для ликвидации пробелов с высоким риском.

Причина 3: оптимизируйте и централизуйте поставщиков и процессы

Последнее, что вам нужно делать, — это управлять несколькими поставщиками и процессами. Зачем иметь одну программу для сканирования сети, одну для тестирования на проникновение и одну для эмуляции угроз, если можно использовать их все вместе?

Консолидируйте своих поставщиков, найдя того, кто предлагает несколько решений под их эгидой, чтобы вы получили многоуровневое наступательное решение для кибербезопасности и плавно переключались между продуктами и функциями, чтобы получить полное представление о том, что происходит в вашей сети. Консолидация также позволяет уменьшить усталость консоли, имея все в одном месте с решениями, которые интегрированы и работают должным образом, помогает обеспечить соответствие нормативным требованиям и создает отчеты для аудиторов безопасности.

Ищите поставщика, который будет выступать в качестве расширения вашей команды, с выделенным представителем по работе с клиентами, который

расширяет ваши возможности и слушает вас. Вам нужен партнер, который постоянно внедряет инновации, внедряя новые функции, преимущества, обновления и продукты в рамках своей приверженности обеспечению наилучшей защиты от кибербезопасности.

Ваш ответ многоуровневому решению для наступательной кибербезопасности

В Digital Defense мы предлагаем продукты Frontline VM, Core Impact и Cobalt Strike в одном комплекте. С «Elite Bundle» сети сканируются, уязвимости расставляются по приоритетам, выявляются области потенциального использования, а операции защиты и безопасности тестируются с помощью моделирования полной атаки, чтобы вы могли быть на шаг впереди злоумышленников.

Не рискуйте тем, что ваша сеть станет недоступной из-за атаки злоумышленника. Не рискуйте надежностью и репутацией вашей компании из-за того, что злоумышленник подменил ваш домен или торговую марку. Свяжитесь с нами, чтобы узнать больше или начать использовать многоуровневый подход к наступательной кибербезопасности». ***(3 Reasons to Take a Layered Approach to Offensive Cybersecurity // Techstrong Group Inc. (https://securityboulevard.com/2022/12/3-reasons-to-take-a-layered-approach-to-offensive-cybersecurity/). 19.12.2022).***

***

«Ваша организация оценивает бюджеты, и безопасность стоит на первом месте в списке. Вы наняли лучших специалистов для своей команды DevSecOps, и, вообще говоря, ваш технический ландшафт заботится о безопасности.

Это отличное начало, но неполный подход к настоящей кибербезопасности. Недостающий кусок? Ваш персонал.

Независимо от того, сколько денег вы вкладываете в свою стратегию безопасности, вы остаетесь уязвимыми без индивидуального вклада. Шокирующие

82% нарушений безопасности были связаны с человеческими ошибками или недосмотром, что подчеркивает важность обучения и действий со стороны конечных пользователей.

Ваши сотрудники службы безопасности понимают важность предотвращения и внимания к угрозам, но знающие игроки не могут быть везде одновременно. Обучение и общение имеют жизненно важное значение для обеспечения того, чтобы ваши конечные пользователи разбирались в вопросах безопасности. В конце концов, учетные записи конечных пользователей — это ворота к вашим данным и системам. Ваши привратники должны быть готовы к угрозам и рискам.

Ключевые элементы эффективного обучения по вопросам кибербезопасности

Как только вы поймете критическую роль, которую играют конечные пользователи в эффективной стратегии кибербезопасности, как вы можете гарантировать, что все будут участвовать и выполнять свои обязанности по обеспечению безопасности организации?

Обучение осведомленности о кибербезопасности гарантирует, что ваши сообщения и позиция ясны, а ваши конечные пользователи понимают не только в чем и почему они принимают участие, но и то, как они могут внести свой вклад в вашу стратегию безопасности. Есть пять элементов, которые необходимо учитывать, чтобы обеспечить эффективность вашего подхода к обучению кибербезопасности.

1. Является ли кибербезопасность частью лексикона вашей организации?

Лучшее место для начала работы с кибербезопасностью — обеспечение того, чтобы эта тема использовалась в лексиконе вашей организации. Риски и угрозы являются частью повседневной жизни в цифровую эпоху, и предприятия не могут позволить себе принимать защиту или образование как должное.

Учебные занятия и статусные встречи, конечно, ценны. Но организациям следует воздержаться от сохранения разговора для ежемесячной или ежеквартальной встречи и вместо этого включить кибербезопасность в свое общение с сотрудниками, начиная с адаптации.

Убедитесь, что ваши сотрудники понимают свою роль в обеспечении безопасности и знают, к кому обратиться, если они не уверены или у них возникают опасения по поводу угрозы. Расскажите об упреждающих подходах к безопасности и современных угрозах, о которых нужно знать.

2. Релевантные угрозы для вашей организации, отрасли и конечного пользователя

Охватить всю широту угроз кибербезопасности не только невозможно, но и неэффективно пытаться это сделать. Вместо этого обучение по повышению осведомленности должно быть сосредоточено на соответствующих рисках, которые влияют на вашу организацию, отрасль и группы пользователей.

Например, ваш курс повышения осведомленности о кибербезопасности может включать в себя обучение соответствию требованиям:

Если ваша организация работает в сфере медицины, подключите обучение киберугрозам к HIPAA и HITECH.

Если вы работаете в сфере финансовых услуг, обсудите соответствие PCI DSS.

Если вы или ваши сторонние партнеры присутствуете в Европейском Союзе, ваши конечные пользователи должны понимать, как GDPR влияет на суверенитет данных.

В США CCPA в Калифорнии был вдохновлен стандартами GDPR.

Каждый из этих стандартов явно возлагает на организации ответственность за данные клиентов и оставляет мало места для прощения, если злоумышленники нарушают бреши в системе безопасности.

Кроме того, в вашей организации, скорее всего, есть множество групп пользователей и элементов управления доступом. Таким образом, только некоторые угрозы имеют отношение к конкретным пользователям. Например, члены вашей финансовой команды, вероятно, имеют доступ к большему количеству систем или более высоким уровням привилегий, чем ваш отдел обслуживания. Обучение и осведомленность должны иметь отношение к присутствующей группе пользователей.

3. Ясность и последовательность являются ключевыми

Кибербезопасность — это большая тема, и она часто может ошеломить тех, кто не заботится о безопасности. Чтобы обеспечить участие и эффективность, держите свои сообщения по делу. Ландшафт угроз постоянно меняется, но ваши сообщения должны быть последовательными и понятными для обучаемых.

Несмотря на изменения в подходах к атакам, существуют передовые методы, которые закладывают основу безопасности, независимо от отрасли или пользователя. К ним относятся:

Надежность пароля — установите четкие правила для длины и состава пароля и применяйте надежные пароли, которые регулярно меняются.

Программа -вымогатель: текущий ландшафт угроз указывает на программу-вымогатель как глобальную угрозу номер один, и конечные пользователи должны понимать, что это такое, как оно работает и как выявлять риски.

Удаленная работа — если, как и во многих организациях, у вас есть конечные пользователи, которые перешли на полностью удаленную или гибридную модель работы, пользователи должны понимать угрозы, характерные для удаленного входа в систему и разрозненных сетей, и соблюдать надлежащую гигиену устройств, чтобы обеспечить их безопасность.

Фишинг — часто предшествует программам-вымогателям, попытки фишинга могут легко обмануть неподготовленных конечных пользователей и отнять финансы, ресурсы и время.

Начните с лучших практик и расширяйте их таким образом, чтобы ваши конечные пользователи могли легко их понять.

4. Реальные примеры наиболее эффективны

Если организации действительно хотят, чтобы их конечные пользователи получали и переваривали информацию об угрозах безопасности, релевантность и ясность — хорошее начало. Один из самых эффективных способов поделиться информацией об угрозах безопасности — использовать примеры из реальной жизни, чтобы проиллюстрировать опасности и способы реагирования на эти риски.

Делитесь историями об организациях и сотрудниках, которым не так повезло и которые стали жертвами нарушения безопасности. Вместо того, чтобы служить тактикой запугивания, реальные примеры успешных кибератак помогают создать контекст вокруг упреждающих мер.

Используя примеры из реальной жизни, обучение кибербезопасности может включать в себя обсуждение действий, которые должен был предпринять конечный пользователь, чтобы избежать нарушения или исхода.

5. Используйте качественную программу обучения

В конечном счете, недостаточно иметь актуальную информацию и практические советы. Это, конечно, не означает, что вы не должны сосредотачиваться на этих вещах. Наоборот: стройте из вышеперечисленных пунктов, а затем убедитесь, что вы доставляете сообщение таким образом, чтобы оно было получено.

Повторное использование слайдов и общение с конечными пользователями (а не с ними) в конечном счете приведет к тому, что ваша стратегия безопасности потерпит неудачу. Исследования доказали, что существует четыре различных стиля обучения, и вовлечение ваших учеников означает использование нескольких методов.

С помощью высококачественной учебной программы и профессионального партнера по обучению кибербезопасности вы не только убедитесь, что ваш контент отражает текущую картину угроз, но и ваши обучаемые сохранят предоставленную вами информацию. Выберите программу обучения и партнера, которые могут быть настроены для ваших конечных пользователей и разработаны с учетом обучения и удержания». ***(Stefanie Shank. 5 Things Every Organization Should Consider When It Comes to Cybersecurity Awareness Training // Techstrong Group Inc. (https://securityboulevard.com/2022/12/5-things-every-organization-should-consider-when-it-comes-to-cybersecurity-awareness-training/). 17.12.2022).***

***

«В 2022 году геополитические волнения и расширяющаяся поверхность онлайн-атак способствовали появлению нескольких тем в киберпространстве. Инфраструктуры, связанные с противоборствующими идеологиями, подвергались целенаправленной атаке: правительственные учреждения, цепочки поставок и устройства IoT становились жертвами громких кампаний. Киберпреступники запускали все более изощренные атаки на уязвимые объекты, используя DDoS, программы-вымогатели и хакерские атаки, которые постоянно попадают в заголовки газет. И правительства по всему миру начали реагировать с помощью законов и правил для борьбы с растущими угрозами, связанными с кибератаками на большие и малые организации.

В преддверии 2023 года эксперты по безопасности Fortra ожидают появления новых кибер-вызовов, а взамен организации и органы власти будут работать вместе, чтобы лучше укрепить свою систему безопасности и реагировать на угрозы. Ниже приведены прогнозы наших экспертов по кибербезопасности на 2023 год.

Хактивизм и геополитика

Конфликт в Украине и надвигающаяся рецессия — два примера факторов, вызвавших в 2022 году всплеск эмоционально мотивированной киберпреступности и вербовки, а государственные учреждения и предприятия являются главными целями.

Экономический спад окажет негативное влияние на киберсообщество, поскольку история диктует рост киберпреступности во время рецессий. Службы безопасности должны следить за мошенничеством, маскирующимся под государственные программы помощи и найма на работу, поскольку злоумышленники пытаются использовать в своих интересах соискателей или тех, кто иным образом сталкивается с трудными обстоятельствами. Последствия онлайн-атак во время рецессии могут усугубиться, если в целях сокращения расходов будут сокращены операции по обеспечению кибербезопасности.

Эти изменения в расходах могут облегчить злоумышленникам задачу вербовки инсайдеров в качестве точки доступа к корпоративным сетям. Этот метод

компрометации систем будет расширяться, поскольку злоумышленники предпочитают платить недовольным сотрудникам за учетные данные, а не проникать в сеть самостоятельно. Кроме того, поскольку данные распределяются между приложениями все шире, последствия того, кто может получить доступ к этим данным, будут все больше и больше зависеть от безопасности на организационном и геополитическом уровнях.

Расширенный обмен оперативной информацией между частными и государственными организациями станет более распространенным явлением, поскольку службы безопасности осознают необходимость более широкого обзора ситуаций по всему миру и того, как они могут повлиять на их организации. В результате ответная реакция на атаку станет более зрелой.

Расширенные цели атаки

В 2023 году поверхность атаки будет продолжать расширяться как для государственных, так и для частных компаний, и ежедневные проверки станут нормой, поскольку преступники используют инструменты для сканирования Интернета на наличие уязвимостей в операционных системах и устройствах IoT. Реализации только одного уровня контроля безопасности для борьбы с компрометацией будет недостаточно.

Специалисты по безопасности должны ожидать увеличения объема и разнообразия фишинговых электронных писем в 2023 году. Программы-вымогатели и вредоносное ПО останутся постоянной угрозой, и кампании, основанные на реагировании, которые не могут помечать средства контроля безопасности на основе индикаторов, такие как BEC и целевой фишинг, будут все чаще превращаться в угрозу. почтовые ящики пользователей. Эти атаки трудно обнаружить, поскольку в них отсутствуют ссылки и вложения, вместо этого они полагаются на призывы к действию на основе переписки, чтобы попасть в почтовые ящики пользователей.

Обман личности станет серьезной угрозой в новом году. Злоумышленники нацелены на бизнес по внешним каналам, таким как социальные сети, SMS и поисковые системы, при этом преступники в значительной степени полагаются на

тактику выдачи себя за другое лицо. Субъекты угроз также будут использовать искусственный интеллект для улучшения кампаний и определения целей. Положительным моментом является то, что эти нетрадиционные методы атаки будут способствовать формированию киберсоюзников между организациями для обмена важной информацией и инструментами, которые помогут в обнаружении атак.

Многофакторная аутентификация (MFA) также станет объектом увеличения эксплойтов. Злоумышленники будут работать над нарушением целостности с помощью таких методов, как вредоносное ПО для проверки подлинности и подмена SIM-карты. Организациям следует рассмотреть возможность реализации аутентификации без пароля в дополнение к MFA.

Улучшенные реакции на атаки

В 2023 году реакция на атаки будет улучшена за счет улучшения контроля и перехода к нулевому доверию. Организации перейдут от базовых средств контроля, реализованных во время спешки, вызванной COVID, к цифровой трансформации и потратят время на защиту активов данных, которые нуждаются в максимальной защите.

Возможности для совместного использования между организациями будут по-прежнему открываться, а знания и контроль над тем, кто имеет доступ к данным, будут иметь приоритет с помощью многофакторной идентификации, мониторинга, нулевого доверия и шифрования.

Непрерывное увлекательное и актуальное обучение будет иметь решающее значение для помощи пользователям в выявлении атак на основе реальных инцидентов и в соответствии с политиками организации.

Злоумышленники будут продолжать охотиться за самыми дешевыми фруктами и нацеливаться на уязвимые объекты в цепочке поставок, инвестируя в организации среднего размера, менее оснащенные с точки зрения безопасности, включая кредитные союзы, страховые и медицинские организации. В результате оценки и аудиты цепочек поставок увеличатся. Также будет увеличительное стекло по базе вендоров и тому, что делается с предоставленными им данными. Ожидания,

возлагаемые на поставщиков, будут только расти, поскольку от них ожидают решения для множества вариантов использования.

Законы и правила

В 2023 году мы можем ожидать большего сотрудничества между правительствами и странами, поскольку кибербезопасность рассматривается как приоритет. На нефедеральном уровне первый раунд грантов в размере 1 миллиарда долларов в виде финансирования FEMA и CISA BIL будет доступен для правительств штатов, местных и территориальных органов, чтобы помочь понять и снизить инфраструктурные риски.

Ожидается, что на федеральном уровне будут приняты дополнительные законы и инструкции, охватывающие темы от конфиденциальности данных до платежей программ-вымогателей, поскольку CISA и Министерство обороны занимаются долгосрочным стратегическим планированием. FTC только что объявила о новом правиле, касающемся выдачи себя за правительство и бизнес, которое поможет сообщать и удалять нарушающие правила веб-сайты, домены, рекламные объявления и многое другое в новом году. В Европе законодатели продолжат устранять недостатки в Общем регламенте защиты данных (GDPR), чтобы обеспечить беспрепятственную передачу данных за пределы ЕС.

По данным Gartner, в 2023 году три четверти населения мира будут соблюдать правила конфиденциальности. С точки зрения бизнеса, расширение присутствия в цифровом пространстве, вероятно, приведет к большему количеству нарушений, поскольку организации изо всех сил пытаются соблюдать правила соблюдения и конфиденциальности.

Киберстрахование

Киберстрахование станет приоритетом для бизнеса в 2023 году, поскольку все большее число клиентов ожидают, что организации будут страхователями. При этом, скорее всего, произойдет коррекция рынка из-за увеличения премий и оправдания расходов, когда организации будут требовать большего от поставщиков.

Повышенная вероятность кибератаки на бизнес в 2023 году также будет способствовать усложнению процессов предварительного аудита и продления, а также увеличению количества споров и сокращению выплат. Страховщики будут продолжать применять все большее количество средств контроля в отношении компаний, прежде чем предоставлять страховое покрытие, чтобы убедиться, что клиенты соблюдают установленные стандарты.

Тактика, методы и процедуры киберпреступников станут более дифференцированными в 2023 году, поскольку злоумышленники будут стремиться к конечной цели либо прибыли, либо исхода конкретного дела. Эти элементы потребуют от групп безопасности постоянного изучения событий в мире через широкую призму и подготовки к тому, как их деятельность может повлиять на их компанию. Поскольку эти угрозы сохраняются, организациям следует уделять первоочередное внимание инициативам в области кибербезопасности, которые будут способствовать улучшению стандартов и повышению осведомленности об угрозах. Команды безопасности также должны установить более упреждающие средства защиты систем за счет раннего обнаружения уязвимостей, видимости по соответствующим каналам и широкого контроля…» ***(A Spotlight on Cybersecurity: 2022 Trends and 2023 Predictions // Techstrong Group Inc. (https://securityboulevard.com/2022/12/a-spotlight-on-cybersecurity-2022-trends-and-2023-predictions/). 14.12.2022).***

***

«Одной из неотъемлемых проблем, связанных с Интернетом или облачными вычислениями, являются проблемы безопасности. С тех пор как предприятия начали внедрять облачные технологии, их бизнес-операции подвергаются различным сложным киберрискам, которые могут иметь серьезные последствия для непрерывности бизнеса.

Для экспертов по кибербезопасности стало сложной задачей защитить свою бизнес-сеть от всех современных киберрисков. Успешный инцидент безопасности

может иметь разрушительные последствия, которые могут разрушить все бизнес-операции и вызвать перебои в движении денежных средств.

Залы заседаний должны обсуждать вопросы кибербезопасности о рисках

Определение риска и понимание скрытых издержек, связанных с утечкой данных, крайне важно для групп SecOps для принятия стратегических решений в области кибербезопасности.

Для директора по информационной безопасности может оказаться непростой задачей определить истинную стоимость инцидентов безопасности до тех пор, пока они не будут атакованы. Многие предприятия считают цену потери или вымогательства данных полной потерей для организации.

Вот несколько скрытых издержек кибератак, о которых директора по информационной безопасности должны знать и которые необходимо рассчитать при анализе воздействия кибератак:

Увеличенная страховая премия

После успешного инцидента кибербезопасности плата за страховые взносы может увеличиться в геометрической прогрессии, что скажется на бюджетах безопасности. Отраслевые эксперты считают, что фактором, влияющим на затраты, является готовность и глубина данных, предлагаемых держателем полиса после инцидента. Предприятиям необходимо разработать надежную систему кибербезопасности на основе ценных сведений, полученных в результате атаки, чтобы свести к минимуму будущее влияние инцидента на денежные потоки и укрепить свою зрелость в области кибербезопасности.

Нарушение бизнеса

Одной из основных скрытых затрат на кибератаку, которую часто упускают из виду, является нарушение работы. Более того, многие группы SecOps также забывают рассчитать затраты, необходимые для восстановления после сбоя. Для восстановления операционных возможностей может потребоваться некоторое время, что может оказать огромное влияние на финансы бизнеса. Предприятиям, возможно, придется потратить значительные суммы на ремонт оборудования, разработку временной инфраструктуры и перенос бизнес-операций на новые

серверы. Если кибератака взломает весь сервер, затраты на внедрение и замену серверов будут значительно выше.

Недоверие к клиентам

Еще одной потенциальной скрытой ценой кибератаки может быть недоверие к клиентам. Поскольку сегодня клиенты ожидают максимальной конфиденциальности своих конфиденциальных данных, если данные становятся доступными злоумышленникам, это может вынудить клиентов перенести свой бизнес к конкурентам. Удержание клиентов — одна из самых больших проблем, с которыми приходится сталкиваться организациям с успешными инцидентами кибербезопасности.

Утрата интеллектуальной собственности (ИС)

Утрата ИС — это потери, которые понесут организации, которые серьезно повлияют на торговлю, авторские права, инвестиционные стратегии и другую конфиденциальную информацию. Потеря интеллектуальной собственности не будет иметь конкурентного преимущества, необходимого бизнесу для поддержания себя в эту цифровую эпоху. Более того, потеря коммерческой тайны может иметь потенциальное влияние на разрушение бизнеса.

Негативный имидж бренда

Успешная кибератака на бизнес-сеть не только затруднит сохранение клиентов, но и затруднит привлечение новых клиентов. Компании, ставшие жертвами инцидента с безопасностью, могут иметь негативную репутацию на рынке, из-за чего клиентам сложно доверять и делиться своей конфиденциальной информацией.

Директорам по информационной безопасности следует учитывать все указанные выше скрытые затраты на кибератаки, чтобы разработать стратегию кибербезопасности в соответствии с укреплением бизнес-сети». ***(Nikhil S. Hidden Costs of a Cyber Attack // ITSecurityWire (https://itsecuritywire.com/featured/hidden-costs-of-a-cyber-attack/amp/). 05.12.2022).***

***

«Колледж Джорджа Брауна (George Brown) запустил новую программу «Кибербезопасность для ИТ-специалистов» в Центре непрерывного обучения. Он основан на приверженности Джорджа Брауна дальнейшему обучению цифровым навыкам и ставит учащихся в авангарде цифровой экономики.

Колледж разработал новую программу при поддержке TD Bank Group (TD) в партнерстве с Коалицией лидеров инноваций против расизма (CILAR). Он ориентирован на варианты обучения для студентов, которые хотят как лучше понять профессию, так и переквалифицироваться или обновить свои учетные данные, и включает в себя модули онлайн-обучения и курсы, которые предлагают микроучетные данные, связанные с отраслью.

В рамках сотрудничества CILAR также поддерживает стратегию охвата программы, направленную на охват различных сообществ, чтобы создать возможности для обучения для всех и помочь повысить интерес к карьере в области кибербезопасности.

«Микроучетные данные помогают учащимся Джорджа Брауна получить удивительные возможности для получения знаний и навыков, необходимых для удовлетворения растущих потребностей в области кибербезопасности. Мы поддерживаем наших студентов и будущие поколения талантов, и именно так мы добиваемся успеха в George Brown», — говорит Джерван Фирон, президент George Brown.

В рамках этой программы учащиеся могут работать над получением шести микроучетных данных в области кибербезопасности, созданных для обучения наборам навыков, которые специально необходимы для этих ролей:

Аналитик уязвимостей

Аналитик Intel по угрозам

Аналитик фишинга

Аналитик Центра операций по кибербезопасности (CSOC)

Аналитик по реагированию на инциденты кибербезопасности (CSIR)

Наблюдайте за аналитикой

Кроме того, TD поддерживает разработку программы, предоставляя экспертные знания в области технологий кибербезопасности в качестве консультанта.

«TD гордится тем, что работает с Джорджем Брауном над новой программой кибербезопасности, чтобы помочь обучить следующее поколение студентов и профессионалов в такой важной и развивающейся области», — говорит Гленн Фостер, старший вице-президент и главный специалист по информационной безопасности, платформы и Управление технологиями, Enterprise Protect, TD.

Ближайшая дата начала программы – 9 января 2023 года». ***(Samira Balsara. George Brown College introduces a new cyber security education program // ITBusiness.ca (https://www.itbusiness.ca/news/george-brown-college-introduces-a-new-cyber-security-education-program/123498). 05.12.2022).***

***

«В настоящее время во всем мире ощущается нехватка выпускников с необходимыми навыками в области кибербезопасности, при этом спрос на этих специалистов намного превышает предложение. Заглядывая в будущее, в недавнем отчете Всемирного экономического форума подчеркивается, что технологии и опыт в области шифрования и кибербезопасности особенно востребованы.

Это не просто вопрос образования, реагирующего на то, чего может хотеть или не хотеть промышленность; стремление к кибербезопасности исходит от правительств.

Как мы можем обеспечить обучение необходимым навыкам? Может ли быть полезным использование национальных и международных структур?

Некоторые исследования, касающиеся различных структур и роли национальных стратегий кибербезопасности в улучшении образования в области кибербезопасности, уже опубликованы, но еще предстоит опубликовать более конкретный анализ для Великобритании.

Казалось бы очевидным восполнение пробела в навыках путем найма и обучения стажеров. Работа в кибериндустрии с получением необходимых навыков и академических знаний должна быть идеальным решением. Однако есть ли разница в восприятии триединства: образование, бизнес и студент.

Восприятие кибербезопасности

Если вы когда-либо смотрели какой-нибудь триллер, связанный с кибербезопасностью или взломом (кроме «Мистера Робота»), то в том, что представлено, есть либо чрезмерное упрощение, либо полная фантазия. И, по правде говоря, так и должно быть, иначе наш бесстрашный герой говорит: «Не волнуйтесь, брандмауэр укреплен, они никогда не проникнут... папиросная бумага между системой и внешним миром» было бы довольно скучно.

Здесь кроется проблема нашего восприятия. Возможно, у студента есть представление, которое может быть нереалистичным: несколько ударов по клавиатуре и вуаля! Мы проникли в Пентагон. Бизнес, очевидно, хотел бы окупаемости инвестиций. Многие работодатели реалистичны в своих ожиданиях; однако многие могут не понимать сложности, лежащие в основе безопасности их технологии.

Они хотели бы, чтобы их новый ученик решил все технические проблемы, анализ рисков, безопасность оборудования и программного обеспечения, а также удостоверился, что они соответствуют Общему регламенту защиты данных (GDPR) и Регламенту конфиденциальности и электронных коммуникаций (PECR).

Затем академическая сторона. Многие киберстепени возникли из компьютерных сетевых степеней. Это логическое соответствие. Но как насчет человеческого фактора, инсайдерской угрозы, закона и регулирования, как насчет GDPR, Закона об устойчивости цифровых операций (DORA), PECR, Закона о свободе информации (FOIA) или правил сетевых и информационных систем (NIS) и многих других?

Это ставит перед нами проблему: ни одна компания не должна позволять новичкам защищать свою сеть. Давать им ключи от серверной как минимум нецелесообразно. Нам нужно задать вопрос: относится ли все это к области

вычислений? С академической точки зрения, должны ли право и регулирование, риск и управление преподаваться в юридических и бизнес-школах? Должны ли психологи обучать человеческому фактору?

С чего начать?

Проблема, с чего начать, связана с восприятием. Компания хочет, чтобы ученик, получивший степень, мог что-то делать, ученик хочет делать забавные вещи, а преподаватель должен учить строительные блоки. Эти три повестки дня не обязательно будут выполнены.

Одним из возможных путей продвижения вперед может быть обучение политике: стандарт ISO/IEC 27001 и Cyber Essentials Plus. Это может быть полезно для бизнеса, дает ученым отправную точку, и многие ученые степени используют этот подход. Но заинтересует ли это студента, который смотрел «Черную шляпу» с Крисом Хемсвортом в главной роли?

Чему следует учить?

Если мы выполним поиск в Google по запросу «что такое кибербезопасность?», мы получим около 1,7 миллиона результатов и, возможно, множество различных мнений. По правде говоря, как и многие предметы, кибербезопасность представляет собой множество тем, объединенных воедино. Вдобавок к этому существует множество различных рабочих ролей. Все это означает, что то, чему следует учить, становится еще более проблематичным вопросом.

Существуют такие структуры, как Свод знаний по кибербезопасности (CyBoK), который включает 21 область знаний. Они сгруппированы по темам, в том числе: человеческие, организационные и нормативные аспекты, атаки и защита, безопасность систем, безопасность программного обеспечения и платформ, а также безопасность инфраструктуры.

Многие из них можно было бы объединить под названием степени, чтобы сформировать согласованные предметы. Однако любая степень, которая пытается охватить все вышеперечисленное, не будет достаточной глубины, чтобы

гарантировать, что студент (или ученик степени) будет иметь достаточно полезных знаний.

Эта проблема усугубляется, если мы рассматриваем промышленные сертификаты, такие как CompTIA, (ISC)2 или ISAC. Добавьте к этому, с точки зрения ученика или студента, что более ценно: отраслевой сертификат (потому что вы уже являетесь практиком) или университетская степень на уровне бакалавриата?

Включите другой аспект «что, по мнению работодателя, лучше для его бизнеса», и понимание того, чему следует учить, становится очень сложным вопросом.

Спросите у студента, кем вы хотите быть? Спросите у бизнеса, что вам нужно? Спрашивать академика, что вы собираетесь учить, чтобы заполнить первые два ответа, — значит пытаться решить трехмерную задачу в двухмерном пространстве.

Необходим более сфокусированный диалог, возможно, работа с бизнесом для создания названий степеней (и контента), которые соответствуют требованиям отрасли.

ЭТО есть везде, так не должно ли оно быть в каждой степени?

Как насчет степени, скажем, в области управления персоналом или организационного поведения? Было бы разумно включить модули по темам, связанным с человеческими, организационными и нормативными аспектами кибербезопасности?

Поступая таким образом, вы расширяете знания о кибербезопасности и интегрируете их в традиционные предметы. Это сделало бы кибербезопасность менее технической, но более привлекательной для студентов и предприятий…» ***(Is cyber security being taught correctly? // BCS, The Chartered Institute for IT (https://www.bcs.org/articles-opinion-and-research/is-cyber-security-being-taught-correctly/). 05.12.2022).***

***

«Douglas Insights оценила все аспекты рынка консалтинга в области кибербезопасности и выявила изменения рыночных тенденций из-за роста числа кибератак после пандемии Covid-19 и последующий рост спроса на консультации по кибербезопасности. Добавление отчетов об исследованиях рынка консалтинговых услуг по кибербезопасности в механизм сравнения Douglas Insights позволит аналитикам, исследователям рынка, предприятиям и отраслевым экспертам точно определять рыночные тенденции, прогнозы на будущее, факторы роста, рыночные ограничения и препятствия.

Douglas Insights, первая в мире система сравнения отчетов об исследованиях рынка, предоставляет доступ к широчайшему спектру частных и общедоступных отчетов о рынке. Это цифровой инструмент, который позволяет исследователям сравнивать различные отчеты по цене, дате выпуска, рейтингу издателя и оглавлению.

Обзор рынка

Ожидается, что глобальный рынок консалтинга в области кибербезопасности значительно расширится в ближайшем будущем, при этом прогнозируемый совокупный годовой темп роста (CAGR) составит 8,4% до 2031 года. Рост числа глобальных кибератак и угроз является ключевым фактором для этого рынка. Наиболее распространенные типы киберугроз, с которыми сталкиваются предприятия и отрасли, включают атаки социальной инженерии, фишинговые атаки, программы-вымогатели, SQL-инъекции, вредоносные программы, атаки типа «отказ в обслуживании» (DoS), межсайтовые сценарии (XSS) и атаки грубой силы.

Что касается рыночных регионов, Северная Америка ранее была лидером рынка консалтинга в области кибербезопасности и продолжит удерживать свое доминирование в течение прогнозируемого периода. Европа и Азиатско-Тихоокеанский регион являются вторым и третьим по величине регионами рынка консалтинга в области кибербезопасности соответственно. Азиатско-Тихоокеанский регион, в частности, показывает многообещающий рост для этого рынка из-за быстрой урбанизации и индустриализации, ожидаемых в

развивающихся странах региона в течение прогнозируемого периода. Существуют также хорошие возможности для роста на каждом уровне предприятия в автомобильной, розничной торговле, производстве, здравоохранении, BFSI, правительстве, обороне, энергетике, ИТ и телекоммуникациях.

После пандемии COVID-19 произошел глобальный рост числа кибератак, что является основным фактором роста рынка консалтинга в области кибербезопасности. В прошлом году кибератаки заняли 5-е место среди факторов риска в государственном и частном секторах. Скорее всего, они сохранят или превзойдут эту позицию в ближайшие годы. Киберугрозы постоянно развиваются, совершенствуются и становятся все более дорогостоящими для бизнеса. По оценкам, стоимость средней корпоративной кибератаки исчисляется миллионами и, вероятно, продолжит расти в ближайшие годы.

Прогнозируется, что только кибератаки IoT удвоятся в ближайшие годы из-за недавнего подъема Индустрии 4.0 и последующего быстрого роста Промышленного IoT (IIoT). Дальнейшее распространение цифровых услуг, таких как облачные сервисы, создает новые потоки киберугроз и консультаций по кибербезопасности. Последние тенденции в консультировании по кибербезопасности — это упреждающий подход к киберугрозам и обучение персонала кибербезопасности и предотвращению кибератак. Кибербезопасность больше не связана с обеспечением соответствия, а с упреждающим снижением рисков и угроз на этапе цифровой трансформации компаний. Поскольку человеческая ошибка является основной причиной большинства взломов и кибератак в организациях, обучение персонала стало приоритетом для компаний на рынке консалтинга в области кибербезопасности.

Некоторые из ключевых мировых игроков на рынке консалтинга в области кибербезопасности включают CrowdStrike Holdings Inc., McAfee, AT&T Inc., Accenture plc, Bureau Veritas, Mythics Inc., KPMG International Limited, Akamai Technologies Inc., Deloitte Touche Tohmatsu Limited, Atos SE., DXC Technology Company, CGI Inc., BAE Systems plc и Capgemini SE.

С точки зрения типа консультирования по кибербезопасности, на рынке в настоящее время доминируют сетевая безопасность, безопасность приложений, облачная безопасность, безопасность конечных точек, безопасность ICS и безопасность контента. Принимая во внимание, что защита данных как услуга (DPaaS), услуги управляемой безопасности (MSS), управляемое обнаружение и реагирование (MDR), управление уязвимостями и соответствием требованиям, консультации по защите данных и консультации по системам управления кибербезопасностью являются одними из основных услуги для рынка консалтинга в области кибербезопасности…» ***(Cyber Security Consulting Market - The Global Market is Growing at a CAGR of 8.4% by 2031 // GlobeNewswire, Inc. (https://www.globenewswire.com/news-release/2022/12/07/2568928/0/en/Cyber-Security-Consulting-Market-The-Global-Market-is-Growing-at-a-CAGR-of-8-4-by-2031-Douglas-Insights.html). 07.12.2022).***

***

«Сегодня компания Huntsman Security объявила о своих прогнозах кибербезопасности на 2023 год, в том числе о важности состояния кибербезопасности, систематического управления рисками и ожидаемых изменений, вызванных страховой отраслью. Кроме того, компания объясняет, почему рекомендации по кибербезопасности, вероятно, станут более глобальными, и почему отрасль должна перейти от принятия решений, основанных на авторитете, к более масштабируемому подходу, основанному на фактических данных.

Управление состоянием кибербезопасности и управление оценкой рисков приобретают все большее значение

Несмотря на то, что рост числа атак программ-вымогателей прекратился, организациям по-прежнему необходимо знать об областях потенциального риска атаки (поверхностях атаки) и иметь возможность продемонстрировать контроль над ними. Организации должны сосредоточиться либо на:

• Состояние кибербезопасности — измерение состояния киберустойчивости или общей готовности к кибербезопасности; или более целенаправленный

• Управление поверхностью атаки (ASM) — точное представление «поверхности атаки» — активов ИТ-инфраструктуры и относительного риска, возникающего в результате уязвимостей и неправильных конфигураций.

По мере того, как организации стремятся к большей эффективности, а злоумышленники продолжают атаковать возникающие слабые места, в 2023 году мы увидим быстрое внедрение этих решений, позволяющих быстро и точно расставлять приоритеты и сообщать о любых изменениях в киберпространстве.

Киберстрахование способствует улучшению контроля безопасности

Средства контроля безопасности будут иметь ключевое значение для страховых компаний, которые будут лучше поддерживать своих клиентов и более точно оценивать кибер-риски. В 2023 году страховщики потребуют усиления контроля и количественного измерения наряду с ужесточением нормативных требований по надзору за киберрисками.

Конвергенция правил киберкорпоративного управления

Правила корпоративного управления сближаются, и правительства и организации сталкиваются со схожими, если не с одинаковыми угрозами. Организации во всем мире должны будут соблюдать эти все более распространенные киберконтроли, чтобы соответствовать многонациональным нормам. В 2023 году киберуправление станет более формализованным, а решения, принимаемые компаниями в области кибербезопасности, будут подвергаться усилению ответственности и контроля.

Переход от авторитета к принятию решений на основе фактических данных

Решения по кибербезопасности часто основываются на известности, репутации и опыте экспертов. Однако с ростом проблем с киберресурсами доказательства в режиме реального времени, новые системы управления рисками и методологии измерения становятся все более важным элементом эффективного управления киберпространством.

В 2023 году произойдет переход к принятию решений на основе фактических данных, чему будет способствовать доступность технологий, позволяющих измерять и систематически управлять данными о рисках.

Компания Huntsman Security опубликовала полный технический документ, в котором содержится дополнительная информация о четырех приведенных выше прогнозах, а также другие прогнозы…» ***(Huntsman Security Shares 2023 Predictions: Cyber Security Risk Management and Governance to Bring About Industry Change // Business Wire (https://www.businesswire.com/news/home/20221205005435/en). 05.12.2022).***

***

«Южная Корея предложила Совету Безопасности ООН (СБ ООН) добавить кибербезопасность в список пунктов его повестки дня.

Посол Сеула в ООН Хван Джун Кук сделал это предложение в штаб-квартире ООН в Нью-Йорке в среду во время открытых дебатов о пересмотре СБ ООН, подчеркнув необходимость модернизации тем, которыми занимается совет.

В соответствии с Уставом ООН СБ ООН может рекомендовать соответствующие процедуры или методы урегулирования в ответ на спор, который угрожает поддержанию международного мира и безопасности.

Однако, учитывая, что Хартия была принята в 1945 году, хакерские атаки и другие вопросы кибербезопасности не входят в число понятий международного спора.

В результате СБ ООН так и не отреагировал ни на какие крупномасштабные глобальные хакерские атаки.

Хван подчеркнул необходимость того, чтобы совет занимался вопросами кибербезопасности, заявив, что определенное государство-член ООН участвует в кибератаках с целью уничтожения объектов другой страны, кражи информации и сбора средств для разработки ядерного оружия.

Посол также подтвердил, что Южная Корея выступает против увеличения числа постоянных членов СБ ООН, чего добиваются некоторые государства-члены

ООН». ***(S. Korea Proposes UNSC Add Cyber Security to Agenda // KBS WORLD (http://world.kbs.co.kr/service/news_view.htm?seq_code=174500&lang=e). 15.12.2022).***

***

«Японская многонациональная компания, занимающаяся разработкой программного обеспечения для обеспечения кибербезопасности, Trend Micro Inc. предупредила, что в наступающем году субъекты киберугроз будут наращивать атаки, нацеленные на слепые зоны безопасности в домашнем офисе, цепочке поставок программного обеспечения и облаке.

В связи с отчетом под названием «Будущее/время: прогнозы безопасности Trend Micro на 2023 год», опубликованным в среду (14 декабря), управляющий директор Trend Micro в Малайзии и развивающихся странах Го Чи Хо заявил, что с конца прошлого года организации в Малайзии либо вернулись к офиса, навсегда переключившись на удаленную работу или выбрав комбинацию того и другого.

«Однако эти механизмы отвлекают сотрудников от более безопасной и контролируемой ИТ-среды в офисе.

«В 2023 году обновленный субъект угроз сосредоточится на неисправленных виртуальных частных сетях (VPN), подключенных устройствах для домашнего офиса и внутренней облачной инфраструктуре.

«В ответ организациям необходимо будет сосредоточиться на помощи перегруженным командам по безопасности, объединив управление поверхностью атаки, обнаружение и реагирование на единую, более экономичную платформу», — сказал Гох.

Он сказал, что виртуальные частные сети представляют собой особенно привлекательную цель, поскольку одно решение может быть использовано для атаки на несколько корпоративных сетей.

По его словам, домашние маршрутизаторы также будут выделены, поскольку они часто остаются неисправленными и не управляются центральной ИТ-службой.

Trend Micro рекомендует организациям смягчить эти новые угрозы в 2023 году с помощью:

- Стратегии нулевого доверия, основанные на мантре «никогда не доверяй, всегда проверяй», чтобы свести к минимуму ущерб без ущерба для производительности пользователей.

- Обучение сотрудников и повышение осведомленности, чтобы превратить слабое звено в цепи безопасности в эффективную линию защиты.

- Консолидация на единой платформе безопасности для мониторинга всех поверхностей атак, обнаружения угроз и реагирования на них. Это улучшит способность компании выявлять подозрительную активность в своих сетях, снизит нагрузку на группы безопасности и обеспечит бдительность защитников.

- Нагрузочное тестирование ИТ-инфраструктуры для обеспечения готовности к атакам в различных сценариях, особенно в тех, где шлюз периметра уже взломан.

- Спецификация программного обеспечения (SBOM) для каждого приложения для ускорения и улучшения управления уязвимостями за счет обеспечения видимости кода, разработанного собственными силами, приобретенного из коммерческих источников и созданного из сторонних источников». ***(Surin Murugiah. Cyber threat actors to ramp up attacks targeting security blind spots in coming year, warns Trend Micro // The Edge Communications Sdn. (https://www.theedgemarkets.com/article/cyber-threat-actors-ramp-attacks-targeting-security-blind-spots-coming-year-warns-trend). 14.12.2022).***

***

«Киберугрозы постоянно развиваются и увеличиваются с точки зрения частоты и серьезности. Фактически, в прошлом году объемы атак на веб-приложения и конкретные приложения увеличились в 7 из 10 наиболее целевых отраслей в Азиатско-Тихоокеанском регионе. Кроме того, было обнаружено, что около 95% приложений имеют встроенные уязвимости в той или иной форме.

Что движет этой тревожной тенденцией? Было обнаружено, что, поскольку компании вкладывают значительные средства в обеспечение безопасности

различных компонентов ИТ-инфраструктуры бизнеса, точкой входа для большинства этих возможностей являются веб-приложения. Эти меры безопасности оставляют желать лучшего. Из-за постоянной нехватки специалистов по кибербезопасности и все более изощренного ландшафта угроз веб-приложения ускользнули от радаров безопасности большинства предприятий.

По мере того, как выплаты за успешный эксплойт растут в геометрической прогрессии, одновременно растут и стимулы для злоумышленников выполнять эти атаки. Одно нарушение может иметь разрушительные последствия для организации, будь то финансовые, репутационные или даже юридические. Примечательно, что удар по репутации бренда может стать похоронным звоном для любой компании, столкнувшейся с утечкой данных.

Несмотря на нынешнюю ситуацию, важно отметить, что это не обязательно все и конец. Значительный объем угроз и рисков, с которыми сталкивается бизнес, можно защитить с помощью комплексных решений безопасности. Организациям рекомендуется использовать эти решения, чтобы обеспечить надлежащую защиту для снижения серьезности таких атак, которые могут нарушить нормальную работу.

Защита конфиденциальных данных

Учитывая, что большинство современных веб-сайтов позволяют собирать, обрабатывать, хранить и передавать конфиденциальные данные о клиентах, этот кладезь информации является прибыльной целью для киберпреступников. Это означает, что соотношение усилий и вознаграждения никогда не было более благоприятным для злоумышленников.

Кроме того, с ростом разнообразия уязвимостей — от SQL-инъекций, межсайтового скриптинга (XSS) до удаленного выполнения кода (RCE) и атак с обходом пути — качество веб-инфраструктуры организации как никогда важно для ее работы.

Один из способов, которым компания может повысить безопасность своих веб-приложений, — это мониторинг, фильтрация и смягчение последствий вредоносного трафика, входящего и исходящего из приложений через брандмауэр

веб-приложений (WAF). Развертывание WAF перед веб-приложением по существу формирует «щит» между веб-приложением и Интернетом.

WAF работает с помощью набора правил безопасности, часто называемых политиками. Их полезность отчасти обусловлена скоростью и легкостью, с которой можно реализовать изменение политики, что позволяет быстрее реагировать на различные направления атак.

Помимо устаревшей модели WAF, в которой одновременно развертывается только один набор конфигураций, этот сектор стал очагом инноваций. Например, Edgio предлагает уникальную модель двойного брандмауэра веб-приложений, которая предлагает конечным пользователям гибкость, необходимую им для тестирования и анализа, гарантируя при этом отсутствие простоев.

Круглосуточная непрерывная работа сайта

Половину всего интернет-трафика составляют боты — от обычных ботов-сканеров до ботов, очищающих вредоносный контент. Задача организаций — отличить хороших ботов от плохих. Плохие боты используются не только для выполнения автоматизированных задач, таких как кража личных данных, злоумышленники используют их программно для посещения веб-сайтов и выявления уязвимостей в коде для выполнения последующих атак. Масштабируемость ботов также снижает скорость веб-сайта, что приводит к оттоку клиентов и конверсии.

Кроме того, незащищенный веб-сайт может попасть в черный список поисковой системы. Когда это происходит, веб-сайт может потерять до 95% своего органического трафика, что сильно сказывается на доходах. В условиях цифровой экономики предприятия не могут игнорировать влияние вредоносных ботов, поскольку они способствуют еще большему взлому учетных записей, увеличению затрат на инфраструктуру и поддержку, оттоку клиентов и ухудшению качества онлайн-сервисов.

Однако компания, использующая целостное решение для обеспечения безопасности приложений, сможет получить представление о трафике ботов на своих веб-сайтах и API. Это позволит им точно определить в режиме реального

времени, поступает ли запрос приложения из мошеннического источника, и если да, то принять необходимые корректирующие меры.

Защита от DDoS-атак

DDoS-атаки всегда были распространенным инструментом в арсенале киберпреступников. Эта постоянная киберугроза представляет собой грубую, но эффективную форму кибератаки, при которой злоумышленники заполняют сеть или серверы организации-жертвы, чтобы вывести их из строя и не дать законным пользователям получить доступ. Усугубляемый растущей доступностью услуг DDoS по найму, которые могут стоить всего 500 долларов США, атаки на любые организации стали дешевыми и легкими — фактически, различные отраслевые исследования подтвердили значительный рост объема атак., интенсивность, а также продолжительность сеанса по сравнению с прошлыми годами.

Кроме того, растущая зависимость от цифровых услуг означает, что любое нарушение работы ключевых цифровых услуг будет иметь далеко идущие последствия для всех вовлеченных сторон. Со стороны конечного пользователя это может быть связано с потерей производительности из-за ограниченного доступа. И наоборот, для организации-жертвы последствия могут варьироваться от затрат на восстановление до ущерба репутации бренда, последствия которого будут ощущаться даже по прошествии многих месяцев.

Компания, которая адекватно инвестировала в свою безопасность и сетевые возможности, сможет предотвратить любое влияние на свою деятельность, мгновенно обнаружив и смягчив атаку. Однако, учитывая значительную сумму требуемых инвестиций, более осуществимой альтернативой, которую предприятия могут изучить, является передача необходимой поддержки на аутсорсинг. Предприятия могут получить доступ к расширенным ресурсам по смягчению последствий и защите за фиксированный бюджет с поставщиками качественных услуг. Это определяется размером их пропускной способности, а также глобально распределенной сетью. В то же время эти системы регулярно обновляются и обслуживаются, устраняя любые уязвимости до того, как злоумышленники получат к ним доступ.

Ключ к целостному применению лежит в управлении ресурсами

В то время как признаки указывают на то, как организации работают над повышением своей безопасности и внедрением решений для борьбы со все более враждебной киберсредой, это тяжелая битва, окруженная множеством проблем. Это варьируется от нехватки квалифицированных специалистов для интеграции решений безопасности, ограниченных финансовых возможностей для инвестирования или владения полным набором необходимых решений, а также ресурсов, чтобы идти в ногу с последними инновациями в этой области.

Угрозы безопасности останутся в центре внимания организаций в 2023 году, поскольку злоумышленники используют гибридные методы работы организаций и геополитическую напряженность. Предприятия столкнутся с растущим спросом на создание целостного приложения, способного противостоять любым существующим и будущим угрозам для данных клиентов, а также для репутации компаний.

На этом фоне роль поставщиков услуг становится все более важной на этом пути. Преимущества распространяются не только на оптимизацию затрат и техническое обслуживание. Он также направлен на дальнейшие инновации в бизнесе с помощью новых технологий и безопасных приложений и процессов, которые позволяют предприятиям использовать новые возможности в условиях все более сложной ситуации». ***(Edwin Koh. How Holistic Application Security is the Key to Navigating an Increasingly Hostile Cyber Environment // The Fast Mode (https://www.thefastmode.com/expert-opinion/29453-how-holistic-application-security-is-the-key-to-navigating-an-increasingly-hostile-cyber-environment). 13.12.2022).***

***

«В мировой индустрии финансовых услуг в третьем квартале 2022 года количество патентных заявок, связанных с кибербезопасностью, сократилось на 11% по сравнению с предыдущим кварталом. По данным патентной аналитики GlobalData, общее количество грантов, связанных с кибербезопасностью, сократилось на 8% в третьем квартале 2022 года.

Примечательно, что количество патентных заявок, связанных с кибербезопасностью, в отрасли финансовых услуг составило 1757 в третьем квартале 2022 года по сравнению с 1977 в предыдущем квартале…

Анализ патентной активности компаний показывает, что в третьем квартале 2022 года компания China Investment подала наибольшее количество патентов в области кибербезопасности в секторе операций и технологий отрасли финансовых услуг. В этом квартале компания подала 180 патентов, связанных с кибербезопасностью, по сравнению с 1 патентом в предыдущем квартале. За ней последовали Visa с 74 подачей заявок на патенты в области кибербезопасности, Capital One Financial (51 подача) и Mastercard (26 заявок) в третьем квартале 2022 года…

Наибольшая доля патентных заявок, связанных с кибербезопасностью, в отрасли финансовых услуг в третьем квартале 2022 года была в США — 35%, за ними следуют Китай (32%) и Япония (4%). Доля, представленная США, была на 1% выше, чем доля в 34%, которая приходилась на них во втором квартале 2022 года…» ***(Who's innovating where? Patent activity related to cybersecurity decreased by 10% in the financialservices industry in Q3 2022 // Verdict Media Limited (https://www.retailbankerinternational.com/dashboards/patents/patent-activity-cybersecurity-financialservices-industry-q3-2022/). 10.12.2022).***

***

«Отчет о глобальном рынке авиационной и оборонной кибербезопасности за 2022 год».

Ожидается, что мировой рынок авиационной и оборонной кибербезопасности вырастет с 56,81 млрд долларов в 2021 году до 65,07 млрд долларов в 2022 году при среднегодовом темпе роста (CAGR) 14,5%. Ожидается, что рынок авиационной и оборонной кибербезопасности вырастет до 100,51 млрд долларов в 2026 году при среднегодовом темпе роста 11,5%.

Основными типами компонентов авиационной и оборонной кибербезопасности являются решения и сервисы. Решение относится к

инструментам и сервисам, которые помогают защитить администрацию от кибератак, которые могут привести к простою приложений, краже конфиденциальных данных и другим неблагоприятным последствиям. Он развертывается в облачных и локальных моделях.

Северная Америка была крупнейшим регионом на рынке авиационной и оборонной кибербезопасности в 2021 году. Регионы, охваченные в отчете о рынке авиационной и оборонной кибербезопасности, включают Азиатско-Тихоокеанский регион, Западную Европу, Восточную Европу, Северную Америку, Южную Америку, Ближний Восток и Африку.

Отчет об исследовании рынка авиационной и оборонной кибербезопасности является одним из серии новых отчетов, в которых представлена статистика рынка авиационной и оборонной кибербезопасности, включая размер мирового рынка авиационной и оборонной кибербезопасности, региональные доли, конкурентов на рынке авиационной и оборонной кибербезопасности. делитесь, детализируйте сегменты рынка авиационной и оборонной кибербезопасности, рыночные тенденции и возможности, а также любые дополнительные данные, которые могут вам понадобиться для процветания в отрасли авиационной и оборонной кибербезопасности. Этот отчет об исследовании рынка обнаружения аномалий дает полное представление обо всем, что вам нужно, с углубленным анализом текущих и будущих сценариев развития отрасли.

Ожидается, что растущие кибератаки в авиационной промышленности будут способствовать росту рынка кибербезопасности в авиации и обороне в будущем. Появление цифровых или подключенных самолетов, а также интернета вещей в аэропортах создает новые опасности и риски кибератак, которые можно предотвратить с помощью кибербезопасности.

Например, по данным Европейской организации по безопасности аэронавигации, международной организации, работающей над обеспечением безопасного и беспрепятственного управления воздушным движением в Европе, в период с 2019 по 2020 год количество кибератак выросло на 530 % (775 кибератак). против авиакомпаний. Таким образом, растущие кибератаки в авиационной

промышленности стимулируют спрос на рынок кибербезопасности в авиации и обороне.

Инновационные продукты стали ключевой тенденцией, набирающей популярность на рынке авиационной и оборонной кибербезопасности. Крупные компании, работающие на рынке авиационной и оборонной кибербезопасности, сосредоточены на разработке передовых продуктов для укрепления своих позиций на рынке.

Страны, охваченные в отчете о рынке авиационной и оборонной кибербезопасности, включают Австралию, Бразилию, Китай, Францию, Германию, Индию, Индонезию, Японию, Россию, Южную Корею, Великобританию, США…» ***(Aviation and Defense Cyber Security Global Market Report 2022: Market to Surpass $100 Billion in 2026 - Long-term Forecasts to 2031 - ResearchAndMarkets.com // Business Wire (https://www.businesswire.com/news/home/20221221005230/en). 21.12.2022).***

***

«Новый опрос показал, что 35% специалистов по кибербезопасности назвали выгорание сотрудников наиболее серьезной проблемой среди растущих киберугроз.

Специалист по услугам кибербезопасности Integrity360 вместе со своим партнером и поставщиком в области обнаружения и реагирования на угрозы с помощью ИИ, Vectra, объявили о новых результатах опроса Twitter, посвященного критическим угрозам кибербезопасности.

Это связано с тем, что на команды по кибербезопасности оказывается все возрастающее давление, связанное со сложностью современного гибридного предприятия и необходимостью защищать корпоративные данные, где бы они ни находились. На самом деле, почти 63 % респондентов указали, что безопасность данных является наиболее важным фактором для их организации при установлении потребности в эффективных службах кибербезопасности. Меньшую озабоченность

вызывали защита репутации (19%), производительность (12%) и экономия денег (7%).

Хорошей новостью является то, что организации стремятся внедрить критически важные меры безопасности, чтобы обеспечить более эффективное обнаружение угроз и реагирование на них в 2023 году, при этом на первом месте в повестке дня стоят управление идентификацией и доступом (29,9%) и облачная безопасность (29,7%), а затем сеть (19,6%). %) и безопасность конечных точек (20,6%).

По мере того, как предприятия ищут новые способы обнаружения и сдерживания угроз, которые обошли превентивные меры безопасности, Integrity360 и Vectra объединились, чтобы расширить свой существующий портфель услуг по обнаружению угроз и реагированию на них, предоставляя сетевое обнаружение и реагирование, а также, что особенно важно, обнаружение и реагирование на облачные технологии, SaaS и удостоверения личности. возможности с запуском услуг Vectra Managed Detection and Response Services.

«Аналитики сталкиваются с серьезным выгоранием из-за усталости от предупреждений и перегруженности Центра управления безопасностью (SOC), а организациям не хватает опыта, навыков и пропускной способности, необходимых для быстрого и эффективного обнаружения и управления инцидентами безопасности и данными», — говорит Ричард Форд, технический директор Integrity360.

«Интеграция Vectra в нашу услугу MDR меняет правила игры. Она позволяет нам предоставлять комплексные возможности для мониторинга и упреждающего поиска угроз по всему гибридному предприятию, предоставляя расширенные услуги по обнаружению угроз и реагированию на них, а также разгружая перегруженные команды SOC. по шуму».

Отвечая на вопрос о лучших подходах к обеспечению безопасности своей организации в будущем, 52 % респондентов указали, что искусственный интеллект (ИИ) и машинное обучение (МО) являются лучшими средствами.

Новая служба Vectra Managed Detection and Response Service (MDR) дополняет SOC возможностями искусственного интеллекта и машинного обучения, применяя обнаружение на основе поведения вместо того, чтобы полагаться только на обнаружение на основе статики или сигнатур. ИИ сочетает в себе понимание окружающей среды с моделями угроз и человеческим анализом угроз, чтобы автоматически обнаруживать угрозы, что позволяет повысить эффективность выявления угроз на 85% и вдвое повысить производительность операций по обеспечению безопасности.

Сервис позволяет организациям обнаруживать угрозы в облаке, SaaS, Identity и Network и реагировать на них, устраняя критические «слепые зоны» и останавливая кибератаки до того, как они перерастут в брешь, с помощью решения Vectra Attack Signal Intelligence, которое постоянно отслеживает использование методов злоумышленников и изучает клиентов. уникальная среда…» ***(Shannon Williams. Employee burnout greatest fear for cyber security professionals // Techday (https://securitybrief.co.nz/story/employee-burnout-greatest-fear-for-cyber-security-professionals). 16.12.2022).***

***

«…для руководителей высшего звена, любое время, проведенное вне офиса в настоящее время, будь то отпуск или работа, увеличивает риск их кибербезопасности. Имея доступ к конфиденциальным данным, они могут стать выгодной целью для киберпреступников. Рост утечек данных больше не ограничивается внутри организаций, и руководители высшего звена должны понимать, что они становятся лично уязвимыми в тот момент, когда выходят за пределы своего физического офиса.

Персональные сети, принадлежащие капитанам индустрии, теперь столь же привлекательны для хакеров, как и сети крупных организаций, которыми они управляют. Проблема связана с тем, что частные устройства и учетные записи, не связанные с работой, используемые даже руководителями самого высокого ранга, как правило, никогда не защищены и не применяются на тех же уровнях, что и в

корпоративной среде. Эта слабая сторона широко распространена, и мы видим, что киберпреступники все чаще ее используют.

Что делает личные атаки на руководителей высшего звена еще более тревожным, так это то, что хакеры нацелены не только на конфиденциальные корпоративные данные — они почти всегда будут искать компрометирующую личную информацию, чтобы использовать ее для вымогательства. Даже такая, казалось бы, безобидная вещь, как история браузера, является хорошей добычей для киберпреступника, ищущего личную информацию, которая может поставить человека в неловкое положение или нанести ущерб его репутации, если попадет в чужие руки. То же самое относится к любым потенциально конфиденциальным данным или другим носителям, хранящимся в личных документах и файлах.

В последнее время хакеры специально нацеливались на личные учетные записи электронной почты и личные телефоны руководителей. Как правило, домашние сети далеко не так сложны, как сети на рабочем месте, и могут быть легкой добычей для киберпреступников, имеющих опыт взлома гораздо более сложных сетей. Руководители также должны учитывать риск, который представляют для них устройства, принадлежащие членам их семей, особенно их детям, и исследовать, как укрепить всю свою домашнюю сеть от потенциальных кибератак. Даже обучение членов семьи тому, как распознавать фишинговые электронные письма, может быть жизненно важной частью защиты личной сети.

Кибератаки на уровне высшего руководства также происходят со всех сторон, а это означает, что любой подход к укреплению личной ИТ-защиты должен быть тщательным и всесторонним. В одном из последних инцидентов, с которыми столкнулся KordaMentha, киберпреступники связывались с телекоммуникационными агентствами, маскируясь под старшего руководителя, на которого они нацелились, и запрашивали обновление конкретных данных учетной записи. В случае успеха эти угрозы открывают потенциальный доступ к закрытым аккаунтам. Мы также видели, как члены совета директоров использовали личные учетные записи электронной почты в качестве метода обмена информацией, связанной с бизнесом, что является прямым путем к катастрофе. В других случаях

мы видим, как руководители пересылают важную и конфиденциальную информацию в защищенных приложениях или платформах на свои минимально защищенные личные учетные записи и устройства.

Киберпреступники часто нацеливаются на сторонних поставщиков, чтобы проникнуть в сеть организации. Руководители высшего звена также должны знать, что та же тактика применима и к их собственным сетям. На этом личном уровне киберпреступники обычно нацелены на тесные связи человека, начиная с его семьи — детей и партнера — и друзей. Масштабы, на которые идут киберпреступники, нельзя недооценивать, равно как и искушение, которое представляет для них уязвимая личная сеть, принадлежащая кому-то, обладающему властью и влиянием.

Резкий рост киберпреступности в этой области застал врасплох множество руководителей и организаций. По мере того, как появляется все больше сообщений о крупных, громких кибератаках, мы видим, что все больше руководителей высшего звена обращаются за помощью к специалистам, чтобы защитить себя от личных кибератак. Можно проводить высококонфиденциальные и подробные оценки, выявляя любые слабые места в личных домашних сетях, которые могут привести к кибер-взлому. Это может включать обзор рисков, связанных с использованием мобильных телефонов и других устройств, использованием паролей (особенно повторяющихся на разных платформах и устройствах), а также учетных записей социальных сетей и обмена сообщениями.

По мере приближения праздничного сезона и все больше времени, проводимого дома, руководители компаний не должны терять времени на решение вопроса безопасности высшего руководства. Привлечение ИТ-отделов и/или внешних экспертов для изучения домашних сетей руководителей является абсолютной необходимостью. Эти персональные сети должны соответствовать как минимум минимальным уровням безопасности и подвергаться регулярным текущим проверкам на наличие нарушений, подозрительной активности и слабых мест. Ибо точно так же, как кибер-взломы в организациях могут оставаться незамеченными в течение нескольких месяцев и более, так же и в личных сетях руководителей». ***(Brendan Read. Company managers should waste no time addressing***

c-suite cybersecurity // KM Holdings Pty Ltd (https://kordamentha.com/insights/cybersecurity-for-the-c-suite). 09.12.2022).

***

Сполучені Штати Америки

«В этом году наибольшее внимание привлекли положения, которые в конечном итоге были исключены из массивного ежегодного законопроекта об санкциях Министерства обороны — несмотря на то, что в некоторых случаях это было достигнуто двухпартийным соглашением между обеими палатами Конгресса.

Члены Палаты представителей и Сената согласовали свои две версии Закона о разрешении на национальную оборону 2023 года, что позволяет выделить 858 миллиардов долларов на расходы Министерства обороны, а также Министерства энергетики и спецслужб.

Комитет Сената по вооруженным силам опубликовал текст окончательного законопроекта вместе с 748-страничным резюме во вторник после нескольких месяцев обсуждения политиками того, что стало одним из немногих «обязательных» законодательных актов, рассматриваемых каждый год.

Вот где законодатели в конечном итоге остановились на положениях, которые Nextgov отслеживает с последствиями для кибербезопасности и новых технологий.

Кибербезопасность

Во-первых, в окончательной версии законопроекта не предусматривается пятилетний срок полномочий директора Агентства по кибербезопасности и безопасности инфраструктуры.

По словам конгрессмена, это положение было включено в NDAA, принятое Палатой представителей, членом палаты представителей Эндрю Гарбарино, RN.Y., высокопоставленным членом комиссии по кибербезопасности Комитета внутренней безопасности, чтобы стабилизировать руководство департамента.

Также было бы разъяснено, что директор CISA должен назначаться президентом и утверждаться Сенатом.

Хотя это уже второй год, когда Гарбарино пытается включить эту меру в NDAA, но не может, наблюдатели рассматривают ее как одно из наименее противоречивых положений о кибербезопасности в законопроекте об обороне этого года, наряду с кодификацией Бюро кибердипломатии в штате. Департамент, который действительно попал в компромисс, опубликованный во вторник.

Аналитики точно предсказали, что ключевые положения о кибербезопасности, связанные с повышением осведомленности правительства о цепочках поставок программного обеспечения их поставщиков и определением системно важных организаций для получения федеральной помощи и регулирующих обязанностей, будут исключены из согласованного NDAA после противодействия со стороны отрасли.

Окончательный законопроект также исключил положение члена палаты представителей Ричи Торреса, DN.Y., которое держало бы Наблюдательный совет по кибербезопасности Министерства внутренней безопасности на крючке для анализа печально известного взлома SolarWinds. После того, как в указе 14028 ему было поручено изучить обстоятельства этого нарушения, чтобы избежать повторения таких событий, CSRB вместо этого сообщил о последствиях для безопасности уязвимостей Log4J и теперь перешел к изучению деятельности группы вымогателей Lapsus$.

Одной из постоянных проблем, которую законодатели пытались решить для повышения кибербезопасности, является обучение и развитие рабочей силы. Но окончательный вариант законопроекта не включал положение о создании пилотной программы обучения кибербезопасности для имеющих право ветеранов и супругов военнослужащих. NDAA, принятый Палатой представителей, включал поправку от члена палаты представителей Крисси Хулахан, демократ от Пенсильвании, а версия Сената была предложена сенаторами Мэгги Хассан, DN.H., и Джоном Корнином, штат Техас.

Положения обеих палат были смоделированы на основе Федерального закона о расширении штата сотрудников в области кибербезопасности, который ранее был представлен в Сенате Хасаном и Корнином, а в Палате представителей — Хулаханом. Законодательство направлено на устранение нехватки кадров в сфере кибербезопасности путем предоставления ветеранам и супругам военнослужащих доступа к бесплатной программе обучения, предназначенной для укрепления их профессиональных навыков работы в сфере кибербезопасности.

Выжившей двухпартийной и двухпалатной инициативой стала повторная авторизация Национального института компьютерной криминалистики. Окончательное соглашение NDAA предусматривает повторную авторизацию до 2028 года финансируемого из федерального бюджета NCFI, который служит национальным учебным центром цифровой криминалистики, предоставляя сотрудникам правоохранительных органов опыт, необходимый для расследования кибер- и электронных преступлений, в том числе уделяя все больше внимания работе с зашифрованными устройствами и реагировать на атаки программ-вымогателей.

NDAA, принятый Палатой представителей, включал в себя закон, который бы повторно санкционировал институт до 2032 года, но в окончательный законопроект была включена поправка от сенаторов Дайанны Файнштейн, штат Калифорния, и Чака Грассли, штат Р-Айова, которая сузила сферу действия закона. Повторная авторизация NCFI. В 2017 году Конгресс принял закон, продлевающий полномочия NCFI до 2022 года, после того как в предложенном бывшим президентом Дональдом Трампом бюджете на 2018 финансовый год была выдвинута идея прекращения финансирования института.

Новые технологии

Под влиянием двухпартийного стремления конкурировать с Китаем новые технологии в значительной степени получили полную поддержку в финальном NDAA.

Некоторые из положений законопроекта, посвященных инновационным технологиям, — это новые пилотные программы по модернизации

государственных проектов на этапе закупок и повышение квалификации персонала для работы с новыми технологиями.

Искусственный интеллект был одной из наиболее заметных новых технологий. Одним из конкретных вариантов использования, который должен получить финансирование в 2023 году, является создание и совместное использование хранилищ данных с информацией от Министерства обороны, которые имеют отношение к дальнейшей разработке программного обеспечения ИИ для различных боевых операций.

В тексте NDAA также разъясняются руководящие роли в разработке ИИ среди персонала Министерства обороны, а также выделяется дополнительное финансирование для создания отчетов, описывающих использование ИИ в федеральных разведывательных операциях.

Технологии цифровой трансформации, а именно программные инструменты для решения задач модернизации, также вошли в итоговый счет. Ожидается, что Космические силы и Военно-воздушные силы обновят свои программные платформы для капитального ремонта и облегчения операций управления.

Явный запрет на полупроводники, произведенные в Китае, был включен в окончательную версию NDAA, опираясь на более широкое общегосударственное стремление стимулировать внутреннее производство полупроводников, чтобы еще больше освободить США от экономических связей с Китаем.

Еще одна функция, которая была включена в NDAA, заключалась в планировании ускорения распространения 5G в военных ведомствах.

Положения о новых технологиях, включенные в окончательный законопроект NDAA, в целом соответствуют поправкам, первоначально предложенным в рамках отдельных версий в Палате представителей и Сенате. Но в окончательной версии законопроекта заметно отсутствовало создание Американо-израильского центра искусственного интеллекта. Это партнерство способствовало бы сотрудничеству между обеими странами в разработке важнейших технологий искусственного интеллекта, таких как классификация изображений и маркировка данных.

Исключенное положение изначально было законопроектом, внесенным в июне 2021 года сенатором Марко Рубио, штат Флорида.

Теперь Конгресс проведет окончательное голосование по документу, прежде чем отправить его в Белый дом на подпись президенту». ***(Mariam Baksh, Edward Graham, Alexandra Kelley. Key Cyber and Tech Provisions Included—and Excluded—from the Final NDAA // Nextgov (https://www.nextgov.com/policy/2022/12/key-cyber-and-tech-provisions-includedand-excluded-final-ndaa/380588/). 07.12.2022).***

***

«Несколько демократов из комитета Палаты представителей по разведке направили письмо генеральному директору Twitter Илону Маску, в котором выразили обеспокоенность национальной безопасностью в связи с сообщениями о том, что Пекин начал кампанию по подавлению информации, чтобы скрыть новости о массовых протестах населения.

Во вторник влиятельные законодатели из комитета Палаты представителей по разведке направили письмо генеральному директору Twitter Илону Маску, в котором выразили «глубокую обеспокоенность» сообщениями о том, что Китайская Народная Республика — или КНР — организовала кампанию манипулирования на платформе социальных сетей, чтобы скрыть новости о массовых публичных демонстрациях. через всю страну.

«Мы серьезно обеспокоены потенциальным воздействием растущих возможностей КНР с использованием кибербезопасности, включая операции по оказанию вредоносного влияния из-за рубежа, на интересы национальной безопасности США как дома, так и за рубежом», — заявил председатель комитета Адам Шифф, штат Калифорния, и конгрессмены Раджа. Кришнамурти, штат Иллинойс, и Джеки Спейер, штат Калифорния, говорится в письме от 6 декабря.

Послание законодателей прозвучало после пожара в квартире в Урумчи — столице западного китайского региона Синьцзян — 24 ноября, в результате которого погибли 10 человек и еще девять получили ранения, что спровоцировало

протесты по всей стране из-за строгой политики Пекина по борьбе с COVID, которую обвиняли в препятствовании способность пожарных быстро реагировать на возгорание.

Когда Пекин расправился с протестующими, появились сообщения о том, что аккаунты в Твиттере на китайском языке, некоторые из которых были бездействующими в течение нескольких лет, начали спамить платформу ссылками на эскорт-услуги и порнографией в постах вместе с названиями городов, где проходят массовые демонстрации. скрыть освещение протестов.

Законодатели потребовали от Маска, который приобрел Twitter в октябре и ранее называл себя сторонником абсолютизма свободы слова, предоставить им «дополнительную информацию о недавней злонамеренной деятельности и указать, была ли эта деятельность направлена КНР».

В письме подчеркивается недавно рассекреченная оценка Национального совета по разведке «Кибероперации, способствующие экспансивному цифровому авторитаризму», первоначально опубликованная 7 апреля 2020 года и опубликованная 25 октября, в которой, в частности, говорится, что «Китай «развивает свой успех». при внутренних репрессиях при проведении кибероперацій в других странах».

«Чтобы гарантировать, что Соединенные Штаты готовы противостоять, предотвращать и сдерживать угрозы иностранного влияния в Интернете, крайне важно, чтобы мы понимали масштабы потенциального манипулирования КНР Твиттером и определяли, как недавние изменения в Твиттере влияют на угрозу иностранного влияния КПК. операций в социальных сетях», — говорится в письме.

Законодатели настаивали на том, чтобы Twitter и Маск ответили на вопросы о том, знала ли платформа, спонсируется ли китайская кампания манипуляций государством; если бы были какие-либо доказательства того, что Китай или другие государственные субъекты работали «по преднамеренному пресечению доступа к информации с помощью ботов или других манипуляций»; если Twitter в настоящее время имеет «возможность выявлять крупномасштабную дезинформацию, дезинформацию и подавление информации на своей платформе»; и меры,

принимаемые в настоящее время для борьбы с кампаниями по подавлению информации, «учитывая упор Twitter на свободу слова». ***(Edward Graham. China's Reported Manipulation of Twitter Draws Lawmaker Questions // Nextgov (https://www.nextgov.com/cybersecurity/2022/12/chinas-reported-manipulation-twitter-draws-lawmaker-questions/380642/). 08.12.2022).***

***

«Законопроект потребует от Административно-бюджетного управления ежегодного отчета перед Конгрессом с целью определения финансирования, необходимого для перехода агентств на постквантовую криптографию.

Четверо законодателей высоко оценили принятие Сенатом их законопроекта о защите конфиденциальной информации от перспективы создания квантового компьютера, способного расшифровывать текущие криптографические стандарты, поддержав план администрации Байдена-Харриса по устранению такой угрозы.

Квантовые компьютеры, способные расшифровывать современное шифрование с более высокой, чем когда-либо, вычислительной мощностью, по-прежнему считаются не раньше, чем через десять или более лет. Но сторонники плана администрации говорят, что злоумышленники могут собирать данные сейчас с намерением расшифровать их в будущем, как только они достаточно разовьют зарождающуюся технологию.

«Утечки данных, используемые квантовыми вычислениями, являются серьезной проблемой национальной безопасности», — заявила в пятницу сенатор Мэгги Хассан, DN.H. «Противники Америки ищут любые уязвимости в наших системах кибербезопасности, чтобы угрожать нашей инфраструктуре, данным и безопасности. Крайне важно, чтобы мы были готовы защищаться от любых противников, использующих эту невероятно сложную и новейшую технологию против нашей страны. Защита нашей национальной безопасности — это двухпартийный вопрос, и я рад, что Сенат принял наш законопроект, и я буду продолжать работать, чтобы довести его до конца».

К Хасану присоединились сенатор Роб Портман, штат Огайо, и представители Ро Ханна, штат Калифорния, и Нэнси Мейс, штат Южная Каролина, которые высоко оценили принятие Сенатом версии законопроекта, принятой Палатой представителей в четверг.

Закон о готовности к кибербезопасности квантовых вычислений во многом перекликается с меморандумом по национальной безопасности, выпущенным администрацией в мае, в котором устанавливаются крайние сроки для агентств для инвентаризации всех развернутых в настоящее время криптографических систем, чтобы определить приоритет их перехода на формы шифрования, которые, по мнению экспертов, будут неуязвимы для быстрых квантовых компьютеров.

Национальный институт стандартов и технологий и Агентство национальной безопасности в настоящее время разрабатывают стандарты для реализации четырех квантово-устойчивых алгоритмов, о которых NIST объявил в июле после того, как пригласил ученых со всего мира представить свои предложения. В ожидании алгоритмов январский меморандум по национальной безопасности предоставил АНБ право издавать обязательные оперативные директивы, чтобы облегчить переход агентств на новые стандарты.

В дополнение к повторению инструкций администрации для агентств, включая Управление управления и бюджета, законодательство предписывает OMB ежегодно отчитываться перед Конгрессом о усилиях по миграции. Согласно пресс-релизу, в отчетах должна быть изложена стратегия администрации и прогнозируемые расходы.

«По мере развития квантовых вычислений нам необходимо предпринять шаги для защиты личных данных американцев, а также данных национальной безопасности США и правительственных учреждений», — сказал Ханна. «Я очень рад, что Сенат принял этот законопроект, чтобы обеспечить безопасность наших систем и ценных данных и установить контрольную роль Конгресса в этом процессе». ***(Mariam Baksh. Preparations for Quantum Cyber Threat Get a Senate Boost // Nextgov (https://www.nextgov.com/cybersecurity/2022/12/preparations-quantum-cyber-threat-get-senate-boost/380698/). 09.12.2022).***

***

«Сенаторы США Роб Портман (R-OH), высокопоставленный член комитета Сената по внутренней безопасности и делам правительства, и Мэгги Хассан (D-NH) объявили, что Сенат принял двухпартийный Закон о готовности к квантовым вычислениям и кибербезопасности для укрепления национальной безопасности путем подготовки защита федерального правительства от утечек данных с помощью квантовых вычислений.

По мере того, как квантовые компьютеры, в том числе разрабатываемые противниками США, продолжают становиться все более мощными и доступными, федеральные агентства должны активно работать над тем, чтобы федеральные средства защиты от кибербезопасности оставались актуальными. Двухпартийный сопутствующий законопроект в Палату представителей был внесен представителями Нэнси Мейс (республиканец от штата Южная Каролина) и Ро Кханна (штат Калифорния).

«Квантовые вычисления обеспечат огромный прогресс в вычислительной мощности, но также создадут новые проблемы в области кибербезопасности», — сказал член рейтинга Портман. «Я рад, что Сенат принял наш двухпартийный закон, требующий от правительства провести инвентаризацию своих криптографических систем, определить, какие из них подвергаются наибольшему риску от квантовых вычислений, и соответствующим образом обновить эти системы».

«Утечки данных, используемые квантовыми вычислениями, являются серьезной проблемой национальной безопасности. Противники Америки ищут любые уязвимости в наших системах кибербезопасности, чтобы угрожать нашей инфраструктуре, данным и безопасности», — сказал сенатор Хассан. «Очень важно, чтобы мы были готовы защищаться от любых противников, использующих эту невероятно сложную и новейшую технологию против нашей страны. Защита нашей национальной безопасности — это двухпартийный вопрос, и я рад, что

Сенат принял наш законопроект, и я буду продолжать работать, чтобы довести его до конца».

«Наша страна должна не только стать мировым лидером в исследованиях и разработках квантовых технологий, но мы также должны стать лидерами в области постквантовых стандартов кибербезопасности в правительстве», — сказал член палаты представителей Мейс. «Принятие этого законопроекта является важным шагом вперед в защите нашей страны от угроз будущего и в подготовке к этому технологическому скачку».

«По мере развития квантовых вычислений нам необходимо предпринимать шаги для защиты личных данных американцев, а также данных национальной безопасности США и правительственных учреждений», — сказал член палаты представителей Ханна. «Я очень рад, что Сенат принял этот законопроект, чтобы обеспечить безопасность наших систем и ценных данных и установить контрольную роль Конгресса в этом процессе».

Закон о готовности к кибербезопасности квантовых вычислений:

Требовать от Административно-бюджетного управления (OMB) расставить приоритеты в приобретении и переводе информационных технологий федеральных агентств на постквантовую криптографию;

Поручить OMB создать руководство для федеральных агентств по оценке критически важных систем через год после того, как Национальный институт стандартов и технологий (NIST) выпустит запланированные стандарты постквантовой криптографии;

Поручить OMB направить в Конгресс ежегодный отчет, который включает в себя стратегию устранения рисков постквантовой криптографии, финансирование, которое может потребоваться, а также анализ общегосударственной координации и перехода на стандарты и информацию постквантовой криптографии. технологии.

Подробнее читайте в Сенатском комитете по внутренней безопасности и делам правительства». ***(Quantum Computing Cybersecurity Act Passes Senate // Homeland Security Today (https://www.hstoday.us/subject-matter-***

areas/cybersecurity/quantum-computing-cybersecurity-act-passes-senate/).
10.12.2022).

***

«Недавно введенные TSA требования к кибербезопасности вызывают проблемы с внедрением и надзором / исправлением из-за нехватки ресурсов.

С июня 2020 года по июнь 2021 года в транспортной отрасли США число еженедельных атак программ-вымогателей увеличилось на 186 процентов. Аналогичными темпами продолжают расти и другие типы кибератак. В октябре 2022 года пророссийские хакеры атаковали общедоступные сайты многих аэропортов США. Хотя эти атаки были в основном неприятными, киберэксперты предполагают, что они, вероятно, были попытками хакеров изучить и запустить новые вредоносные атаки в будущем.

По мере того, как количество кибератак продолжает расти, транспортные операторы одновременно сталкиваются с требованиями рынка по автоматизации функций, начиная от продажи билетов и заканчивая использованием автономных транспортных средств. Рост автоматизации требует от операторов еще большей зависимости от информационных систем, что приводит к уловке 22 между инновациями и уязвимостью.

В ответ Управление транспортной безопасности (TSA) и Агентство по кибербезопасности и безопасности инфраструктуры (CISA) расширяют требования к кибербезопасности для операторов аэропортов, авиакомпаний, железных дорог, трубопроводов и общественного транспорта. Эти подробные требования включают назначение координатора по кибербезопасности, отчетность о киберинцидентах, проведение оценки кибербезопасности и разработку планов исправления и реагирования на инциденты.

Сторонники приветствуют эти новые требования как необходимый первый шаг к повышению уязвимости нашей транспортной системы к атакам. Другие, в том числе некоторые операторы аэропортов, утверждают, что это просто

контрольный список действий, которые на самом деле мало что делают для улучшения кибербезопасности.

Новые кибертребования TSA подчеркивают существующие проблемы с ресурсами с обеих сторон

Одной из основных причин критики является нехватка ресурсов кибербезопасности на уровне оператора и правительства. Что касается оператора, в недавнем отчете Института Mineta говорится, что немногие транспортные системы США достаточно укомплектованы персоналом для обеспечения кибербезопасности, независимо от их размера, сложности или даже того, понесли ли системы потери в результате предыдущей кибератаки.

Точно так же TSA и более широкое Министерство внутренней безопасности (DHS) изо всех сил пытаются нанять и удержать персонал кибербезопасности. Несмотря на усилия по ускорению процесса найма, TSA и DHS должны конкурировать как с частным сектором, так и с другими правительственными ведомствами США за одни и те же таланты. По данным Cyberseek, поддерживаемого Национальным институтом стандартов и технологий, по состоянию на август 2022 года в Соединенных Штатах было более 714 000 вакансий в области кибербезопасности.

В результате недавно введенные TSA требования к кибербезопасности вызывают проблемы с реализацией и надзором/исправлением из-за нехватки ресурсов для достижения целей TSA требуемым совместным образом. Кроме того, и на более высоком уровне, недавние усилия TSA вызывают вопрос о том, не слишком ли в данном случае TSA занимается чрезмерным регулированием. Например, европейские законодатели устанавливают требования высокого уровня, согласно которым операторы аэропортов должны иметь программы кибербезопасности, но они не диктуют подробно, что должно быть включено в такие программы. Они оставляют это частному сектору.

TSA отлично справляется с соблюдением нормативных требований, и с годами его регулирующая роль совершенствовалась, чтобы создать совместный подход с регулируемыми сторонами, особенно в авиации и наземных объектах. Тем

не менее, большая часть этой выдающейся работы связана с тем, что в TSA были сотни опытных и хорошо обученных авиационных и наземных инспекторов, которые работали над требованиями безопасности с эксплуатантами, выходящим за рамки контрольного списка соответствия. У TSA нет аналогичного персонала для решения развивающейся ситуации в области кибербезопасности.

Точно так же, как ресурсы TSA могут не соответствовать потребностям, требование держать под контролем информацию о безопасности также создает дополнительные препятствия для повышения безопасности. Метки конфиденциальной информации о безопасности (SSI) не позволяют потенциальным поставщикам просматривать требования кибербезопасности до тех пор, пока они не вступят в отношения поставщиков/подрядчиков с операторами. Это запрещает потенциальным поставщикам разрабатывать новые и конкурентоспособные по цене предложения. Вместо этого операторам остается пытаться решать свои кибер-проблемы собственными силами, опасаясь передачи SSI неавторизованным сторонам.

Преодоление проблем с ресурсами за счет использования промышленности

Чтобы преодолеть эти проблемы, TSA необходимо будет укрепить свои партнерские отношения между государственным и частным секторами и может принять решение о подходе к требованиям одним из двух способов: установить требования высокого уровня и позволить частному сектору позаботиться об этом или создать штат сертифицированных частных оценщиков, которые могут работать с операторами для удовлетворения постоянно растущих потребностей в кибербезопасности наших транспортных систем. Учитывая, что TSA не склонен выбирать первый вариант, второй может иметь большее значение.

Подобно использованию сертифицированных фирм K9 в средствах досмотра грузов, TSA может сертифицировать фирмы по кибербезопасности, чтобы они выступали в качестве квалифицированных оценщиков программ. После этого операторы смогут использовать сертифицированных специалистов по оценке программ для обеспечения соответствия требованиям и действительного укрепления кибербезопасности. Оценщики программы будут помогать операторам

в проведении первоначальной оценки, требуемой TSA, разработке плана восстановления и разработке плана реагирования на инциденты.

После того, как эта оценка будет завершена в соответствии со стандартами TSA, инспектору TSA по кибербезопасности просто нужно будет провести беглый просмотр документов и подписать план. В свою очередь, инспектор по кибербезопасности TSA может затем направить свою ограниченную полосу пропускания на более уязвимые системы, требующие повышенного внимания.

Преимущества предлагаемой структуры

Поддерживает цели соответствия TSA, ориентированные на результат. В 2018 году TSA выпустила Административное намерение 1.0, в котором говорилось о партнерстве с отраслью для достижения положительных результатов в области безопасности за счет соответствия требованиям, ориентированным на результат (OFC), и акцентировалось внимание на сотрудничестве, а не на соблюдении предписаний. Привлечение частных кибер-экспертов для помощи в адаптации планов к потребностям оператора и сети, при этом обеспечивая соответствие нормативным требованиям, будет способствовать достижению этой цели и позволит TSA наладить отношения сотрудничества и среду со своими операторами.

Позволяет TSA сосредоточиться на наиболее уязвимых системах. Опыт и ресурсы TSA в области кибербезопасности должны быть направлены на решение системных проблем и работу с наиболее уязвимыми системами в нашей транспортной сети. Создавая пул частных оценщиков, TSA сокращает круг операторов, на которых ему необходимо сосредоточиться, и позволяет экспертам TSA по кибербезопасности сосредоточиться на решении общесистемных проблем и работе с наиболее уязвимыми операторами, что приводит к более целенаправленному охвату.

Гибкая и надежная сеть квалифицированных поставщиков услуг кибербезопасности обеспечивает более быструю киберзащиту. В соответствии с предлагаемой структурой эта программа будет открыта для любого поставщика услуг кибербезопасности, который проходит процесс сертификации и соглашается с соответствующими ограничениями SSI. Создание этой сети доверенных

поставщиков дает TSA расширенную сеть для распространения и получения информации о возникающих угрозах. Например, если возникнет новая атака программы-вымогателя, TSA может привлечь сторонних поставщиков, которые уже знают операторов и их системы, для устранения уязвимостей.

Экономия на издержках. Согласно опросу Mineta, руководство транспортных систем часто недофинансирует кибербезопасность. Частные оценщики могут предоставить экономически эффективное решение без долгосрочных расходов на персонал, занятый полный рабочий день. Кроме того, предоставление поставщикам услуг кибербезопасности доступа к требованиям SSI поможет им разрабатывать более экономичные предложения, включая автоматизацию большей части необходимой рутинной работы по кибергигиене. Наконец, когда этот процесс оценки и сертификации станет зрелым, транспортные операторы смогут работать со страховыми компаниями, чтобы продемонстрировать кибер-устойчивость при обсуждении премий и других мерах по предотвращению рисков.

Подходы к регулированию должны развиваться, чтобы противостоять новым угрозам

Кибербезопасность ставит новые задачи перед TSA и регулируемыми ею отраслями. Когда TSA создало свою нормативную базу для авиации, iPhone еще не был выпущен, а сетевая интеграция во все аспекты транспорта еще не была реализована. Теперь сети контролируют все, начиная от продажи авиабилетов и заканчивая железнодорожным движением и потоком ресурсов по трубопроводам по всей стране. Эта новая реальность требует новых подходов и решений для возникающих угроз. Использование государственно-частных партнерств — это один из шагов на пути к созданию киберустойчивой системы». **(Scott Mulligan. PERSPECTIVE: Leveraging Public-Private Partnerships to Improve Cybersecurity in the Transportation Sector // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/perspective-leveraging-public-private-partnerships-to-improve-cybersecurity-in-the-transportation-sector/). 10.12.2022).**

***

«Содействие гибкому конвейеру от исследований к операциям становится важным для решения проблем, с которыми сталкивается Министерство обороны при разработке программных систем.

Киберкомандование США (CYBERCOM) и DARPA запускают пилотную программу, направленную на то, чтобы быстрее передать новые кибервозможности в руки кибероператоров.

Пилотная программа, известная как Constellation, обеспечит поток новых кибервозможностей, являющихся результатом высокорискованных и высокодоходных исследований в области кибернауки и технологий (S&T), путем создания ориентированного на пользователя, поэтапного и итеративного конвейера для ускорения создания, доказывая, внедрение и внедрение этих возможностей в программную экосистему CYBERCOM.

«Инновации являются основой стратегии командования, поэтому CYBERCOM и DARPA сотрудничают более тесно, чем когда-либо, чтобы развивать новые тактические и стратегические кибервозможности и интегрировать их в боевые платформы», — сказал Майк Кларк, директор по киберзахватам и технологиям в Киберкомандование США. «Успех Constellation означает увеличение скорости перехода от исследований и разработок DARPA к CYBERCOM для оперативного использования».

В научно-исследовательском сообществе «долина смерти» — это метафора, обычно используемая для описания самого сложного этапа перехода от прототипа к эксплуатационным возможностям. Содействие гибкому конвейеру от исследований к операциям становится важным для решения проблем, с которыми сталкивается Министерство обороны при разработке программных систем, таких как быстрое развитие технологий, принятие и удобство использования как для опытных, так и для неспециализированных поставщиков.

Constellation предоставит основу и создаст механизмы для обеспечения виртуальной и физической инфраструктуры, людей и контрактов, поддержания отношений, необходимых для преодоления разрыва между наукой и технологиями, исследованиями, разработками и оперативными возможностями ведения боевых

действий, а также обратной связи научно-техническому сообществу относительно развития киберпространства. угрозы и потребности миссии.

«Чтобы оказать максимальное операционное и стратегическое влияние, эти новые возможности должны непрерывно достигать операторов в короткие сроки, намного более короткие, чем традиционные процессы приобретения», — сказала д-р Кэтлин Фишер, директор отдела информационных инноваций DARPA. «Мы с оптимизмом смотрим на потенциал Constellation для обеспечения долгосрочной поддержки быстрого прототипирования и интеграции кибер-возможностей. Запуск проектов Constellation параллельно с разработкой DARPA может помочь нам снизить риски и сроки перехода и преодолеть «долину смерти». ***(U.S. Cyber Command, DARPA Initiate Rapid Cyber Capability Prototyping and Integration Pilot // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/u-s-cyber-command-darpa-initiate-rapid-cyber-capability-prototyping-and-integration-pilot/). 02.12.2022).***

***

«После атаки на цепочку поставок программного обеспечения на Solarwinds и всемирной паники из-за уязвимости, затрагивающей Log4j, государственные и регулирующие органы по всему миру пытаются решить эту надвигающуюся проблему: как обеспечить безопасность и защиту цепочек поставок программного обеспечения, поскольку они становятся все большей мишенью для кибератаки?

В Соединенных Штатах два указа президента от февраля 2021 года и мая 2021 года положили начало разговору о защите критически важных федеральных систем США от кибератак. С тех пор это превратилось в устойчивый барабанный бой активности, усиливающейся и распространяющейся за пределы Соединенных Штатов и в частный сектор.

Например:

NIST выпустил несколько публикаций, в том числе подробное руководство «Безопасность программного обеспечения в цепочках поставок».

OMB выпустил еще один меморандум под названием «Повышение безопасности цепочки поставок программного обеспечения с помощью безопасных методов разработки программного обеспечения».

Обсуждаются несколько законодательных путей, в том числе Закон о защите открытого исходного кода от 2022 года (внесенный в Сенат в сентябре).

Существуют отраслевые инициативы, такие как план мобилизации безопасности программного обеспечения с открытым исходным кодом OpenSSF от Linux Foundation (в котором я принимал участие), которые также направлены на предоставление рекомендаций по этой теме.

Существуют отраслевые инициативы, такие как план мобилизации безопасности программного обеспечения с открытым исходным кодом OpenSSF от Linux Foundation (в котором я принимал участие), которые также направлены на предоставление рекомендаций по этой теме.

Поскольку это глобальная проблема, другие правительства также действуют:

В июле 2022 года правительство Великобритании опубликовало Предложение по законодательству «Повышение киберустойчивости Великобритании», в котором подчеркивается огромное влияние, которое могут оказать даже небольшие риски безопасности в цепочке поставок.

В Германии принят Закон об информационной безопасности 2.0 (IT-SiG).

Япония приняла «Закон о содействии экономической безопасности путем комплексного внедрения…» ***(Brin Fox. EU Cyber Resilience Act: Good for Software Supply Chain Security, Bad for Open Source? // Techstrong Group Inc. (https://securityboulevard.com/2022/12/eu-cyber-resilience-act-good-for-software-supply-chain-security-bad-for-open-source/). 22.12.2022).***

***

«Киберустойчивость — это следующий рубеж кибербезопасности, поскольку организации все больше внимания уделяют смягчению последствий с трезвым признанием неизбежности взлома.

Рост как объема, так и сложности кибератак на критически важную инфраструктуру по всему миру продемонстрировал необходимость повышения ставки, и многие федеральные агентства в настоящее время настаивают на внедрении Zero Trust.

Агентство кибербезопасности и безопасности инфраструктуры (CISA) одним из последних заявило о необходимости повышения устойчивости в рамках своего Стратегического плана на 2023–2025 годы. Этот план является первым для агентства с момента его создания в 2018 году и всего за год до меморандума президента Байдена, призывающего правительственные учреждения ускорить внедрение Zero Trust. Министерство обороны США также только что выпустило свою Стратегию нулевого доверия и дорожную карту.

Что интересно во всех этих планах, так это смещение акцента с мышления на предотвращение в пользу снижения риска.

Это важно, потому что подчеркивает повествование «не вопрос о том, произойдет ли нарушение, а когда произойдет».

Хотя профилактика всегда будет священным Граалем, очевидно, что учреждениям и организациям будет лучше сосредоточить свои усилия на выявлении рисков и управлении ими. Это начинается с понимания риска.

Понимание риска — недостающая часть головоломки устойчивости

Одним из ключевых принципов нулевого доверия является возможность отображать важные данные, приложения, устройства организации, а также то, как пользователи получают доступ к конфиденциальной информации и взаимодействуют с ней.

Последнее особенно важно, особенно когда речь идет об инцидентах, связанных с инсайдерскими рисками, число которых, как показывают наши исследования, серьезно возрастает.

Некоторые статистические данные для рассмотрения:

Увеличение числа инсайдерских инцидентов клиентов DTEX на 72% в 2021 г. (Отчет об инсайдерских рисках DTEX за 2022 г.)

42% внутренних угроз были связаны с кражей IP или данных (Отчет об инсайдерских рисках DTEX за 2022 г.)

82% взломов связаны с человеческим фактором (отчет Verizon Data Breach Investigations за 2022 г.)

Ориентировочная стоимость известных инсайдерских инцидентов составляет 15,3 млн долларов (стоимость инсайдерских угроз за 2022 г.: глобальный отчет).

Видимость является ключом к пониманию инсайдерского риска, но еще важнее исходные исходные данные и способность их осмыслить.

Есть расхожая фраза, что нельзя обезопасить то, чего не видишь. То же самое можно сказать и об инсайдерском риске: вы не можете управлять тем, чего не понимаете.

Риск — это человеческий фактор, а контекст — это все

Понимание внутреннего риска начинается с понимания человеческого поведения и намерений. К сожалению, большинство технологий кибербезопасности на сегодняшний день не разработаны для измерения, не говоря уже о том, чтобы зафиксировать это.

Возьмите аналитику поведения пользователей и объектов (UEBA). Многие продукты и услуги UEBA утверждают, что снижают внутренние угрозы за счет консолидации и анализа больших наборов данных из нескольких потоков, чтобы предоставить полезную информацию и выявить риски.

Но утверждение вводит в заблуждение. Чаще всего UEBA имеет высокий уровень ложных срабатываний. Это происходит не по вине технологии, а по вине поступающих данных (и, что более важно, данных, которые НЕ поступают).

Инсайдерский риск — это человеческая проблема, которая требует решения, ориентированного на человека.

Понимание риска требует понимания человеческого поведения, психосоциальных факторов, а также умения видеть (и чувствовать) ненормальное. Одни только технологии не могут зафиксировать такие идеи. Сбор данных, ориентированных на человека, требует значительного межорганизационного

сотрудничества с отделами кадров, юристов, финансов, технологий и кибербезопасности.

Благодаря правильному сочетанию контекстно-зависимой информации о намерениях пользователей организации могут понимать, измерять и снижать внутренние риски до того, как они превратятся в угрозы.

В нашем отчете об инсайдерских угрозах перечислены конкретные рекомендации по защите от инсайдерских угроз.

Заглядывая вперед: наведение мостов между «психо-кибер»

DTEX усердно работает с нашими партнерами, включая корпорацию MITRE, для повышения осведомленности и предоставления критически важным инфраструктурным отраслям повышения их киберустойчивости за счет лучшего понимания и управления инсайдерскими рисками.

MITRE создает развивающуюся, основанную на данных структуру внутренних угроз, которая включает психосоциальные и киберфизические характеристики в качестве общих и наблюдаемых индикаторов внутренних рисков. Эта структура поможет программам инсайдерских угроз/рисков более точно нацеливать и реализовывать их сдерживание, обнаружение и смягчение инсайдерских угроз.

Как указывает MITRE, «существующие системы внутренних угроз игнорируют психосоциальные характеристики, сосредоточены исключительно на кибербезопасности и/или основаны на минимальных или некачественных данных».

По завершении MITRE's Insider Threat Framework (но не необработанные или агрегированные данные) будет конфиденциально передана проверенным лидерам сообщества инсайдеров по мере необходимости». ***(Kellie Arbuckle. Why Understanding Risk is Key to Cyber Resilience // Techstrong Group Inc. (https://securityboulevard.com/2022/12/why-understanding-risk-is-key-to-cyber-resilience/). 15.12.2022).***

***

«В понедельник Верховный суд США присудил Cisco Systems многомиллиардную победу, когда он отказался рассматривать апелляцию Centripetal Networks о восстановлении компенсации Cisco в размере 2,75 миллиарда долларов США в споре о патентах в области кибербезопасности.

Награда стала крупнейшей в патентном праве США.

Но решение федерального судьи суда низшей инстанции в 2020 году было недавно отменено Апелляционным судом США по федеральному округу, который заявил, что судья суда низшей инстанции Генри Морган неправильно рассмотрел дело после того, как признал, что он узнал на поздних стадиях судебное разбирательство без присяжных за то, что его жена владела примерно 100 акциями Cisco на сумму около 4688 долларов.

Морган, который умер ранее в этом году, сказал в 2020 году, что он уже вынес решение по ключевым вопросам судебного спора до того, как узнал о том, что акции принадлежат его жене. Он также сказал, что может продолжать выносить решения по делу беспристрастно.

Федеральный апелляционный суд не согласился, заявив, что Морган должен был отказаться от участия в деле или продать акции, а не передавать их в слепой траст. Поскольку он не взял самоотвод и не продал акции, апелляционный суд отменил решение в июне прошлого года.

«Когда судье становится известно о возможной видимости нарушения правил, существует значительный риск того, что он или она может из кожи вон лезть, чтобы вынести решение против этой стороны, чтобы попытаться доказать отсутствие предвзятости», — написал апелляционный суд.

Centripetal Networks, американская компания, занимающаяся кибербезопасностью, подала апелляцию на решение апелляционного суда.

Без комментариев Верховный суд США в понедельник фактически отклонил апелляцию.

Итак, дело вернулось на круги своя.

«Мы довольны результатом (Верховного суда) и с нетерпением ждем рассмотрения дела по существу в Окружном суде», — заявил представитель Cisco.

Связаться с представителем Centripetal для комментариев не удалось.

Патентное дело восходит к 2018 году, когда Centripetal Networks подала в суд на Cisco, утверждая, что сетевой гигант внедрил их технологию защиты сети в свои сетевые коммутаторы и маршрутизаторы, а также в предложения по мониторингу, которые анализируют их данные». ***(Jay Fitzgerald. Cisco scores win over Centripetal Networks in cybersecurity patent dispute // nextmedia Pty Ltd. (https://www.crn.com.au/news/cisco-scores-win-over-centripetal-networks-in-cybersecurity-patent-dispute-588767). 06.12.2022).***

***

Країни ЄС та Великобританія

«Правительство Великобритании настаивает на предложении взимать плату за регулирование

Консервативное правительство Великобритании заявляет, что предприятия должны платить больше за административные расходы, связанные с регулированием кибербезопасности, и пообещало в среду получить одобрение парламента на расширенный механизм возмещения затрат.

Предприятия, подпадающие под действие главной директивы страны по кибербезопасности, Регламента о сетях и информационных системах, уже должны возмещать своим государственным надзорным органам, таким как Управление комиссара по информации, или отраслевым специалистам, таким как регулятор энергетики Ofgem, некоторые регулирующие действия, включая проверки.

Консерваторы, в том числе Джулия Лопес, министр, возглавляющий Департамент цифровых технологий, культуры, СМИ и спорта, заявили, что частный сектор должен платить больше, в том числе, возможно, за расходы на правоприменение или независимые проверки правоприменительных действий, запрашиваемых регулируемыми организациями. Потенциальные модели включают прямое выставление счетов или периодические платежи регулируемых организаций в регулирующий фонд.

«Политика правительства заключается в том, что плата за услуги, предоставляемые организациями государственного сектора, обычно включает полную стоимость их предоставления», — написало правительство ранее в этом году в ходе публичных консультаций по поводу возможных обновлений NIS.

«Я предполагаю, что их логика будет заключаться в следующем: «Почему британские налогоплательщики должны субсидировать регулирование Amazon, если они не платят здесь налоги и конкурируют со старыми добрыми британскими магазинами», — сказал Джонатан Армстронг, лондонский адвокат.

Большинство организаций отреагировали на консультации с общественностью с неудовольствием по поводу перспективы оплаты правоприменения, заявив департаменту, что у них есть опасения по поводу создания порочных стимулов для регулирующих органов.

В заявлении департамента от 30 ноября Лопес заявил, что правительство будет настаивать на увеличении формы возмещения затрат, заявив, что предстоящее предложение установит регулирование, «более прозрачное и учитывающее более широкое нормативное бремя, размер компании и другие факторы». Факторы снижения нагрузки на налогоплательщиков».

Правительство преуменьшило опасения по поводу создания стимулов для правоприменения, написав в своем ответе на консультации с общественностью, что «предложение состоит в том, чтобы расширить возмещение затрат, чтобы покрыть расходы на правоприменение, а не использовать правоприменение в качестве дополнительного дохода для покрытия более широких расходов НИС». Регулирующие органы будут взимать с предприятий плату только за расходы, непосредственно связанные с правоприменением, написали представители ведомства.

Обновления NIS поступят, «как только позволит парламентское время», говорится в заявлении. Это заявление предполагает, что правительство осознает, что это предложение может вызвать разногласия, сказал Армстронг в интервью Information Security Media Group.

Дополнительные изменения, одобренные правительством, включают расширение сферы регулирования, чтобы более жестко охватить поставщиков управляемых ИТ-услуг. В дополнение к критически важным секторам инфраструктуры, таким как газ, железнодорожный и воздушный транспорт и здравоохранение, NIS предписывает «поставщикам цифровых услуг», таким как поисковые системы и службы облачных вычислений, принимать меры кибербезопасности и сообщать в Управление Комиссара по информации о любом инциденте, который имеет существенное влияние. об оказании услуг.

По словам Армстронга, существует дублирование между поставщиком цифровых услуг и поставщиком управляемых услуг, что делает расширение масштабов значительным, но в значительной степени и разъяснением. Правительство заявляет, что не считает разработку программного обеспечения управляемой услугой.

Правительство также заявляет, что хочет потребовать больше отчетов об инцидентах кибербезопасности, поскольку текущий порог NIS предназначен для событий, влияющих на непрерывность обслуживания». ***(David Perera. Tories: Firms Should Pay More for Cybersecurity Regulation // Information Security Media Group, Corp. (https://www.govinfosecurity.com/tories-firms-should-pay-more-for-cybersecurity-regulation-a-20617). 02.12.2022).***

***

«Европейская комиссия в сотрудничестве с Европейским центром компетенции в области кибербезопасности (ECCC) запускает призыв к выражению заинтересованности для выбора организаций в государствах-членах, которые будут размещать и эксплуатировать трансграничные платформы обнаружения киберугроз, каждая из которых объединяет соответствующие государственные организации из несколько государств-членов, а также частные лица.

Объявленный в Европейской стратегии кибербезопасности на 2020 год и более подробно описанный недавно в Совместном сообщении о европейской

политике киберзащиты, это первый этап создания трансграничной инфраструктуры европейских центров операций по обеспечению безопасности (SOC), работающей на основе искусственного интеллекта (ИИ) и другие передовые технологии.

Центры трансграничных операций по обеспечению безопасности закупят инструменты и услуги по обнаружению киберугроз вместе с Европейским центром компетенции в области кибербезопасности, который первоначально внесет 30 миллионов евро в рамках программы «Цифровая Европа». Программа также профинансирует до 72,5 млн евро в виде грантов на обнаружение киберугроз после недавно открытого конкурса предложений.

Центры или платформы также могут подавать заявки на такие гранты с целью дополнить инвестиции, полученные в результате совместных закупок с ECCC». ***(European Commission Seeks Cross-Border Cyber Threat Detection Providers // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/european-commission-seeks-cross-border-cyber-threat-detection-providers/). 05.12.2022).***

***

«Поставщики управляемых услуг (MSP) в Великобритании вскоре будут подчиняться условиям обновленных законов о кибербезопасности, так как правительство Великобритании продолжает обновлять Положения о сетях и информационных системах (NIS) после своего отделения от ЕС.

MSP будут подчиняться тем же правилам, которые регулируют основные услуги, такие как критическая инфраструктура и здравоохранение. Этот шаг в значительной степени связан с растущим вниманием к MSP со стороны самых передовых субъектов национальной безопасности, которые часто видят в них самое слабое или самое быстрое звено в правительственных учреждениях или объектах шпионажа в частном секторе.

Новые законы Великобритании о кибербезопасности подвергнут MSP жесткому регулированию

Новые законы о кибербезопасности, которые обязывают энергетические и водные компании к более строгим стандартам безопасности и отчетности, также будут применяться к британским MSP, поскольку обновлены правила NIS, которые были разработаны в 2018 году в соответствии с предыдущими условиями GDPR ЕС.

Серьезные атаки на MSP, без сомнения, вызвали этот пересмотр, начиная с кампании «Операция Cloudhopper» с 2014 по 2017 год, которая поразила цели по всему миру. Эта атака была приписана поддерживаемым государством злоумышленникам в Китае; аналогичные группы в России были привлечены к атаке на SolarWinds. Но частные преступные группы также заинтересованы в MSP, а банда вымогателей REvil несет ответственность за атаку на Kaseya в 2021 году.

Новые законы о кибербезопасности вступают в силу не сразу, требуя дополнительных парламентских процедур, и многие ожидают, что компаниям, на которые будут распространяться новые правила, будет предоставлен некий льготный период для внесения необходимых изменений. Ситуации, в которых требуется отчетность, будут расширены для этих компаний, включая поставщиков облачных услуг и поисковые системы. Некоторые компании также могут быть обязаны отчитываться перед регулирующими органами, чего они раньше не делали. И пересмотренные правила оставляют открытой возможность того, что в будущем будет включено больше отраслей.

Существующие правила NIS предусматривают штрафы в размере до 17 миллионов фунтов стерлингов за нарушения.

MSP в нескольких отраслях нацелены на значительное улучшение кибербезопасности

MSP имеют привилегированный доступ к потенциально тысячам клиентских сетей, в которые иногда входят государственные учреждения и поставщики критически важной инфраструктуры и услуг. Это обоснование, которое теперь поставит их в число наиболее строго регулируемых отраслей с точки зрения законов о кибербезопасности.

Новые требования к отчетности уделяют большое внимание потенциальным сбоям не только для MSP, но и для всех охваченных отраслей. Требования носят не только реактивный характер с точки зрения простой установки временных окон, в течение которых охватываемые организации должны сообщать о нарушениях и инцидентах после того, как они произошли, но и упреждающие требования об инцидентах, которые потенциально могут привести к нарушению или отключению службы, даже если такая проблема не возникла. еще развитая. Уведомления о подобных инцидентах в настоящее время основаны на пороге затронутых клиентов или субъектов данных, который, вероятно, изменится в течение этого периода проверки.

Новые законы о кибербезопасности, похоже, также вносят некоторые изменения в суммы штрафов, обещая новую «систему возмещения затрат», которая будет более прозрачной и будет учитывать такие факторы, как размер компании и бремя, которое штраф ляжет на организацию. Это, по-видимому, дает ICO больше гибкости в адаптации суммы штрафа к сумме фактического ущерба или фактического риска в каждом конкретном случае.

MSP стали приоритетной целью в Великобритании отчасти просто потому, что сейчас их использует большинство организаций. Они особенно важны для малого и среднего бизнеса (МСП): некоторые довольно недавние опросы показали, что 83% используют их в той или иной степени. Тем не менее, предприятия, которые не соглашаются, в подавляющем большинстве называют недоверие к обработке своих данных основной причиной, по которой они не будут взаимодействовать с MSP. Новые законы о кибербезопасности могут привести к некоторым принудительным улучшениям в этой области.

Но даже по мере того, как их принятие и нацеливание на них со стороны опытных хакеров росли, британские MSP продемонстрировали проблемы с соответствием современным требованиям безопасности. Опрос, проведенный ранее в этом году, показал, что 80% клиентов подвергались кибератакам, и что большинство из них не были уверены в своей способности отражать атаки. Влияние на рынок, таким образом, будет интересным, особенно если у MSP не

будет много времени, чтобы приспособиться к регулированию. Но хотя у этих компаний могут быть свои проблемы с кибербезопасностью, они жизненно важны для небольших предприятий, у которых просто нет ИТ-ресурсов для обеспечения собственной безопасности.

Подавляющее большинство малых и средних предприятий заявили, что они были бы готовы сменить MSP, чтобы найти того, который предлагает им удовлетворительную безопасность, что может привести к консолидации на рынке, поскольку те, кто уже лучше всего подходит для выполнения и соблюдения нормативных требований, собирают бизнес. С другой стороны, MSP могут разделиться на предприятия, ориентированные на одну индивидуальную потребность, а не на «универсальные магазины», как они в настоящее время склонны позиционировать себя.

Но Оз Алаше MBE, генеральный директор CybSafe, предостерегает от любого типа организаций, рассматривающих MSP в качестве своего единственного волшебного средства безопасности: «Требование к аутсорсинговым ИТ-провайдерам соблюдения минимальных стандартов безопасности, несомненно, является законодательным шагом в правильном направлении. Предприятия обязаны защищать как себя, так и своих потребителей, и мы не должны ожидать того же от третьих лиц. Однако нормативные акты не могут защитить данные от киберпреступников. Государственный и частный секторы должны работать вместе, чтобы гарантировать, что организации рассматривают кибербезопасность как приоритет бизнеса. Кибератаки происходят не только чаще; они также становятся все более сложными. Поэтому компаниям необходимо начать относиться к позитивной культуре кибербезопасности как к активной основной ценности. Нам нужно сосредоточиться на измерении и изменении конкретных моделей поведения в сфере безопасности, не просто ставить галочки в реестре рисков. Хотя этот шаг со стороны правительства является позитивным, многое еще предстоит сделать». ***(Scott Ikeda. New Cybersecurity Laws Coming for UK MSPs // CPO Magazine (https://www.cpomagazine.com/cyber-security/new-cybersecurity-laws-coming-for-uk-msps/). 08.12.2022).***

***

«Майже через два десятиліття після народження Facebook, що поклало початок епосі соціальних мереж, ЄС запроваджує амбітне законодавство, спрямоване на очищення найбільших у світі онлайн-форумів.

Закон про цифрові послуги (DSA) призначений для боротьби з мізогінією, захисту дітей, припинення шахрайства споживачів, обмеження дезінформації та захисту демократичних виборів. Велика Британія запроваджує власний статут, законопроект про безпеку в Інтернеті, але правила ЄС, ймовірно, матимуть більший вплив, оскільки вони охоплюють більший ринок, а ЄС є більш впливовим як регуляторна сила.

«Закон про цифрові послуги є новаторським законодавством, яке встановить світові стандарти для регулювання вмісту та захисту користувачів від онлайн-шкоди», — сказав Пітер Черч, юрист з технологій Linklaters.

І DSA вже має в полі зору технологічні компанії. Нового власника Twitter Ілона Маска попередили, що його платформа не готова до нових правил, які можуть набути чинності для основних платформ наступного літа. Тьєррі Бретон, комісар ЄС з контролю за законодавством, сказав Маску, що у нього «попереду величезна робота», щоб переконатися, що Twitter дотримується закону.

У п’ятницю після призупинення доступу до Twitter групи американських технічних журналістів, віце-президент комісії з цінностей і прозорості Вера Йоурова виступила. Вона нагадала Маску, що DSA «вимагає поваги до свободи ЗМІ».

Ось посібник із DSA та його значення для технологічних платформ та їхніх користувачів.

Що таке DSA?

DSA застосовується в ЄС і регулює, кажучи типовим законодавчим жаргоном, цифрові послуги, які діють як «посередники» у своїй ролі підключення споживачів до контенту, товарів і послуг. Це означає, що в сферу дії законопроєкту входять не тільки лайки Facebook і Google, а й Amazon і магазини додатків.

Його положення включають: захист дітей від створення профілю в рекламних цілях на сайтах соціальних мереж; надання користувачам засобів оскарження видалення контенту; забезпечення того, що продукти, що продаються на онлайн-ринках, таких як Amazon, не є підробленими; і вжиття заходів проти таких ризиків, як дезінформація та «кібернасильство» щодо жінок.

За порушення загрожує штраф у розмірі 6% світового обороту, а в найсерйозніших випадках – тимчасове припинення надання послуги. ЄС також може вимагати від сайтів вжити негайних заходів для розв'язання проблем. Користувачі зможуть вимагати відшкодування будь-якої шкоди, завданої їм порушенням закону.

Коли він набирає чинності?

Закон поділяє технологічні компанії на рівні. Найсуворіше регульований рівень охоплює дуже великі онлайн-платформи (VLOP) і дуже великі онлайн-пошукові системи (VLSE), які мають понад 45 мільйонів активних користувачів щомісяця. На початку наступного року ЄС визначить, які платформи підходять для цієї категорії. Для цього рівня, який може включати Facebook, Instagram, Google, TikTok і Amazon, є жорсткіші вимоги. Для VLOP і VLSE закон може набути чинності влітку та на початку наступного року для решти.

Великі оператори повинні проводити щорічну оцінку ризиків, в якій викладено ризики шкідливого контенту, такого як дезінформація, женоненависництво, шкода дітям і маніпуляції на виборах. Вони також повинні вжити заходів для пом’якшення цих ризиків, хоча всі основні соціальні медіа-платформи та пошукові системи вже мають групи модераторів вмісту. Однак, тепер ці системи будуть перевірені ЄС.

Великі платформи також повинні будуть опублікувати незалежний аудит дотримання ними закону, а також кількість людей, які вони використовують для модерації контенту. Вони також повинні надавати регуляторам подробиці роботи своїх алгоритмів, які контролюють те, що ви переглядаєте в Інтернеті, рекомендуючи вміст. Незалежним дослідникам також дозволять стежити за дотриманням закону.

Великі ринкові платформи, такі як Amazon, які не є виробниками контенту соціальних мереж, все одно повинні будуть проводити оцінку ризиків і публікувати незалежні аудити.

Спільне використання алгоритмів є великим кроком для технологічних компаній. Алгоритми рекомендацій – це «чорна скринька», де критерії пріоритетності вмісту можуть бути непрозорими. Однією з причин, чому компанії охороняють деталі, є захист від хакерів, спамерів і ворожих осіб.

Як захистить дітей?

Соціальним медіа-платформам буде заборонено створювати профілі дітей-користувачів, щоб компанії могли націлювати на них рекламу. Ті платформи, до яких можуть отримати доступ неповнолітні – по суті, більшість платформ соціальних медіа – повинні вжити заходів для захисту їх конфіденційності та безпеки. Основні платформи також повинні проводити оцінку ризиків вмісту, який завдає шкоди дітям, і вживати заходів, щоб запобігти охопленню такого вмісту особами віком до 18 років. Запропоноване законодавство ЄС має на меті охопити видалення онлайнових матеріалів сексуального насильства над дітьми.

А як щодо малих платформ?

Менші платформи, як і великі, звичайно, повинні надавати користувачам право скаржитися на видалення їх вмісту, а також додаткову можливість позасудового процесу оскарження, якщо їм не подобається, як розглядалася скарга. Однак рецидивістів, які постійно публікують незаконний контент, необхідно відсторонити.

Вони також повинні бути прозорими щодо оголошень і алгоритмів. Відповідно до DSA, платформи повинні надавати користувачам інформацію про те, чому їм показали рекламу. У ньому також має бути детально описано алгоритми, які використовуються для керування роботою користувача в Інтернеті». ***(Дмитро Сизов. ЄС планує очистити соціальні мережі від дезінформаторів і шахраїв // Internetua (https://internetua.com/yes-planuye-ocsistiti-socialni-mereji-vid-dezinformatoriv-i-shahrayiv). 18.12.2022).***

***

«Правительство Великобритании опубликовало свои планы по внесению поправок в Положение о сетях и информационных системах от 2018 года. Реформы приведут к тому, что намного больше ИТ-компаний подпадет под действие Положений в качестве «поставщиков цифровых услуг», а также расширит обязательства по отчетности об инцидентах. Также будет введен двухуровневый режим для поставщиков цифровых услуг, детали которого не совсем ясны. Об изменениях было объявлено сразу после того, как ЕС одобрил внедрение Директивы о сетевой и информационной безопасности 2 («NIS2»), и есть интересные точки сравнения между двумя параллельными наборами реформ.

Расширенный круг поставщиков цифровых услуг

Согласно действующему Регламенту определение поставщика цифровых услуг («DSP»), регулируемая организация, ограничивается поисковыми системами, онлайн-рынками и поставщиками услуг облачных вычислений. DSP обязаны как регистрировать, так и сообщать об инцидентах. В настоящее время правительство планирует расширить сферу применения DSP, включив в нее «поставщиков управляемых услуг». Это относится к сценариям, в которых клиент полагается на сеть и информационные системы поставщика услуг для предоставления по крайней мере одной из широкого спектра «управляемых услуг», например: интеграция и управление услугами (SIAM); услуги по обеспечению непрерывности бизнеса и аварийного восстановления; различные формы аутсорсинга бизнес-процессов (BPO); и управляемые службы безопасности (такие как управляемый центр операций по обеспечению безопасности, мониторинг безопасности и управление угрозами и уязвимостями). Однако следует отметить, что это широкое определение не охватывает традиционные услуги центров обработки данных.

Посредством этого изменения правительство включает в сферу действия Регламента широкий круг поставщиков ИТ-услуг, чья инфраструктура используется клиентами, в том числе заказчики критически важной национальной инфраструктуры Великобритании для выполнения важных технологических операций.

Двухуровневый режим для поставщиков цифровых услуг

Одной из наиболее интересных реформ является план создания «двухуровневого режима» регулирования DSP. В частности, правительство намерено провести различие между более легким «реактивным» (постфактум) регулированием для одних DSP и более интенсивным «упреждающим» (автоматическим) режимом для других.

Те DSP, чьи услуги особенно важны для киберустойчивости страны, будут подпадать под более интенсивный режим. Правительство планирует поручить Управлению Комиссара по информации (ICO) разработать критерии для выявления этих «критических» DSP. Критерии еще предстоит определить, но предполагается, что они будут гибкими и подлежат пересмотру с течением времени по мере развития зависимости страны от определенных ИТ-услуг.

Критические DSP будут контролироваться ICO, и ожидается, что они будут демонстрировать свою устойчивость к внешним воздействиям на активной и постоянной основе.

Регулирование «критических зависимостей»

В дополнение к регулированию поставщиков управляемых услуг в качестве DSP правительство намерено также начать регулирование важнейших поставщиков до «операторов основных услуг».

Оператор жизненно важной услуги является поставщиком одной из определенного количества услуг, которые считаются критически важными для национальной инфраструктуры (например, водоснабжение, энергия, транспорт). Таким образом, в него входят, например, компании водоснабжения, энергетические компании, больничные тресты и железнодорожные операторы. В соответствии с действующими Правилами такие операторы несут широкие обязательства по поддержанию надлежащих мер безопасности, подлежат проверкам со стороны их компетентных органов в отношении этих мер; а также обязаны сообщать об инцидентах.

В настоящее время правительство хочет закрыть то, что оно считает важным пробелом, из-за которого многие операторы основных услуг зависят от

инфраструктуры третьих сторон в отношении критических частей предоставления своих услуг, но сами эти третьи стороны не подпадают под действие Правил. Поэтому правительство намерено наделить полномочиями определять организации как «критически зависимые» и требовать от этих организаций выполнения тех же обязанностей и обязательств, что и у операторов основных услуг.

В отличие от включения поставщиков управляемых услуг в число DSP, детали этого элемента реформы еще не доработаны, и правительству необходимо будет работать с отраслевыми компетентными органами для разработки соответствующих критериев для выявления «критических зависимостей». Однако, поскольку эти третьи стороны будут в первую очередь поставщиками услуг, связанных с ИТ, еще неизвестно, как будет управляться дублирование между DSP и критическими зависимостями, и будут ли некоторые компании подлежать двойному регулированию.

Расширенные обязательства по уведомлению

О киберинцидентах в соответствии с Правилами сообщается только в том случае, если они влияют на предоставление основных (или цифровых) услуг. Это означает, что операторы основных услуг или соответствующие поставщики цифровых услуг могут столкнуться со значительным инцидентом — например, атакой программы-вымогателя, затронувшей всю их базу данных по персоналу, — о которой нельзя будет сообщить в соответствии с Правилами, если соответствующая организация все еще может предоставить свои основные (или цифровой) сервис. Несмотря на инцидент, потенциально свидетельствующий о незащищенности базовой системы или возможности дальнейших проблем, регулятор NIS не будет уведомлен об этом.

Поэтому правительство хочет расширить объем этого обязательства, включив в него инциденты, которые, хотя и не влияют напрямую на непрерывность обслуживания, тем не менее представляют значительный риск для безопасности и устойчивости рассматриваемой организации. Обоснование состоит в том, что некоторые инциденты настолько значительны, что даже в тех случаях, когда организация может продолжать предоставлять свои основные услуги,

правительство захочет знать о более широком потенциальном воздействии на критически важную национальную инфраструктуру. Как и в случае с реформой «критических иждивенцев», детали этого изменения еще предстоит определить.

Сравнение с ЕС NIS2

Регламент является результатом переноса Великобританией, которая все еще является государством-членом ЕС, Директивы о сетях и информационных системах 2016 года. В отсутствие Соединенного Королевства 27 оставшихся государств-членов завершили свои собственные реформы режима ННГ, результатом которых стал ННГ2.

Реформы ЕС предусматривают охват более широкого круга секторов режимом оператора основных услуг, чего Великобритания не планирует (вместо этого сосредоточив внимание на охвате «критических зависимостей» уже регулируемых секторов). В качестве другого изменения, которое не рассматривалось Великобританией, ЕС добавляет более строгие 24-часовые сроки к обязательству сообщать об инцидентах.

По мере того как два режима объединяются, организациям, предоставляющим основные и цифровые услуги в Великобритании и ЕС, необходимо будет адаптироваться к более строгому, но расходящемуся регулированию в обеих юрисдикциях». ***(James Clark, David Cook. UK NIS - Get ready for expansion of the UK's critical national infrastructure cyber security laws // DLA Piper (https://blogs.dlapiper.com/privacymatters/uk-nis-get-ready-for-expansion-of-the-uks-critical-national-infrastructure-cyber-security-laws/#page=1). 05.12.2022).***

***

«Поставщики социального жилья в Великобритании получили доступ к бесплатному набору инструментов кибербезопасности, поскольку сектор стремится снизить риск кибератак.

Housemark активно поддержал этот шаг, и его Форум по информационной безопасности работал вместе с правительственным Национальным центром кибербезопасности (NCSC), чтобы сделать это возможным. Поставщики жилья

могут подписаться на ряд инструментов, которые являются частью программы активной киберзащиты, которая предоставляется организациям государственного сектора. Сюда также входят арендодатели местных органов власти и независимые управляющие организации (ALMO).

Этот инструментарий предназначен для борьбы с массовыми массовыми атаками, которые затрагивают повседневную жизнь людей, а не с очень сложными и целенаправленными атаками.

Доступ к инструментарию NCSC рассматривается как ключевой шаг в предоставлении всем поставщикам социального жилья доступа к инструментам, повышающим безопасность и снижающим риск кибератак. Эта работа совпала с несколькими громкими примерами кибер-инцидентов, затронувших поставщиков социального жилья в последние месяцы, когда хакеры получили доступ к ИТ-системам домовладельцев.

Провайдеры социального жилья могут подписаться на инструменты программы активной киберзащиты через веб-сайт NCSC. Это включает в себя веб-проверку и проверку почты, которые помогают защититься от наиболее распространенных угроз кибербезопасности, и PDNS (на экспериментальной основе), который помогает блокировать доступ пользователей к вредоносным веб-сайтам. Инструменты предназначены для того, чтобы помочь отдельным поставщикам социального жилья и сектору в целом повысить киберустойчивость…» ***(Free Access for Social Housing Providers to Cyber Defence Tools from the National Cyber Security Centre // Housemark (https://www.housemark.co.uk/news/free-access-for-social-housing-providers-to-cyber-defence-tools-from-the-national-cyber-security-centre/). 06.12.2022).***

***

«Почти треть приложений, используемых Министерством окружающей среды, продовольствия и сельского хозяйства Великобритании (Defra), устарели (EOL), в результате чего государственный сектор Великобритании стал уязвимым для кибератак.

Отчет Национального контрольно-ревизионного управления (НАО) показал, что, хотя департамент сосредоточен на цифровых услугах, у него нет плана по замене устаревшего и рискованного программного обеспечения, которое составляет 30% всего программного обеспечения департамента.

По оценкам самой Defra, 76% ее общих расходов на цифровые технологии, данные и технологии направляются на поддержку этих устаревших систем.

Defra потратила более десяти лет, пытаясь исправить проблему с устаревшими приложениями, но не получила для этого достаточного финансирования до Обзора расходов 2021 года. Это позволило выделить 366 миллионов фунтов стерлингов на цифровые инвестиции в период с 2022 по 2025 год. Согласно текущим планам, устаревшие системы не будут полностью исправлены до 2030 года.

Устаревшее программное обеспечение представляет собой угрозу кибербезопасности, поскольку это означает, что приложение больше не получает никакой поддержки от исходного разработчика, включая обновления безопасности.

Это означает, что у хакера достаточно времени, чтобы разработать эксплойт для уязвимости в любом из этих устаревших приложений. Попытка использовать поддерживаемый продукт зависит от времени, поскольку уязвимости часто исправляются поставщиком до разработки эксплойтов.

NAO также заявило, что департамент по-прежнему не справляется со своей стратегией цифровой трансформации. Он считает, что средств недостаточно, чтобы снизить текущий риск до «приемлемого уровня», не говоря уже о расширении цифровой трансформации в департаменте.

Это текущая проблема, поскольку департамент по-прежнему выполняет только треть из 21 миллиона транзакций клиентов в год в цифровом виде.

Чтобы добиться успешной цифровой трансформации, NAO также рекомендовала государственным ведомствам разработать стратегию, в основе которой лежат соображения, связанные с цифровыми технологиями и данными. В 2021 году NAO заявило, что на протяжении 25 лет правительственных цифровых программ наблюдается «постоянный образец неудовлетворительной работы».

Defra — это департамент правительства Великобритании, отвечающий за защиту окружающей среды, а также пищевой, сельскохозяйственной и рыбной промышленности. Большая часть работы отдела зависит от цифровых услуг, включая его обязанности по профилактике заболеваний, поддержанию качества воздуха и контролю за защитой от наводнений.

«Правительство продолжает полагаться на многие устаревшие ИТ-системы со значительными затратами», — сказал Гарет Дэвис, глава NAO.

«Defra сталкивается с особенно сложной задачей по замене своих устаревших приложений и начала решать ее структурированным образом.

«Полный потенциал технологий в улучшении государственных услуг и снижении затрат для налогоплательщиков может быть доступен только в том случае, если эта и другие подобные программы в правительстве будут реализованы эффективно».

Как независимый парламентский орган, ответственный за проверку государственных расходов парламента, НАО имеет опыт привлечения внимания к неудачам в цифровой стратегии правительства.

В октябре было обнаружено, что цифровые проекты в Министерстве обороны (МО) подрываются из-за острой нехватки технических навыков, и были выявлены неправильные методы работы с данными в таких департаментах, как HMRC, ONS и Департамент бизнеса.

Плохое обслуживание основных приложений или дальнейшее использование приложений, которые больше не поддерживаются разработчиками, может представлять серьезную угрозу безопасности, особенно если приложения содержат уязвимости нулевого дня.

«Это разрастание приложений поднимает вопросы о рисках цепочки поставок программного обеспечения», — сказал Майкл Уайт, технический директор и главный архитектор Synopsys Software Integrity Group.

«Любое приложение, выбранное ИТ-отделом, вероятно, будет подвергнуто тщательной проверке, но так называемые теневые ИТ-проекты или серые ИТ-

проекты могут обойти эту проверку — либо напрямую, либо через подкомпоненты и платформы, на которые они полагаются.

«Это также может включать компоненты с открытым исходным кодом, которые случайно или преднамеренно содержат уязвимости или вредоносный код. Как указано в отчете, ответственность за применение исправлений безопасности для этих «бесхозных» приложений может также представлять риск на уровне организации при рассмотрении таких событий, как известная уязвимость log4j, которая произошла в прошлом году».

В США Агентство по кибербезопасности и безопасности инфраструктуры (CISA) в прошлом году запустило программу обязательных исправлений, требующую от государственных учреждений исправления обнаруженных эксплойтов безопасности в течение двух недель. Агентство ведет тщательно подобранный каталог уязвимостей, которые были использованы в реальных условиях». ***(Rory Bathgate. Defra's legacy software problem 'threatens' UK gov cyber security until 2030 // Future Publishing Limited (https://www.itpro.co.uk/business/business-strategy/369647/defra-legacy-software-problem-threatens-uk-gov-cyber-security). 06.12.2022).***

***

«Стоимость киберинцидента, которую платит средняя организация в Румынии, составляет примерно 750 000 леев, сказал Дэн Симпин, генеральный директор Национального управления кибербезопасности (DNSC), в ходе специализированного обсуждения.

«Количество инцидентов и атак программ-вымогателей увеличилось из года в год, где-то на 30% (…). Есть организации, которые зашифровали данные, заплатили вознаграждение, и мы, Дирекция, рекомендуем этого не делать, потому что это поощряет это явление и стимулирует эту преступную деятельность. Очевидно, что резервное копирование данных намного быстрее и проще, и гораздо дешевле вернуться к нормальной деятельности. Помимо программ-вымогателей, у нас все еще есть риски, связанные с удаленной работой для пользователей. (...)

Оценка мы сделали в Управлении, было то, что кибер-инцидент для организации среднего размера в Румынии достигает стоимости где-то около 750 000 леев, примерно 150 000 евро. Стоимость восстановления данных, очистки всей сети, систем и так далее...» заявил Симпин.

По мнению главы DNSC, рост числа кибератак обусловлен ускоренной цифровой трансформацией, вызванной переходом на систему удаленной работы». ***(Mirea Andreea. Head of Cyber Security Authority: A cyber incident costs an average company around 750,000 RON // STIRIPESURSE.RO (https://www.stiripesurse.ro/head-of-cyber-security-authority-a-cyber-incident-costs-an-average-company-around-750000-ron_2696610.html). 09.12.2022).***

***

«…Почти половина британских предприятий имеют базовые пробелы в кибербезопасности, из-за чего они остаются незащищенными. Эта суровая реальность была раскрыта в отчете Департамента цифровых технологий, культуры, СМИ и спорта (DCMS)(i). Было обнаружено, что людям, ответственным за кибербезопасность в 48% британских компаний, не хватает уверенности в выполнении основных задач, и они не получают поддержки от внешних поставщиков кибербезопасности. Итак, если ваш штатный сотрудник не уверен в выполнении основных задач по обеспечению безопасности, а вы не ищете поддержки, кто же проверяет, что ваши бизнес-системы безопасны, а ваши данные не были скомпрометированы?

Размер имеет значение

Многие малые и средние предприятия не готовы к угрозам кибербезопасности, скрывающимся в Интернете, полагая, что они слишком малы, чтобы стать мишенью. Реальность такова, что в 2019/2020 гг. почти половина британских предприятий пострадала от нарушения кибербезопасности или атаки (ii). Большинство киберпреступников ищут быструю зарплату. Если атака сработала хорошо, они будут продолжать ее повторять. Вот почему фишинговые атаки, когда злоумышленники рассылают мошеннические сообщения, чтобы

заставить человека раскрыть конфиденциальные данные, остаются наиболее распространенным типом атак, с которыми сталкиваются организации: 90% всех утечек данных связаны с фишингом (iii).

МСП необходимо понимать, что киберпреступность — это организованный и прибыльный бизнес, хотя и незаконный и морально несостоятельный. Киберпреступники хотят быстрой финансовой отдачи от своей деятельности и намеренно преследуют легкие цели. МСП считаются легкими жертвами, потому что у них меньше шансов обеспечить достаточную безопасность для защиты своих систем и данных. Хакеры ищут информацию, которую МСП хранят о своих клиентах и поставщиках, например номера кредитных карт, реквизиты банковского счета и т. д. Они либо используют ее сами, либо продают в даркнете тому, кто предложит самую высокую цену.

Кредитные карты, удостоверения личности и кибермошенничество обходятся Великобритании в 190 миллиардов фунтов стерлингов в год (iv). По данным британского аналитического центра Королевского института объединенных служб (RUSI), мошенничество достигло уровня эпидемии и должно рассматриваться как проблема национальной безопасности. Пока прибыль продолжает расти, киберпреступники будут продолжать свои атаки, и чем раньше малые и средние предприятия поймут это, тем скорее они смогут серьезно заняться безопасностью и начать более эффективно защищать себя.

Наиболее распространенные пробелы в навыках кибербезопасности, выявленные в отчете, связаны со следующими аспектами:

- Настройка брандмауэров
- Установка исправлений
- Хранение или передача личных данных
- Обнаружение и удаление вредоносных программ.

Помощь всегда рядом — создайте надежный фундамент с помощью Cyber Essentials

Задачи кибербезопасности изложены в одобренной правительством схеме Cyber Essentials (CE), которая была разработана для защиты британских

организаций от наиболее распространенных киберугроз. Эти фундаментальные задачи являются основой хорошей безопасности.

В схеме изложены основные технические средства контроля, которые могут использовать организации. Он также закладывает основу для разработки политик и процедур для смягчения угроз, которые могут повлиять на бизнес-операции. Преимущество соответствия CE заключается в том, что оно снижает 80% рисков, с которыми сталкиваются предприятия, таких как фишинг, заражение вредоносным ПО, атаки с использованием социальной инженерии и взлом.

Когда начать?

Сделать первые шаги в решении проблемы кибербезопасности может быть сложно, но последствия, которые вы не сделаете, могут иметь разрушительные последствия для вашего бизнеса. Кибератаки и утечка данных часто наносят малым и средним предприятиям финансовый ущерб. Помимо затрат на восстановление, это также потеря клиентов, поставщиков и деловой репутации, а также штрафы за нарушение правил защиты данных GDPR.

Лучше всего начать с использования онлайн-системы управления политиками, разработанной для кибербезопасности, которая шаг за шагом проведет вас через все важные рабочие процессы безопасности. Он проведет вас через действия, которые необходимо предпринять, выделит области бизнеса, на которых следует сосредоточиться, и внедрит принципы GDPR и Cyber Essentials, чтобы вы могли пройти сертификацию.

Ни одна компания не может позволить себе быть наивной в отношении киберпреступности и важности защиты данных, последствия слишком велики. Решение для управления политикой кибербезопасности может упростить процесс и помочь вашей компании пройти сертификацию Cyber Essentials экономически эффективным способом. Сертификация по заслуживающей доверия схеме укрепит киберзащиту, внедрит политики, гарантирующие, что вы предпринимаете правильные шаги для защиты своих конфиденциальных данных, и будет иметь большое значение для защиты вашего бизнеса от распространенных атак. Воспользуйтесь доступной помощью, чтобы ваша компания не стала жертвой

киберпреступности и не пополнила удручающую статистику кибербезопасности». ***(Nick Denning. Mind the Gap: a lack of cyber security skills is leaving SMEs exposed // ResponseSource Ltd. (https://pressreleases.responsesource.com/news/103521/mind-the-gap-a-lack-of-cyber-security-skills-is/). 12.12.2022).***

***

«Румыния приняла закон, запрещающий приобретение и использование государственными органами программных продуктов и услуг в области кибербезопасности из Российской Федерации, сообщает Национальное управление кибербезопасности (DNSC).

Закон о защите информационных систем органов государственной власти и учреждений в условиях вторжения Российской Федерации против Украины вступил в силу 14 декабря с момента публикации в Официальном журнале. Законопроект был инициирован Министерством исследований, инноваций и цифровизации (MCID) и одобрен парламентом 23 ноября 2022 года.

Согласно DNSC, закон устанавливает правовые и институциональные рамки для запрета на приобретение и использование государственными органами и учреждениями программных продуктов и услуг в области кибербезопасности и ИТ-безопасности, происходящих прямо или косвенно из Российской Федерации, у экономического оператора в соответствии с прямой или косвенный контроль физического или юридического лица из Российской Федерации, со стороны хозяйствующего субъекта, капитал которого сформирован с участием, поступающим непосредственно или через компании, учрежденные в Российской Федерации, или в управленческие органы которого входят лица из Российской Федерации.

Закон относится ко всем сетям и компьютерным системам, управляющим секретной информацией, принадлежащим публичным и частным юридическим лицам, расположенным на территории Румынии, за исключением тех, которые принадлежат государственным органам и учреждениям, обладающим

собственными полномочиями в сфере национальной безопасности, в сфере кибербезопасности, национальной обороны и общественного порядка.

DNSC уточняет, что закон имеет прямое влияние только на определенные категории организаций, однако Управление рекомендует всем пользователям и лицам, принимающим решения в Румынии, тщательно проанализировать используемые ими решения в области безопасности в контексте гибридного конфликта между Россией и Украиной». ***(Andreea Năstase. Purchase and use of cyber security software products and services from Russia, prohibited // STIRIPESURSE.RO (https://www.stiripesurse.ro/purchase-and-use-of-cyber-security-software-products-and-services-from-russia-prohibited_2705365.html). 15.12.2022).***

***

«…новый отчет Департамента цифровых технологий, культуры, СМИ и спорта показал, что почти половине британских предприятий не хватает базовых навыков кибербезопасности, что делает их уязвимыми для атак.

В отчете говорится, что сотрудники, отвечающие за кибербезопасность в 48% британских малых и средних предприятий, не были достаточно уверены в выполнении основных задач онлайн-безопасности, а также не получали поддержки от внешних экспертов по кибербезопасности.

Такое недоверие и отсутствие экспертного надзора означает, что почти половина британских предприятий подвержена угрозе кибербезопасности и, вероятно, не имеет ресурсов для ее устранения.

Малый бизнес по-прежнему подвержен риску угроз кибербезопасности

Многие малые и средние предприятия считают, что они слишком малы для киберпреступников, хотя на самом деле почти половина британских предприятий пострадала от утечки данных или онлайн-атак в 2019/2020 годах.

Большинство киберпреступников ищут эти предприятия, которые не принимают меры кибербезопасности, поскольку это позволяет быстро заработать — если атака увенчается успехом, они, скорее всего, снова нацелятся на компании того же типа.

Малые и средние предприятия обычно рассматриваются как легкие жертвы киберпреступлений, потому что у них меньше шансов иметь надежную защиту от киберугроз. Они обычно нацелены на информацию, которую они хранят о клиентах, поставщиках, номерах кредитных карт и банковских реквизитах, которую хакеры либо используют сами, либо продают в даркнете для получения прибыли.

В отчете показано, что наиболее распространенными пробелами в навыках кибербезопасности у МСП являются:

– Настройка брандмауэров

- Исправление

– Хранение или передача персональных данных

- Мониторинг и удаление вредоносных программ

Мошенничество с кредитными картами, удостоверениями личности и кибермошенничество обходятся Великобритании в 190 миллиардов фунтов стерлингов в год, и страна достигла уровня эпидемии мошенничества. Пока малые и средние предприятия в Великобритании не восполнят пробел в навыках кибербезопасности и не защитят себя, онлайн-атаки и киберугрозы будут продолжаться…» ***(Cyber skills gap leaving UK SMEs vulnerable to attacks // PROFESSIONAL SECURITY MAGAZINE (https://www.professionalsecurity.co.uk/news/announcement/cyber-security-skills-gap-is-leaving-uk-smes-vulnerable-to-attacks/). 19.12.2022).***

***

«Новое исследование из отчета Cyber Security Insights Report 2022 показало, что бюджеты на кибербезопасность в британских компаниях увеличатся на 11% в течение следующих 2-3 лет.

Однако при текущем высоком уровне инфляции в Великобритании это фактически приводит к сокращению их бюджетов на кибербезопасность до 2025 года, при этом 13% респондентов сообщили, что они ожидали сокращения своих бюджетов в этот период времени.

Больше внимания кибербезопасности внутри организаций

В отчете также показано, что в среднем на кибербезопасность приходится 25% годового бюджета на ИТ, что означает пятипроцентный рост расходов на кибербезопасность в Великобритании по сравнению с ответами на опросы 2021 года.

Это указывает на то, что даже несмотря на сбои на рынке, наблюдавшиеся в прошлом году, компании по-прежнему сосредоточены на инвестициях в кибербезопасность для защиты своей организации и стимулирования роста бизнеса.

Имея это в виду, среднего роста в 11% может быть недостаточно для противодействия инфляции; Угрозы кибербезопасности будут продолжать расти, страховое покрытие может сократиться, а правила соответствия будут адаптироваться по мере развития цифрового ландшафта в Великобритании.

Почему растут бюджеты на кибербезопасность

С ростом угрозы кибератак становится ясно, почему организациям необходимо продолжать инвестировать в свою онлайн-безопасность. В отчете указаны некоторые важные причины, по которым британские компании увеличивают свои бюджеты на кибербезопасность:

– Защита от постоянно меняющихся угроз (40%)

– Обеспечение соответствия ИТ-инфраструктуры (38%)

– Руководители уровня совета директоров уделяют повышенное внимание кибербезопасности (38%).

Небольшие компании сообщили, что они с большей вероятностью используют от 40 до 60% своего ИТ-бюджета на кибербезопасность, а более крупные компании выделяют меньше своего бюджета на поддержание и улучшение своей онлайн-безопасности.

Что ждет кибербезопасность в будущем

Хотя предполагаемое увеличение бюджета на онлайн-безопасность звучит многообещающе, отделы кибербезопасности будут работать только в том случае, если их бюджеты смогут вместить необходимые ресурсы. Это означает, что может

потребоваться больший бюджет для противодействия инфляции и обеспечения того, чтобы организации опережали потенциальные нарушения безопасности.

В то время как небольшие, более гибкие компании могут быть лучше оснащены, чтобы выделять больше ресурсов в свой бюджет на кибербезопасность, более крупные организации также должны учитывать риск ненадлежащего инвестирования в свой отдел кибербезопасности». ***(Cyber Security Budgets Expected To Increase // PROFESSIONAL SECURITY MAGAZINE (https://www.professionalsecurity.co.uk/news/announcement/cyber-security-budgets-expected-to-increase/). 15.12.2022).***

***

Австралія та Нова Зеландія

«Сегодня австралийские организации работают в условиях растущих и изощренных киберугроз. Преступники и поддерживаемые государством злоумышленники в киберпространстве нацелены на предприятия и правительственные организации в наиболее важных секторах страны. Воздействие этих злонамеренных действий продемонстрировано недавней волной получивших широкую огласку утечек данных клиентов в таких секторах, как финансовые услуги и телекоммуникации. Предприятия и государственные организации должны рассматривать кибербезопасность как стратегический императив.

Однако до недавнего времени многие инициативы в области кибербезопасности в Австралии работали изолированно за счет более широкого сотрудничества между различными секторами экономики. В CyberArk мы считаем, что сотрудничество в масштабах всей экономики, развиваемое через совместные сети, использующие опыт новаторов и лидеров отрасли, является ключом к преодолению сложных проблем кибербезопасности.

Использование опыта

Важным шагом вперед является создание Австралийского центра сотрудничества в области кибербезопасности в качестве некоммерческой организации, деятельность которой направлена на то, чтобы сделать

киберпространство более безопасной ареной для ведения бизнеса. Центр стремится использовать ресурсы и опыт предприятий всех размеров, государственных и научно-исследовательских учреждений, а также разрабатывать решения, инициативы и предложения для развития более кибербезопасной цифровой экономики.

Центр расположен на четырнадцатом участке Аделаиды, который считается крупнейшим инновационным центром в южном полушарии с более чем 1 миллиардом долларов федерального финансирования, правительства штата и промышленности. Подобно тому, как ведущие глобальные инновационные центры играют ключевую роль в создании зрелых национальных инновационных экосистем, Lot Four уделяет особое внимание объединению ряда высокотехнологичных секторов экономики. Кибербезопасность является одной из этих вертикалей, способствующей внедрению инноваций и выведению коммерческих результатов на рынок, а также концентрированному присутствию ведущих исследовательских институтов, поставщиков технологий и фирм, предоставляющих профессиональные услуги.

Чтобы помочь австралийским предприятиям любого размера справиться с передовыми угрозами кибербезопасности и принять участие в совместных инициативах по укреплению кибербезопасности Австралии, мы заключили членство в Австралийском центре сотрудничества в области кибербезопасности. Объявляя о нашем сотрудничестве, директор и председатель центра Ким Скотт отметила актуальность соглашения, «учитывая текущую нехватку навыков и талантов, а также сложный ландшафт угроз, затрагивающий все сектора отрасли».

Итак, что означает это членство для нашего присутствия на этом рынке, а также для наших клиентов, партнеров и других заинтересованных сторон?

Как поставщик, специализирующийся на решениях для защиты личных данных, мы можем внести свой вклад в улучшение кибербезопасности. Управление привилегированным доступом — это основа обеспечения безопасности удостоверений, охватывающего бизнес-приложения, распределенные рабочие ресурсы, гибридные облачные рабочие нагрузки и жизненный цикл DevOps.

Присоединение к Австралийскому центру сотрудничества в области кибербезопасности укрепляет наше сотрудничество в австралийской экосистеме кибербезопасности и инноваций. Это позволит нам участвовать в инициативах интеллектуального лидерства, включающих широкий спектр различных точек зрения на австралийскую экономику, и работать рука об руку с другими организациями в рамках различных инициатив по созданию возможностей кибербезопасности.

Во-вторых, это соглашение обеспечивает нам присутствие на рынке Южной Австралии, благодаря чему мы можем принимать клиентов и партнеров и сотрудничать в решении стратегических проблем кибербезопасности с промышленностью и нашими коллегами на рынке. Это поможет нам удовлетворить потребности предприятий Южной Австралии в кибербезопасности и еще больше укрепит нашу позицию мирового лидера в области защиты личных данных.

С этой инициативой мы готовимся сделать больше, чтобы информировать австралийских клиентов о том, как CyberArk предлагает комплексные решения, которые помогут им снизить риски, связанные с утечкой данных, и контролировать доступ к их наиболее конфиденциальным активам. Будучи первым бизнесом в Австралии и Новой Зеландии, мы также хотим поделиться своим опытом и более эффективно работать над проблемами и решениями с нашими партнерами на этом рынке…» ***(Stephenie Andal. CyberArk: Working with the Australian Cyber Collaboration Centre to boost Australia's cyber security maturity // nextmedia Pty Ltd. (https://www.itnews.com.au/feature/cyberark-working-with-the-australian-cyber-collaboration-centre-to-boost-australias-cyber-security-maturity-588912). 08.12.2022).***

***

«Недавние утечки данных привлекли внимание к уязвимостям веб-API, и, что может быть не случайно, Австралийский центр кибербезопасности добавил их в свое авторитетное Руководство по информационной безопасности.

Последняя редакция ISM, опубликованная ACSC, добавляет новый элемент управления, «чтобы обеспечить аутентификацию клиентов при вызове интерфейсов программирования веб-приложений, которые облегчают доступ к данным, не разрешенным для публикации в открытом доступе».

Кроме того, «был добавлен новый элемент управления для обеспечения аутентификации клиентов при вызове интерфейсов программирования веб-приложений, которые облегчают изменение данных».

Эти элементы управления отсутствовали в сентябрьском выпуске ISM.

ACSC также нацелен на то, что можно было бы назвать «культурой соответствия», в частности на подход «установил и забыл» к средствам контроля безопасности.

Три элемента управления были пересмотрены, чтобы было ясно, что их следует активно поддерживать.

Надзор за повышением осведомленности о кибербезопасности: «Существующий контроль, связанный с надзором за разработкой и функционированием программы повышения осведомленности о кибербезопасности, был изменен, чтобы обеспечить его сохранение».

Программа доверенных инсайдеров: «Существующий контроль, относящийся к разработке и внедрению программы доверенных инсайдеров, был изменен, чтобы обеспечить его сохранение».

Были обновлены 33 различных элемента контроля, относящихся к документации: «Существующие элементы контроля, относящиеся к разработке и внедрению документации по кибербезопасности, были изменены, чтобы обеспечить сохранение документации на протяжении всего срока ее действия».

Также подчеркивается другой аспект культуры соответствия, стратегии, которые существуют только в виде документов: «Существующий контроль, относящийся к разработке и поддержанию стратегии коммуникации в области кибербезопасности, был изменен для обеспечения ее реализации (выделение добавлено)».

Впервые ISM прямо вовлекает растущий — и часто небезопасный — мир Интернета вещей в свою компетенцию.

«В определение ИКТ-оборудования были внесены поправки, чтобы прямо указать, что «интеллектуальные устройства» считаются ИКТ-оборудованием, и поэтому все меры контроля, относящиеся к ИКТ-оборудованию, в равной степени применяются к интеллектуальным устройствам, таким как интеллектуальные телевизоры и интеллектуальные холодильники», — отмечается в журнале изменений». ***(Richard Chirgwin. Australian Cyber Security Centre takes aim at web API vulnerabilities // nextmedia Pty Ltd. (https://www.crn.com.au/news/australian-cyber-security-centre-takes-aim-at-web-api-vulnerabilities-589146). 15.12.2022).***

***

Інші країни

«Федеральному министерству информационных технологий (ИТ) было поручено модернизировать «безопасные» планшеты, используемые членами федерального кабинета министров, с помощью программного обеспечения собственной разработки после киберугроз и утечек аудио.

Должностные лица министерства информационных технологий заявили, что в связи с надвигающимися угрозами кибербезопасности и поразительным открытием, что эти планшеты работали с использованием индийского программного обеспечения, премьер-министр Шехбаз Шариф поручил проверить планшеты членов кабинета.

Они сказали, что после проверки в существующем программном обеспечении были выявлены лазейки безопасности.

Министерство представило отчет правительству, в котором говорится, что существующее программное обеспечение может поставить под угрозу кибербезопасность членов федерального кабинета и данные, важные для национального управления, включая безопасность и другие конфиденциальные вопросы.

Они также выразили опасение, что планшеты могут быть взломаны.

В свете полученных данных премьер-министр Шехбаз поручил министерству информационных технологий разработать собственное программное обеспечение для запуска планшета и подготовить устройства на месте для предотвращения угроз кибербезопасности.

Чиновники министерства информационных технологий также добавили, что ведомство выпустило в связи с этим уведомление о закупке новых планшетов отечественного производства.

Кроме того, перед Национальным советом по безопасности телекоммуникаций будет поставлена задача обеспечить, чтобы программное обеспечение, установленное на таких планшетах, соответствовало необходимым стандартам безопасности». ***(Zaheer Ali Khan. Cyber security threat: Federal cabinet seeks to upgrade tablets with local software // SAMAA TV (https://www.samaaenglish.tv/news/40022878/pakistan-cyber-security-threat-federal-cabinet-seeks-to-upgrade-tablets-with-local-software). 07.12.2022).***

***

«Центральный банк Нигерии (CBN) и заинтересованные стороны в области информационной безопасности предпринимают шаги для проверки растущих случаев кибератак в киберпространстве Нигерии.

Выступая на ежегодной конференции по кибербезопасности Общества информационной безопасности Африки и Нигерии (ISSAN) в Лагосе, директор департамента управления платежной системой CBN Муса Джимо заявил, что высший банк твердо привержен созданию устойчивой платежной экосистемы в стране.

Он сказал, что CBN будет продолжать сотрудничать с организациями, которые привержены борьбе с растущей активностью кибератак.

В своем выступлении президент Ассоциации финтех-технологий Нигерии (FinTechNGR) Аде Баджомо сказал, что для адекватного реагирования на рост числа кибератак организациям следует наладить сотрудничество и обмен информацией о кибер-взломах.

По его словам, молчание со стороны организаций, которые подверглись атаке, не поможет другим, подчеркнув, что полное раскрытие, синергия и обмен информацией о зарегистрированных кибератаках и о том, как ими управляли, помогут другим организациям принять превентивные и ответные меры.

Он призвал организации постоянно модернизировать свои технологии для противодействия кибератакам, призвав их делать резервные копии данных.

Соучредитель/главный дальновидный директор Digital Encode Адевале Обадаре, выражая свое мнение на панельной сессии, привел доводы в пользу сотрудничества между заинтересованными сторонами, отметив необходимость найти баланс между инвестициями в людей, технологии и процессы для борьбы с кибератака и мошенничество.

Он также заявил о необходимости создания коэффициента разведки кибербезопасности, который будет состоять из расширенного интеллекта для проверки того, что происходит в системе в режиме реального времени, упреждающего интеллекта для анализа того, что может произойти, и вспомогательного интеллекта для определения того, что необходимо сделать. Он рекомендовал заняться оцифровкой, цифровизацией и цифровой трансформацией.

В своем приветственном слове президент ISSAN Дэвид Исиавве сказал, что конференция посвящена дальнейшему выявлению новых угроз и тенденций в сфере кибербезопасности, а также предлагает практические шаги в отношении того, что предприятиям и частным лицам необходимо знать и делать, чтобы сдержать растущую волну кибербезопасности. деятельности киберпреступников. Он отметил, что кибер-злоумышленники во всем мире становятся все более изощренными, что является следствием пандемии Covid 19, подчеркнув, что необходимо повысить осведомленность, чтобы свести к минимуму атаки на предприятия, которые могут привести к потерям для различных организаций.

Кроме того, Исиавве, который также является генеральным директором Ecobank, обосновал осведомленность клиентов, а также сотрудничество всех заинтересованных сторон». ***(Collins Nweze.CBN, security experts move against cyber***

attackers // The Nation Newspaper, Ltd. (https://thenationonlineng.net/cbn-security-experts-move-against-cyber-attackers/). 06.12.2022).

***

«Согласно отчету Агентства США по международному развитию (USAID), ситуация с кибербезопасностью на Филиппинах выглядит безрадостной, подвергая риску десятки тысяч сотрудников, занимающихся аутсорсингом бизнес-процессов (BPO).

Это произошло после того, как различные заинтересованные стороны представили снимок плохой инфраструктуры информационных и коммуникационных технологий (ИКТ) в стране при запуске оценочного исследования Национального плана кибербезопасности на 2022 год.

Согласно отчету, составленному организацией USAID Better Access and Connectivity (BEACON), Филиппины «готовы поставить под угрозу» американскую часть своего рынка аутсорсинга бизнес-процессов. Контракты BPO в США составляют 75 процентов филиппинского рынка BPO стоимостью 23 миллиарда долларов.

Согласно исследованию, проведенному фирмой онлайн-маркетинга Reboot Digital PR Agency, Филиппины являются одной из наименее кибербезопасных стран Азии для работы.

Исследование поставило Филиппины на девятое место с 19 загрузками в месяц и в среднем с 880 сайтами с вредоносными программами в Интернете, что на 20 сайтов больше на 100 000 URL-адресов, чем у их относительно близкого соседа, Малайзии, которая занимает третье место.

Недавно компания Global Security «Лаборатория Касперского» определила Филиппины как главную цель банковского вредоносного ПО в Азиатско-Тихоокеанском регионе. В стране самое большое количество пользователей, атакованных банковскими троянами.

USAID BEACON в своей презентации для Департамента информационных и коммуникационных технологий (DICT) отметил, что Филиппины должны

инвестировать в свои возможности в области кибербезопасности, чтобы лучше подготовить страну к противостоянию растущим и непрекращающимся кибератакам и нарушениям информационной безопасности.

«Точки данных, которые были представлены в отчете, были скорее условными и показательными, чем очень конкретными, но путем реализации некоторых наших рекомендаций... (например,) поощрения большего числа специалистов по кибербезопасности в государственном секторе. Способ сделать то есть обеспечить наличие конкретных должностных инструкций, связанных с функциями кибербезопасности, которые оплачивают и удерживают специалистов по кибербезопасности», — сказал Джон Гэррити, руководитель группы USAID BEACON Activity.

Гэррити добавил, что только в Соединенных Штатах открыто более 700 000 вакансий в области кибербезопасности, и нехватка еще более остра в развивающихся странах, таких как Филиппины, где дефицит технических кадров является самым большим.

BEACON USAID пришел к выводу, что киберэкосистема Филиппин может оказаться в «тупике», если текущая ситуация сохранится.

IBM добавила, что у страны могут возникнуть «большие трудности» с набором и удержанием кибер-талантов в национальном правительстве.

Между тем DICT признал, что страна все еще находится в «стадии становления», когда речь идет о кибербезопасности, поскольку само агентство было создано только в 2016 году.

«Мы пытаемся получить гранты из других стран, чтобы расширить возможности нашего агентства», — сказал заместитель министра DICT Пол Джозеф Меркадо.

Меркадо также подчеркнул важность учета вопросов кибербезопасности в школах.

DICT заявила, что опубликует Национальный план кибербезопасности в начале следующего года, который будет действовать до 2028 года». ***(Jacque Manabat. Weak cyber security is a risk to Philippines' US BPO workforce: USAID //***

ABS-CBN Corporation (https://news.abs-cbn.com/business/12/12/22/weak-ph-cyber-security-seen-as-risk-to-bpo-sector). 12.12.2022).

***

«Россияне не впервые атакуют сайты официальных учреждений разных стран мира

Компьютерная группа реагирования на киберинциденты CSIRT рассказала об увеличении количества атак на итальянские учреждения со стороны русских хакерских групп. Вероятно, атаки будут усиливаться.

Об этом пишет итальянское издание ANSA со ссылкой на анонимный источник.

Подробности

По мнению киберспециалистов, эти атаки носили "демонстративный" характер и не привели к нарушениям целостности и конфиденциальности систем. Но они также отмечают, что атаки, вероятно, усилятся в ближайшие месяцы, и рекомендовано государственным учреждениям уделить большое внимание безопасности своих ИТ-систем и оценить, нужно ли повышать уровень защиты от DDoS-атак.

Атаки русских хакеров

Как известно, русские хакеры уже не в первый раз атакуют сайты официальных учреждений разных стран мира. Так, недавно прокремлевские хакеры нанесли ущерб пяти энергокомпаниям Эстонии. Тогда из-за масштабной кибератаки не работали электронные каналы концерна Eesti Energia, в частности сетевой компании Elektrilevi.

Также были атакованы Министерство экономики Эстонии, Банк Эстонии и EAS — система экстренного оповещения. По данным департамента государственной инфосистемы (RIA), атаки прокремлевских преступников были нацелены также на предприятия и ведомства Латвии, Польши и Украины».

(Татьяна Слободянюк. Снова россияне: прокремлевские хакеры атаковали сайты итальянских учреждений // Новини.Live (https://world.novyny.live/ru/snova-rossiiane-prokremlevskie-khakery-atakovali-saity-italianskikh-uchrezhdenii-66789.html). 05.12.2022).

***

«Веб-сайт парламента ЕС подвергся распределенной кибератаке типа «отказ в обслуживании» (DDoS) через несколько мгновений после того, как Россия была объявлена государством-спонсором терроризма и призвала к дальнейшей изоляции. DDoS-атака включает в себя заполнение целевого веб-сайта запросами, чтобы предотвратить доступ к нему законных пользователей.

Ответственность за атаку взяла на себя группа кибер-хактивистов Anonymous Russia, связанная с группой Killnet DDoS.

«Изощренная кибератака» вывела из строя сайт парламента ЕС

Чиновники парламента ЕС связали кибератаку с пророссийской группой, известной проведением DDoS-атак против стран, выступающих против России.

«Европейский парламент подвергается изощренной кибератаке. Прокремлевская группировка взяла на себя ответственность», — написала в Твиттере председатель Европарламента Роберта Метсола.

Она добавила, что ИТ-эксперты парламента ЕС «борются с этим и защищают наши системы. И это после того, как мы объявили Россию государством-спонсором терроризма».

Жауме Даух, генеральный директор по коммуникациям и пресс-секретарь Европарламента, также указал, что простои веб-сайта Европарламента были вызваны внешним трафиком.

«На доступность веб-сайта Europarl_EN в настоящее время влияет извне из-за высокого уровня внешнего сетевого трафика», — сказал он, добавив, что трафик был «связан с событием DDOS-атаки (распределенный отказ в обслуживании)».

По словам Оливера Пинсона-Роксбурга, генерального директора Defense.com, время кибератаки было значительным.

«Похоже, что атака на Европейский парламент была специально рассчитана по времени, ударив по их системам в момент максимального спроса, который гарантированно привлечет наибольшее внимание со стороны наблюдающего мира», — сказал Пинсон-Роксбург.

Приписывая кибератаку DDoS-группе Killnet, он предположил, что кибератаки, предположительно, стали жизнеспособными геополитическими инструментами для национальных государств.

«Российская группа, которая, вероятно, стоит за атакой, Killnet, имеет форму использования DDoS-атак, чтобы сеять разрушения в странах, которые, как считается, выступают против войны в Украине».

Европарламент призвал к дальнейшей изоляции России

Согласно не имеющей обязательной силы резолюции, «преднамеренные нападения» России на гражданское население Украины, а также «разрушение гражданской инфраструктуры и другие серьезные нарушения прав человека и международного гуманитарного права приравниваются к актам террора против населения Украины и представляют собой военные преступления».

Таким образом, парламент ЕС признал Россию государством-спонсором терроризма и государством, которое использует терроризм для достижения своих целей. Впоследствии парламент ЕС хочет, чтобы Европейский Союз еще больше изолировал Россию от международных органов, таких как Совет Безопасности ООН. Кроме того, члены парламента ЕС хотят, чтобы союз сократил дипломатические связи и контакты с российскими официальными лицами до минимума и закрыл государственные организации, распространяющие пропагандистскую пропаганду. Однако закон ЕС не может объявить террористическим государством всю страну, но может преследовать конкретных лиц за их ответственность за террористические акты.

Множественные DDoS-атаки с ограниченным воздействием

Killnet несет ответственность за несколько DDoS-атак с разной степенью успеха с тех пор, как Россия вторглась в Украину в конце февраля. Среди них DDoS-атаки на аэропорты США в октябре, атаки на сайты правительств штатов

США в Колорадо, Кентукки и Миссисипи, ФБР, Министерство финансов США и Лондонскую фондовую биржу. Группа Killnet DDoS также нацелена на союзников Украины, таких как Румыния и Италия.

В ноябре 2022 года ФБР заявило, что DDoS-атаки пророссийской группировки оказали ограниченное влияние на цели, поскольку они нацелены на общедоступные веб-сайты, а не на базовые службы. Однако, по словам генерального директора CybSafe Оза Алаше, кибератака на сайт парламента ЕС стала напоминанием о том, что жертвой кибератаки может стать любой.

«Часто сети, используемые для инициирования этих атак, были скомпрометированы из-за плохой гигиены кибербезопасности, осведомленности и поведения. Однако есть способы подготовиться, включая надежную сетевую безопасность, непрерывный мониторинг веб-трафика и использование нескольких серверов, которые сложно атаковать одновременно».

Алаше посоветовал организациям относиться к кибербезопасности как к активному процессу, а не как к соблюдению требований.

«Будь то DDoS-атаки, фишинг или программа-вымогатель, одно можно сказать наверняка — текущий статус-кво должен измениться. Нам необходимо коренным образом изменить наш подход к кибербезопасности, ориентируясь на поведение, а не просто на осведомленность». ***(Alicia Hope. Killnet DDoS Group Executes a Cyber Attack on the EU Parliament Website After Resolution Against Russia // CPO Magazine (https://www.cpomagazine.com/cyber-security/killnet-ddos-group-executes-a-cyber-attack-on-the-eu-parliament-website-after-resolution-against-russia/). 05.12.2022).***

***

«Влада Японії з 2023 року планує вести «активну кібероборону» — планується ухвалити поправки до законодавства, яке дозволить японським фахівцям вести превентивну боротьбу з хакерами, — про це повідомила газета Nikkei.

Це рішення японська влада вводить для попередження кіберзагроз, що знизить ризики для інформаційних систем, що використовуються в японській економіці. Згідно з чинним законодавством, такі заходи можна вживати лише реагуючи на надзвичайні ситуації після кібератаки.

Видання зазначає, що в Японії до кінця 2022 року мають бути представлені та оновлені три документи щодо національної безпеки — стратегія національної безпеки, норми програми національної оборони та середньострокова програма оборони». ***(Наступного року Японія легалізує запобіжні кібератаки для свого захисту // No worries! (https://noworries.news/nastupnogo-roku-yaponiya-legalizuye-zapobizhni-kiberataky-dlya-svogo-zahystu/). 11.12.2022).***

***

Кіберзахист критичної інфраструктури

«Чи можливо маніпулювати дорожнім рухом у великому місті, використавши для цього комп'ютерні технології та трохи знань?

Нещодавні приклади зі злому інтелектуальної транспортної системи у нідерландських містах вже дали ствердну відповідь на це питання. А в Німеччині тим часом дослідники попереджають про застарілість деяких протоколів, що використовуються для управління світлофорами у країні.

Доволі проста техніка злому

На підтвердження своїх слів дослідники продемонстрували можливість перемикання за допомогою простих комп'ютерних маніпуляцій окремих світлофорів із червоного на зелене світло швидше, ніж це має відбуватися за планом. Або, навпаки, – повільніше. Для проведення злому знадобляться лише лептоп, радіопередавач та проста антена.

Аби підтвердити свою теорію на практиці, два комп'ютерних інженери запросили групу журналістів на перехрестя з дуже інтенсивним рухом, розташоване у північному Ганновері.

Сидячи в автомобілі, в салоні якого було встановлено необхідну апаратуру, комп'ютерники під час демонстрації з легкістю змінювали тривалість часу, коли світлофор горів зеленим світлом.

Система захищена достатньо для того, аби, наприклад, унеможливити ситуацію, коли всі світлофори одночасно стануть зеленими. Однак, нею все ж можна певною мірою маніпулювати, створюючи величезні корки на автошляхах чи збільшуючи ризик аварій.

Проводячи цю демонстрацію, дослідники мали на меті показати потенційну небезпеку, пов'язану з експлуатацією системи, що є доволі застарілою.

Експерти зазначили, що вони не мали жодних інших цілей, окрім бажання вказати на чинну проблему. При цьому хакери побажали зберегти анонімність, аби уникнути можливої кримінальної відповідальності.

Застаріла система в епоху цифрових технологій

Насправді виявлена дослідниками «дірка» у захисті пов'язана із роботою системи, яка створена для того, аби зробити дорожній рух більш плавним. Комп'ютерні інженери, що виявили проблему, використали той самий аналоговий радіосигнал, який використовується автобусами та трамваями, даючи їм змогу проїжджати на зелене світло при наближенні до світлофорів. Ця технологія була розроблена ще у 80-х роках, і сигнал, звісно, не кодується.

Журналісти звернулися до фахівців з управління дорожнім рухом з 13-ти великих міст Німеччини. В них запитали про те, чи використовується в їхніх містах подібна технологія, що дозволяє контролювати рух та вмикати зелене світло, даючи дорогу автобусам та потягам.

У результаті з'ясувалося, майже всі ці міста використовують стару аналогову радіотехнологію. А фахівці з управління дорожнім рухом визнали, що це може нести у собі ризик. Загалом майже 80 міст Німеччини все ще використовують аналоговий сигнал.

На щастя, в Німеччині існує закон, який зобов'язує всі німецькі міста до 2028 року перевести світлофори на цифровий радіосигнал. Цей сигнал передаватиметься у закодованому вигляді, і тому він більш безпечний…». ***(Борис Скуратівський.***

Дуже просто: німецькі дослідники попереджають про можливість злому світлофорів хакерами // Mediasat (https://mediasat.info/uk/2022/12/28/duzhe-prosto-nimecki-doslidniki-poperedzhayut-pro-mozhlivist-zlomu-svitloforiv-xakerami/). 28.12.2022).

***

Кіберзахист закладів охорони здоров'я

«Инцидент выявляет несколько общих, но серьезных данных и опасения поставщиков

Инцидент со взломом облачного поставщика программного обеспечения для электронных медицинских карт и управления практикой затронул десятки клиентов педиатрической практики компании и более 2,2 миллиона их пациентов и других лиц.

Компания Connexin Software Inc. из Пенсильвании, которая ведет бизнес под названием Office Practicum, сообщила о взломе в Министерство здравоохранения и социальных служб США 11 ноября, заявив, что он был связан с сетевым сервером.

Connexin в своем заявлении об уведомлении о нарушении перечисляет около 120 педиатрических клиник, затронутых инцидентом.

В заявлении Connexin говорится, что 26 августа компания обнаружила «аномалию данных» во внутренней сети. Судебно-медицинская экспертиза установила, что неавторизованная третья сторона получила доступ к внутренней компьютерной сети, удалив некоторые данные, содержащиеся в «автономном» наборе данных пациента, используемом для преобразования данных и устранения неполадок.

В заявлении говорится, что к «живой» системе электронных медицинских карт Connexin не было доступа, и инцидент также не затронул какие-либо системы групп педиатрической практики, базы данных или системы медицинской документации.

В любом случае диапазон данных пациентов, которые могут быть скомпрометированы в результате инцидента, широк. Connexin сообщает, что затронутая информация о пациенте могла включать имя, имя поручителя, имя родителя/опекуна, адрес, адрес электронной почты, дату рождения, номера социального страхования, информацию о медицинском страховании, а также медицинскую информацию и/или информацию о лечении, включая процедуры, диагноз, информацию о рецепте и фамилии врачей.

Финансовая информация, такая как заявки на выставление счетов, счета-фактуры и идентификаторы счетов пациентов, используемые поставщиками, также содержалась в затронутом наборе данных.

Риски педиатрических данных

Риски безопасности данных и конфиденциальности, связанные с педиатрическими пациентами, могут вызывать особую тревогу по целому ряду причин.

«Каждый раз, когда вы имеете дело с педиатрическими данными или системами, возникает повышенное чувство риска», — говорит Брайан Селфридж, руководитель отдела кибербезопасности и рисков в сфере здравоохранения в охранной фирме CORL Technologies.

Несанкционированный доступ к номерам социального страхования, демографическим данным, информации о выставлении счетов и лечении детей может привести к краже личных данных, краже медицинских данных и другим видам мошенничества.

Ситуация усложняется тем, что педиатрические данные обычно требуют более длительного хранения данных, говорит Венделл Бобст, старший консультант по безопасности в консалтинговой компании по вопросам конфиденциальности и безопасности tw-Security. «Это означает, что педиатрические провайдеры, как правило, хранят данные дольше, чем взрослые пациенты», — говорит он.

«В случае с детьми вы видите потенциальную возможность злоупотребления этой информацией на протяжении десятилетий, что может негативно сказаться на пациентах», — говорит Селфридж.

Автономные данные

Connexin не сразу ответила на запрос Information Security Media Group о дополнительных подробностях инцидента.

Описание компанией того, что скомпрометированный набор данных находится в автономном режиме, указывает на несколько возможных сценариев.

Connexin предоставляет свой офисный практикум в виде облачного решения. Ссылка компании на «автономный набор данных пациентов» подразумевает, что их приложение, управляемое в их экземпляре AWS, не было взломано, а скорее «неавторизованная сторона» получила доступ к копии, которая хранилась на локальном сервере, говорит Бобст.

«Connexin может периодически получать новые клиентские данные от других EMR и преобразовывать эти данные в свою платформу», — говорит он. Оперативные данные могут использоваться для завершения или тестирования процесса преобразования. Connexin также может тестировать обновления своих версий с оперативными данными в тестовой среде, чтобы спрогнозировать продолжительность обновления и гарантировать успешное обновление клиентских данных.

Часто организации используют производственные данные для тестирования и устранения неполадок — во время разработки или при реагировании на проблемы клиентов, — говорит Джон Мур, директор по рискам в консалтинговой фирме Clearwater, занимающейся вопросами конфиденциальности и безопасности.

По его словам, они также могут иметь дело с большими наборами данных при переносе клиента на свою платформу или с нее.

«К сожалению, нередко можно увидеть, что организации не имеют таких же средств контроля безопасности в средах разработки, тестирования и миграции, как в производственной среде», — говорит он.

«Это особенно рискованно при использовании реальной личной информации в среде разработки или тестирования, а не фиктивной информации или иной обезличенной информации».

По словам Мура, еще одна возможная интерпретация сообщения Connexin о том, что набор данных находится в автономном режиме, заключается в том, что рассматриваемый сервер не работал.

«Это будет означать, что злоумышленник либо получил физический доступ к серверу, либо достаточный доступ к консоли управления, чтобы позволить им запустить сервер и получить к нему доступ».

По словам Бобста, любые автономные копии данных должны быть зашифрованы, храниться в месте, доступ к которому контролируется, и требовать авторизации для «извлечения» данных из архива.

«Отметка «PHI — клиент X» служит визуальной подсказкой для персонала службы поддержки и аналитиков конверсии», — предлагает он. Кроме того, по словам Бобста, технологии предотвращения потери данных, которые помогают обнаруживать PHI, к которой осуществляется доступ или которые покидают организацию, являются важным средством контроля PHI за пределами приложения». ***(Marianne Kolbasuk McGee. Pediatric EMR Vendor Hack Affects 2.2 Million // Information Security Media Group, Corp. (https://www.govinfosecurity.com/pediatric-emr-vendor-hack-affects-22-million-a-20618). 02.12.2022).***

***

«Подключенные устройства приносят организациям больше информации и удобства, но они также увеличивают поверхность атаки организации — и медицинские устройства не являются исключением. Согласно опросу, опубликованному поставщиком обзорной платформы Capterra, по мере того, как организации здравоохранения подключают к своей сети все больше медицинских устройств, они также чаще подвергаются атакам.

В октябре 2022 года компания Capterra провела исследование 2022 Medical IoT Survey, в котором приняли участие 151 респондент из США. Capterra сообщила, что респонденты должны были занимать должности в области информационных технологий или службы безопасности в организациях

здравоохранения, которые также использовали медицинские устройства, подключенные к Интернету.

Что они нашли? Согласно отчету, те медицинские организации, у которых более 70% устройств, подключенных к Интернету, на 25% чаще подвергаются атакам, чем те медицинские организации, у которых 50% или меньше устройств, подключенных к Интернету. Организации с большим количеством подключений также имеют на 54% больший риск многократной атаки.

Кроме того, почти половина (48%) кибератак на здравоохранение повлияла на уход за пациентами, а две трети (67%) — на данные пациентов. Более половины (53%) ИТ-персонала здравоохранения считают текущую картину угроз кибербезопасности высокой или чрезвычайной.

Эта тревога существует по уважительной причине. Хотя подключенные медицинские устройства могут сделать здравоохранение более удобным, эти устройства производятся и поставляются с дефектами безопасности, которые могут быть использованы злоумышленниками. Эти недостатки включают в себя все, от фундаментальных ошибок проектирования до тех же типов недостатков программного обеспечения, которые преследуют бизнес-технологии и системы электронной коммерции.

Кроме того, в целом поставщики медицинских услуг, как правило, недостаточно финансируют технологии и программы безопасности. Опрос Capterra показал, что 82% респондентов используют подключенные медицинские устройства на устаревших системах Windows; 68% своевременно не обновляют устройства, а 57% не всегда меняют стандартные логины и пароли на вновь полученных устройствах. Подобные методы непосредственно приведут к атакам программ-вымогателей и утечкам данных, которые мы считаем обычным явлением в более широком отраслевом ландшафте.

Capterra предлагает ряд методов обеспечения безопасности, которые должны учитывать все поставщики медицинских услуг, использующие медицинские устройства:

Измените учетные данные по умолчанию и убедитесь, что все операционные системы обновлены до последних исправлений.

Поддерживайте актуальную, полную и точную инвентаризацию всех подключенных медицинских устройств и связанного с ними программного или микропрограммного обеспечения, включая такую информацию, как поставщик, операционная система, номер модели и даты обслуживания.

Проводите регулярные оценки уязвимостей и сканирование перед установкой или повторным подключением медицинских устройств к вашей ИТ-сети.

Используйте программное обеспечение для управления IoT для мониторинга и защиты соответствующих подключенных медицинских устройств.

Разверните стратегии сегментации сети, создав виртуальные локальные сети (VLAN) для разделения различных типов устройств и потоков данных, чтобы снизить общий риск.

Сосредоточьтесь на разработке надежных политик доступа к сети и применяйте стратегии нулевого доверия, когда они доступны». ***(George V. Hulme. Health Care Under Cyberattack: Unprotected Medical IoT Devices Threaten Patient Care // Techstrong Group Inc. (https://securityboulevard.com/2022/12/health-care-under-cyberattack-unprotected-medical-iot-devices-threaten-patient-care/). 14.12.2022).***

***

«Расследуя кибератаку на некоторые серверы Всеиндийского института медицинских наук (AIIMS) в Дели, Индийская группа реагирования на компьютерные чрезвычайные ситуации (CERT-In) обнаружила, что компьютерный факультет AIIMS не принял никаких мер для обеспечения безопасности сети; что никакие политики не были определены на их брандмауэре и в их сети; и большинство коммутаторов были неуправляемыми.

CERT-In, главное агентство кибербезопасности страны, также обнаружило, что все файлы и данные на зараженных серверах AIIMS отображают сообщение

«бесплатная расшифровка в качестве гарантии, вы можете отправить нам до трех бесплатных расшифрованных файлов перед оплатой».

Полиция Дели зарегистрировала FIR в соответствии с разделом 385 IPC (запугивание человека травмой с целью совершения вымогательства), 66 и 66-F Закона об информационных технологиях после получения жалобы от некоего Нареша Кумара Ядава, помощника сотрудника службы безопасности в AIIMS.

«Первоначальный анализ CERT-In показал, что четыре сервера — два сервера приложений, один сервер базы данных и один сервер резервного копирования — были заражены», — сказал источник. «Команда CERT-In обнаружила, что шифрование было запущено одним из серверов Windows, подключенных к той же сети, но файлы этого сервера не были зашифрованы».

Ядав сообщил полиции в своей жалобе, что он получил информацию от некоего доктора Пуджи Гупты, ответственного профессора компьютерного центра AIIMS, об атаке программы-вымогателя на серверы электронной больницы ведущего учреждения 23 ноября. FIR заявил, что после двух зашифрованных писем, было сообщение: «что случилось, ваши файлы зашифрованы, все файлы защищены сильным шифрованием с RSA-2048, общедоступного программного обеспечения для расшифровки нет, какова цена ремонта, цена зависит от того, как быстро вы можете оплатить нам, после получения денег, мы отправим программу и закрытые ключи в ваш ИТ-отдел прямо сейчас, не пытайтесь расшифровать ваши данные после использования стороннего программного обеспечения, это может привести к безвозвратной потере данных, наша программа может восстановить все файлы за несколько минут и все серверы будут работать точно так же, как и раньше, бесплатная расшифровка как гарантия,вы можете отправить нам до трех бесплатных расшифрованных файлов перед оплатой».

Источник сообщил, что CERT-In после проверки всех систем AIIMS обнаружил, что его компьютерный факультет не предпринял никаких мер для защиты сети, а в учреждении не было определено политик для доступного брандмауэра. «Большинство их коммутаторов были неуправляемыми», — сказал источник. «Все зараженные серверы были отключены командой Национального

центра информатики (NIC) от сети и Интернета, чтобы избежать распространения заражения на другие службы».

NIA отправило команду в AIIMS. Источники сообщили, что помимо групп CERT-In и NIC этим вопросом занимается группа из Организации оборонных исследований и разработок (DRDO). Полиция Дели, Бюро разведки, CBI и Министерство внутренних дел также расследуют инцидент.

Первоначальное расследование также показало, что у злоумышленника есть два протонных почтовых адреса — «dog2398» и «mouse63209», которые были идентифицированы по заголовкам зашифрованных файлов. «Нарушение безопасности особенно затронуло приложение электронной больницы, которое предоставлялось и управлялось NIC с 2011–2012 годов, что остановило онлайн-функционирование OPD, неотложной помощи и других служб по уходу за пациентами в помещениях AIIMS», — сказал источник». ***(Mahender Singh Manral. Probing server attack, CERT-In finds holes in AIIMS cyber security // The Indian Express [P] Ltd. (https://indianexpress.com/article/cities/delhi/probing-server-attack-cert-in-finds-holes-in-aiims-cyber-security-8304657/). 04.12.2022).***

***

«…В отчете IBM «Стоимость утечки данных 2022» подчеркивается, что средняя глобальная стоимость утечки данных обойдется организации примерно в 4,35 млн долларов, в то время как средняя стоимость утечки данных в Соединенных Штатах составляет поразительные 9,44 млн долларов.

Дело в том, что большинство организаций не смогут восстановиться, если их данные будут взломаны.

Несмотря на эту статистику, к сожалению, большинство организаций по всему миру по-прежнему не располагают необходимыми навыками, процессами, технологиями и людьми для борьбы с этими угрозами.

По мере роста сложности и масштаба угроз страховые компании были вынуждены ужесточать свои требования, что привело к тому, что подавляющее

большинство организаций столкнулись с трудностями в соблюдении стандартов соответствия, требуемых страховыми компаниями.

Усложняются не только требования, но и по мере увеличения угроз растут и расходы на страхование. По данным CNBC, «премии по киберстрахованию выросли в среднем на 28% в первом квартале 2022 года по сравнению с четвертым кварталом 2021 года, по данным Совета страховых агентов и брокеров (CIAB), ассоциации посредников по коммерческому страхованию и вознаграждениям работникам».

Крайне важно иметь MSSP для оценки рисков и решения проблем безопасности бизнеса. Без принятия правильных мер кибербезопасности компаниям сложно выполнять нормативные требования инвесторов, партнеров и страховых компаний. С MSSP организации могут защитить системы и учетные записи от целевых атак. Знайте, какие шаги необходимо предпринять для повышения вашей кибербезопасности.

Как MDR можно использовать для улучшения стратегии кибербезопасности и соответствия требованиям

Управляемое обнаружение и реагирование (MDR) используется для быстрого выявления и ограничения воздействия угроз и рисков безопасности с круглосуточным мониторингом угроз, обнаружением и целенаправленным реагированием на основе аналитики журналов в реальном времени с инструментами оркестрации безопасности, автоматизации и реагирования. для расследования, поиска угроз и реагирования.

Объедините информацию об угрозах и человеческий опыт для расширенной аналитики и контекстуальных событий.

Какую пользу организация получает от MDR?

Полная видимость. Визуализируйте рискованное поведение и неправильные настройки, чтобы выявить источник угрозы.

Снижение затрат и рисков. Вероятность взлома снижается, а обнаружение и реагирование в режиме 24/7 обеспечиваются за небольшую часть стоимости создания специальной группы внутри компании.

Душевное спокойствие — возможности и возможности для предоставления специализированных услуг в масштабе за счет объединения информации об угрозах и человеческого опыта.

Быстрое реагирование — схемы реагирования на инциденты, платформа SOAR и сертифицированные обработчики инцидентов для сдерживания угроз и защиты вашей спины.

Партнер, на которого можно положиться — партнерство, которое работает как продолжение вашей команды для выявления моделей незаконного поведения и снижения рисков…» ***(Eleanor Barlow. How to Enhance Your Cyber Security Posture with MDR // Informa PLC Informa UK Limited (https://www.informationweek.com/security-and-risk-strategy/how-to-enhance-your-cyber-security-posture-with-mdr). 13.12.2022).***

***

Захист персональних даних та соціальні мережі

«На SIM-картах хранится много информации о владельце, которая может быть использована злоумышленниками в корыстных целях.

По словам экспертов, объем памяти SIM-карты составляет до 128 Кб. Память используется даже для записи координат ближайшей к телефону башни сотовой связи. Приблизительно раз в полчаса SIM-карта передает эту информацию в эфир. Таким образом, при должном уровне технической подкованности злоумышленники могут перехватить этот сигнал и установить слежку за жертвой, зная ее номер телефона.

«Это, безусловно, полезная функция в случае, например, поиска без вести пропавшего человека. С другой стороны, данные могут быть использованы и для установления внешнего наблюдения, если человек по каким-то причинам стал объектом оперативной разработки силовых ведомств и даже злоумышленников», — отмечают специалисты.

SIM-карта записывает и ряд другой информации: контакты, сообщения и даже платежная информация. Последнее, по словам экпертов, является не номерами банковских карт, а историями онлайн-покупок, совершаемых с помощью телефонного номера.

Вся информация, которую SIM-карта записывает, передается провайдеру. Однако, в случае кражи, хранящиеся на ней данные также могут быть изъяты преступниками». ***(Украинцам рассказали, по каким данным на SIM-карте охотятся злоумышленники // China review (https://china-review.com.ua/22452-ukraincam-rasskazali-po-kakim-dannym-na-sim-karte-ohotjatsja-zloumyshlenniki.html). 04.12.2022).***

***

«Хакеры получили доступ к информации, украденной в ходе предыдущей атаки

Хакеры получили информацию о клиентах, но не пароли, сообщил менеджер паролей LastPass в среду, сообщая об инциденте кибербезопасности, впервые обнаруженном в августе.

Специалист по контролю доступа сказал, что неавторизованная сторона использовала информацию, украденную во время инцидента, длившегося несколько дней в августе, чтобы совсем недавно взломать стороннее облачное хранилище.

Хакер «смог получить доступ к некоторым элементам информации наших клиентов», — написал генеральный директор LastPass Карим Тубба в своем блоге, не уточнив, какие элементы.

Пароли не изменились, настаивал Тубба. «Пароли наших клиентов остаются надежно зашифрованными благодаря архитектуре LastPass с нулевым разглашением». Он также написал, что расследование было начато сразу после первого инцидента при посторонней помощи со стороны Mandiant.

Mandiant также расследовал августовский инцидент безопасности и определил, что субъект угрозы проникал в среду разработки LastPass в течение четырех дней. Хакер проник через скомпрометированную конечную точку.

Оказавшись внутри, хакер выдал себя за разработчика после того, как реальный сотрудник предоставил учетные данные многофакторной аутентификации.

Компания заявляет, что у нее более 33 миллионов зарегистрированных клиентов и она обслуживает более 100 000 предприятий. По понятным причинам менеджеры паролей являются магнитами для взлома, но эксперты по кибербезопасности продолжают рекомендовать их в качестве решения распространенных ошибок безопасности, таких как слабые или повторяющиеся пароли. Недавний опрос Consumer Reports показал, что только 39% потребителей используют менеджер паролей.

Пользователи, которые сочетают надежные и уникальные пароли с многофакторной аутентификацией, особенно в виде ключа безопасности, делают свои учетные записи еще более устойчивыми к взлому, уменьшая потенциальные последствия, если произойдет немыслимое, и менеджер паролей действительно полностью поддастся хакерам». ***(Prajeet Nair. LastPass Breach Exposes Customer Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/lastpass-breach-exposes-customer-data-a-20600). 01.12.2022).***

***

«Відомий сервіс для зберігання паролів LastPass зізнався у витоку бази з даними користувача. Про це повідомляє TechCrunch.

Раніше LastPass неодноразово з’являвся у новинах у зв’язку з витоками та зломами його серверів. Після кожного такого витоку сервіс запевняв користувачів, що найцінніше – паролі користувача – цілі і неушкоджені і знаходяться в безпеці. Але не цього разу.

В офіційному блозі LastPass генеральний директор сервісу Карім Тубба зізнався, що раніше цього року хакери змогли скопіювати резервну копію бази даних сховища паролів клієнтів. Для цього вони скористалися вкраденими у співробітника LastPass ключами від хмарного сховища.

Повідомляється, що всі паролі користувача зашифровані «пропрієтарною двійковою системою» і можуть бути розшифровані тільки за допомогою майстер-пароля, який знає тільки сам користувач. Однак LastPass попередив, що тепер зловмисники можуть спробувати отримати майстер-паролі, вдавшись до соціальної інженерії або просто «грубою силою».

Крім сховища з паролями користувача зловмисники отримали безліч особистих даних клієнтів LastPass, включаючи імена, email, номери телефонів і платіжну інформацію». ***(Скарбик Павло. У мережу потрапила повна база LastPass з паролями користувачів // iTechua.com (https://itechua.com/news/198931). 24.12.2022).***

***

«Комиссар по информации Австралии расследует методы обеспечения безопасности страховой компании

Базирующаяся в России банда вымогателей, стоящая за взломом крупнейшей частной страховой компании Австралии, утверждает, что разместила полный набор украденных данных, несмотря на то, что анализ, проведенный Medibank, назвал эти данные неполными и трудными для понимания.

Хакеры разместили необработанные данные Medibank в шести заархивированных файлах размером более 5 гигабайт в папке под названием «полная».

В заявлении Medibank говорится, что данные о заявлениях о медицинском обслуживании не были объединены с именами и контактными данными.

Октябрьский взлом затронул 9,7 млн нынешних и бывших клиентов, в том числе 1,8 млн иностранцев, проживающих в Австралии.

Банда вымогателей, стоящая за взломом, начала утечку информации после того, как генеральный директор Medibank Дэвид Кочкар принципиально отказался вести переговоры с хакерами (см.: Medibank говорит «нет» оплате требований хакера о вымогательстве).

Федеральная полиция Австралии продолжает расследование, и в настоящее время нет никаких признаков того, что хакеры украли финансовые или банковские данные.

Министр кибербезопасности Клэр О'Нил опубликовала совместное заявление с генеральным прокурором Марком Дрейфусом, назвав сброс данных ожидаемым событием. «Разглашение таких конфиденциальных и личных данных предосудительно с моральной точки зрения», — заявили они.

Комиссар по информации Австралии объявил, что инициировал отдельное расследование практики обработки личной информации в Medibank.

Основное внимание расследования будет сосредоточено на том, предпринял ли Medibank разумные шаги для защиты личной информации, которой он располагал.

Если уполномоченный OAIC по вопросам конфиденциальности обнаружит «серьезные и/или неоднократные нарушения конфиденциальности», Medibank может быть оштрафован на сумму до 2,2 млн австралийских долларов за каждое нарушение.

Парламент Австралии в понедельник одобрил закон, увеличивающий максимальные штрафы за серьезные или повторные нарушения корпоративной конфиденциальности с нынешних 2,22 миллиона австралийских долларов до того, что больше из 50 миллионов австралийских долларов, 30% скорректированного оборота или трехкратного размера любой корпоративной выгоды. полученный путем неправомерного использования информации». ***(Mihir Bagwe. Medibank Hackers Dump Stolen Data on the Dark Web // Information Security Media Group, Corp. (https://www.govinfosecurity.com/medibank-hackers-dump-stolen-data-on-dark-web-a-20604). 01.12.2022).***

***

«В сегодняшней взаимосвязанной глобальной среде предприятиям необходим предсказуемый и оптимизированный правовой механизм для передачи персональных данных из Европейского Союза в Соединенные Штаты. В свете этой насущной потребности бизнеса Европейская комиссия и правительство США исторически совместно разрабатывали механизмы для облегчения законной передачи персональных данных. Эти предыдущие рамки, известные как Safe Harbor и Privacy Shield (пришедшие на смену Safe Harbor), в конечном итоге были признаны недействительными Судом Европейского Союза (CJEU). Учитывая отмену Privacy Shield в 2020 году, администрация Байдена и Европейская комиссия предприняли шаги по созданию нового механизма поддержки трансграничных потоков данных из ЕС в США, на этот раз известного как Trans-Atlantic Data Privacy Framework.

Предшественники: Safe Harbor и Privacy Shield

Концепция Safe Harbor, выпущенная в 2000 году, представляла собой соглашение между Европейской комиссией и Министерством торговли США, которое обеспечивало правовой механизм, обеспечивающий передачу персональных данных из ЕС в США. Safe Harbor требовал, чтобы сертифицирующие организации публично заявляли, что они соблюдали семь принципов конфиденциальности. Это был популярный выбор среди американских импортеров персональных данных из ЕС, касающихся сотрудников, клиентов и других лиц. В 2015 году CJEU в деле, названном Schrems I, объявил Safe Harbor недействительным, в основном из-за отсутствия ограничений на сбор и использование правительством США персональных данных, передаваемых в рамках Safe Harbor.

В 2016 и 2017 годах Европейская комиссия и правительство Швейцарии, соответственно, утвердили новый механизм, позволяющий передавать данные из ЕС и Швейцарии в США. Гавань до этого, при условии самосертификации по существу аналогичный набор из семи принципов конфиденциальности: уведомление; выбор; ответственность за дальнейшую передачу; безопасность;

целостность данных и ограничение цели; доступ; и регресс, правоприменение и ответственность. В течение следующих нескольких лет более 5000 компаний, расположенных в США, подтвердили свое соответствие принципам Privacy Shield, что позволило им использовать Shield для свободного импорта личных данных из ЕС и Швейцарии без необходимости использования дополнительных механизмов передачи данных.

16 июля 2020 г. CEC в деле Шремса II признал недействительным Соглашение о защите конфиденциальности между ЕС и США на основании опасений, что (1) программы наблюдения правительства США не ограничивались тем, что было «соразмерным» и «строго необходимым» для их целей., и (2) в США не было органа и средств для удовлетворения жалоб граждан ЕС на обращение с их личными данными, которые по существу эквивалентны тем, которые требуются в соответствии с законодательством ЕС. 8 сентября 2020 г. Федеральный уполномоченный по защите данных и информации Швейцарии также опубликовал заключение о том, что соглашение между Швейцарией и США о правилах обмена конфиденциальной информацией не может использоваться в качестве правовой основы для передачи персональных данных из Швейцарии в Соединенные Штаты.

Трансатлантическая структура конфиденциальности данных

Внезапное и неожиданное аннулирование Privacy Shield в июле 2020 года заставило тысячи американских компаний, сертифицированных Shield, попытаться легализовать текущую передачу данных из ЕС и Швейцарии. Большинству экспортеров данных необходимо было быстро перейти к использованию стандартных договорных условий в поддержку передачи в США и проведению оценки рисков передачи, также требуемой постановлением Шремса II, что создавало значительную административную нагрузку. В ответ на это решение власти ЕС и США быстро взяли на себя обязательство пересмотреть жизнеспособную структуру передачи данных.

25 марта 2022 года президент Байден и президент Европейской комиссии фон дер Ляйен объявили о принципиальном соглашении о запуске преемника Privacy Shield для решения проблем CJEU в Schrems II. В соответствии с соглашением

США обязались внедрить новые меры безопасности для обеспечения того, чтобы деятельность радиотехнической разведки была необходимой и пропорциональной для достижения определенных целей национальной безопасности. США также согласились создать новый механизм для лиц из ЕС, которые могли бы добиваться возмещения ущерба, если они считают, что они являются незаконными объектами разведывательной деятельности.

В своем указе от 7 октября 2022 года президент Байден предписал конкретные действия по выполнению обязательств США. ЭО устанавливает дополнительные гарантии для разведывательной деятельности США, в том числе требования о том, чтобы неприкосновенность частной жизни и гражданские свободы всех лиц учитывались независимо от гражданства, и чтобы соответствующая разведывательная деятельность проводилась только тогда, когда это необходимо и соразмерно продвижению определенных целей национальной безопасности. ЭО также создает двухуровневый механизм для удовлетворения требований субъектов данных о том, что их персональные данные были собраны или обработаны США в нарушение применимого законодательства США, включая ЭО. На первом уровне Управление директора национальной разведки проведет расследование для оценки квалификационных требований и возможных средств правовой защиты. Под вторым ярусом,

ЭО не касается коммерческих условий Privacy Shield. Это уместно, учитывая недостатки, выявленные CEC в деле Schrems II, в котором основное внимание уделялось правительственному надзору и предполагаемым недостаткам возмещения ущерба. Обязанности ЭО ограничены государственными органами США; нет прямого влияния на сертификацию предприятий.

ЕО представляет собой значительные усилия правительства США по решению проблем, вызывающих обеспокоенность CJEU. Это гигантский шаг вперед на пути к обновленной системе трансатлантической передачи персональных данных.

Следующие шаги и практические советы

Следующим шагом для Европейской комиссии является определение того, достаточны ли новые обязательства США, включая ЭО, для восстановления структуры передачи персональных данных из ЕС в США. Ратификация ожидается весной 2023 года. Великобритания и Швейцария, вероятно, последуют их примеру, как только власти ЕС одобрят новый автомобиль.

Если в ЕС не будет принято решение о том, что новая структура является адекватной, организациям, стремящимся передать персональные данные из ЕС в США, придется продолжать полагаться на доступные альтернативные механизмы для такой передачи данных, такие как стандартные договорные положения, обязательные корпоративные правила и отступления. предусмотрено в GDPR для определенных ограниченных передач (например, когда передача необходима для выполнения контракта). Организации, получившие сертификат Privacy Shield, продолжают выполнять свои обязательства до тех пор, пока они не откажутся от участия…

Поскольку ожидается, что коммерческие условия новой платформы будут отражать условия Privacy Shield, организациям, которые в настоящее время сертифицированы в соответствии с Privacy Shield, рекомендуется придерживаться курса и оставаться сертифицированными. Импортеры данных, не сертифицированные в настоящее время в соответствии с Privacy Shield, должны внимательно следить за ситуацией и, когда новый механизм будет завершен, рассмотреть вопрос о том, обеспечит ли сертификация новой структуры более беспрепятственное решение для передачи данных». ***(Lisa J. Sotto, Aaron Simpson. Privacy Shield Redux: Looking Ahead to a New EU-U.S. Data Transfer Framework // CPO Magazine (https://www.cpomagazine.com/data-protection/privacy-shield-redux-looking-ahead-to-a-new-eu-u-s-data-transfer-framework/). 07.12.2022).***

***

«TikTok необходимо будет удалить с любых правительственных устройств в Южной Дакоте, поскольку штат станет первым, кто запретит приложение из соображений национальной безопасности. Перспектива

национального запрета TikTok витала в воздухе с последнего года правления администрации Трампа, при этом администрация Байдена, а также Конгресс и Комитет по иностранным инвестициям продолжают тщательно изучать приложение на предмет потенциальных рисков его использования в качестве шпионажа. или инструмент пропаганды китайского правительства.

Запрет TikTok в Южной Дакоте демонстрирует сохраняющиеся подозрения, несмотря на шаги по локализации пользовательских данных в США

Запрет Южной Дакоты TikTok распространяется на устройства государственных учреждений, сотрудников и подрядчиков; приложение больше нельзя загрузить или получить к нему доступ через веб-браузер в соответствии с указом, подписанным губернатором Кристи Ноем 29 ноября. Если устройство принадлежит или арендовано государством, TikTok больше не приветствуется на нем.

Ноем сослался на широко обсуждаемые проблемы национальной безопасности в качестве причины запрета TikTok, заявив, что Южная Дакота больше не будет участвовать в «операциях по сбору разведданных стран, которые нас ненавидят». Ноэм прямо обвинил Коммунистическую партию Китая в сборе личной информации через приложение, но до сих пор нет четких публичных доказательств того, что это происходит. Обеспокоенность национальной безопасностью больше основывается на законах о национальной безопасности Китая, которые позволяют правительству в любое время изымать любую информацию, хранящуюся на любых серверах в стране, без какого-либо ордера или судебного разбирательства. Другая проблема заключается в том, что китайское правительство может дать указание TikTok манипулировать своим алгоритмом рекомендаций для распространения пропаганды от его имени.

Ноэм также призвал Конгресс принять аналогичный запрет TikTok на федеральном уровне. Возможность отрицательного влияния TikTok на национальную безопасность обсуждается с 2020 года, когда администрация Трампа пригрозила ему запретом в магазинах приложений в США. TikTok избежал этой участи благодаря сочетанию обещания переместить все данные США за пределы

Китая и оградить их от страны брандмауэром, а также перехода в 2021 году к администрации Байдена, которая до сих пор гораздо медленнее рассматривала приложение.

Однако TikTok продолжает подвергаться тщательному анализу, особенно после недавних инцидентов, которые показали, что китайские инженеры и персонал, вероятно, все еще имеют доступ к пользовательским данным в США. В настоящее время основным объектом рассмотрения является Комитет по иностранным инвестициям (CFIUS), межведомственный орган, который занимается вопросами влияния иностранных денег или доступа к операциям США на национальную безопасность. Республиканская партия также недавно взяла под свой контроль Палату представителей на выборах 2022 года, и ее члены уже связались с TikTok, чтобы сообщить ему, что он, по-видимому, предоставил вводящую в заблуждение информацию и может ожидать дальнейшего изучения от законодателей в следующем году.

Однако существует двухпартийная обеспокоенность, поскольку директор ФБР Кристофер Рэй и министр финансов Джанет Йеллен также недавно выразили обеспокоенность по поводу того, как приложение может быть использовано Китаем для нарушения национальной безопасности. Сенатор-демократ и председатель сенатского комитета по разведке Марк Уорнер также заявил СМИ, что считает запрет TikTok неизбежным и что Конгрессу необходимо «стиснуть зубы» и добиться этого.

Опасения национальной безопасности по поводу TikTok теоретические, но вполне обоснованные

Новый виток проблем TikTok начался в начале этого года, когда множество просочившихся внутренних совещаний показало, что китайские инженеры сохранили большой доступ к пользовательским данным в США (несмотря на заверения в обратном). Американская сторона TikTok, по-видимому, не обладает техническими знаниями, необходимыми для того, чтобы делать все необходимое для поддержания функционирования платформы, и ей необходимо достаточно

часто обращаться к пекинскому персоналу, чтобы были открыты широкие пути доступа.

Так же, как TikTok пытался подавить эту проблему обещаниями, что китайские инженеры будут иметь доступ только к неконкретным данным для защиты личной информации, ноябрьское обновление политики конфиденциальности в ЕС показало, что жители блока теперь могут ожидать, что их данные будут переданы. с персоналом в Китае (наряду с рядом других третьих стран).

Раджив Пимпласкар, генеральный директор Dispersive Holdings, отмечает, что создаваемая этим угроза выходит за рамки китайского правительства. Потенциальное присутствие бэкдоров и широкий обмен данными с удаленными работниками и сторонними подрядчиками создает дополнительные риски безопасности, о которых должны знать пользователи TikTok: «Основная проблема здесь — растущее преобладание субъектов, представляющих угрозу на уровне государства, в структуре общедоступной облачной инфраструктуры. и интернет-приложения, которые могут создавать коварные бэкдоры и обходить типичные меры безопасности. Помимо управления черным списком поставщиков, правительствам и предприятиям необходимо более активно использовать передовые стратегии нулевого доверия, такие как скрытые сети, которые скрывают пользователей, приложения и данные и в первую очередь уменьшают сбор потенциально конфиденциальной информации».

Учитывая, что приложение имеет около 80 миллионов активных пользователей в месяц в Соединенных Штатах, или почти четверть населения страны, запрет TikTok на магазины приложений (как изначально предлагал Трамп), безусловно, вызовет бурю недовольства. Запрет на использование федеральным правительством по соображениям национальной безопасности, за которым, вероятно, вскоре последует принятие аналогичных запретов другими штатами, кажется более вероятным исходом в наступающем году. Но правительство может также попытаться повысить осведомленность о личных рисках, связанных с продолжением использования TikTok, наряду с постоянным давлением на

операции США, чтобы они полностью отделились от Китая». ***(Scott Ikeda. South Dakota Enacts TikTok Ban for Government Employees Over National Security Concerns // CPO Magazine (https://www.cpomagazine.com/data-privacy/south-dakota-enacts-tiktok-ban-for-government-employees-over-national-security-concerns/). 07.12.2022).***

***

«Наиболее часто используемое в мире приложение для обмена сообщениями, возможно, пострадало от утечки данных, затронувшей около 487 миллионов его пользователей, если верить публикации в даркнете.

Злоумышленник предлагает информацию по относительно низкой цене, разделяя ее по странам происхождения и предлагая каждый пакет по цене в диапазоне нескольких тысяч долларов. Еще неизвестно, является ли вся коллекция законной, но образцы, предоставленные хакерами, были проверены исследователями безопасности. Если полная утечка данных окажется законной, она повлияет примерно на четверть глобальной базы пользователей WhatsApp.

Масштабная утечка данных раскрывает личные телефонные номера, возможно, это была атака со скрейпингом API

Похоже, что утечка данных никоим образом не скомпрометировала сообщения WhatsApp, по крайней мере, судя по информации и образцам, размещенным в даркнете. Вместо этого он содержит номера телефонов, которые используются для проверки и создания учетной записи и которые обычно хранятся в тайне.

Хакер не стал раскрывать свои методы, но акцент на телефонных номерах, связанных с учетными записями (в сочетании с огромным масштабом утечки данных), указывает на уязвимость API как на наиболее вероятного виновника. В то время как скрытый номер телефона, скорее всего, имел бы некоторую непосредственную ценность только в том случае, если бы он принадлежал знаменитости или общественному деятелю, хакеры могут объединить его с другой доступной информацией о человеке (часто удобно доступной в массивных

«комбинационных файлах») и использовать ботов для бомбардировать цели мошенничеством и попытками фишинга. Особый риск представляют атаки типа «смишинг» и «вишинг», при которых используются текстовые сообщения и телефонные звонки для обхода обычных линий защиты.

В сообщении даркнета говорится, что информация была собрана в 2022 году и содержит записи из 84 стран. Некоторые из самых крупных наборов поступают из Египта (44 миллиона), Италии (35 миллионов), США (32 миллиона), Саудовской Аравии (29 миллионов), Франции и Турции (по 20 миллионов в каждой). Мало что известно об исполнителе угрозы, но вполне вероятно, что он не базируется в России, поскольку записи 10 миллионов пользователей WhatsApp в этой стране также были выставлены на продажу; неписаные правила приличия в регионе, как правило, не позволяют российским нападающим преследовать внутренние цели или союзников страны.

Злоумышленники запрашивают разные цены за набор данных каждой страны, при этом наибольшая сумма (7000 долларов США) запрашивается за набор из 32 миллионов телефонных номеров США. Это составляет немногим менее половины предполагаемых пользователей WhatsApp в стране. 817 американских номеров были среди выборки, подтвержденной исследователями безопасности как законные. Охранная фирма Check Point получила данные и сообщает, что в общей сложности они содержат не менее 360 миллионов законных телефонных номеров, но также указывает, что некоторые из них могут быть раздуты материалами из утечки данных Facebook в 2019 году.

В последнее время использование уязвимостей API для сбора информации из личных профилей стало более распространенным явлением, и ряд крупных технических платформ недавно подверглись атакам. Утечки данных сотен миллионов записей недавно были раскрыты Facebook и LinkedIn, и аналогичное крупное нарушение данных профиля Twitter, имевшее место в 2021 году, было только что бесплатно доступно на форуме темной сети. Хотя дыры в API, как правило, не позволяют злоумышленникам получить доступ к очень конфиденциальной информации, личные данные, представляющие определенную

ценность для преступников, могут быть извлечены быстро и в больших количествах практически без каких-либо трудностей со стороны безопасности компании (или даже обнаружения).

Парсинг API становится все более выгодным для злоумышленников

WhatsApp еще не подтвердил утечку данных, а представитель заявил, что единственным доказательством на данный момент являются необоснованные скриншоты, размещенные в даркнете. Преступники нередко берут старые материалы из предыдущих утечек данных и пытаются переупаковать их в новую коллекцию, надеясь совершить пару быстрых продаж в даркнете, прежде чем подпольные покупатели их обнюхают.

Независимо от фактического размера или легитимности утечки данных WhatsApp, ожидается, что уязвимости API станут одним из наиболее распространенных векторов атак в следующем году, по мнению ряда аналитиков по кибербезопасности. В дополнение к тому, что его легко найти и использовать, риск настолько низок, насколько это вообще возможно; во многих местах это даже не незаконное действие, а просто нарушение условий обслуживания платформы в худшем случае. Списки даркнета демонстрируют ценность, которую имеет даже довольно простая информация профиля.

И полученная информация неизбежно будет использоваться для подпитки незаконных действий через темную сеть, наиболее опасными из которых являются целенаправленные мошенничества и попытки фишинга. И это пиковое время года для такого рода деятельности, когда преступники пользуются безумием онлайн-покупок, которое проходит между распродажами в Черную пятницу / Киберпонедельник и Рождеством. Некоторые крупные компании, такие как Amazon, заметили, что количество попыток фишинга почти удвоилось за этот период года.

Альмог Апирион, генеральный директор и соучредитель CyoloКонтроль доступа на основе идентификации помогает компаниям интегрировать улучшенную систему безопасности, а также получать видимость и контроль над своими системами. Организации будут лучше оснащены для смягчения этих угроз

по мере их возникновения и защиты своих критически важных для бизнеса систем и информации». ***(Scott Ikeda. Nearly 500 Million WhatsApp Records Allegedly Stolen in Data Leak, Offered on Dark Web for a Few Thousand Dollars // CPO Magazine (https://www.cpomagazine.com/cyber-security/nearly-500-million-whatsapp-records-allegedly-stolen-in-data-leak-offered-on-dark-web-for-a-few-thousand-dollars/). 05.12.2022).***

***

«Уязвимость, которая присутствовала в API Twitter в 2021 году, вызвала утечку данных, которая раскрыла информацию о личном профиле пользователя, затронув не менее 5,4 миллиона из примерно 200–300 миллионов пользователей платформы (на тот момент). Информация теперь доступна бесплатно на темном веб-форуме.

Сообщается, что несколько сторон смогли очистить API, вставив в него номера телефонов и адреса электронной почты; совпадения с учетной записью вернут закрытый контакт и информацию об использовании платформы. Сообщается, что Twitter закрыл дыру в безопасности в январе 2022 года.

Утечка данных Twitter раскрыла личные адреса электронной почты и номера телефонов

Содержимое утечки данных было впервые выставлено на продажу на подпольном форуме в июле 2022 года, когда один из хакеров попросил 30 000 долларов за коллекцию из 5,4 миллиона пользовательских файлов Twitter. Уязвимость API раскрывала адрес электронной почты и номер телефона, связанные с учетной записью, а также город, в котором проживает пользователь (если указан), а также некоторые закрытые показатели использования и вовлеченности.

Неясно, отказалась ли та же сторона, которая выставила файлы на продажу в июле, и избавилась от коллекции, но, по-видимому, она была размещена на форуме в сентябре, а затем снова на другом публичном форуме в конце ноября. Сообщается, что частный обмен утечкой данных содержал дополнительные 1,4 миллиона скопированных профилей от пользователей Twitter, которые были

заблокированы, которые были собраны с использованием другого API. Сообщается, что тот, который в настоящее время доступен для публики по состоянию на ноябрь, не содержит информации о приостановленной учетной записи.

Хотя было подтверждено, что утечка 5,4 миллиона данных теперь находится в свободном доступе в нескольких СМИ, исследователь безопасности Чад Лодер полагает, что существует другая утечка данных, гораздо более крупная, которая все еще циркулирует в частном порядке среди злоумышленников. Он разместил образец в своих учетных записях Twitter и Mastodon, который связан с файлом, содержащим более 1,3 миллиона телефонных номеров, принадлежащих пользователям Twitter во Франции, набор данных, которого нет в предыдущей утечке.

Новый образец показывает, что неясно, сколько именно людей использовали уязвимость API до того, как она была исправлена, и 5,4 миллиона файлов могут быть лишь верхушкой айсберга. Другая утечка данных может содержать до 17 миллионов файлов и, как сообщается, имеет профили со всей Европы, а также из Израиля и США.

Уязвимости API создают возможности для мошенничества и фишинговых кампаний

Несмотря на то, что были высказаны серьезные опасения по поводу способности Twitter обезопасить себя, поскольку новый владелец Илон Маск сокращает персонал, этот инцидент произошел полностью под руководством предыдущего руководства (которое само находится под пристальным вниманием после того, как осведомитель Пайтер «Мадж» Затко дал показания Конгрессу о многочисленных проблемах бесхозяйственности в прошлом). Сентябрь). Воды заявлений Лодера также несколько омрачены его публичной позицией «антифашистского исследователя» и заявлениями против Маска; Недавно Лодер был отстранен от участия в Твиттере из-за обвинений в связях с группами Антифа, пропагандирующими политическое насилие (которые были сметены с платформы волной массовых банов в конце ноября), и его регулярное профилирование

предполагаемых фашистских деятелей, возможно, поставило его на неправильную сторону. иногда правила «доксинга» в Твиттере.

Но хотя проблема, похоже, возникла задолго до того, как Маск заинтересовался компанией, Ричард Берд (главный сотрудник службы безопасности Traceable) не уверен в том, что компания продолжает реагировать на проблему: «Сроки и путаница, отраженные в заявлениях Twitter для рынка о его последнем взломе, отражают широко распространенное непонимание рисков, связанных с API, а также неспособность своевременно защищать эти API. Twitter создал путь к неработающему эксплойту авторизации на уровне объектов, а затем решил, что никто не воспользовался этой ошибкой. К сожалению, это оказалось неверным. Это проблема с API; когда вокруг вас нет программы безопасности, плохие действия ничем не отличаются от действий обычных пользователей. Twitter просто не понимал разницы между вариантом использования и случаем злоупотребления в своем коде, и это то, что регулярно происходит с компаниями любого размера.

Даже если количество украденных профилей в Твиттере ближе к пяти миллионам, чем к десяткам миллионов, это все равно огромный объем данных, которые разбросаны по разным странам и, вероятно, будут использоваться в целевых схемах фишинга и конфиденциальности. Эксперты по безопасности советуют тщательно проверять любые электронные письма, которые, как представляется, исходят от Twitter, или любые прямые сообщения, полученные на платформе от ранее неизвестных сторон. Известные фишинговые подходы на платформе включают в себя тщательно созданные поддельные сообщения о приостановке действия учетной записи, проблемах со входом в систему и утверждениях о том, что проверенные учетные записи могут потерять свой статус, если они не предпримут никаких действий.

Инцидент показывает, что уязвимости API по-прежнему живы и здоровы, и хотя они могут не обеспечивать немедленную точку входа в сети, их можно использовать для создания брешей. Некоторые эксперты по безопасности считают, что атаки через API могут стать очень популярными и даже могут стать самым

распространенным типом атак в следующем году. По крайней мере, одно исследование показало, что почти каждая компания сталкивалась с проблемой безопасности API, и что в 20% этих случаев это приводило к утечке или взлому данных.

Брайан Джонсон, начальник службы безопасности Armorblox, полагает, что умные злоумышленники попытаются использовать общие проблемы безопасности Twitter в сочетании с этой утечкой данных: «Нарушения, раскрывающие адреса электронной почты и номера телефонов, почти всегда сопровождаются целевыми кампаниями фишинга и SMiShing. Учитывая, что Twitter в последнее время также часто фигурирует в новостях, злоумышленники могут использовать наши когнитивные предубеждения, такие как предубеждение относительно новизны, для отправки поддельных электронных писем или SMS-сообщений для сброса пароля пользователям Twitter с целью кражи их учетных данных. Украденные пароли теперь позволяют им опробовать эти пароли на других сайтах, потому что многие пользователи используют один и тот же пароль у разных провайдеров. Мы рекомендуем пользователям настроить многофакторную аутентификацию во всех своих личных и рабочих учетных записях и, в частности, следить за подозрительными электронными письмами, которые кажутся исходящими из Twitter». ***(Scott Ikeda. Data Leak Exposes Private Profile Information of 5.4 Million Twitter Users, Dumped for Free on Underground Forum // CPO Magazine (https://www.cpomagazine.com/cyber-security/data-leak-exposes-private-profile-information-of-5-4-million-twitter-users-dumped-for-free-on-underground-forum/). 02.12.2022).***

***

«The Wall Street Journal сообщает, что утечка внутренних документов Meta раскрывает как минимум год внутреннего злоупотребления инструментом восстановления учетных записей различными сторонами, которые брали взятки в размере до нескольких тысяч долларов за

восстановление заблокированных учетных записей, а в некоторых случаях даже играли в азартные игры. роль соучастника в захвате аккаунта.

Мошеннические сотрудники и подрядчики злоупотребили внутренней функцией под названием «Oops», которая в первую очередь предназначена для внутреннего восстановления учетных записей сотрудников и деловых партнеров. Все более широкий доступ к этому инструменту привел к резкому росту злоупотреблений, поскольку в период с 2017 по 2020 год его использование увеличилось более чем вдвое.

Быстрое обслуживание, взлом аккаунта были доступны по цене в Facebook и Instagram.

Любой, кто когда-либо терял доступ к учетной записи Facebook, знает, что процесс восстановления учетной записи в лучшем случае обременительный, а в некоторых случаях невозможен. У Meta никогда не было ничего, кроме костяка команды, обслуживающей клиентов, которая полагалась на крайне несовершенные автоматизированные инструменты и алгоритмы для обработки подавляющего большинства запросов о помощи с заблокированными или украденными учетными записями. В отчаянии, чтобы связаться с настоящим человеком, некоторые обратились к покупке гарнитур Oculus VR (которые стоят сотни долларов) просто потому, что в этом филиале компании есть специальная линия обслуживания клиентов для владельцев оборудования.

В то время как большинство людей с трудом восстанавливают учетную запись Facebook или Instagram, избранная группа инсайдеров и известных общественных деятелей получает специальный доступ для быстрого решения своих проблем. Внутренний инструмент Meta «Онлайн-операции» (Oops) предназначен для них, предоставляя личный канал электронной почты, доступный для определенных квалифицированных лиц, когда у них возникают проблемы с учетной записью. Сообщается, что этот канал существует уже много лет, но не сталкивался с серьезными проблемами до недавнего времени, когда количество внутренних сотрудников, получивших к нему доступ, резко возросло.

Одним из источников всплесков злоупотреблений Oops, по-видимому, является подрядчик Allied Universal, который обеспечивает физическую безопасность объектов Meta. Охранникам, размещенным на этих объектах, по-видимому, был предоставлен доступ к Oops, несмотря на то, что они были сторонними подрядчиками, и просочившиеся документы указывают на то, что некоторая сумма быстро получила побочный эффект от этого доступа. Документы показывают, что некоторые из этих сторон брали взятки (или «взносы») в размере до 7000 долларов, чтобы либо ускорить восстановление учетной записи посторонней стороны, которая обычно не имеет доступа к Oops, либо просто помочь с чьей-то схемой захвата учетной записи.

Документы являются частью внутреннего расследования проблемы, заказанного руководителями Meta. После того, как была обнаружена активная торговля доступом к Oops, по сообщениям, прошла волна увольнений как сотрудников Meta, так и подрядчиков, которые получали прибыль от системы. Неясно, когда Oops впервые стал доступен, но документы показывают, что его использование неуклонно росло с 22 000 запросов в 2017 году до более 50 000 в 2020 году.

Инструмент восстановления аккаунта ограничен после внутреннего расследования

Система Oops позволяла сотрудникам Facebook (и некоторым подрядчикам) отправлять по электронной почте личный адрес с адресом электронной почты учетной записи, которую они хотели бы восстановить. Пока запрос исходил из утвержденного источника, правила, регулирующие это, казались довольно свободными, что позволяло сотрудникам запрашивать услугу ускоренного восстановления учетной записи от имени семьи, друзей и деловых партнеров. Сотрудников попросили только указать, был ли запрос от имени личного контакта, делового партнера Meta, знаменитости или члена личной команды Марка Цукерберга.

По крайней мере, один из этих внутренних источников снабжал стороннюю службу восстановления учетных записей, которая взимала с людей тысячи

долларов за этот специальный доступ. Один из случаев, перечисленных WSJ, касается модели Instagram, которая заплатила 7000 долларов одному из этих сервисов, владелец которого подтвердил, что у них был «внутренний контакт» в Meta, который способствовал восстановлению аккаунта.

В отчете также указывается, что некоторые из уволенных подрядчиков не хотели отказываться от этой прибыльной побочной работы после того, как их выгнали из помещения, и обратились к сотрудникам Facebook с просьбой помочь в схемах захвата аккаунтов Instagram. Одному из них, имя которого упоминается во внутренних документах и с которым беседовали, угрожали обвинениями в соответствии с Законом о компьютерном мошенничестве и злоупотреблениях. Мужчина утверждает, что охранники информируются о сервисе Oops в рамках трудоустройства, но не сообщают о каких-либо ограничениях на его использование. Meta говорит, что проводит стандартное обучение использованию Oops в рамках процесса адаптации, включая обучение фишингу.

В общей сложности около 24 сотрудников и подрядчиков Meta были уволены за получение взяток или захват аккаунтов. Meta сообщила СМИ, что предприняла «соответствующие действия» для защиты системы. В последнее время угон учетных записей становится все более серьезной проблемой, поскольку преступники находят новые творческие способы монетизации учетных записей социальных сетей, которые ранее считались слишком малоценными для того, чтобы тратить реальную энергию на атаку». ***(Scott Ikeda. Document Leak Reveals Meta Employees Took Bribes To Use Account Recovery Tool for Expedited Service, Account Hijacking // CPO Magazine (https://www.cpomagazine.com/cyber-security/document-leak-reveals-meta-employees-took-bribes-to-use-account-recovery-tool-for-expedited-service-account-hijacking/). 02.12.2022).***

***

«После решения по делу Schrems II ведущие регуляторы данных ЕС в значительной степени приняли абсолютистскую точку зрения о том, что любой потенциальный ущерб из-за перехвата данных иностранным

правительством (даже если он незначительный) является нарушением Общего регламента по защите данных и что эти правительства должны продемонстрировать паритет с bloc законы о конфиденциальности данных, прежде чем они смогут стать надежным партнером. В новом документе транснациональных корпораций глобального права DLA Piper и Clifford Chance излагаются аргументы в пользу основанного на оценке риска подхода к этой международной передаче данных, утверждая, что статус-кво слишком обременительный и что экспортеры данных страдают от несправедливого бремени в условиях «незаконно строгого толкование постановления Шремса.

Следует ли заменить «деспотичные» условия GDPR подходом, основанным на оценке рисков?

Текущая позиция надзорных органов ЕС по защите данных заключается в том, что статья 46 GDPR полностью запрещает передачу данных (без надежных гарантий) в страну, не входящую в ЕС, если есть основания полагать, что правительство этой страны перехватывает международную передачу данных для любой цели. Однако так было только в середине 2020 года. Эта точка зрения основана на решении Schrems II, в котором основное внимание уделялось передаче данных в Соединенные Штаты; утечки разведывательной информации Эдварда Сноудена и несколько официальных политик (раздел 702 Закона о наблюдении за внешней разведкой, Исполнительный указ 12333 и Директива президента 28), которые позволяют спецслужбам США без разбора собирать личную информацию лиц за пределами страны, которые не являются обязательно под следствием или подозрением в чем-либо.

Хотя дело Шремса было сосредоточено на данных, отправленных в США, политика ЕС теперь распространяется на международную передачу данных со всеми странами, не входящими в ЕС. DLA Piper утверждает, что следует вернуться к подходу, основанному на индивидуальном риске, учитывая, что, по крайней мере, в некоторых случаях риск фактического вреда для отдельных лиц несущественен. И, помимо того, что они несправедливы по отношению к некоторым предприятиям, на которые они распространяются, драконовские условия просто поощряют

«широко распространенное несоблюдение», что в конечном итоге хуже для субъектов данных.

Часть этого аргумента в пользу обычного человека заключается в том, что обмен жизненно важной информацией может быть затруднен во время кризиса, такого как пандемия Covid-19 и война в Украине. Но документ выходит за рамки простого мнения и взывает к сочувствию к отдельным лицам и предприятиям, испытывающим трудности, и доказывает, что предыдущие решения, связанные с условиями GDPR, устанавливают, что для международной передачи данных должен требоваться подход, основанный на оценке риска.

Дело об изменении точки зрения на международную передачу данных

Юридический аргумент сосредоточен на статье 45 GDPR, которая регулирует принятие решений об адекватности, и статье 46, которая устанавливает условия для передачи в страны, которые не считаются адекватными партнерами по данным. Статья 46 устанавливает условия Стандартных договорных пунктов (SCC), которые разрешают эти передачи, если личные данные по существу зашифрованы и защищены на удаленном конце, так что субъекты данных могут быть уверены, что иностранное правительство не перехватывает их по пути.

Статья 46 была в центре внимания решения Шремса II, поскольку предыдущая схема передачи (Safe Harbor) позволяла гораздо больше свободы действий при разработке SCC. После Schrems II SCC продолжают функционировать, но подлежат гораздо более тщательной проверке (например, обязательной оценке воздействия). Некоторые компании, такие как Facebook, открыто обдумывали возможность полного выхода из ЕС, если непрекращающаяся цепочка юридических баталий, связанных с этими условиями, в конечном итоге не приведет к желаемому результату.

Аргумент риск-ориентированного подхода DLA Piper относится к фундаментальному принципу «соразмерности», заложенному в основу права ЕС (статья 5(4) Договора о Европейском Союзе). По сути, это гласит, что свобода ведения бизнеса является фундаментальным правом наряду с неприкосновенностью частной жизни, и, следовательно, налагаемые на нее

ограничения должны быть соразмерными, применяться только в случае необходимости и действительно отвечать необходимости защиты прав и свобод других лиц.

Таким образом, аргумент состоит в том, что баланс между деловыми и личными правами слишком сильно смещен в сторону бизнеса. То, что описывается как несправедливое бремя соблюдения требований для предприятий, может быть облегчено с помощью подхода, основанного на оценке рисков, который потребует от предприятий взять на себя эти дополнительные обязанности только в тех случаях, когда можно определить, что реальный вред может быть нанесен субъекту данных в результате иностранного перехвата. конкретных передаваемых данных.

Далее в аргументе отмечается, что сам GDPR признает принципы пропорциональности в Декларации 4, в которой говорится, что право на защиту персональных данных не является «абсолютным правом». Некоторые предыдущие прецеденты, такие как решение Lindqvist от 2003 года, похоже, подтверждают концепцию рассмотрения права на ведение бизнеса в противовес правам на конфиденциальность данных.

На данный момент аргумент в пользу подхода, основанного на оценке риска, не более чем мнение, опубликованное в блоге. Тем не менее, некоторые считают, что у него достаточно достоинств, чтобы в конечном итоге получить юридическую поддержку в споре о том, как международная передача данных регулируется GDPR. Гуннар Сакс, член глобальных групп по защите технологий и данных в Clifford Chance, комментарии: «Направление движения судебных решений после Шремса II рискует создать де-факто запрет на международную передачу данных в определенные страны. Это не соответствует самому решению Schrems II, в котором CEC фактически просил европейских экспортеров данных не полагаться на абсолютистскую интерпретацию GDPR, возлагая на них задачу независимого проведения индивидуальных оценок для каждого ограниченного Передача данных. Пропорциональный подход позволяет экспортерам данных соответствующим образом калибровать средства защиты и выделять больше ресурсов на те передачи, которые представляют реальный риск причинения вреда субъектам данных». ***(Scott***

Ikeda. Risk-Based Approach to International Data Transfers Necessary to the Future of Cross-Border Data Flows Under GDPR // CPO Magazine (https://www.cpomagazine.com/data-protection/risk-based-approach-to-international-data-transfers-necessary-to-the-future-of-cross-border-data-flows-under-gdpr/). 01.12.2022).

***

«Американский закон о защите конфиденциальности данных (ADPPA) является первым общенациональным законопроектом о конфиденциальности в США, который имеет шанс быть принятым в законодательном порядке и изменить облик всего ландшафта конфиденциальности в США. На сегодняшний день адвокаты, ученые, некоммерческие организации и политики из разных школ все еще высказывают различные опасения по поводу законопроекта, в частности, насколько он будет эффективным и в какой степени он будет применяться.

Тем не менее, существует общее мнение, что, когда речь идет конкретно о правилах минимизации данных, предложенные ADPPA рекомендации могут значительно изменить процессы и процедуры, которые предприятия будут использовать для сбора данных о потребителях. Но остановится ли на этом изменение минимизации данных? Мы верим, что ответ «нет», и надеемся, что его влияние выйдет далеко за рамки формального правоприменения.

Минимизация данных привлекает особое внимание законодателей

Из всех своих разделов и пунктов особое внимание ADPPA уделяет минимизации данных. Правда, при сравнении ADPPA с другими правилами конфиденциальности, такими как GDPR или CCPA, жесткость раздела минимизации данных может показаться не особенно уникальной. Он даже предоставляет предприятиям немного больше свободы, чем старшие братья и сестры. Но по сравнению с остальными положениями о конфиденциальности в ADPPA (которые, кажется, появляются в наши дни), раздел минимизации данных выделяется, как клоун на свадьбе с черным галстуком.

В то время как многие разделы предложенного законопроекта о правах на неприкосновенность частной жизни расплывчаты или несколько нечетки (что, возможно, является результатом того, что ADPPA является двухпартийным законопроектом), раздел минимизации данных является более строгим и дает меньше свободы для толкования или лазейку для минимизации правоприменение.

Поскольку в законопроекте в первую очередь используется подход к минимизации данных, предприятиям разрешено собирать только тот объем данных, который им разумно необходим, и только по определенному набору причин. Это сводит к минимуму риск злоупотребления личными данными отдельных лиц, намеренно или случайно, со стороны самой компании или внешнего хакера.

Как это происходит?

ADPPA требует от компаний свести к минимуму сбор и использование данных.

Де-факто это означает, что предприятия и другие организации имеют право собирать, обрабатывать и передавать персональные данные только в той мере, в какой это необходимо и пропорционально их предложению, и не более того. Также интересно отметить, что в этом смысле ADPPA даже выходит за рамки других законов, а именно CCPA, и применяет эти ограничения также к некоммерческим организациям и малому бизнесу (хотя у них есть некоторые исключения).

В качестве дополнительного уровня требований к минимизации данных ADPPA запрещает передачу или совместное использование особо конфиденциальной личной информации, такой как номера социального страхования, биометрические данные и т. д. идти. Наконец, ADPPA расширяет ограничения и инструктирует бизнес о том, что делать для достижения этих практик. Вещи не оставлены на волю случая. Компании должны внедрить принципы конфиденциальности путем разработки политик и процедур, обеспечивающих соблюдение стандартов конфиденциальности в своих продуктах и услугах. Эти политики и процедуры должны также уделять особое внимание снижению рисков для детей в возрасте до 17 лет. Владельцы крупных данных также должны будут предоставлять метрики и отчетность, а также представлять

ежегодную оценку воздействия, если они используют алгоритм, который представляет «косвенный риск причинения вреда». Наконец, большинству предприятий придется раз в два года представлять оценку воздействия на конфиденциальность.

ADPPA также требует, чтобы предприятия предоставляли физическим лицам возможность доступа, исправления, удаления и предотвращения передачи их информации, аналогично правам, предоставляемым GDPR и CCPA. Это последний способ для ADPPA достичь своих целей по минимизации данных. Во-первых, инструктируя бизнес, что делать. Во-вторых, определяя, как они должны это делать. В-третьих, демократизация минимизации данных для потребителей путем изъятия части контроля из рук предприятий и предоставления отдельным лицам возможности действовать в рамках системы сдержек и противовесов (удваивая роль субъектов интересов), чтобы помочь обеспечить минимизацию данных.

Чтобы прояснить этот момент, раздел минимизации данных даже появляется в разделе «Обязанность лояльности», т. е. минимизация данных должна осуществляться на основе доверия и прозрачности. Это означает, что компании должны быть в состоянии продемонстрировать, что они сделали все возможное при работе с личными данными.

17 разрешенных целей сбора данных

Но есть еще кое-что. В то время как обработка данных разрешена только для «разумно необходимых и пропорциональных» требований для предоставления продуктов или услуг по запросу человека, ADPPA разрешает сбор данных для одной или нескольких из семнадцати определенных целей. К ним относятся, среди прочего, выполнение транзакции, разработка или ремонт продукта или услуги, а также отзыв продукта.

По сравнению с другими законами о конфиденциальности, и особенно с калифорнийским CCPA (и CPRA), с которым часто сравнивают ADPPA, ADPPA является более разрешительным в своих случаях использования для сбора данных. В частности, ADPPA слабее разрешает сбор данных для рекламных и маркетинговых целей, включая целевой маркетинг.

Остановится ли здесь доллар?

Сторонники ADPPA пытаются протолкнуть законопроект и принять его в законодательном порядке. Они утверждают, что ADPPA, наконец, закрепит единый общеамериканский стандарт конфиденциальности с четкими рекомендациями по минимизации данных. Прежде всего, утверждают они, это поможет большинству граждан США, которые в настоящее время не защищены законами о минимизации данных, пользоваться преимуществами защиты своих данных.

Но в ADPPA может быть нечто большее, чем просто непосредственные последствия принятия законопроекта. ADPPA не должно быть концом общенациональных дебатов и пути к конфиденциальности в США. Скорее, это может быть ее началом.

GDPR и CCPA предусматривали местные юридические требования и ограничения, но их влияние распространилось далеко за пределы страны. GDPR вдохновил глобальные инициативы и правила в отношении конфиденциальности как в государственном, так и в частном секторах. Например, одной из самых последних громких частных инициатив было требование Apple, чтобы владельцы приложений легко разрешали удаление учетных записей.

GDPR также произвел революцию в глобальных дебатах и повысил осведомленность о важности личной конфиденциальности. Отношение общественности к конфиденциальности четко разграничено на две части: до GDPR и после GDPR.

Законодательство CCPA и последующие дебаты также имели эффект снежного кома. CCPA превращается в CPRA, что, в свою очередь, влияет на саму нынешнюю ADPPA — как с точки зрения формирования законодательства ADPPA, так и с точки зрения самой роли в обсуждении ADPPA.

Для жителей Калифорнии ADPPA в нынешнем виде — это шаг назад. Неудивительно, что Калифорнийское агентство по защите конфиденциальности недавно проголосовало против текущего состояния ADPPA и любого законопроекта, который вытесняет CCPA.

Но общенациональный законопроект, помимо его юридических последствий, почти наверняка вызовет общенациональные дебаты за пределами Калифорнии. Такие дебаты могли бы помочь повысить осведомленность граждан США, помочь переформулировать общие концепции минимизации данных и пересмотреть то, как предприятия взаимодействуют с данными своих клиентов и используют их. На глобальном уровне США могли бы возглавить работу по информированию глобальных компаний и вдохновить законы о конфиденциальности в странах, которые еще не завершили этот процесс. Хотя ADPPA ни в коем случае не является первым или самым обширным регулированием конфиденциальности, глобальное влияние США само по себе имеет достаточно влияния, чтобы вызвать волновые эффекты и изменения из-за их ведущей роли в глобальном экономическом и техническом ландшафте.

Также есть что сказать об относительной гибкости ADPPA по сравнению с жесткостью GDPR. В то время как многие высказывают опасения, что это означает, что предприятиям сойдет с рук деятельность, направленная против конфиденциальности, более мягкий подход ADPPA также позволяет компаниям смягчить такие правила и внедрить их без стресса, сохраняя при этом подход, ориентированный на потребителя, а не на работу. исключительно из страха быть оштрафованным. Это особенно важно для компаний, которые хотят поступать правильно со своими клиентами, но не имеют огромной команды юристов или штатных специалистов по конфиденциальности, которые могли бы помочь им внедрить и собрать все движущиеся части немедленно и эффективно. Для многих этот подход, ориентированный на конфиденциальность, вероятно, является новым и требует корректировок и привыкания.

Поскольку ADPPA реализуется путем защиты прав потребителей, здесь есть возможность создать новую динамику взаимодействия между бизнесом и потребителем — вместе. Тот, который построен на доверии и правильных действиях, но без поиска виноватых или обвинений, которые могут сопровождать агрессивные реформы.

Для профессионалов в области конфиденциальности четкое федеральное требование может даже стать важной ступенькой к достижению целей конфиденциальности с внутренними заинтересованными сторонами вместо того, чтобы им приходилось вести непростые сражения, как многим приходится делать сегодня.

Что делать сегодня

Эти дебаты о минимизации данных и конфиденциальности реальны, даже до того, как (и если) ADPPA будет установлен в камне. Это означает, что его влияние реально, и мы считаем, что это влияние будет усиливаться по мере того, как дебаты по ADPPA станут более громкими. С демократической точки зрения это благо, поскольку наша культура и нормы формируются голосами разных игроков. Как бизнес, стоит подумать о том, как опередить игру и извлечь выгоду из уже происходящих изменений.

Мы считаем, что результаты ADPPA понравятся игрокам, которые примут принципы минимизации данных и конфиденциальности. ADPPA также облегчит компаниям внедрение методов стандартизации, таких как внедрение «золотого правила», стандартизированного способа обработки запросов на конфиденциальность, независимо от географического местоположения, что может сделать использование прав на конфиденциальность для компаний более беспрепятственным, принимая во внимание требования к учетной записи, как с точки зрения соответствия, так и как способ создания чувства доверия и прозрачности с клиентами». ***(Gal Ringel. The ADPPA Butterfly Effect: Limited Bill, Broad Consequences // CPO Magazine (https://www.cpomagazine.com/data-protection/the-adppa-butterfly-effect-limited-bill-broad-consequences/). 06.12.2022).***

***

«Штат Калифорния повышает ставки на конфиденциальность данных для компаний, которые обрабатывают личную информацию своих жителей, с новыми правилами, вступающими в силу 1 января на основе недавно принятого Закона о правах на конфиденциальность в Калифорнии (CPRA).

CPRA является продолжением действующего Закона о конфиденциальности потребителей Калифорнии (CCPA), который основывается на его основах и расширяет требования к предприятиям, которые обрабатывают конфиденциальную личную информацию жителей Калифорнии (SPI).

Новый CPRA является частью общенациональной тенденции, когда отдельные штаты США откликнулись на призывы своих жителей решить растущую проблему конфиденциальности данных. Калифорния присоединилась к этой инициативе по обеспечению конфиденциальности Коннектикут, Колорадо, Юта и Вирджиния — все они приняли законы, регулирующие обработку конфиденциальной личной информации и защищающие конфиденциальность данных своих жителей.

В этой статье я рассмотрю, как CPRA расширяет определения и сферу действия CCPA, как предприятия должны думать о соблюдении CPRA и что CPO могут сделать, чтобы помочь своим компаниям обеспечить эффективное и беспрепятственное соблюдение CPRA.

CPRA в двух словах

Итак, на какие компании влияет CPRA и какие типы данных регулирует CPRA? И какие права он предоставляет жителям Калифорнии (и каким жителям)?

Компании, затронутые CPRA

CPRA расширяет и изменяет Закон Калифорнии о конфиденциальности потребителей от 2018 года несколькими способами. Общим для обоих законов является то, что они применяются к любой компании с доходом в 25 миллионов долларов США, которая соответствует любому из следующих двух дополнительных критериев:

Ежегодно продавать, покупать, получать или делиться личной информацией 100 000 или более потребителей в Калифорнии в коммерческих целях. Это обновление добавляет слово «доля» к формулировкам предыдущего закона и повышает пороговое значение для жителей Калифорнии с 50 000 до 100 000 (за исключением малых предприятий).

Получать 50% или более своего годового дохода от продажи или показа целевой рекламы с использованием личной информации. Это добавляет «выполнение целевой рекламы» к формулировкам предыдущего закона.

Если бы эти изменения были в полной мере обновлениями CPRA, оценка того, влияет ли CPRA на ваш бизнес, была бы простой. Но эта простая оценка может ввести в заблуждение, если не учитывать два смешанных фактора: расширение CPRA того, какая личная информация защищена, и расширение защиты CPRA за пределы потребителей.

Какие типы данных защищает CPRA?

CPRA определяет конфиденциальную личную информацию (SPI), чтобы расширить объем защищаемой информации по сравнению с предыдущим законом, который определял категорию данных, называемую личной информацией (PI), и устанавливал требования к этой информации. Это означает, что в дополнение к защите более распространенных форм личной информации в соответствии с текущими требованиями каждая компания, на которую может повлиять CPRA, должна оценить, обрабатывают ли они (и как) личную информацию, относящуюся к любому из следующего:

Номера водительских прав

Номера социального страхования (SSN)

Государственные идентификационные номера

Членство в Союзе

Номера паспортов

Учетные данные пользователя, такие как имена пользователей и пароли

Биометрические данные и генетика

Этническое или расовое происхождение

Точные геолокации

Религиозные или философские убеждения

Информация о сексуальной ориентации, сексуальной жизни или здоровье потребителя.

Содержимое текстовых, почтовых и электронных писем потребителя

Этот список стоит большего, чем краткий обзор, особенно с учетом того, что, хотя некоторые из этих типов данных (например, геолокация) могут быть четко идентифицированы в системах и службах, используемых вашей компанией, другие, такие как информация о философских или религиозных убеждениях, могут быть найдены внутри текстовых полей или неструктурированных данных, которые вы можете пропустить при беглом просмотре. Для CPO это означает, что любые инструменты, которые вы используете для идентификации личной информации, должны быть проверены и обновлены, чтобы гарантировать, что они могут идентифицировать эти типы личной информации.

Еще один аспект CPRA, требующий тщательного рассмотрения, касается того, какие жители Калифорнии защищены CPRA.

Кого защищает CPRA?

CPRA вносит поправки в Калифорнийский закон о конфиденциальности потребителей, который (как следует из названия) регулирует конфиденциальность данных потребителей. Но CPRA не только защищает потребителей и не только регулирует работу компаний, ориентированных на потребителей.

CPRA защищает жителей Калифорнии, которые находятся в деловых отношениях с компаниями, затронутыми CPRA, отменяя предыдущее исключение для данных B2B и HR. Это означает, что CPRA регулирует сбор личной информации сотрудников, включая инструменты управления персоналом и соответствующие политики и процедуры обработки данных. И это также означает, что CPRA влияет на компании B2B, которые не взаимодействуют с потребителями, но обрабатывают данные потребителей.

Итак, какие права CPRA предоставляет жителям Калифорнии?

Расширение прав по CPRA

CPRA расширяет права, предоставленные жителям Калифорнии Законом о конфиденциальности потребителей Калифорнии, который предоставляет такие права, как доступ к личной информации, право запрещать продажу этой информации и право на равное обслуживание и цену после отстаивания этих прав.

CPRA добавляет в этот список следующие новые права:

Право на исправление неточностей, чтобы жители могли не только получить доступ к личной информации, но и потребовать ее исправления.

Право ограничивать использование и распространение конфиденциальной личной информации.

Право отказаться от целевой рекламы

Наряду с этими изменениями у CPRA появился новый подход к правоприменению, создание нового агентства и усиленное право частных действий.

Правоприменение CPRA

Предшественник CPRA обеспечивался Генеральной прокуратурой Калифорнии, но CPRA использует новый подход с созданием нормотворческого и правоприменительного агентства и расширением частного права на иск:

Правоприменение со стороны Калифорнийского агентства по защите конфиденциальности (CPPA): ранее Генеральная прокуратура Калифорнии отвечала за принудительные действия, связанные с нарушениями прав на неприкосновенность частной жизни. С принятием CPRA было создано новое правоприменительное агентство - CPPA. Наряду с принятием мер по устранению нарушений прав на неприкосновенность частной жизни перед CPPA также стоит задача просвещения общественности и разъяснения того, как он будет интерпретировать CPRA в целях обеспечения соблюдения. Существование этого нового агентства означает, что CPO и другие лидеры в области конфиденциальности должны добавить веб-сайт CPPA в закладки и часто его проверять.

Правоприменение посредством частного права на иск: Калифорнийский закон о конфиденциальности потребителей допускает частное право на иск в случае утечки данных, связанной с незашифрованной личной информацией. CCPA расширяет это частное право действий, включая любое нарушение, связанное с именем пользователя (часто принимающим форму адреса электронной почты) в сочетании с паролем или ответами на контрольные вопросы. Целью этого

изменения является снижение частоты утечек данных, которые могут привести к компрометации и неправомерному использованию учетных записей пользователей.

Как CPO могут привести к конфиденциальности данных и соблюдению CPRA

Вот мой список действенных шагов, которые помогут вашей организации стать более активной в защите личной информации, чтобы вы были готовы, когда CPPA начнет применять CPRA, а также готовы обрабатывать любые новые законы или правила о конфиденциальности данных, которые другие штаты или другие регулирующие органы, как и федеральное правительство США, может создать:

Следуйте принципам минимизации данных. На самом базовом уровне минимизация данных начинается с проверки того, что вам действительно нужен определенный тип личной информации или конфиденциальной личной информации, прежде чем собирать ее. Затем вам следует провести инвентаризацию конфиденциальных данных, чтобы оценить, какие типы личной информации вы собираете. После завершения инвентаризации данных еще раз проверьте, почему вы собираете эти данные, где они хранятся (по базе данных и стране), кто имеет к ним доступ и как долго данные будут храниться. Вы можете реализовать элементы управления минимизацией данных, используя методы повышения конфиденциальности, такие как маскирование, токенизация, полиморфное шифрование и деидентификация.

Внедрите и соблюдайте принципы хранения данных: после того, как вы определили, какую личную информацию вы собираете, вы должны определить, как долго вам нужно хранить эти данные, а затем разработать официальную программу и политику хранения данных, чтобы гарантировать, что вы не сохраняете личную информацию. дольше, чем это необходимо.

Укрепляйте и периодически пересматривайте меры безопасности. Конфиденциальность данных невозможна без обеспечения безопасности, поэтому поддержание шифрования, аутентификации и других элементов управления в актуальном состоянии имеет решающее значение для защиты конфиденциальных

данных, доверенных вам вашими клиентами. кража или несанкционированное использование.

Внедрение эффективного управления данными. Внедрение управления данными начинается с сопоставления и инвентаризации данных, чтобы определить, какие типы личной информации вы собираете, классифицировать отдельные наборы данных и понять, где эти данные хранятся, кому они передаются и почему. Если применимо, рассмотрите возможность классификации этих данных как личной информации, конфиденциальной личной информации и т.д. И не забудьте включить данные, обрабатываемые вашими поставщиками. Затем, оценив состояние конфиденциальных данных вашей организации, пришло время внедрить или усилить контроль доступа на основе учетных записей или ролей, чтобы вы могли гарантировать, что доступ к конфиденциальным данным предоставляется только для авторизованных рабочих процессов в случае необходимости.

Подготовьтесь к запросам субъектов данных: Запросы субъектов данных были впервые введены GDPR, но также присутствуют в CPRA. Такие запросы обычно делятся на две категории: запросы на доступ субъекта данных (DSAR), которые позволяют отдельным лицам или другим организациям запрашивать копию данных о себе, и запросы о праве на забвение (RTBF), которые позволяют отдельным лицам или другим организациям запрашивать обнаружение и удаление всех данных о себе. CPRA расширяет это, добавляя право потребителям и другим организациям исправлять данные о себе. Мой ориентир здесь? Если вам нужно поддерживать этот процесс для клиентов в Калифорнии и ЕС, вы должны опережать события и относиться ко всем своим клиентам как к жителям Калифорнии и ЕС. Таким образом, вы не будете застигнуты врасплох, когда новый закон или нормативный акт включают положения DSAR или RTBF.

Оценка и снижение рисков, связанных с конфиденциальностью данных. Вы должны задать себе и своей организации вопросы о мерах безопасности и средствах контроля, которые у вас есть для защиты конфиденциальных данных клиентов. Такие вопросы, как: где находятся наши конфиденциальные данные и можно ли сделать их более централизованными, чтобы предотвратить их

разрастание? Кто имеет доступ к этим данным, сколько и для каких целей? Затем примите меры по реализации мер безопасности для решения любых проблем, которые вы обнаружите. Применяя глобальный подход к ответам на эти вопросы и устраняя любые обнаруженные пробелы, вы можете помочь снизить риск утечки данных.

Примите глобальную структуру конфиденциальности. В индустрии конфиденциальности разработаны некоторые стандартные отраслевые рамки конфиденциальности. Для начала рекомендую ознакомиться с фреймворком конфиденциальности от NIST. Вы можете найти аналогичные структуры от других органов по стандартизации кибербезопасности и конфиденциальности.

Ознакомьтесь с постановлениями FTC о согласии на конфиденциальность и мерами законодательства штата по обеспечению соблюдения конфиденциальности. Внимательное прочтение постановлений FTC о согласии на конфиденциальность и мер по обеспечению соблюдения конфиденциальности штата — отличный способ узнать, как избежать дорогостоящих и досадных ошибок в отношении конфиденциальности. Существующие постановления FTC о согласии содержат рекомендации о методах, которых компании должны избегать, чтобы избежать принудительных действий FTC. И, как недавно обнаружил производитель косметики Sephora, когда они согласились на 1,2 миллиона долларов, раскрытие передачи личной информации клиентов третьим сторонам не заменяет предоставление клиентам простого способа отказаться от обмена данными.

Следование этим рекомендациям поможет привести вашу организацию в соответствие с техническими требованиями CPRA. Такая бдительность позволяет перейти от реактивного подхода к реагированию на каждое новое изменение в законодательстве к проактивному подходу, при котором ваша организация находится на переднем крае конфиденциальности данных и готова быстро реагировать на любые новые правила, которые могут появиться.

Последние мысли

Адаптация вашего бизнеса к постоянно меняющимся законам и правилам о конфиденциальности данных может стать серьезной проблемой, которая может

нарушить ваши бизнес-операции. Многие компании теперь понимают, что им нужен новый подход, который был бы комплексным и упреждающим, чтобы соответствовать требованиям, оставаясь при этом гибким.

Skyflow Data Privacy Vault изолирует, защищает и жестко контролирует доступ для управления, мониторинга и использования личной информации. Используя упреждающий подход к конфиденциальности данных, когда личная информация ваших клиентов хранится в Skyflow, вы можете эффективно изолировать, защищать и управлять этими данными.

Это позволяет вам опережать нормативные акты о конфиденциальности, удовлетворять потребительский спрос на конфиденциальность данных и быть уверенным, что вы готовы к началу применения CPRA. И этот подход гарантирует, что вы хорошо подготовлены для любых законов и правил конфиденциальности данных, которые будущее приготовит для вашего бизнеса». ***(Robin Andruss. How CPOs Can Prepare for CPRA Rules and Enforcement // CPO Magazine (https://www.cpomagazine.com/data-protection/how-cpos-can-prepare-for-cpra-rules-and-enforcement/). 05.12.2022).***

***

«Група була розпущена незабаром після того, як троє членів пішли у відставку та розкритикували дії Маска. За годину члени ради мали зустрітися із керівництвом Twitter.

Twitter розпустив свою Раду з довіри та безпеки електронною поштою менш ніж за годину до зустрічі її членів у Zoom з керівництвом компанії. Повідомляється, що рада мала обговорити останні події та зміни на сайті під керівництвом Ілона Маска. У листі було сказано, що допомога членів більше не потрібна. Її членів, поінформували, що Twitter «переоцінює, як найкраще залучити зовнішню інформацію» і що рада більше не є «найкращою структурою для цього», пише Engadget.

Компанія розпустила групу лише через кілька днів після того, як троє членів звільнилися зі своїх добровільних посад. У листі вони заявили, що добробут

користувачів Twitter падає, незважаючи на заяви Маска, і що виконавчій владі не можна дозволяти визначати цифрову безпеку. У відповідь на новину про їхнє звільнення Маск написав у Twitter: «Це злочин, що вони роками відмовлялися вжити заходів щодо експлуатації дітей!» Після цього твіту NPR повідомила, що деякі члени, що залишилися, надіслали лист до Twitter, вимагаючи від компанії припинити спотворювати роль ради, оскільки напади на колишніх і нинішніх радників продовжують посилюватися.

Члени Ради довіри та безпеки не є працівниками, які займаються модерацією сайту, і вони не мають права приймати рішення або переглядати заборонені облікові записи та конкретні твіти. Це група зовнішніх консультантів із експертних організацій та організацій, які займаються боротьбою з жорстоким поводженням, у тому числі Національний центр для зниклих безвісти та експлуатованих дітей, YAKIN (Youth Adult Survivors & Kin in Need), Samaritans і GLAAD, які добровільно витрачають свій час, щоб допомогти Twitter розібратися як боротися з ненавистю та переслідуваннями. Коли Twitter сформував раду в 2016 році, він заявив, що мета групи — зробити сайт менш токсичним місцем, щоб «будь-хто міг висловлюватися безпечно та впевнено».

«Розпустивши [раду], нас звільнили. Ілон не хоче критики, і він справді не хоче отримати поради, які він, швидше за все, отримав би від консультативної ради з безпеки, яка, ймовірно, скаже йому повторно найняти частину персоналу, якого він позбувся, і відновити деякі правила, які він відмінив, і розвернути компанію в іншому напрямку, звідки він її звертає», — сказав виконавчий директор некомерційної організації ConnectSafely Кремнієвої долини Ларрі Мегід…». ***(Катерина Колонович. Маск розпустив Раду довіри та безпеки Twitter напередодні зустрічі, щоб не чути критики // Speka.Media (https://speka.media/mask-rozpustiv-radu-doviri-ta-bezpeki-naperedodni-zustrici-shhob-ne-cuti-kritiku-py47jp). 13.12.2022).***

***

«Ілон Маск повертає Twitter Blue з новими функціями для запобігання видаванню себе за іншу особу. Підписка коштуватиме $11 в App Store та онлайн $7. Про це повідомив Reuters з посиланням на електронний лист до рекламодавців Twitter.

В листі анонсуються деякі нові функції безпеки Twitter Blue і елементи керування для рекламодавців.

Фізичні особи зможуть купувати сині позначки, а перевірені компанії будуть відрізнятися золотими «галочками», державні – сірими.

Таким чином компанія намагається погасити скандал, коли анонімні акаунти з синьою верифікацією видавали себе за відомих політичних та світських діячів.

Додатково анонсовані нові засоби контролю, які дозволяють рекламодавцям запобігати появі фірмової реклами «над або під твітами, що містять певні ключові слова», повідомляє Reuters.

Водночас в п'ятницю три члени Ради довіри та безпеки Twitter — Ейрліані Абдул Рахман, Енн Коллієр і Леслі Подеста — подали у відставку. Вони наголосили, що «всупереч заявам Ілона Маска, рівень безпеки та добробуту користувачів Twitter погіршується». Вони нагадали про сплески ненависті, відновлення Маском заборонених облікових записів і скорочення штату модераторів контенту як причини дистанціюватися від платформи.

«Твіттер, яким керує диктат, — це не місце для нас», — підкреслили вони, додавши що Маск не визнав ради, до якої у 2019 році входило понад 40 експертів та організацій, відколи він прийшов на посаду…» ***(Кіра Іванова. Маск анонсував платний Twitter з додатковою верифікацією // Speka.Media (https://speka.media/mask-anonsuvav-platnii-twitter-z-dodatkovoyu-verifikacijeyu-pkr8x9). 10.12.2022).***

***

«Колишній оглядач New York Times Барі Вайс опублікував другу частину «Файлів Twitter» у четвер увечері, поділившись зображеннями акаунтів, які Twitter нібито вніс до різних типів чорних списків.

Вайс опублікував кілька зображень того, що, здається, є внутрішньою системою Twitter, яка позначала певні облікові записи як такі, що перебувають у різних чорних списках, на додаток до позначення іншої інформації про облікові записи, повідомляє The Hill.

Згідно з фотографіями, Джей Бхаттачар'я, професор політики охорони здоров'я зі Стенфордського університету, який виступав проти карантину через COVID-19, потрапив до чорного списку трендів, як і правий обліковий запис Libs of TikTok.

Обліковий запис консервативного коментатора Дена Бонгіно, очевидно, внесли до чорного списку пошуку. Водночас на фотографіях видно, що президент Turning Point США Чарлі Кірк має свій обліковий запис із позначкою «Не поширювати».

На зображеннях також видно, що кілька облікових записів позначили як «Нещодавнє попередження про порушення», а також зазначили більш загальну інформацію, наприклад, коли облікові записи були «Twitter Blue Verified» або «High Profile».

Вайс також поділився нібито скриншотами внутрішніх повідомлень від Йоеля Рота, колишнього керівника відділу безпеки та цілісності Twitter, разом із тим, у якому він, схоже, просив дослідити «втручання політики невидалення, як-от відключення взаємодії та фільтрування видимості».

Нагадаємо, що повідомлення Вайса у Twitter є другою частиною того, що генеральний директор Ілон Маск назвав «файлами Twitter». Перший випуск опублікував незалежний журналіст Метт Тайббі, він стосувався історії New York Post із Хантером Байденом. При тому що перша частина «файлів Twitter» викликала обурення серед правих ЗМІ, її також критикували за те, що вона не змогла зробити новаторські викриття.

Публікація «файлів Twitter» відбулася трохи більше ніж через місяць після того, як Маск придбав соціальну мережу. Мільярдер, який пообіцяв перетворити Twitter на платформу «свободи слова», поділився з Вайсом і Тайббі багатьма внутрішніми документами, очевидно, намагаючись показати, що модерація

контенту за попереднього керівництва була упередженою щодо правих сил». ***(Катерина Колонович. Колишній оглядач NYT опублікував другу частину «файлів Twitter» // Speka.Media (https://speka.media/kolisnii-oglyadac-nyt-opublikuvav-drugu-castinu-failiv-twitter-93r4q9). 09.12.2022).***

***

«За словами дослідників штучного інтелекту, використовуючи фотографії з соцмереж, нейромережа може «зламати життя» будь-якому користувачеві. Щоб довести це спеціалісти Arstechnica провели незвичний експеримент — за допомогою нейромережі Stable Diffusion створили вигаданого персонажа та змінили його образ.

Штучний інтелект розробив 7 фотографій неіснуючої людини, якій дали ім'я Джон. За сценарієм штучного інтелекту, Джон — вчитель початкових класів, який упродовж 12 років публікував абсолютно звичайні фотографії, на яких він працює, відпочиває та проводить свої вихідні.

Щоб зруйнувати буденний образ Джона у соцмережах, нейромережа згенерувала справжній компромат, створивши фото, на яких вигаданий персонаж:

сидить напівголий у навчальному класі;

фотографується з оголеною порноактрисою;

ходить у костюмі клоуна;

входить до складу екстремістського військового угруповання;

відбуває термін у в’язниці за вживання наркотиків.

Як зауважили дослідники, процес навчання штучного інтелекту зайняв близько 1 години, генерування фейкових зображень — 2 години. Тобто, витративши всього 3 години часу, команді Arstechnica вдалось створити неіснуючу людину та зруйнувати її репутацію. Такі результати не можуть не лякати, адже зрозуміло, що розробка несправжніх фото для реального користувача соцмереж займе ще менше часу…». ***(Штучний інтелект навчився розробляти компромат на користувачів соціальних мереж // No worries! (https://noworries.news/shtuchnyj-intelekt-navchyvsya-rozroblyaty-kompromat-na-korystuvachiv-soczialnyh-merezh/). 17.12.2022).***

***

«Додаток Lensa, який використовує алгоритми штучного інтелекту для автоматичного редагування фото, опинився в центрі скандалу — ШІ звинуватили у сексуалізації жінок та використанні фотографій без згоди їх власників. Зауважимо, що Lensa належить компанії Prisma Labs, зареєстрованій у Каліфорнії. Втім, її засновники — росіяни Андрій Усольцев і Олексій Моїсеєнков, тому конфіденційність додатка є під питанням, навіть без гучних скандалів.

За словами деяких користувачів, нейромережа створює потенційну можливість сексуальної експлуатації та переслідування, адже ШІ малює жінок оголеними, навіть без їх згоди. Як і в інших додатках для редагування фото, користувачі можуть завантажувати будь-чиї фотографії та редагувати їх як завгодно. Часто додаток створює жіночі зображення оголеними та в позах із сексуальним підтекстом.

Lensa використовує моделі для безкоштовної системи машинного навчання під назвою Stable Diffusion. Моделі навчали на мільярдах комбінацій зображень з інтернету. Додаток відправляє завантажені користувачем фотографії у своє хмарне сховище, запускає модель, створену спеціально для кожного користувача, і видає новий портрет.

Хоча представники Prisma Labs неодноразово наголошували, що компанія не передає особисті фотографії третім сторонам, користувачі турбуються про свою безпеку. Адже правила конфіденційності, з якими має погодитися кожен перед використанням додатка, «залишають компанії можливість ділитися інформацією з іншими». Як заявив, один із засновників Lensa Андрій Усольцев, компанія зберігає «мінімальну кількість» даних із фотографій користувачів, втім які саме дані збираються Усольцев не пояснив.

За словами спеціалістів з ШІ, колекція зображень Lensa, на якій навчається штучний інтелект, містить тисячі фотографій людей, які не давали згоду на використання їх зображень. Як з’ясували журналісти видання Forbes, одна художниця навіть виявила в базі даних Lensa фотографії зі своєї особистої медичної карти. Для перевірки, чи використовують системи машинного навчання штучного інтелекту її фотографії, художниця скористалась безкоштовним сайтом HaveIBeenTrained.com.

Зауважимо, окрім відредагованих штучним інтелектом фотографій, причиною нещодавнього обурення в мережі стала книга, написана за допомогою ШІ. Співробітник фінтех-компанії Brex Аммаар Реші розробив дитячу книгу «Alice and Sparkle» («Аліса та Іскорка»), використовуючи алгоритми штучного інтелекту. Коли видання надійшло у продаж, Реші зіткнувся зі шквалом критики у соцмережах та навіть з погрозами смерті.

Авторка дитячих книг Анупа Ропер заявила: «Я подумала, невже так просто створити щось, куди мені довелося вкласти своє серце і душу?». Ще одна авторка Джозі Дім написала, що Реші не заслуговує отримувати гроші за книгу, оскільки «не вклав багато праці». Вона також вказала на безліч дефектів у зображеннях та назвала історію «шаблонною». ***(Штучний інтелект навчився роздягати жінок без їх згоди // No worries! (https://noworries.news/shtuchnyj-intelekt-navchyvsya-rozdyagaty-zhinok-bez-yih-zgody/). 16.12.2022).***

***

«…5 декабря 2022 года в федеральный суд Сан-Франциско был подан коллективный иск против Apple. В иске утверждалось, что Apple продавала устройство, которое способствовало электронной слежке, преследованию, страху и, в конечном итоге, смерти: Hughes v. Apple, Dkt. № 5:22-cv-07668-NC (Северная Дакота, 5 декабря 2022 г.). В иске утверждалось, что Apple проявила небрежность при разработке и производстве AirTag, что AirTag был спроектирован с дефектами, что продукт способствовал правонарушению «вторжение в уединение», что сбор данных о местоположении был ложным, вводящим в заблуждение, несправедливым и мошенническим в соответствии с требованиями Калифорнии. и законов Нью-Йорка о защите прав потребителей, что устройство представляет собой запрещенное «электронное устройство слежения» в соответствии с уголовным кодексом Калифорнии, что Apple нарушила конституционное право потребителей Калифорнии на неприкосновенность частной жизни. В число названных истцов входит жительница округа Трэвис, штат Техас, Лорен Хьюз, чей бывший бойфренд использовал AirTag, чтобы сообщать ему, где

она была. Когда Хьюз переехала из своего дома в номер отеля, чтобы избежать преследователя, она получила уведомление на свой iPhone о том, что с ней путешествует неизвестный AirTag. Она нашла устройство в пластиковом пакете, окрашенном маркером Sharpie, в колесной арке заднего пассажирского колеса своей машины. Другого названного истца, описанного как «Джейн Доу» из Бруклина, Нью-Йорк, преследовал ее бывший супруг, который положил AirTag в рюкзак своего ребенка.

Как работают AirTags

Apple AirTags, как и устройство Life360 Tile, представляет собой небольшое устройство, которое можно положить в сумочку, рюкзак, велосипед, бумажник или на цепочку для ключей, чтобы сообщить владельцу, где находятся эти предметы. Это особенно полезно для выяснения, где вы припарковали свой автомобиль, где вы оставили свой кошелек, где находится ваш украденный велосипед и даже (во время курортного сезона), где авиакомпания оставила ваш потерянный багаж.

Они работают, устанавливая соединение Bluetooth с любым ближайшим устройством Apple, используя GPS этого устройства для определения местоположения трекера и интернет-соединение устройства для передачи этого местоположения в Apple, а затем потребителю. Конечно, если у кого-то есть идентификатор пользователя и пароль к приложению «FindMyIPhone» владельца (или к самому сотовому телефону), они могут отслеживать AirTags так же легко, как и владелец AirTag (особенно если они могут поменять SIM-карту телефона и получать текстовые сообщения аутентификации).

Таким образом, даже для авторизованных пользователей существуют серьезные проблемы с конфиденциальностью данных. Информация, собранная AirTag в моей машине или кошельке, подлежит обыску и/или повестке в суд (неясно какой именно) полицией, прокуратурой, регулирующими органами или другими лицами в любое время, когда мое текущее или историческое местонахождение имеет отношение к какому-либо делу или расследованию. Даже если Apple по какой-то причине не обязана предоставлять данные, вы можете быть вынуждены предоставить данные или предоставить доступ к историческим данным

«FindMy…» в ходе судебного разбирательства. Это как видеорегистратор; отличная защита, если вас сбил пьяный водитель, а также доказательство того, что вы превышали скорость или не смогли полностью остановиться на знаке «стоп». Данные о местоположении FindMy, такие как данные о местоположении на картах Google, могут отслеживать каждое место, где вы находитесь и были в течение многих лет. Довольно изящно в случае неверности/развода! Но в отличие от данных карт Google, вам даже не нужно иметь мобильный телефон, чтобы AirTag мог отслеживать вас. Поток данных собирается, если у вас есть ключи, отслеживаемый кошелек или отслеживаемый рюкзак. Все это делается с вашего ведома и согласия, даже если вы не в полной мере понимаете, как это может повлиять на вас. Ваш босс думает, что вы опоздали на работу или рано ушли? AirTag в помощь (если они смогут законно получить доступ к данным).

Коллективный иск в Калифорнии демонстрирует гнусное (и несколько повсеместное) использование средств отслеживания местоположения, таких как AirTag. Они особенно полезны при преследовании, особенно когда у преследователя есть (даже краткий) физический доступ к чему-то, принадлежащему жертве — сумочке, машине, рюкзаку и т. д. Сталкер использует свой собственный AirTag, чтобы передать преследователю местонахождение жертвы.

Неизвестный AirTag путешествует с вами

Как отмечается в иске, Apple предприняла некоторые усилия, чтобы ограничить эту проблему — в основном после представления продукта. Когда телефон Apple некоторое время «путешествует» с неизвестной меткой AirTag, на телефоне Apple отображается сообщение о том, что поблизости находится неизвестная метка AirTag. Но это уведомление доставляется только (a) если у жертвы есть устройство Apple; (b) если это устройство Apple включено и подключено и (c) установлена ли на нем последняя версия операционной системы. Даже в этом случае могут быть задержки на часы или дни, пока не появится сообщение «подозрительное устройство, путешествующее с вами», и это

предполагает, что вы проверяете свои сообщения. Это лучше, чем ничего, чтобы предупредить пользователей о наличии трекера, но это не идеально.

Битва дроидов

Если жертва использует телефон Android, она не получает сообщения Apple. Они могут загрузить на свой телефон приложение, которое позволяет им сканировать неизвестные AirTags, но это предполагает, что у них есть основания полагать, что их преследуют, и что они живут в районе, где такое сканирование может дать значимую информацию. Если они находятся в Бруклине или центре Сан-Франциско, им будет трудно найти место, где поблизости не будет чьего-либо AirTag.

Дин Дин Дин Звонит в Звонок

AirTag также предназначен для подачи звукового сигнала, если он находится вдали от «владельца» в течение длительного периода времени, но неясно, как долго это время. Как отмечается в иске, многие вещи в наших домах, машинах и жизни издают звуковой сигнал, гудение, лязг, звон или звон. Мы привыкаем к этому. Более того, часто бывает сложно найти источник звона, когда нет причин искать маленький металлический AirTag. Умные сталкеры просто отключают крошечный динамик или устанавливают устройство в нише колеса автомобиля, где дорожный шум заглушал бы жестяное чириканье AirTag…

Конкурирующие ценности

Одна проблема, однако, заключается в том, что AirTag должен помогать своим владельцам находить потерянные или украденные вещи. У меня есть один, спрятанный в стволе моего велосипеда в месте, которое трудно найти. Суть в том, чтобы быть скрытным. Если (ну, когда) мой велосипед украдут, я не хочу, чтобы вор знал, что в велосипеде есть устройство слежения (надеюсь, воры не читают эту публикацию). Если AirTag подаст звуковое предупреждение: «Эй, вор! На этом велосипеде есть Lojack, и вот где он!» — это ограничило бы полезность AirTag как инструмента, помогающего найти украденный велосипед. Велосипедист просто прослушивал звуковой сигнал AirTag и удалял или отключал его. AirTag либо незаметен, либо нет.

Законное основание

В иске, по сути, утверждается, что AirTags небрежно способствуют вредоносному преследованию и не предназначены должным образом для предотвращения их использования таким образом. Истцы должны будут доказать, что Apple была обязана перед жертвами преследования (а не покупателями AirTags) предотвращать неправомерное использование устройств против них. Например, я мог бы бросить активный сотовый телефон в чью-то машину, чтобы отследить их (на самом деле, у меня есть старый телефон-раскладушка в багажнике моей машины, подключенный к розетке именно для этой цели).

В целом, однако, иск отражает обеспокоенность тем, что компании должны учитывать (и смягчать) соображения конфиденциальности для продуктов, которые они производят. Точно так же, как венчики для миксера могут быть использованы не по назначению (важный совет по безопасности — выключите миксер, прежде чем позволить детям лизать венчики!) Все виды технологий могут быть использованы не по назначению. Вопрос, который предстоит решить суду, заключается в том, кто несет ответственность за неправомерное использование технологии — в данном случае сталкер или Apple? Я буду следить за делом. Легально». ***(Mark Rasch. AirTag Stalking – Murder, Fear and Litigation // Techstrong Group Inc. (https://securityboulevard.com/2022/12/airtag-stalking-murder-fear-and-litigation/). 15.12.2022).***

***

«В какой бы точке мира вы ни находились, всегда есть риск стать жертвой утечки данных.

Индекс потребительского доверия Thales за 2022 год показал, что 33% людей во всем мире пострадали от утечки данных. Данные миллиардов людей были раскрыты и украдены. Вот почему мы стараемся помочь вам сделать все возможное, чтобы уменьшить радиус риска.

В этом выпуске четвергового обновления BlackCloak Threat Update мы рассмотрим утечку криптографических данных, в результате которой были

раскрыты миллионы адресов электронной почты. Кроме того, мы изучаем обновления безопасности Apple и Google для их устройств.

Взлом криптобиржи привел к утечке миллионов адресов электронной почты

Что мы знаем: около 13 декабря на бирже криптовалют Gemini произошла утечка данных. Неавторизованные лица смогли получить доступ к более чем 5,7 миллионам строк данных клиентов. Сюда входят номера счетов, адреса электронной почты и неполные номера телефонов. Имена клиентов, адреса и другая конфиденциальная информация не были включены в инцидент.

Рекомендации: Если вы являетесь пользователем Gemini, следите за подозрительными электронными письмами. Киберпреступники могут отправлять вам фишинговые электронные письма в попытке украсть более конфиденциальную информацию или денежные средства. Следите за любыми электронными письмами, которые сообщают о срочности или запрашивают личную информацию и учетные данные для входа в систему для решения несуществующей проблемы. Помните, что ни одна законная организация никогда не попросит вас предоставить эти точки данных. Хотя телефонные номера были раскрыты лишь частично, вам также следует остерегаться фишинговых кампаний, которые приходят с помощью текстовых сообщений — практика, известная как «смишинг». Киберпреступникам нетрудно собрать воедино полные телефонные номера после получения неполных цифр.

Apple и Google выпускают обновления безопасности для устройств

Что мы знаем: Apple и Google выпустили обновления безопасности для своих устройств. Apple выпустила исправления для iPhone, iPad, Apple Watch и компьютеров Mac. Компания выпустила исправления после обнаружения уязвимости нулевого дня, которая «могла быть активно использована. Обновление безопасности Google для Android от декабря 2022 года исправило 81 обнаруженную уязвимость, хотя хакеры до сих пор не воспользовались этими недостатками.

Рекомендации: Всякий раз, когда на одном из ваших устройств есть обновление, вы должны загрузить и установить его как можно скорее. Хакеры всегда ищут уязвимости устройств. Например, это 10-я уязвимость нулевого дня,

которую Apple исправила в 2022 году. Если вы оставите любую из этих уязвимостей открытой, вы рискуете, что злоумышленники скомпрометируют ваши устройства и контролируют их, а также украдут ваши личные данные». ***(Millions of Emails Leaked in Crypto Data Breach; Google, Apple Release Device Security Updates // Techstrong Group Inc. (https://securityboulevard.com/2022/12/millions-of-emails-leaked-in-crypto-data-breach-google-apple-release-device-security-updates/). 15.12.2022).***

***

«На этой неделе на киберпреступном форуме была выставлена на продажу база данных с контактной информацией о более чем 80 000 участников InfraGard (программа Федерального бюро расследований США (ФБР) по налаживанию партнерских отношений с частным сектором по обмену информацией о кибер- и физических угрозах). Тем временем ответственные хакеры общаются напрямую с участниками через онлайн-портал InfraGard, используя новую учетную запись под вымышленным именем генерального директора финансовой индустрии, которая была проверена самим ФБР.

10 декабря 2022 года на относительно новом форуме по киберпреступности Breached была представлена новая тема продаж: база данных пользователей InfraGard, включая имена и контактную информацию десятков тысяч участников InfraGard.

Предполагается, что программа ФБР InfraGard будет проверять, кто есть кто среди ключевых людей в частном секторе, связанных как с кибер-, так и с физической безопасностью в компаниях, которые управляют большей частью критически важных инфраструктур страны, включая питьевое водоснабжение и электроснабжение, фирмы связи и финансовые услуги, транспорт. и производственные компании, поставщики медицинских услуг и фирмы, работающие в атомной энергетике.

«InfraGard связывает владельцев критически важной инфраструктуры, операторов и заинтересованных лиц с ФБР для обучения, создания сетей и обмена информацией об угрозах и рисках безопасности», — говорится в информационном бюллетене InfraGard ФБР.

KrebsOnSecurity связался с продавцом базы данных InfraGard, участником форума Breached, использующим никнейм «USDoD» и чей аватар является печатью Министерства обороны США.

Тема продаж InfraGard USDoD на Breached.

Министерство обороны США заявило, что они получили доступ к системе InfraGard ФБР, подав заявку на новую учетную запись, используя имя, номер социального страхования, дату рождения и другие личные данные главного исполнительного директора компании, которая, скорее всего, получит членство в InfraGard.

Упомянутый генеральный директор — в настоящее время глава крупной финансовой корпорации США, которая оказывает прямое влияние на кредитоспособность большинства американцев — не ответил на запросы о комментариях.

Министерство сельского хозяйства США сообщило KrebsOnSecurity, что их фальшивое заявление было подано в ноябре от имени генерального директора, и что в нем содержался контактный адрес электронной почты, который они контролировали, а также настоящий номер мобильного телефона генерального директора.

«Когда вы регистрируетесь, они говорят, что одобрение может занять не менее трех месяцев», — сказал USDoD. «Не ожидалось, что меня одобрят[d]».


InfraGard Account Notification

[redacted]

Attention [redacted]

You are the newest member of InfraGard

To get started on the InfraGard system,

Url: https://www.infragard.org/Applicati

User Name: [redacted]

Upon login, additional information is av

Respectfully,

Federal Bureau of Investigation
Office of Private Sector
InfraGard Program Office

Please do not reply directly to this email

[redacted]

Но USDoD сообщил, что в начале декабря на их электронный адрес от имени генерального директора пришел ответ о том, что заявка одобрена (см. отредактированный скриншот справа). Хотя система InfraGard ФБР по умолчанию требует многофакторной аутентификации, пользователи могут выбирать между получением одноразового кода через SMS или по электронной почте.

«Если бы дело было только в телефоне, я был бы в плохой ситуации», — заявили в USDoD. «Потому что я использовал телефон человека, которого выдаю за себя».

USDoD заявил, что пользовательские данные InfraGard были легко доступны через интерфейс прикладного программирования (API), встроенный в несколько ключевых компонентов веб-сайта, которые помогают членам InfraGard подключаться и общаться друг с другом.

Министерство сельского хозяйства США заявило, что после того, как их членство в InfraGard было одобрено, они попросили друга написать скрипт на

Python, чтобы запросить этот API и получить все доступные пользовательские данные InfraGard.

«InfraGard — это информационный центр социальных сетей для высокопоставленных лиц», — говорится в сообщении Министерства обороны США. «У них даже есть [] форум для обсуждения вещей».

KrebsOnSecurity поделился с ФБР несколькими снимками экрана и другими данными, которые могут помочь изолировать самозваную учетную запись InfraGard, но агентство отказалось комментировать эту историю.

Чтобы доказать, что у них все еще был доступ к InfraGard на момент публикации во вторник вечером, Министерство обороны США отправило прямую записку через систему обмена сообщениями InfraGard члену InfraGard, чьи личные данные были первоначально опубликованы в качестве тизера в ветке продаж базы данных.

Этот член InfraGard, возглавляющий службу безопасности крупной американской технологической фирмы, подтвердил получение сообщения Министерства обороны США, но попросил остаться анонимным для этой истории.

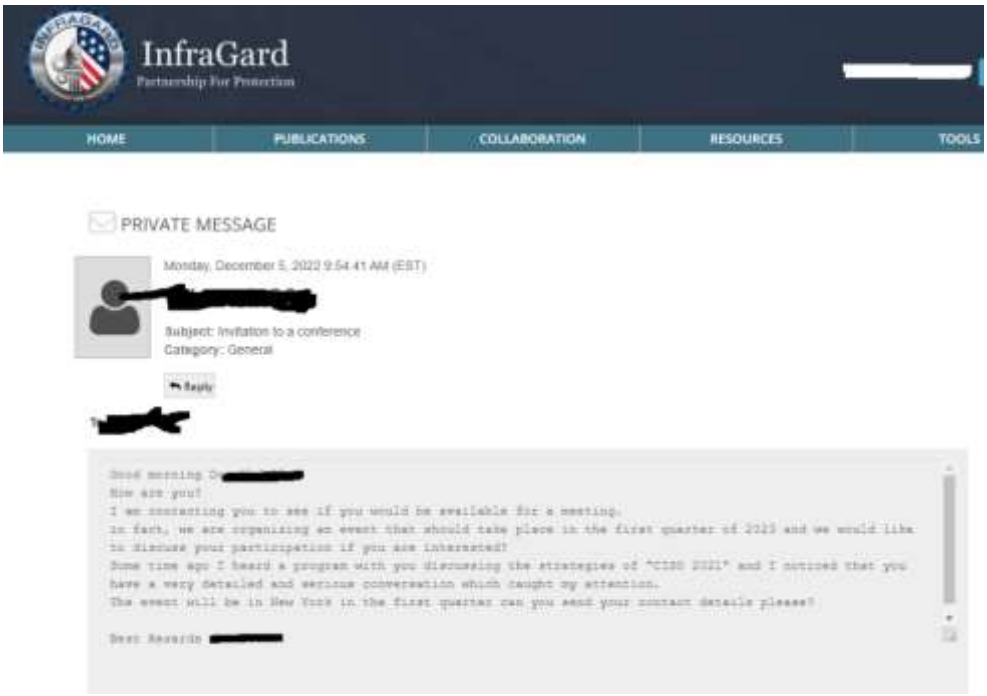
USDoD признал, что их запрашиваемая цена в размере 50 000 долларов за базу данных InfraGard может быть немного высокой, учитывая, что это довольно простой список людей, которые уже очень заботятся о безопасности. Кроме того, только около половины учетных записей пользователей содержат адрес электронной почты, а большинство других полей базы данных, таких как номер социального страхования и дата рождения, совершенно пусты.

«Я не думаю, что кто-то заплатит такую цену, но я должен [оценить] немного выше, чтобы [договориться] о цене, которую я хочу», — объяснили они.

Хотя данные, обнаруженные в результате проникновения в InfraGard, могут быть минимальными, пользовательские данные могли не быть истинной конечной целью для злоумышленников.

Министерство обороны США заявило, что они надеются, что учетная запись самозванца просуществует достаточно долго, чтобы они могли закончить отправку прямых сообщений в качестве генерального директора другим руководителям,

используя портал обмена сообщениями InfraGuard. USDoD поделился следующим отредактированным скриншотом из того, что, по их утверждению, было одним из таких сообщений, хотя они не предоставили никакого дополнительного контекста по этому поводу.



Скриншот, предоставленный USDoD, показывает цепочку сообщений в системе InfraGard ФБР.

USDoD заявил в своей ветке продаж, что гарантом сделки будет Помпомпурин, администратор форума о киберпреступности Breached. Приобретая базу данных через службу условного депонирования администратора форума, потенциальные покупатели теоретически могут избежать обмана и гарантировать, что транзакция будет завершена к удовлетворению обеих сторон до того, как деньги перейдут из рук в руки.

Помпомпурин был занозой в боку ФБР в течение многих лет. Их форум Breached широко считается вторым воплощением RaidForums, удивительно похожего англоязычного форума по киберпреступности, закрытого Министерством юстиции США в апреле. До проникновения ФБР RaidForums продал доступ к более чем 10 миллиардам потребительских записей, украденных в результате некоторых из крупнейших в мире утечек данных.

В ноябре 2021 года KrebsOnSecurity подробно рассказал, как Помпомпурин злоупотребил уязвимостью на онлайн-портале ФБР, предназначенном для обмена

информацией с правоохранительными органами штата и местными властями, и как этот доступ использовался для рассылки тысяч ложных сообщений электронной почты — все они были отправлены с электронной почты ФБР и Интернет-адрес». ***(Brian Krebs.FBI's Vetted Info Sharing Network 'InfraGard' Hacked // Techstrong Group Inc. (https://securityboulevard.com/2022/12/fbis-vetted-info-sharing-network-infragard-hacked/). 13.12.2022).***

***

«Франція наклала найбільший за рік штраф на техгіганта Microsoft у сумі 60 млн євро за політику збору даних користувачів у пошуковику Bing.

Про це повідомляє France24.

Французький регулятор заявив, що після розслідування виявив, що «коли користувачі відвідували цей сайт (Bing – ЕП), файли cookie зберігалися на їхньому терміналі без згоди, при цьому ці файли використовувалися, серед іншого, в рекламних цілях».

Регулятор зауважив також відсутність кнопки, що дозволяє відмовитися від збереження файлів cookie так само легко, як і прийняти їх.

Значна сума штрафу зумовлена, зокрема, прибутком, який компанія отримувала від реклами, що опосередковано генерується даними, зібраними за допомогою cookie – файлів, які відстежують перегляд веб-сторінок в Інтернеті.

Компанії було надано три місяці для виправлення ситуації, з потенційним подальшим штрафом у розмірі 60 тисяч євро за кожен день прострочення.

Зазначається, що торік за аналогічні порушення до компаній Google та Facebook були застосовані санкції у вигляді штрафів у розмірі 150 млн євро та 60 млн євро відповідно». ***(Франція оштрафувала Microsoft на 60 мільйонів євро // UA.NEWS (https://ua.news/ua/technologies/frantsiya-oshtrafovala-microsoft-na-60-millionov-evro). 22.12.2022).***

***

«Щойно ви подумали, що різні суперечки навколо Twitter завершуються, хакер заявив, що продає дані 400 млн користувачів. Стверджується, що дані були отримані ще у 2021 році за допомогою вразливості API, яка відтоді була виправлена. Зловмисник, який називає себе Ryushi, порадив Ілону Маску та Twitter викупити дані за ціною $200 тис., або ж зіткнутися з ще більшим штрафом.

Автор загрози, який, судячи з усього, приєднався до хакерського форуму Breached у грудні 2022 року, написав: «Ваш найкращий варіант уникнути сплати $276 млн штрафів за порушення GDPR, як це зробив Facebook (через витік даних 533 млн користувачів), – це виключно купити ці дані… після цього я видалю цю тему і більше нічого не продаватиму».

У Мережу просочилися вибіркові дані понад 1 тис. користувачів, включаючи ряд знаменитостей, з їх адресами електронної пошти, іменами користувачів, кількістю підписників, датами створення та номерами телефонів деяких користувачів.

Якщо ексклюзивний продаж Twitter (або будь-якій іншій стороні, яка хоче отримати інформацію) не буде здійснено за $200 тис., хакер стверджує, що він продасть дані кільком покупцям за $60 тис. кожному.

Видання Bleeping Computer повідомляє, що API, який спричинив вразливість, був виправлений у січні 2022 року, проте було підтверджено, що його використовували численні зловмисники, що наражає понад 400 млн користувачів на ризик шахрайства та фішингових атак.

З іншого боку, нещодавно WhatsApp опинився під тиском через витік персональних даних понад 500 млн користувачів, хоча зараз вважається, що це було повторне використання старішого витоку даних з Facebook у 2019 році». ***(Julia Alexandrova. Хакер стверджує, що викрав приватні дані 400 млн користувачів Twitter // Root Nation (https://root-nation.com/ua/news-ua/it-news-ua/ua-haker-stverdzhue-scho-vikrav-privatni-dani-400-mln-koristuvachiv-twitter/). 28.12.2022).***

***

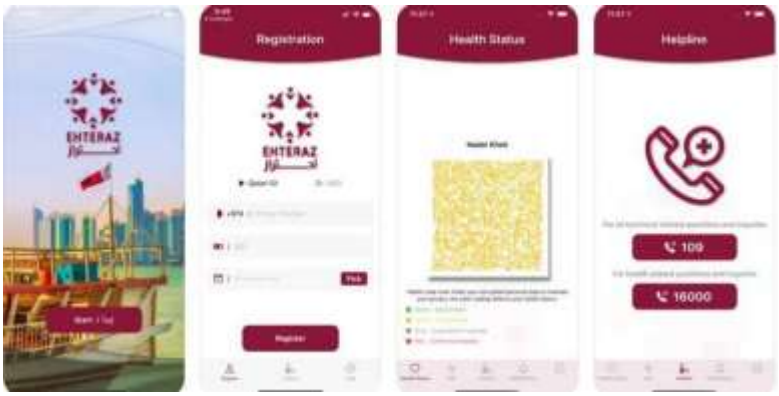
«…SPEKA розповість про технологічні маніпуляції, які використовував Катар на чемпіонаті світу, а також про те, чому уряд країни потенційно має доступ до усіх персональних даних відвідувачів стадіонів.

Обов'язковий шпигунський софт для усіх відвідувачів Катару

Ще задовго до початку чемпіонат світу з футболу у Катарі потрапив до низки скандалів. Звинувачення уряду країни у хабарі для керівництва ФІФА за право проводити змагання, трудове рабство та смерть працівників, гомофобія урядових осіб… Але чемпіонат таки дозволили провести у цій країні

Для відвідування стадіонів потрібні два застосунки: Ehteraz та Hayya, які розробили у Катарі. Перший — це система відстеження COVID-19, який має завантажити кожен, хто прибув до країни, а Hayya використовують для доступу вболівальників на територію стадіону, перегляду розкладу та безкоштовного громадського транспорту.

В обох застосунків, особливо у Ehteraz, є колосальні проблеми з безпекою даних. Окрім того що Ehteraz відстежує місцеперебування (доволі логічно для застосунку для локалізації хворих), користувачі надають йому ще багато дозволів — фактично доступ до всіх операцій у телефоні та можливість їх відстежувати.



Застосунок Ehteraz

Керівник служби безпеки норвезької телерадіокомпанії NRK та дві IT-компанії перевірили цей застосунок і виявили, що він може:

завжди відстежувати місцеперебування телефону за GPS;

мати повний доступ до телефону, зокрема читати, видаляти та змінювати дані;

мати віддалений доступ для підключення до Wi-Fi та Bluetooth;

відкриватися згори над усіма іншими програми на телефоні;

мати повний контроль, що гарантує, що пристрій неможливо вимкнути або перевести у режим сну.

«Щойно користувач завантажить застосунок Ehteraz (а це обов'язково під час в'їзду до країни), Катар фактично володіє вашим пристроєм, — розповідає Ойвінд Васаасен, керівник служби безпеки NRK. — Вони можуть змінити вміст усього вашого телефону, адже мають повний контроль над наявною там інформацією».

Застосунок Наууа потребує менше дозволів, але також має низку критичних аспектів. Наприклад, програма запитує доступ, щоб ділитися вашою інформацією майже без обмежень. Крім того, Наууа дозволяє точно визначати місцеперебування телефону, запобігає переходу в режим сну та бачить мережеве з'єднання телефону.

І все це у країні, де гомосексуалізм незаконний, а будь-яке оголене фото на вашому телефоні можуть вважати ввезенням порнографії, а це кримінальний злочин.

Розпізнавання облич на стадіонах та на вулицях столиці

Катар використовує камери з функцією розпізнавання облич на усіх восьми стадіонах та на вулицях столиці Дохи. Загалом понад 15 тис. камер. Уряд країни запевняв, що це потрібно, щоб моніторити активність футбольних уболівальників та забезпечити менші черги у транспорті, туалетах та кафе, а також ловити злочинців і терористів. Правозахисники стверджують, що дуже мало доказів того, що навіть «традиційні» системи відеоспостереження знижують злочинність, радше вони створюють видимість безпеки.

Стадіон у Лусаїлі, який приймав фінал чемпіонату світу з футболу і де технологію розпізнавання облич використовували для відстеження вболівальників. © Hussein Sayed/AP

Більшість європейських стадіонів вже випробовували ідею камер із розпізнаванням людей, щоб не допускати до гри футбольних хуліганів та шахраїв із квитками. Ці камери використовували домашні стадіони таких клубів, як данський «Брондбю», французький «Метц», іспанські «Атлетіко» та «Валенсія», англійський «Манчестер Сіті».

Однак алгоритми не досить точні. У 2017 році технологія сканування обличчя помилково ідентифікувала 2470 людей як можливих злочинців на фіналі Ліги чемпіонів. У 2019-му нідерландський футбольний клуб «Ден Бош», який використовує розумні камери, неправильно ідентифікував 20-річного вболівальника і заборонив йому вхід, заявивши, що він бився на трибунах та заходив у зони обмеженого доступу. Окрім того, його оштрафували.

Та проблема не у точності, а у правомірності таких дій. У квітні 2021 року Європейська комісія подала пропозицію щодо правового статусу штучного інтелекту. Наразі Європейський парламент визначається щодо пропозиції, але його члени підтримали повну заборону віддаленої біометричної ідентифікації у публічних місцях як державою, так і приватними особами.

Але заборона не міститиме використання систем для розпізнавання емоцій, а також біометричну категоризацію (наприклад, профілювання людей за віком, статтю чи етнічними ознаками).

Цензура у мережі та профінансовані пропагандисти на чемпіонаті

Оскільки звинувачення у корупції, порушенні прав людей та ненависті до ЛГБТК-спільноти вже завдали Катару та чемпіонату репутаційних втрат, уряд намагався відбілити себе у соцмережах. Журналісти The New York Times з'ясували, що Катар пропонував лідерам фанатських спільнот безкоштовні квитки на літаки, проживання та відвідування матчів за позитивний піар у соцмережах. Учасників спеціальної негласної фанатської програми попереджали, що хоча їх не просять бути «рупором» Катару, але кажуть, «не зневажати» країну чи турнір.

Вони також мали стежити за подібним негативом у коментарях до своїх публікацій. Пункт у кодексі поведінки вимагав від них «повідомляти організаторам

про будь-які образливі або принизливі коментарі». Там, де це можливо, йдеться у кодексі, вони повинні надавати скриншоти усіх образливих публікацій.


We are not asking you to [be] a mouthpiece for Qatar, but it would obviously not be appropriate for you to disparage Qatar the Supreme Committee for Delivery & Legacy (or other relevant entities related to the FIFA World Cup Qatar 2022) or the FIFA World Cup Qatar 2022. We know you have your own opinions, and your own style, so based on the facts we present to you, share them in a manner that suits you.

Уривок із кодексу поведінки лідерів уболівальників

У компанії Meta (Facebook та Instagram) вже заявили, що фільтруватимуть образливий контент у соцмережах. На тлі чемпіонату є одразу кілька загроз: торік Instagram розкритикували за те, що він не захистив чорношкірих гравців збірної Англії від расистських образ.

Компанія навчала гравців використовувати обмеження та ліміти для образливих слів у повідомленнях та коментарях, а минулого року запровадила нові алгоритми, які перешкоджають користувачам відповідати на образливі коментарі. Однак жодна з цих функцій не є новою чи спеціально розробленою для роботи на чемпіонаті світу…». ***(Олександр Тартачний. Шпигунські застосунки та розпізнавання облич: темний бік технологій на чемпіонаті світу у Катарі // Speka.Media (https://speka.media/spigunski-zastosunki-ta-rozpiznavannya-oblic-temna-storona-pl0l0p). 19.12.2022).***

***

Кібербезпека та хмарні технології

«Тысячи пострадавших клиентов призвали использовать Microsoft 365 хотя бы временно

Обновление: 5 декабря 2022 г., 21:24 UTC: акции Rackspace завершили торги в понедельник с понижением на 15,46% без каких-либо дополнительных

обновлений о статусе продолжающегося отключения биржи компании. Nasdaq Composite, индекс, отслеживающий производительность биржи технологических компаний, на которой торгуется Rackspace, завершил день снижением на 1,9%.

Тысячи клиентов Rackspace по всему миру продолжают сталкиваться с перебоями в работе Microsoft Exchange Server, которые, по словам гиганта управляемых услуг, связаны с нарушением безопасности.

Rackspace заявляет, что будет держать свою размещенную службу Exchange в автономном режиме на неопределенный срок, пока исследует конкретную проблему, о которой она еще не сообщила публично.

Rackspace со штаб-квартирой в Техасе — крупнейший в мире поставщик управляемых облачных услуг, насчитывающий более 300 000 клиентов по всему миру, в том числе две трети из 100 крупнейших публичных компаний мира.

Проблемы начались в четверг вечером, а в пятницу днем Rackspace сообщила, что «произошла серьезная ошибка в нашей среде Hosted Exchange» и что она «заблаговременно закрыла среду, чтобы избежать дальнейших проблем, пока мы продолжаем работу по восстановлению службы» и выявляем «основная причина проблемы». Впоследствии компания сообщила, что основной причиной стала очевидная атака.

Rackspace рекомендовала всем затронутым клиентам перейти на Microsoft 365 в качестве временной меры и заявляет, что предоставляет им «лицензии Microsoft Exchange Plan 1 на Microsoft 365 до дальнейшего уведомления» без дополнительной платы. Службы, затронутые его предложением Hosted Exchange, которые остаются в автономном режиме, включают MAPI/RPC, POP, IMAP, SMTP, ActiveSync и интерфейс Outlook Web Access, используемый для доступа к экземплярам Hosted Exchange для управления электронной почтой в Интернете.

Рано утром в понедельник Rackspace сообщила, что добилась прогресса в восстановлении службы — опять же, при условии, что клиенты размещенной на хостинге Exchange перестанут использовать ее размещенную на хостинге службу Exchange. Вместо этого они должны либо временно перенаправить свою

электронную почту на внешний адрес для каждого пользователя, либо перейти с размещенного Exchange на Microsoft 365.

«Мы успешно восстановили почтовые службы для тысяч клиентов в Microsoft 365 и продолжаем работать над восстановлением почтовых служб для каждого пострадавшего клиента», — говорится в сообщении Rackspace, опубликованном рано утром в понедельник. «В настоящее время переход на Microsoft 365 — лучшее решение для клиентов, которые теперь также могут реализовать временную переадресацию».

Rackspace заявляет, что, хотя инцидент безопасности и меры по смягчению последствий не затронули его собственную службу электронной почты Rackspace, любой клиент с гибридной хостинговой средой, использующей как Rackspace Email, так и Exchange для одного домена, «будет обязан переместить все почтовые ящики (Rackspace Email и Rackspace Email). Exchange) на M365 для правильной работы почтового потока. Чтобы сохранить ваши данные, очень важно, чтобы вы не удаляли исходные почтовые ящики при внесении этого изменения».

В воскресенье Rackspace сообщила клиентам, что «задействовала обширные внутренние ресурсы и привлекла внешних экспертов мирового уровня для минимизации негативных последствий для клиентов».

«Мы продолжаем добиваться прогресса в урегулировании инцидента», — говорится в сообщении. «Доступность вашего сервиса и безопасность ваших данных имеют большое значение».

Несколько пользователей сообщили о длительных задержках и недовольстве переносом своей электронной почты на M365, а также о частом отключении от поддержки по телефону. «Сидел сегодня в ожидании 5 часов. Да, 5 часов», — сообщил один из клиентов через Twitter.

Другой клиент также подробно описал время ожидания в течение нескольких часов. «Мне нужно восстановить мою электронную почту и получить доступ к моей учетной записи электронной почты. Я потерял так много денег за последние три дня», — написал клиент в Твиттере.

Клиенты также угрожали коллективными исками из-за простоя.

Rackspace не сразу ответила на запрос о комментарии.

Обходят ли злоумышленники средства защиты ProxyNotShell?

Хотя компания еще не поделилась подробностями инцидента с безопасностью, британский эксперт по кибербезопасности Кевин Бомонт говорит, что данные свидетельствуют о том, что Rackspace использовала серверы Microsoft Exchange, которые оставались уязвимыми для двух недостатков, известных как ProxyNotShell.

Microsoft исправила пару уязвимостей нулевого дня Exchange в начале ноября, после того как они были впервые обнародованы в конце сентября и, как известно, использовались злоумышленниками в дикой природе, отображающими индикаторы китайского происхождения (см.: Microsoft Patches ProxyNotShell Exchange Vulnerabilities).

Бомонт говорит, что исследование с поисковой системой интернета вещей Shodan показало, что Rackspace использовала по крайней мере несколько кластеров Exchange с номерами сборки от августа, которые предшествовали исправлениям Microsoft.

Rackspace, возможно, внедрила рекомендованные Microsoft меры по устранению последствий до тех пор, пока не сможет исправить все системы, например, создать правила с помощью модуля IIS Rewrite и реализовать их с помощью сценариев PowerShell или службы Exchange Emergency Mitigation.

Но если бы это было так, системы все равно были бы в опасности.

«Предоставленные Microsoft средства защиты от ProxyNotShell можно обойти, — говорит Бомонт. «Перезапись IIS, которую Microsoft использовала для смягчения последствий, неправильно декодирует все URL-адреса, и поэтому ее можно обойти для эксплуатации. Если вы полагались на смягчение PowerShell или приложение EEMS, ваш Exchange Server по-прежнему уязвим — Microsoft просто не ясно сказал вам это. Исправление - это патч.» ***(Prajeet Nair. Rackspace Hosted Exchange Still Offline Over Security Issue // Information Security Media Group, Corp. (https://www.govinfosecurity.com/rackspace-hosted-exchange-still-offline-over-security-issue-a-20624). 05.12.2022).***

***

«Apple позволит пользователям iPhone шифровать резервные копии iPhone, хранящиеся в облаке ее клиентов, говорится в заявлении компании, которое рекламируется как благо для безопасности, но правительство может осудить это как эскалацию давней напряженности в отношении доступа правоохранительных органов к данным на мобильных устройствах.

В среду компания из Купертино, штат Калифорния, заявила, что к концу этого года у большинства пользователей в США будет возможность включить сквозное шифрование резервных копий iPhone, заметок и фотографий, размещенных в Apple iCloud. Эта функция будет запущена во всем мире в начале 2023 года.

Apple, которая позиционирует себя как редкая компания Кремниевой долины, которая защищает конфиденциальность пользователей, приложила все усилия, чтобы сформулировать свое заявление в контексте утечек данных облачных вычислений «Эксперты говорят, что общее количество утечек данных увеличилось более чем в три раза в период с 2013 по 2021 год, и только в 2021 году было раскрыто 1,1 миллиарда личных записей по всему миру», — пишет компания. В новые параметры шифрования не будут включены почта, контакты и события календаря iCloud «из-за необходимости взаимодействия с глобальными системами электронной почты, контактов и календаря», говорится в сообщении компании.

Apple подчеркнула, что сквозное шифрование обеспечивает целостность данных даже в случае их утечки.

В январе 2020 года агентство Reuters сообщило, что компания воздержалась от предложения полного сквозного шифрования для резервного копирования iCloud после того, как ФБР пожаловалось на влияние на расследования (см. Отчет: планы Apple Scuttled Encryption for iCloud Backups).

Правоохранительные органы используют фразу «затемнение», чтобы описать то, что, по их словам, является препятствием для получения данных, созданным шифрованием. Сторонники конфиденциальности и технологи говорят, что

беспокойство неуместно, особенно с учетом огромного количества незашифрованных метаданных, раскрывающих такую информацию, как местонахождение людей и контакты, созданные цифровыми устройствами. Их возражение правоохранительным органам заключалось в том, что мы живем в «золотой век слежки».

Правительство США на протяжении десятилетий то оказывало давление на промышленность, чтобы предоставить ей черный доступ к зашифрованным коммуникациям, то часто неохотно признавало преимущества шифрования. Администрация Трампа усилила давление, привлекая в 2020 году Великобританию, Австралию и Новую Зеландию, чтобы призвать технологические компании обеспечить, чтобы «шифрование применялось таким образом, чтобы полностью исключить любой законный доступ к контенту».

Подобных усилий не предпринималось при администрации Байдена, которая вместо этого в мае выпустила меморандум о национальной безопасности, призывающий к разработке квантово-устойчивой криптографии.

Министерство юстиции и ФБР не сразу ответили на просьбу прокомментировать заявление Apple.

Сегодняшнее объявление о продукте также включает упоминание об усилении контроля многофакторной аутентификации для доступа к учетным записям Apple за счет поддержки аппаратного ключа безопасности. Пользователи также смогут добавить проверку контактов для чатов iMessage. По словам Apple, функция проверки предупредит пользователей, если субъект угрозы, такой как спонсируемый государством хакер, взломает серверы iMessage для отслеживания сообщений.

В этом году Apple усилила защиту для борьбы с продвинутыми шпионскими программами, которые заражают ее устройства, объявив в июле о «экстремальной дополнительной защите», которая позволяет пользователям ограничивать функциональность своего устройства». ***(David Perera. Apple to Enable End-to-End Encryption of iCloud Backups // Information Security Media Group, Corp.***

(https://www.govinfosecurity.com/apple-to-enable-end-to-end-encryption-icloud-backups-a-20649). 07.12.2022).

***

«Проблемы, связанные с облачной безопасностью, управлением и оркестровкой, сохраняются

Четыре основных поставщика облачных услуг — Amazon Web Services, Google, Microsoft и Oracle — будут участвовать в контракте Министерства обороны США на удаленные вычисления на сумму 9 миллиардов долларов, объявил сегодня Пентагон. Решение о привлечении четырех американских поставщиков облачных вычислений к своему контракту Joint Warfighting Cloud Capability знаменует собой отход от прежнего подхода «победитель получает все», который в течение многих лет тормозил переход военных в коммерческое облако после того, как проигравшие, исключенные из контракта, протестовали против его справедливости.

В пресс-релизе министерство обороны заявило, что оно «стремится довести возможности облачных вычислений в масштабах предприятия до… всех доменов и уровней классификации», от «стратегического уровня до тактического уровня».

Что касается судебного иска, поданного AWS, оспаривающего присуждение Пентагоном контракта JWCC с Microsoft в 2021 году, в примечании к контракту Министерства обороны США говорится, что в настоящее время средства не выделяются. «Средства будут выделяться по индивидуальным заказам по мере их выдачи», — говорится в заявлении.

Гибридный контракт основан на условиях «твердо фиксированной цены и времени и материалов, неопределенной доставки / неопределенного количества» и называет других поставщиков для предоставления услуг ВМФ, ВВС, армии, DARPA и Агентству материально-технического обеспечения обороны.

Облачная борьба

Споры по поводу крупного контракта начались в 2019 году, когда министерство заключило с Microsoft контракт на создание совместной корпоративной оборонной инфраструктуры на сумму 10 миллиардов долларов.

Amazon подала в суд, утверждая, что награда JEDI была испорчена конфликтом интересов, в том числе предполагаемым неправомерным участием бывшего президента Дональда Трампа. Oracle ранее возражала против контракта JEDI, поэтому в июле 2021 года Министерство обороны объявило об аннулировании контракта и заявило, что планирует заменить его контрактом JWCC в 2022 году. Аналогичным образом Microsoft в прошлом году подала протест в Счетную палату правительства. против облачного контракта на 10 миллиардов долларов с Агентством национальной безопасности.

На брифинге для СМИ Джон Шерман, исполнявший тогда обязанности ИТ-директора департамента, заявил, что Министерство обороны свяжется с «другими поставщиками облачных услуг, не упомянутыми в документах», имея в виду Google, Oracle и IBM.

Главный аналитик Forrester Девин Дикерсон (Devin Dickerson) сказал, что стратегия DOD в отношении нескольких облачных сред имеет смысл и соответствует растущей тенденции заключения государственных контрактов с несколькими поставщиками облачных услуг, что является заметным отходом от концепции JEDI с одним поставщиком облачных услуг.

«Переход к мультиоблачной среде является признаком двух событий: более высокого доверия к возможностям безопасности и сервисов общедоступного облака, а также совершенствованию технологий и сервисов CSP для соответствия жестким мультиоблачным стратегиям», — говорит Дикерсон. «Это не означает, что отдельные программы Министерства обороны США должны переходить на многооблачные среды. Но благодаря этой награде Министерство обороны как предприятие окажется в многооблачном мире».

Включение Oracle и Google в JWCC стало неожиданностью для отраслевых обозревателей, поскольку в прошлом году Администрация общих служб заявила, что только Amazon и Microsoft способны удовлетворить требования Пентагона. Облачный бизнес Oracle намного меньше, чем у других; за квартал, закончившийся 31 августа, он получил всего 900 миллионов долларов дохода от облачной инфраструктуры.

«Захват JWCC — это огромное благо для OCI, которая резко отстает от AWS, Azure и GCP по большому отрыву в доходах и доле рынка», — говорит Дикерсон. «Тем не менее, Oracle имеет значительное присутствие в государственных учреждениях. Внедрение облачных сервисов Oracle означает потенциальные возможности для роста государственных приложений для гибридных и общедоступных облачных рабочих нагрузок.

Объем продаж Amazon Web Services в третьем финансовом квартале компании составил 20,5 млрд долларов. Группа Synergy Research Group в октябре обнаружила, что AWS контролирует 34% рынка услуг облачной инфраструктуры стоимостью 57,5 млрд долларов, в то время как Microsoft и Google занимают 21% и 11% рынка соответственно. Oracle даже не попала в первую пятерку; Alibaba и IBM заняли последние два слота.

Уолл-стрит благосклонно отреагировала на награду JWCC, в результате чего акции Amazon, Microsoft и Oracle немного выросли вскоре после открытия рынка в четверг, в то время как акции материнской компании Google Alphabet торгуются немного ниже. Четыре компании очень мало говорили в публичных комментариях о награде JWCC с тех пор, как она была объявлена поздно вечером в среду.

Microsoft заявила в своем блоге: «Мы считаем, что многооблачный подход для JWCC является правильным для корпоративной инфраструктуры Министерства обороны. доступ к лучшим технологиям от поставщиков».

Но относительное молчание, вероятно, связано с неуверенностью в том, какой кусок пирога в 9 миллиардов долларов в конечном итоге получит каждый из четырех технологических гигантов. Природа контрактов с неопределенной поставкой и неопределенным количеством означает, что решения о том, с какой компанией работать, будут приниматься на основе каждого заказа.

«Поставщики будут конкурировать на протяжении всего жизненного цикла контракта», — говорит Дикерсон. «По мере того, как будут добавляться заказы на отдельные задачи, поставщики должны будут показать, что их возможности и цены лучше всего подходят для удовлетворения этих потребностей миссии. Только когда

эти заказы на отдельные задачи будут присуждены, средства будут выделены, поэтому настоящая конкуренция только начинается».

Хотя предполагается, что JWCC предоставит военнослужащим по всему миру доступ к несекретным, секретным и сверхсекретным данным, Пентагон пока мало говорит о том, что он ищет с точки зрения безопасности. «Усиленная безопасность» является одной из девяти возможностей, которые, по словам Пентагона, JWCC позволит Министерству обороны получить наряду с такими активами, как «расширенная аналитика данных» и «тактические пограничные устройства».

В ноябре Минобороны объявило, что его стратегия безопасности будет основываться на принципах нулевого доверия, но серьезная приверженность облачным технологиям ставит фундаментальные вопросы безопасности — от потенциальных ошибок конфигурации до субъектов национального государства, нацеленных на этих облачных провайдеров, говорит Чейз Каннингем, бывший аналитик Forrester, известный как «Доктор нулевого доверия», который руководит безопасностью в Ericom Software. Бывший начальник отдела криптологических технологий Агентства национальной безопасности США Каннингем говорит, что военные уже работают в многооблачной среде, дополняя центры обработки данных Министерства обороны США.

«Это похоже на нерассказанную историю, которую никто на самом деле не признал бы: верхние слои управляли этим материалом, а затем, под ним, была эта мешанина из всего, что вы могли заставить работать, чтобы двигать электроны для выполнения миссии», — говорит Каннингем. «Это было мультиоблако с тех пор, как о мультиоблаке даже не говорили, и в течение долгого времени это было похоже на курение метамфетамина в мультиоблаке с деньгами, брошенными на него, и со временем оно становилось все больше, быстрее и безумнее».

Более быстрое развертывание

Поскольку части ИТ-инфраструктуры Министерства обороны США потенциально распределены по четырем облачным платформам, контракт поднимает вопросы о том, как Министерство обороны США будет эффективно

управлять инфраструктурой и как оно обеспечит координацию в облаках и прозрачность управления и затрат.

По словам Дикерсона, одним из преимуществ будет скорость. Скорость является серьезной проблемой с государственными контрактами и усилиями по модернизации.

«Шесть лет — это долгий срок для технологий, — говорит Дикерсон. «Программы DOD иногда продвигаются медленно, но эта награда на самом деле значительно упростит и потенциально ускорит использование облака отдельными программами. Предоставление программам возможности использовать контрактный механизм JWCC для приобретения облачных услуг не только обеспечивает доступность облачных сервисов. в требуемых доменах безопасности и уровнях классификации, но может сократить сроки приобретения на месяцы или годы». ***(Brian Perera. DOD Awards $9B Contract to Top 3 Cloud Providers and Oracle // Information Security Media Group, Corp. (https://www.govinfosecurity.com/dod-awards-9b-contract-to-top-3-cloud-providers-oracle-a-20664). 08.12.2022).***

***

«…Облачные вычисления были модным словечком в ИТ-индустрии в течение последних нескольких лет, но становятся ли они угрозой? Недавнее исследование показало, что наблюдается значительный рост облачных сервисов и угроз облачной безопасности. В отчете утверждается, что этот внезапный рост числа атак на системы усугубит существующую проблему, открыв для них новые уязвимости.

Популярность облачных вычислений растет. Для будущего расширения и роста бизнеса требуются большая вычислительная мощность и огромная инфраструктура хранения данных. Кажется разумным, что по мере того, как все больше компаний и частных лиц переносят свои ИТ-системы и данные в облако, возникают проблемы с безопасностью. Безопасность облачных вычислений должна быть приоритетом для каждого предприятия, хотя бы часть рабочих процессов

которого находится в облаке. Сейчас, когда общество больше осознает необходимость защиты персональных данных от потери и несанкционированного доступа, это особенно важно. В результате существует большой спрос на доказательства того, что данные управляются правильно и безопасно, чтобы предотвратить утечку данных и киберпреступность.

Что такое облачные вычисления?

Облачные вычисления — это вычислительная модель, в которой пользователи могут получать доступ и использовать общие вычислительные ресурсы (например, серверы, хранилища, приложения) через Интернет. Вместо того, чтобы поддерживать свою собственную физическую инфраструктуру, пользователи могут получать доступ к этим ресурсам и использовать их на основе оплаты по мере использования или подписки, а поставщик заботится об обслуживании и управлении базовым оборудованием и программным обеспечением. Это позволяет пользователям увеличивать или уменьшать свои вычислительные потребности по мере необходимости и платить только за те ресурсы, которые они фактически используют. Облачные вычисления становятся все более популярными в последние годы из-за их экономической эффективности и гибкости, и многие компании и частные лица используют их для хранения и доступа к данным, запуска приложений и размещения веб-сайтов.

Почему облачные сервисы распространяются?

После того, как мир испытает огромную волну цифровой трансформации, внедрение услуг облачных вычислений поможет предприятиям и отраслям оставаться актуальными. Ожидается, что к 2024 году 90% предприятий со штатом более 1000 сотрудников перейдут в облачные среды.

Облачные сервисы получили широкое распространение по ряду причин.

Во-первых, они предлагают модель оплаты по мере использования, которая может быть очень рентабельной для организаций.

Во-вторых, они легко масштабируются и легко адаптируются к изменяющимся потребностям.

В-третьих, они обеспечивают высокую степень гибкости, позволяя организациям использовать услуги, которые наилучшим образом соответствуют их потребностям.

В-четвертых, они обеспечивают высокий уровень безопасности и конфиденциальности.

Наконец, они предлагают ряд других преимуществ, таких как возможность доступа к данным из любого места и возможность обмена данными с другими.

Последствия использования больших облачных сервисов

По мере того, как все больше компаний переходят на облачные сервисы, увеличивается вероятность утечки данных и других угроз безопасности. Хотя облако может предложить большую гибкость и масштабируемость, оно также создает новые уязвимости, которые необходимо устранить.

Организации должны знать о рисках, связанных с облачными сервисами, и предпринимать шаги для их снижения. В частности, они должны учитывать следующее:

1. Утечки данных. Когда конфиденциальные данные хранятся в облаке, существует риск того, что к ним могут получить доступ неавторизованные лица. Чтобы защититься от этого, организациям следует шифровать свои данные и предоставлять доступ только тем, кто в них нуждается.

2. Атаки типа «отказ в обслуживании»: облачные сервисы могут стать мишенью для атак типа «отказ в обслуживании», которые могут помешать законным пользователям получить к ним доступ. Для защиты от этих атак организациям следует применять меры безопасности, такие как брандмауэры и системы обнаружения вторжений.

3. Злонамеренные инсайдеры: у поставщиков облачных услуг есть сотрудники, которые могут иметь злонамеренные намерения или могут непреднамеренно создавать уязвимости в системе безопасности. Чтобы защититься от этого, организациям следует тщательно проверять поставщиков и внимательно следить за их деятельностью.

Принимая эти меры предосторожности, организации могут снизить риски, связанные с использованием облачных сервисов.

Проблемы облачных вычислений

Внедрение решений безопасности в облачной среде сопряжено с рядом трудностей из-за ее размера и гибкости. Вот несколько из них:

Небезопасные API-интерфейсы. В облачной среде существует множество точек атаки. Незащищенные API — один из потенциальных источников опасности. Крайне важно убедиться, что уровень API также полностью безопасен, поскольку хакеры могут вторгаться и получать доступ к данным через незащищенные API.

Неправильные настройки. Кроме того, нарушения конфиденциальности и данных происходят из-за настроек облачной среды по умолчанию. Неправильные настройки могут включать в себя, среди прочего, невозможность изменить пароли по умолчанию или настройки конфиденциальности.

ИТ-экспертиза – поддержание Внедрению облачных решений по обеспечению безопасности, по мнению многих фирм, мешает отсутствие понимания и опыта работы с облачными настройками. Для преодоления этого препятствия требуются ресурсы с опытом работы с определенными облачными элементами и облачными экспертами.

Мультитенантность. В общедоступном облаке размещается множество инфраструктур. В результате гораздо выше вероятность того, что враждебные атаки поставят под угрозу облачную среду.

Угрозы будущему облачных вычислений

Услуги облачных вычислений — это угроза будущего, поскольку они предлагают модель оплаты по факту использования, которая может быть очень привлекательной для бизнеса. Этот тип услуг позволяет предприятиям платить

только за те ресурсы, которые они используют, что может сэкономить им много денег в долгосрочной перспективе. Проблема с этим типом услуг заключается в том, что может быть очень сложно предсказать, сколько ресурсов потребуется бизнесу в будущем, что может привести к перерасходу средств на облачные услуги.

Нет никаких сомнений в том, что за облачными вычислениями будущее вычислений. Однако есть несколько угроз будущему облачных вычислений.

Одна из самых больших угроз для будущего облачных вычислений — утечка данных. Хотя облако обычно считается безопасным, в последние годы произошло несколько громких утечек данных. Эти нарушения вызвали опасения по поводу безопасности облака и заставили некоторые компании переосмыслить свое использование облачных сервисов.

Еще одна угроза будущему облачных вычислений — государственное регулирование. Правительство США уже несколько лет изучает возможные правила для облачных сервисов. Эти правила могут ограничивать возможности компаний использовать определенные типы данных или могут налагать другие ограничения на то, как компании могут использовать облачные сервисы.

Наконец, еще одной угрозой для будущего облачных вычислений является возможность появления новых технологий, которые сделают облака устаревшими. Это риск для любой новой технологии, но особенно это касается чего-то столь разрушительного, как облака. Хотя кажется маловероятным, что что-то сможет заменить облака в ближайшем будущем, вполне возможно, что появятся какие-то непредвиденные технологии, которые сделают их ненужными.

Заключение

Надежный и эффективный вариант для компаний любого размера, услуги облачных вычислений от Kratikal Tech Pvt Ltd, сертифицированной организации Empaneled. показали себя. Он предлагает масштабируемое и гибкое решение, которое позволяет компаниям получать доступ к необходимым им ресурсам, не неся при этом высоких первоначальных затрат на обычную ИТ-инфраструктуру. Эти варианты включают инфраструктуру как услугу (IaaS), платформу как услугу (PaaS) и программное обеспечение как услугу (SaaS). Наши облачные решения

позволяют удаленно хранить данные и приложения, а также обрабатывать их, управлять ими и поддерживать их, устраняя необходимость в дорогостоящем оборудовании и обслуживании. Ваши данные и приложения доступны через наши службы облачных вычислений, когда они вам нужны, из любого места и с любого устройства. Мы предлагаем различные варианты, в том числе гибридные, частные и общедоступные облака, чтобы удовлетворить ваши уникальные требования и спецификации.

Прокомментируйте ниже свои идеи о дополнительных преимуществах облачных вычислений для компаний. Мы ценим ваше время, потраченное на чтение этого блога». ***(Deepti Sachdeva. Cloud Computing Services: The Threat of the Future // Techstrong Group Inc. (https://securityboulevard.com/2022/12/cloud-computing-services-the-threat-of-the-future/). 20.12.2022).***

***

«Организации по всему ОАЭ активизируют свои цифровые инициативы и внедряют облачные инструменты для поддержки своих сотрудников. Однако на пути к этому есть препятствия. Поскольку данные перемещаются туда и обратно между корпоративными сетями и облаком, организации продолжают сталкиваться с проблемами, связанными с неадекватными возможностями миграции, управлением сложностью мультиоблачных сред, неожиданной производительностью приложений и безопасностью.

В отчете Markets and Markets MEA Cloud Computing Report прогнозируется, что к 2026 году рынок облачных вычислений в ОАЭ вырастет до 31,4 млрд долларов США. для расширения облачных приложений. Ожидается, что рост будет вызван ростом числа компаний, занимающихся модернизацией операций, центров обработки данных, подразделений и, возможно, целых корпораций с помощью технологий. Благодаря постоянно меняющимся бизнес-требованиям, которые включают в себя доступ в любом месте и в любое время, ИТ-отделы имеют стратегическое положение для быстрого развертывания эффективных решений для

поддержки организационного роста и передовых инициатив, связанных с гибкостью, масштабируемостью, снижением затрат и ускорением выхода на рынок.

СИЛЬНЫЕ СЛЕДУЮТ В ЗАЛИВ

Неудивительно, что в рынок центров обработки данных Ближнего Востока и Африки в 2021 году было инвестировано 6,55 млрд долларов, а к 2027 году объем инвестиций составит 12,19 млрд долларов. Инвесторы обратили на это внимание. Ожидается, что технологические гиганты ОАЭ потратят более 2 миллиардов долларов на услуги центров обработки данных. Гиперскейлеры, такие как Amazon, Microsoft, Google, IBM и Oracle, борются за господство на рынке, чтобы предприятия могли передавать ИТ-задачи на аутсорсинг крупным удаленным центрам обработки данных. AWS, которая удивила многие известные технологические компании, доминируя на рынке внедрения облачных вычислений, инвестировала в Бахрейн, чтобы разместить свой первый центр обработки данных на Ближнем Востоке, и планирует открыть еще три в ОАЭ. Google создаст и будет управлять облачным регионом в Даммаме совместно с государственной компанией Saudi Aramco.

Amazon также сталкивается с жесткой конкуренцией со стороны таких конкурентов, как Microsoft и Oracle. Microsoft открыла два центра обработки данных в ОАЭ; Oracle запустила подземную облачную зону с двумя центрами обработки данных в Абу-Даби.

Это свидетельствует о тщательном рассмотрении инновационного потенциала региона. У нас есть быстро расширяющаяся среда запуска и масштабирования, а также высококлассный предпринимательский интеллект, решающий сложные проблемы, и тот факт, что крупные интернет-компании вкладывают значительные средства в создание региональных центров обработки данных, является заслугой усердной работы местных технических специалистов.

НЕРВНЫЙ ЦЕНТР ЦИФРОВОЙ ИНФРАСТРУКТУРЫ

Ближний Восток является «приоритетным регионом» для интернет-компаний, поскольку они вкладывают огромные средства в улучшение своей инфраструктуры. Он становится центром цифровой инфраструктуры,

соединяющим людей, организации и остальной мир. Явной тенденцией последних лет стало создание специализированных облачных центров обработки данных на Ближнем Востоке гиперскейлерами, включая Microsoft, Oracle, Alibaba и Google Cloud. AWS заявила, что планирует создать облачный центр обработки данных в этом районе в этом году. Эти разработки имеют неоспоримое значение для местного бизнеса. Центры обработки данных являются центром ИТ-инфраструктуры в банковской, энергетической, транспортной и медицинской отраслях. Каждый сектор зависит от быстрых и безопасных приложений, которые может предложить современный центр обработки данных. Компании по хранению данных, такие как AWS,

Клиенты могут использовать предложения «Платформа как услуга» (PaaS) и «Инфраструктура как услуга» (IaaS), что позволяет другим поставщикам «Решения как услуги» (SaaS) делать свои облачные решения доступными через региональные зоны доступности.

СТАРТАПЫ ПРИНОСЯТ ПОЛЬЗУ

Чем больше данных будет анализировать бизнес, тем больше ему придется тратить на серверы и место для хранения. Организации всех размеров, включая стартапы, государственные и частные предприятия и образовательные учреждения, используют центры обработки данных и Интернет для масштабирования своей деятельности. Дешевле арендовать пространство в центрах обработки данных, в которых размещается несколько предприятий. Например, базирующийся в Дубае стартап Digiteam занимается оцифровкой продаж и геймификацией решений для внедрения облачных технологий и расширяет свое присутствие на новых клиентов в различных регионах. Аналогичным образом, Norbloc, поставщик технологий, управляющий экосистемой блокчейна KYC в ОАЭ, обеспечивает более быстрый и безопасный обмен данными о клиентах, используемый крупнейшими финансовыми учреждениями страны.

Поскольку 90% компаний в регионе присоединились к цифровизации, эти гиперскейлеры прокладывают путь корпорациям для переноса приложений и рабочих нагрузок в облачные приложения, соблюдая при этом местные требования,

требующие сохранения определенных данных внутри страны. Наличие «зоны» центра обработки данных в стране необходимо для соблюдения требований к наиболее конфиденциальным типам данных. Безопасность данных все больше и больше интегрируется в дизайн продукта, поскольку правила меняются вместе с ожиданиями потребителей в отношении того, как обрабатываются их данные.

Эти гиперскейлеры позволяют региональным клиентам создавать резервные копии своих данных внутри страны, что важно для клиентов, работающих в регулируемых отраслях и соблюдающих национальное законодательство.

Фундаментальный принцип законодательства о конфиденциальности данных в Объединенных Арабских Эмиратах и Саудовской Аравии заключается в том, что предприятия должны собирать как можно меньше данных, отслеживать их местонахождение и защищать их. В ответ на объявление AWS о своих инвестициях в ОАЭ, создание Google своего центра обработки данных в Саудовской Аравии в партнерстве с Aramco, стратегические инвестиции Huawei в этом регионе и присутствие в регионе Oracle, Microsoft и IBM, глобальных поставщиков технологий будет либо увеличивать мощности существующих центров обработки данных, либо строить новые. Что касается инноваций, каждая компания вкладывает значительные средства в решения по автоматизации, мониторингу и управлению для контроля в режиме реального времени над операциями инфраструктуры, чтобы выделиться в качестве универсального поставщика центров обработки данных. В настоящее время есть признаки периферийных вычислений и более экологически чистой, устойчивой инфраструктуры и продуктов. В регионе все больше говорят об экологически чистых центрах обработки данных, что соответствует международным целям устойчивого развития. В свои облачные решения эти гиперскейлеры добавляют AI/ML, расширенную аналитику и интеллектуальную автоматизацию, чтобы дифференцировать свои продукты и привлекать новых клиентов.

Заключительные слова

Несмотря на множество препятствий для внедрения облачных технологий, в том числе потребности в безопасности, нехватку навыков и правила суверенитета данных, цифровые технологии постоянно развиваются.

Одно можно сказать наверняка: по мере того, как Ближний Восток превращается в глобальный технологический центр и создает передовую цифровую экономику, все больше компаний Кремниевой долины будут устанавливать там свои флаги для строительства центров обработки данных по мере того, как этот сектор будет процветать. Индустрия центров обработки данных быстро развивается благодаря пионерам и деловым людям в этой области, и в ближайшее время не ожидается, что она замедлится…». ***(Dariel Marlow. UAE businesses are increasingly utilizing cloud-based applications // Techstrong Group Inc. (https://securityboulevard.com/2022/12/uae-businesses-are-increasingly-utilizing-cloud-based-applications/). 16.12.2022).***

***

Вопросы, которые нужно задавать себе перед переходом в облако. «В то время как цифровая трансформация привела к целому ряду изменений, сдвигов парадигмы и преимуществ, одним из самых значительных результатов стал переход в облако. Помните, как вы впервые вошли в приложение по URL-адресу, и вам не нужно было загружать его на жесткий диск? Все, что вам нужно, это логин и пароль. Это было так круто и легко. Не нужно смотреть и надеяться, что исполняемый файл вашего нового приложения запустится правильно. Да, было здорово войти в удивительный мир (и эпоху) облака.

Облако, конечно, полезно не только для пользователей и клиентов. Для организаций, которые переносят приложения в облако, это обеспечивает маневренность, гибкость и способность внедрять инновации быстрее и проще, простоту, которую он приносит в ИТ, переход от модели капитальных затрат к модели эксплуатационных расходов и, конечно же, экономию средств. (если все сделано правильно). Все хорошо, конечно, но, к сожалению, иногда случается так, что безопасность становится запоздалой мыслью, когда организации

придерживаются мышления «мы вернемся к этому позже». Это не лучший способ думать о кибербезопасности. Это всегда должно быть «Давайте позаботимся о том, чтобы мы учитывали безопасность на каждом этапе пути».

Хотя приведенное ниже, конечно же, не означает, что наши клиенты относятся к ИТ-безопасности с позиции «Мы вернемся позже» (в конце концов, они используют Radware!), нам нравится расспрашивать их по целому ряду вопросов кибербезопасности, потому что мы всегда получаем проницательную информацию., интересные и, пожалуй, самое главное, поучительные ответы. Вы увидите, что этот месяц ничем не отличается.

«Что бы вы хотели знать о проблемах облачной безопасности до перехода в облако?»

Всегда весело и интересно получать десятки ответов и видеть, что несколько ответов появляются снова и снова. В этом случае снова и снова всплывали 3 момента: отсутствие навыков безопасности у персонала, степень, в которой конфигурация играла неотъемлемую роль, влияние на API и отсутствие информации об их облачной инфраструктуре и приложениях. Опять же, всегда интересно.

«Я хотел бы знать пару вещей, включая то, как мало опыта у нас было в штате, и прямую связь между неправильными настройками параметров безопасности и утечкой данных».

«Неправильные настройки параметров облачной безопасности, по-видимому, являются основной причиной утечек облачных данных. Кроме того, я не был готов к тому, что облачные сервисы не будут контролировать мои приложения».

«Многие из нашего ИТ-персонала, включая меня, считали, что все данные, связанные с правительством, можно перенести в общедоступное облако. Хотя многие правительства в настоящее время требуют, чтобы приложения для мэйнфреймов были перенесены в облако, это не означает, что все может быть автоматически выполнено».

«Я был удивлен, что в облаке вообще отсутствует безопасность».

«Есть несколько вещей, которые мне хотелось бы знать и к которым можно было подготовиться до миграции в облако: у нас было гораздо меньше специалистов по безопасности, чем я предполагал. Кроме того, я не понимал, в какой степени неправильная конфигурация облачного сервера может привести к утечке данных; это означает, что ключевые данные становятся доступными непосредственно в Интернете».

«Я не ожидал проблем, связанных с обеспечением безопасности данных. Миграция в облако требует тщательного и тщательного планирования. Без такого уровня знаний и опыта критически важные данные могут сразу же стать уязвимыми для атак. Звучит элементарно, но вы должны помнить, что передается много конфиденциальных и важных данных. Это автоматически делает его уязвимым для атак».

«Я не знал и не понимал, что это значит для безопасности API. А неправильные настройки могут создать множество уязвимостей, о которых вы можете не знать, даже если ваши приложения защищены».

«Когда вы настолько увлечены своим портфелем приложений, что легко отодвинуть вопросы безопасности в сторону. Но это нужно тщательно обдумать с самого начала».

«Я не ожидал отсутствия информации об облачной безопасности. Кроме того, незащищенные API и интерфейсы могут легко и быстро стать серьезными проблемами безопасности облачных вычислений. Хотя API-интерфейсы необходимы для персонализированного облачного взаимодействия, просто помните, что они представляют реальную угрозу безопасности».

«Легко увлечься переходом в облако, но понимать, что у вас будет меньше видимости и контроля, чем вы могли себе представить. Вы должны знать об этом и быть готовыми к этому».

«Я не ожидал, что у наших сотрудников не будет навыков и знаний в области безопасности. И помните, что многие команды DevOps и облачных инженеров часто «берут все в свои руки», даже если у них может не быть опыта или даже

четкого понимания облачных технологий, не говоря уже о том, как они влияют на безопасность».

«Создайте свой план облачной безопасности заранее и обязательно в тандеме со всем остальным. Это поможет вам оставаться честными и думать о безопасности на протяжении всего вашего путешествия в облако».

Вот отличный способ узнать об облачной безопасности

Цифровая революция началась около 40 лет назад, и, бесспорно, одним из ее самых значительных преимуществ является миграция приложений и рабочих нагрузок в облако. Конечно, это не означает, что переход в облако не будет сопряжен со многими проблемами. Просто помните об этом — не сводите глаз с охраны. Надеемся, что наши клиенты дали вам пищу для размышлений перед миграцией в облако. Опять же, это то, что они хотели бы знать.

Для получения дополнительной информации о том, как сосредоточиться на защите своего облака, обратитесь к специалистам по кибербезопасности в Radware…». ***(“What I Wish I Would Have Known About Cloud Security Prior to our Cloud Migration” // Techstrong Group Inc. (https://securityboulevard.com/2022/12/what-i-wish-i-would-have-known-about-cloud-security-prior-to-our-cloud-migration/). 15.12.2022).***

***

«Опубликованный сегодня опрос показал, что более половины (59%) респондентов считают, что переход в облако сделал их предприятие менее безопасным. Опрос, проведенный CloudBolt Software, поставщиком платформы автоматизации ИТ, в котором приняли участие 350 ИТ-руководителей крупных предприятий с более чем 5000 сотрудников, показал, что более трех четвертей (79%) респондентов также задавались вопросом, применяют ли их компании последовательные уровни применения политики облачной безопасности.

Более двух третей (68%) заявили, что набор навыков безопасности их организаций во всех облаках лишь в некоторой степени развит. Еще 20% охарактеризовали свои навыки как относительно нейтральные.

Почти три четверти респондентов (72%) признали, что их организации перешли либо в облачную, либо в мультиоблачную среду, не имея надлежащего понимания связанных с этим навыков, кривой зрелости и сложности безопасности. Более половины (56%) также отметили нехватку опыта и ресурсов в области мультиоблачной и облачной безопасности, а 48% назвали операционную сложность и поддержку мультиоблачной среды ключевыми проблемами.

В целом, три четверти респондентов (75%) описали облачные вычисления как крупнейшее расширение корпоративной поверхности атаки за последние 20 лет.

Генеральный директор CloudBolt Software Джефф Куковски сказал, что способ предоставления сред облачных вычислений лежит в основе большинства этих проблем с безопасностью. Разработчики, практически не имеющие опыта в области кибербезопасности, обычно предоставляют облачные ресурсы, а затем развертывают приложения практически без средств защиты от кибербезопасности. Тот факт, что ошибки совершаются, почти неизбежен, отметил он.

По словам Куковски, большинство развертываний локальных приложений, напротив, обрабатывается централизованной командой, которая обычно проверяет настройки на наличие неправильных конфигураций. Он добавил, что единственный способ обеспечить такой же уровень гарантии кибербезопасности в облаке — это полагаться на платформы автоматизации, которые ограничивают количество ошибок.

С другой стороны, опрос также показывает, что организации больше внимания уделяют вопросам безопасности в облаке. Более трех четвертей респондентов (79%) заявили, что, по их мнению, совет директоров и руководители их организаций продемонстрировали готовность сделать все необходимое для обеспечения безопасности облачных вычислений. Целых 83% также выразили уверенность в том, что их директор по информационной безопасности сможет достичь этой цели.

Тем не менее, исследование показывает, что организациям еще предстоит пройти долгий путь, прежде чем платформы облачных вычислений станут безопасными. Только 8 % респондентов заявили, что при развертывании новых

вычислительных ресурсов и сред они внедрили высокоэффективные методы обеспечения облачной безопасности. Только 6% заявили, что их компании заранее автоматически встраивают средства безопасности в каждую рабочую нагрузку и координируют процессы во всех облаках, чтобы разработчикам не приходилось об этом беспокоиться.

Еще меньше (3%) заявили, что их организация постоянно использует неизменяемую инфраструктуру в качестве меры безопасности, с помощью которой облачные ресурсы автоматически уничтожаются и восстанавливаются каждые установленное количество дней.

Возможно, проблемы безопасности в облаке сегодня больше связаны с культурным разрывом между командами по кибербезопасности и разработчиками приложений внутри организаций. Этот разрыв увеличился с тех пор, как первый облачный ресурс был программно запущен более 10 лет назад. Теперь задача состоит в том, чтобы найти способ преодолеть этот разрыв без существенного влияния на скорость развертывания и обновления новых приложений в облачную эпоху». ***(Michael Vizard. Survey Surfaces General Sense of Cloud Insecurity in the Enterprise // Techstrong Group Inc. (https://securityboulevard.com/2022/12/survey-surfaces-general-sense-of-cloud-insecurity-in-the-enterprise/). 14.12.2022).***

***

«Reportlinker.com объявляет о выпуске отчета «Отчет о глобальном рынке внешних облачных автомобильных услуг кибербезопасности за 2022 год: влияние войны между Украиной и Россией»...

Ожидается, что мировой рынок внешних облачных услуг кибербезопасности для автомобилей вырастет с 1,74 млрд долларов в 2021 году до 2,12 млрд долларов в 2022 году при среднегодовом темпе роста (CAGR) в 21,8%. Российско-украинская война подорвала шансы на восстановление мировой экономики после пандемии COVID-19, по крайней мере, в краткосрочной перспективе. Война между этими двумя странами привела к экономическим санкциям в отношении нескольких стран, росту цен на сырьевые товары и сбоям в цепочке поставок, что затронуло

многие рынки по всему миру. Ожидается, что рынок внешних облачных услуг кибербезопасности для автомобилей вырастет до 4,14 млрд долларов в 2026 году при среднегодовом темпе роста 18,3%.

Рынок внешних облачных автомобильных услуг кибербезопасности состоит из продаж внешних облачных автомобильных услуг кибербезопасности субъектами (организациями, индивидуальными предпринимателями и партнерствами), которые полезны для защиты автомобильных электронных систем, сетей связи, алгоритмов и пользовательских данных от вредоносных атак или несанкционированный доступ. Кибербезопасность — это практика защиты и защиты компьютеров, периферийных устройств, сетей и систем от вредоносных атак и вирусов.

Автомобили подключены к Интернету и уязвимы для киберугроз. Таким образом, автомобильная кибербезопасность имеет важное значение для автопроизводителей.

Основными типами безопасности во внешних облачных автомобильных службах кибербезопасности являются безопасность конечных точек, безопасность приложений и безопасность беспроводной сети. Различные типы транспортных средств включают легковые и коммерческие автомобили.

Легковые автомобили используются для перевозки пассажиров. Легковые автомобили - это дорожные транспортные средства, предназначенные для перевозки пассажиров, с большой площадью сидения и предметами роскоши.

Различные типы электромобилей включают аккумуляторные электромобили, гибридные электромобили и подключаемые гибридные электромобили, которые используются в телематических системах, информационно-развлекательных системах, системах трансмиссии, системах управления телом и комфорте, системах связи, а также ADAS и системах безопасности.

Северная Америка была крупнейшим регионом на рынке внешних облачных автомобильных услуг кибербезопасности в 2021 году. Регионы, охваченные в отчете о рынке внешних облачных автомобильных услуг кибербезопасности, включают Азиатско-Тихоокеанский регион, Западную Европу, Восточную Европу, Северную Америку, Южную Америку, Ближний Восток. и Африка.

Ожидается, что рост числа подключенных автомобилей будет способствовать росту рынка внешних облачных автомобильных услуг кибербезопасности в будущем. Подключенный автомобиль — это транспортное средство, которое может получить доступ к Интернету для подключения к другим автомобилям через встроенную систему подключения.

В последнее время количество подключенных автомобилей и автомобилей с интеллектуальными функциями подключения растет. Эти автомобили могут иметь доступ к Интернету, но они также уязвимы для кибератак и поэтому нуждаются в услугах кибербезопасности.

Например, согласно отчету о подключенных автомобилях британского поставщика новостей о технологиях Internet of Business, ожидается, что количество подключенных автомобилей увеличится на 270% до 125 миллионов автомобилей в 2022 году. стимулирует спрос на рынок внешних облачных автомобильных услуг кибербезопасности.

Технологический прогресс является ключевой тенденцией, набирающей популярность на рынке внешних облачных автомобильных услуг кибербезопасности. Игроки на рынке постоянно внедряют инновации и внедряют новые технологии, чтобы лидировать на рынке.

Например, в марте 2022 года индийская компания информационных технологий Wipro запустила платформу Cloud Car, оснащенную комплексной системой кибербезопасности. С ее помощью производители автомобилей могут устранять сбои программного обеспечения с помощью беспроводных обновлений.

Платформа разделит ранее интегрированное аппаратное и программное обеспечение, что позволит производителям масштабно обновлять программное обеспечение.

В сентябре 2021 года LG Electronics, южнокорейская компания по производству бытовой электроники, приобрела Cybellum за 240 миллионов долларов. Это приобретение позволит LG Electronics расширить свои возможности кибербезопасности и предложения автономных систем.

Cybellum — израильская автомобильная компания по кибербезопасности, которая выявляет уязвимости в автомобильном оборудовании и программном обеспечении.

Страны, охваченные в отчете о рынке внешних облачных автомобильных услуг кибербезопасности, включают Австралию, Бразилию, Китай, Францию, Германию, Индию, Индонезию, Японию, Россию, Южную Корею, Великобританию, США.

Отчет об исследовании рынка внешних облачных автомобильных услуг кибербезопасности является одним из серии новых отчетов, в которых представлена статистика рынка внешних облачных автомобильных услуг кибербезопасности, включая размер мирового рынка, региональные доли, конкурентов с долей рынка внешних облачных автомобильных услуг кибербезопасности, подробные внешние данные. сегменты рынка облачных автомобильных услуг кибербезопасности, рыночные тенденции и возможности, а также любые дополнительные данные, которые могут вам понадобиться для достижения успеха в отрасли внешних облачных автомобильных услуг кибербезопасности. Этот отчет об исследовании рынка внешних облачных автомобильных услуг кибербезопасности дает полное представление обо всем, что вам нужно, с углубленным анализом текущих и будущих сценариев развития отрасли». ***(External Cloud Automotive Cyber Security Services Global Market Report 2022: Ukraine-Russia War Impact // GlobeNewswire, Inc. (https://www.globenewswire.com/news-release/2022/12/05/2567655/0/en/External-Cloud-Automotive-Cyber-Security-Services-Global-Market-Report-2022-Ukraine-Russia-War-Impact.html). 05.12.2022).***

***

Кіберзлочинність та кібертероризм

«Згідно з новим звітом фірми безпеки блокчейну CertiK, у 2022 році число шахрайських YouTube-відео на тему криптовалют зросло у шість разів

— зловмисники активно просувають фейкові ролики з рекламою ботів для трейдингу. Аналітики нарахували 168 таких відео у 2022 році, а у 2021 — всього 28. Таким чином кількість шахрайського контенту зросла на 500%.

Сама афера зазвичай полягає у тому, що жертв заманюють обіцянкою щоденного заробітку за відсутності вкладень. Постраждалі завантажують програмне забезпечення фейкового бота, сам бот сканує непідтверджені великі транзакції та сплачує більшу комісію за газ, щоб гарантувати пріоритетне проведення його угоди. Аналітики наголошують, що таким чином бот може маніпулювати ринковими цінами.

CertiK у звіті наводить приклади реальних YouTube-відео з сумнівними назвами — наприклад, «Uniswap Front Running Bot 2022 — ЛЕГКІ ІНСТРУКЦІЇ (Величезний прибуток)!», у якому шахраї пропонують користувачам підроблені методички із завантаження та використання ботів для трейдингу. Деякі учасники навіть стверджували, що алгоритм YouTube пропонував їм відео у головних рекомендаціях. Захоплені коментарі під таким контентом також написані ботами — це робиться з метою відвернення уваги від реальних відгуків користувачів, які можуть повідомити про хакерську загрозу.

Аналітики CertiK також опублікували окремий звіт, в якому зазначено, що криптошахраї використовують ідентифікаційні дані впливових гравців галузі,

куплені на чорному ринку. Експерти підкреслили, що потрібну інформацію можна придбати у даркнеті, ціна стартує від $ 8.

У криптовалютному просторі шахрайство за допомогою фальшивого медіаконтенту вже не викликає великого здивування. В кінці листопада ми розповідали про поширення діпфейку із зображенням ексдиректора збанкрутілої криптобіржі FTX Сема Бенкмана-Фріда, який обіцяв інвесторам повернути втрачені кошти. Підроблене відео поширював верифікований профіль, який раніше піддався злому». ***(Атаки криптошахраїв в YouTube зросли на 500% // No worries! (https://noworries.news/ataky-kryptoshahrayiv-v-youtube-zrosly-na-500/). 02.12.2022).***

***

«Американський метал-гурт Metallica звернувся до своїх фанатів у соцмережах з попередженням про криптовалютних шахраїв, які почали викрадати токени у користувачів після анонсу про випуск нового альбому гурту.

Представники Metallica вирішили застерегти своїх прихильників після підтвердження інформації про те, що один із шанувальників гурту втратив $ 25 500 через фейковий канал Metallica на YouTube. Зловмисники поширили повідомлення про те, що на честь виходу нового альбому всі фанати Metallica зможуть подвоїти власні криптовалютні заощадження.

«На жаль, ми зіткнулись із неприємною стороною соціальних мереж. Шахрайські YouTube-канали та сайти пропонують роздачу токенів Metallica Crypto. Будь ласка, пам’ятайте — це фейк», — йдеться у зверненні групи.

Використання YouTube для викрадення криптовалюти вже довгий час є популярним методом серед хакерів. Так наприкінці вересня YouTube-канали уряду Південної Кореї постраждали від атаки хакерів, які видавали себе за мільярдера Ілона Маска — під загрозою опинились тисячі користувачів. За стандартною схемою, для більшої правдоподібності зловмисники публікували інтерв'ю з Маском та іншими прихильниками криптовалют. Очевидно, головною метою шахраїв було спонукати користувачів перейти за фішинговим посиланням, розміщеним в описі,

щоб отримати доступ до криптовалютних гаманців жертв. Втім, південнокорейський уряд оперативно відреагував на інцидент і вже через декілька годин доступ до каналів був відновлений, а шахрайські відео видалені». ***(Криптовалютні шахраї крадуть токени фанатів Metallica // No worries! (https://noworries.news/kryptovalyutni-shahrayi-kradut-tokeny-fanativ-metallica/). 06.12.2022).***

***

«Не теряйте времени, сообщая о подозрительном веб-сайте, который подвергает риску вас и других.

Статистика количества мошеннических сайтов, засоряющих Интернет, вызывает тревогу. В течение 2020 года только Google зарегистрировал более 2 миллионов фишинговых сайтов. Это означает, что каждый день появляется более 5000 новых фишинговых сайтов, не говоря уже о тех, которые не были обнаружены Google. В 2021 году Федеральное бюро расследований США (ФБР) сообщило об убытках почти в 7 миллиардов долларов от киберпреступлений, совершаемых через эти сайты.

Что такое мошеннические сайты? Под мошенническими веб-сайтами понимаются любые незаконные веб-сайты, которые используются для обмана пользователей с целью мошенничества или злонамеренных атак. Многие мошенники управляют этими поддельными веб-сайтами и загружают вирусы на ваш компьютер или крадут пароли или другую личную информацию.

Сообщать об этих сайтах по мере их обнаружения — важная часть борьбы с ними. Другими словами, если вы что-то видите, скажите что-нибудь. Молчание, даже если вы избегаете стать жертвой, позволяет мошенникам нацелиться на другую цель.

Возможно, вы получили подозрительную ссылку по электронной почте? Или, может быть, странное текстовое сообщение, на которое вы не нажали. К счастью, есть много организаций, которые предприняли усилия, направленные на снижение угрозы, которую они представляют. Как правило, эти организации выявляют

мошеннические веб-сайты, собирая и распространяя информацию о них. В некоторых случаях они побуждают к расследованию мошенников, стоящих за сайтами.

Сообщить о подозрительном веб-сайте, с которым вы столкнулись, можно бесплатно, и это займет всего минуту. Вот восемь способов сообщить о предполагаемом мошенническом веб-сайте, чтобы остановить киберпреступников и защитить себя и других в Интернете.

1. Центр жалоб на интернет-преступления

IC3, как известно, является офисом ФБР, который получает жалобы от тех, кто стал жертвой интернет-преступлений. IC3 определяет интернет-преступления, которые она рассматривает, как включающие незаконную деятельность с участием веб-сайтов. Жалобы, поданные в IC3, рассматриваются и исследуются обученными аналитиками ФБР.

2. Агентство кибербезопасности и безопасности инфраструктуры

CISA, агентство Министерства внутренней безопасности США, нацелено на широкий спектр злонамеренной киберактивности. Он специально запрашивает отчеты о фишинговой активности с использованием мошеннических веб-сайтов. Информация, предоставленная CISA, передается Рабочей группе по борьбе с фишингом, некоммерческой организации, деятельность которой направлена на снижение воздействия мошенничества, связанного с фишингом, во всем мире.

3. www.econsumer.gov

Сайт econsumer.gov, управляемый Международной сетью защиты прав потребителей и правоприменения, предназначен для сообщения о международном мошенничестве. Он поддерживается агентствами по защите прав потребителей и соответствующими офисами в более чем 65 странах. Защищенная версия их сайта используется правоохранительными органами для обмена информацией о мошенничестве.

4. Безопасный просмотр Google

Хотя у Google нет механизма для сообщения обо всех видах мошенничества с веб-сайтами, существует форма для сообщения о сайтах, которые подозреваются в

использовании для фишинга. Отчеты, сделанные с помощью формы, обрабатываются командой безопасного просмотра Google. Отчет о прозрачности Google предоставляет информацию о сайтах, которые были определены как «опасные для посещения в настоящее время».

5. Фиштанк

Эта услуга была основана Cisco Talos Intelligence Group, чтобы «пролить солнечный свет на некоторые из темных переулков Интернета». Phishtank включает в себя постоянно растущий список URL-адресов, о которых сообщается, что они связаны с фишингом. На сегодняшний день он получил более 7,5 миллионов сообщений о потенциальных фишинговых сайтах. В нем говорится, что более 100 000 сайтов все еще находятся в сети.

6. Антивирусные приложения

Поставщики антивирусных программ, такие как Norton, Kaspersky и McAfee, имеют формы, которые можно использовать для идентификации страниц, которые, по мнению пользователей, должны быть заблокированы. Мошеннические сайты определенно подпадают под эту категорию. На некоторых антивирусных платформах доступ к формам отчетности возможен только для зарегистрированных пользователей. Нортон открыт для всех.

7. Веб-хостинг

Есть вероятность, что служба DNS, на которой размещен мошеннический сайт, примет меры, чтобы закрыть его. Существует множество онлайн-ресурсов, которые могут помочь вам найти DNS определенного сайта. Как только вы определите его, отправьте сообщение в их службу поддержки клиентов, сообщив о рассматриваемом сайте и опыте, который у вас был.

8. Поделитесь своим опытом в социальных сетях

На самом деле это больше похоже на сигнал тревоги, чем на подачу отчета, но это может защитить одного из ваших знакомых, который наткнется на тот же сайт или станет жертвой того же типа мошенничества. По крайней мере, это может привлечь внимание к тому факту, что мошеннические сайты влияют на реальных людей. Сообщение на Facebook о том, что вы были на грани мошенничества, может

лучше подготовить вашу сеть, чтобы избежать любых опасных запутываний. Если это произойдет, они будут вам благодарны». ***(Jay Feldman. Think You've Just Been Exposed to a Cyber Criminal? Here Are 8 Ways You Can Save Yourself and Others From Being Scammed // Entrepreneur Media, Inc (https://www.entrepreneur.com/growing-a-business/8-ways-you-can-save-yourself-and-others-from-being-scammed/438213). 03.12.2022).***

***

«Кампания может исходить от северокорейской группы, печально известной социальной инженерией

Злоумышленник, возможно, северокорейская Lazarus Group, заманивает крупных трейдеров в чат-группах Telegram по криптовалютам для установки бэкдоров, якобы запрашивая их отзывы о структуре комиссий торговой платформы.

Поддерживаемые государством хакеры Пхеньяна все больше специализируются на краже криптовалюты, поскольку режим ищет источники твердой валюты для подпитки своей программы оружия массового уничтожения. Группа экспертов ООН в 2019 году подсчитала, что киберпреступность принесла наследственной монархии чучхе около 2 миллиардов долларов, и с тех пор эта сумма только росла.

Исследователи из Microsoft и компании Volexity, специализирующейся на цифровой криминалистике, говорят, что заметили кампанию, которая манипулирует жертвами, заставляя их открывать электронные таблицы Excel, загруженные вредоносными макросами. Volexity связывает кампанию с Lazarus Group, в то время как Microsoft обозначает субъекта угрозы как DEV-0139, используя номенклатуру, зарезервированную для неизвестных или новых кластеров активности угроз. Вычислительный гигант отслеживает известную активность Lazarus под псевдонимом «Цинк».

Lazarus печально известен тем, что использует тактику социальной инженерии в качестве начального вектора доступа, прибегая к таким методам, как

размещение поддельной рекламы профилей LinkedIn, чтобы заманить пользователей к загрузке вредоносных полезных нагрузок (см.: Северная Корея Троянизирует программное обеспечение с открытым исходным кодом).

В статье Volexity бэкдор, загруженный кампанией, идентифицируется как вредоносное ПО AppleJeus — вредоносное приложение, которое, по словам федерального правительства США, северокорейские хакеры использовали как минимум с 2018 года для кражи криптовалюты.

Microsoft отслеживает активность кампании в группах Telegram, используемых для облегчения связи между VIP-клиентами и криптовалютными платформами, и говорит, что инженеры злоумышленников нацеливали жертв на открытие зараженного файла Excel, запрашивая их мнение о структурах торговых комиссий. Telegram стал коммуникационным центром по умолчанию для трейдеров криптовалюты — «основой криптосообщества», как один человек описал его ранее в этом году TechCrunch.

Электронная таблица содержит законные данные о комиссиях, взимаемых платформами с пользователей. Платформы для торговли криптовалютой часто предлагают трейдерам скидки на комиссионные сборы, чья стоимость и отсутствие прозрачности являются источником давних жалоб в криптовалютном сообществе.

Злоумышленник побуждает жертв включать файловые макросы, защищая паролем главный лист и предоставляя им парольную фразу, которая называется «дракон».

Microsoft заявляет, что файл Excel, созданный с применением оружия, выполняет запутанный макрос, который извлекает вторую электронную таблицу, которая, в свою очередь, запускает макрос, открывающий файл png из учетной записи облачного хранилища.

В png файл встроены три исполняемых файла, включая закодированный бэкдор. Один из файлов, logagent.exe, загружает вредоносный wsock32.dll, который проксирует легитимный файл wsock32.dllдля декодирования и запуска бэкдора.

wsock32.dll 32-разрядная библиотека Windows Socket, является важным компонентом операционной системы, обеспечивающим правильную работу

программ Windows, и logagent.exe является системным приложением, используемым для регистрации ошибок проигрывателя Windows Media и отправки информации для устранения неполадок». ***(Prajeet Nair. Social Engineering Hackers Use Excel to Target Crypto VIPs // Information Security Media Group, Corp. (https://www.govinfosecurity.com/social-engineering-hackers-use-excel-to-target-crypto-vips-a-20644). 07.12.2022).***

***

«Индийская фирма обвиняет «печально известную компанию по кибербезопасности» в продолжающемся инциденте

Индийская фирма, занимающаяся кибербезопасностью, обвинила другое подразделение кибербезопасности в использовании скомпрометированных учетных данных платформы для совместной работы для получения доступа к своему внутреннему учебному сайту.

Рахул Саси, генеральный директор CloudSEK из Бангалора, не назвал предполагаемого преступника, кроме как охарактеризовать его как «печально известную компанию по кибербезопасности, которая занимается мониторингом темной сети».

CloudSEK, которая заявляет, что использует искусственный интеллект для прогнозирования киберугроз, поздно вечером во вторник опубликовала обновленную информацию о продолжающемся инциденте кибербезопасности, заявив, что кто-то получил учетные данные сотрудника для входа в систему отслеживания проблем Atlassian Jira и использовал их для доступа к Atlassian Confluence. сервер.

Злоумышленник взял «некоторые внутренние данные, такие как скриншоты, отчеты об ошибках, имена клиентов и диаграммы схем», но «ни база данных, ни доступ к серверу не были скомпрометированы», — написал Саси.

В обновлении от Sasi, опубликованном примерно через два часа, говорится, что индикаторы атак привели к неопознанной компании, занимающейся мониторингом даркнета.

Саси также написал, что хакер под ником «sedut» присоединился к ряду форумов по киберпреступности и оспорил утверждения хакера о том, что он получил доступ к VPN компании, а также к ее основной базе данных и ее учетной записи в Twitter. CloudSek признает, что хакер получил доступ к его экземпляру Jira и получил некоторые заказы клиентов.

По словам компании, хакер не получил доступа к основной учетной записи компании в Twitter, но взломал учетную запись, используемую для удаления. Предполагаемые скриншоты и видео базы данных, размещенные в Интернете «sedut», на самом деле были взяты с обучающих веб-страниц, размещенных на платформах Atlassian, добавляет он. Компания заявляет, что хакер не получил учетные данные VPN, но получил доступ к ее IP-адресам VPN.

Что касается того, как в первую очередь были скомпрометированы учетные данные сотрудника Jira, компания заявляет, что отправила неисправный ноутбук сотрудника стороннему поставщику, и когда ноутбук был возвращен, на нем был установлен Vidar Stealer. CloudSEK заявляет, что злоумышленник приобрел файлы cookie сеанса сотрудника в тот же день, когда оператор похитителя информации загрузил их на криминальный рынок.

Криминальный форум содержит пост от «sedut», который предлагает продать предполагаемые данные CloudSek — 10 000 долларов за базу данных, 8 000 долларов за кодовую базу и 8 000 долларов за документацию для сотрудников и инженерных продуктов. CloudSEK заявляет, что не обнаружил «подозрительной активности» в своих репозиториях кода.

«Не спонсируется государством (пожалуйста, наймите меня, лол). Здесь только для того, чтобы зарабатывать деньги. Все об этих деньгах, детка», — написал «sedut» в посте». ***(Akshaya Asokan. CloudSEK Pins Blame for Hack on Other Cybersecurity Firm // Information Security Media Group, Corp. (https://www.govinfosecurity.com/cloudsek-pins-blame-for-hack-on-other-cybersecurity-firm-a-20652). 07.12.2022).***

***

«Хакеры, похоже, искали список контактов Amnesty.

Этой осенью канадское отделение Amnesty International стало жертвой изощренного нарушения кибербезопасности — атака, по мнению судебно-медицинских экспертов, была совершена в Китае с благословения правительства Пекина.

Вторжение было впервые обнаружено 5 октября, сообщила правозащитная группа в понедельник.

По данным компании по кибербезопасности, проводившей судебно-медицинское расследование, атака показала признаки работы так называемой группы продвинутых постоянных угроз (APT).

В отличие от типичной атаки киберпреступников, атака на Amnesty включала в себя установление скрытого наблюдения за операционной системой сети Amnesty, говорится в отчете, подготовленном для Amnesty International Canada британской фирмой по кибербезопасности Secureworks.

Похоже, хакеры пытались получить список контактов Amnesty и следить за ее планами.

Откровение приходит, когда отношения между Канадой и Китаем остаются холодными на нескольких фронтах.

Secureworks заявила, что уверена в своем выводе о том, что Пекин или группа, связанная с правительством Китая, несет ответственность за взлом.

«Эта оценка основана на характере целевой информации, а также на наблюдаемых инструментах и поведении, которые соответствуют тем, которые связаны с китайскими группами угроз кибершпионажа», — говорится в отчете.

Кетти Нивьябанди, генеральный секретарь Amnesty International Canada, сказала, что этот опыт должен стать четким предупреждением для других правозащитных групп и членов гражданского общества.

«Этот случай кибершпионажа говорит о все более опасном контексте, в котором сегодня должны ориентироваться активисты, журналисты и гражданское общество», — сказала она.

«Наша работа по расследованию и выявлению этих актов никогда не была более важной и актуальной. Мы продолжим освещать нарушения прав человека, где бы они ни происходили, и осуждать использование правительствами цифрового наблюдения для удушения прав человека».

Майк Маклеллан, директор по разведке Secureworks, сказал, что преследование правозащитных групп подпадает под недавние методы работы Китая.

«Китай использует свои кибервозможности для сбора политической и военной разведывательной информации и шпионажа, а такие организации, как Amnesty, интересны Китаю из-за людей, с которыми они работают, и работы, которую они выполняют», — сказал Маклеллан CBC News. «Мы видим, что подобные организации становятся мишенью, потому что Китай заинтересован в слежке».

Он сказал, что не верит, что существует какая-либо связь между нынешним напряженным характером канадско-китайских отношений и временем кибератаки.

«Я думаю, что это гораздо больше об Amnesty Canada, чем о Канаде и Китае», — сказал Маклеллан.

Через четыре дня после публикации доклада Amnesty International посольство Китая в Оттаве выступило с резким опровержением, обвинив правозащитную группу в том, что она вводит общественность в заблуждение и «распространяет ложь и слухи о Китае».

«Как стойкие защитники кибербезопасности, мы решительно выступаем против атак любого рода и боремся с ними. Китай никогда не будет поощрять, поддерживать или потворствовать таким кибератакам», — говорится в неподписанном заявлении.

Прошлым летом другая фирма по кибербезопасности из Массачусетса — Recorded Future — выпустила отчет, предупреждающий о том, что хакерские группы, подозреваемые в том, что они действуют на правительство Китая, были вовлечены в многолетнюю шпионскую кампанию против многочисленных

правительств, неправительственных организаций, аналитических центров и информационных агентств.

В отчете говорится, что кампания нацелена на Международную федерацию прав человека (FIDH), Amnesty International, Институт китайских исследований Меркатора (MERICS), Радио «Свободная Азия» (RFA), Американский институт на Тайване, правящую Демократическую прогрессивную партию Тайваня (ДПП) и Национальный центр информатики Индии с 2019 года.

Канадская организация Citizen Lab, занимающаяся наблюдением за интернетом, в 2016 году опубликовала крупное исследование, которое показало, что в нее и другие организации гражданского общества проникли кибершпионы, многие из которых связаны с Китаем.

Нацелен на шпионов, спонсируемых государством

Исследование основано на четырехлетнем исследовании с Tibet Action и девятью другими сотрудничающими группами гражданского общества. Восемь были ориентированы на Китай или Тибет; две из них были крупными международными правозащитными организациями.

В рамках этого новаторского исследования более 800 подозрительных электронных писем были проверены на наличие вредоносного программного обеспечения Citizen Lab, междисциплинарной лабораторией, базирующейся в Школе международных отношений и государственной политики Мунка Университета Торонто.

Нивьябанди сказал, что Amnesty International Canada осознает, что работа, которую она делает, может сделать ее мишенью.

«Как организация, выступающая за права человека во всем мире, мы прекрасно понимаем, что можем стать мишенью спонсируемых государством попыток сорвать нашу работу или наблюдать за ней», — сказала она.

«Это не запугает нас, и безопасность и конфиденциальность наших активистов, сотрудников, доноров и заинтересованных сторон остаются нашим главным приоритетом».

Она сказала, что соответствующие органы, персонал, доноры и заинтересованные стороны были проинформированы о взломе, и организация продолжит работу с экспертами по безопасности для защиты от будущих рисков». ***(Murray Brewster. Amnesty International Canada hit by cyberattack out of China, investigators say // CBC (https://www.cbc.ca/news/politics/amnesty-international-canada-cyber-attack-china-1.6674788). 05.12.2022).***

***

«Боковое смещение в течение некоторого времени было обычным фактором нарушений. Поскольку эффективность защиты периметра постепенно снижается, основной проблемой для злоумышленников является не то, как проникнуть в организацию, а то, как перемещаться по сети, чтобы получить доступ к своей конечной цели.

Типичная среда со временем превратилась в фрагментированный набор технических ресурсов — различных приложений, серверов, ИТ-инфраструктуры, облачных рабочих нагрузок и многого другого. Хотя эти ресурсы являются отдельными, все они связаны управлением идентификацией и доступом — инфраструктурой, управляющей доступом во всем.

Это то, что злоумышленники используют для бокового перемещения. Начиная с нулевого пациента, они переходят с одной машины на другую, злоупотребляя личными данными, пока не прибудут к месту назначения, чтобы сбросить программы-вымогатели, украсть конфиденциальную информацию и многое другое.

Понимание основ бокового движения

Как уже упоминалось, все начинается с того, что злоумышленники получают точку опоры на одной машине, что обычно достигается с помощью вредоносных программ или эксплойтов.

Используя нулевого пациента в качестве стартовой площадки, злоумышленник получит доступ к различным машинам, скомпрометировав учетные данные. Пароли, хэши и имена пользователей извлекаются из системной

памяти и после дампа используются для подключения к последующим машинам и ресурсам. Цель состоит в том, чтобы постоянно повышать уровни доступа для получения разрешений со все более ценными ресурсами. Злоумышленники также могут использовать уязвимости повышения привилегий, чтобы сократить этот процесс. Используя основные недостатки в инфраструктуре идентификации, злоумышленник может быстро назначить роли администратора злонамеренной учетной записи.

В конечном счете, эта цепная реакция повторяется до тех пор, пока злоумышленники не доберутся до своей цели, чтобы развернуть вредоносное ПО, эксфильтровать данные или получить доступ к критически важным ресурсам. Такие кажущиеся сложными методы стали обычным явлением; как и во всем, что касается безопасности, знания и инструменты, необходимые для проведения таких атак, теперь свободно доступны в Интернете.

Критические проблемы обнаружения бокового движения

Основные проблемы, связанные с остановкой бокового движения, — это недостаточная видимость и неспособность действовать в режиме реального времени.

Видимость затруднена по трем основным причинам. Во-первых, такие атаки злоупотребляют самой инфраструктурой, созданной для того, чтобы действовать как арбитр доверия для домена. IAM управляет доступом. Подрывая центральную систему, решающую, кто и к чему имеет доступ, действиям злоумышленника неявно доверяют независимо от злонамеренных намерений.

Во-вторых, боковое движение имеет очень ограниченный след. Злоумышленники «живут за счет земли»: выдавая себя за доверенных пользователей, они используют ресурсы, уже доступные в среде, для достижения своих целей. Их действия кажутся подлинными. Поскольку требуется очень мало дополнительных инструментов или процессов и часто используются доверенные протоколы для внешней связи, шансы средств контроля обнаружить аномалии невелики.

Фрагментарная природа идентичности бросает последний вызов видимости. В настоящее время большинство организаций используют комбинацию локальных каталогов и облачных IdP, которые не полностью взаимодействуют друг с другом. Это создает слепые зоны, которыми могут воспользоваться злоумышленники, и значительно усложняет управление, что также увеличивает затраты.

Без видимости остановить боковое движение сложно. Понять базовый уровень активности ключевых ресурсов, таких как учетные записи служб, на которые злоумышленники нацелены для перемещения по среде, невозможно. Без этого создание правил для предотвращения злонамеренного использования невозможно. Не только это, но и общие цели, такие как интерфейсы доступа, устаревшие приложения, ИТ-инфраструктура и многое другое, не защищены MFA и широко открыты для злоупотреблений. В конечном счете, службы безопасности остаются в затруднительном положении.

Создание проактивной защиты с использованием MFA следующего поколения и анализа рисков

Эффективная защита от горизонтального перемещения зависит от консолидированной видимости удостоверений во множестве разрозненных хранилищ в среде, а также от проактивной и адаптивной аутентификации.

Хотя исторически это было сложно, теперь можно собирать, анализировать и лучше понимать консолидированные идентификационные данные. Это можно использовать для построения картины поведения человеческих и автоматизированных учетных записей, чтобы понимать события на детальном уровне, вплоть до отдельных запросов на доступ. Делая это, организации могут использовать анализ рисков для выявления аномального поведения, выявляя случаи, когда субъект угрозы злоупотребляет удостоверением личности в злонамеренных целях.

Однако без возможности запретить доступ к каскадному набору технологий, используемых для горизонтального перемещения, организации в конечном итоге не смогут решить проблему. Часто используемые интерфейсы доступа, такие как PsExec или Remote Powershell, например, являются подарком для

злоумышленников, которые выдают себя за администраторов и запускают команды в удаленных системах. Другие ресурсы, такие как общие файлы, устаревшие приложения и другая важная ИТ-инфраструктура, также обычно широко открыты и используются в качестве трамплина для горизонтального перемещения. Закрытие подозрительного доступа к ним имеет решающее значение для пресечения движения злоумышленника.

Для этого необходимо развернуть проактивную аутентификацию на таких ресурсах, чтобы заблокировать попытки злонамеренного доступа. Именно здесь MFA, широко успешный метод управления доступом к периметру, может оказать реальное влияние на горизонтальное перемещение при развертывании в элементах сети, на которую нацелены злоумышленники. Боковое движение эффективно остановлено.

Для групп безопасности, стремящихся устранить эту угрозу, невозможно недооценить важность консолидации. Инфраструктура идентификации обычно развивается со временем, что приводит к сочетанию локальной и облачной инфраструктуры идентификации, часто от множества конкурирующих поставщиков. Соединительная ткань необходима для обеспечения стабильных результатов. Централизованная защита удостоверений позволит организации настраивать, управлять и применять политики аутентификации и доступа таким образом, чтобы сократить потребление ресурсов и обеспечить более стратегический подход к снижению рисков.

Хотя боковое смещение является давней проблемой, возможность решить ее таким образом только сейчас становится реальностью. Слишком долго злоумышленники имели свободу передвижения, используя идентичность в качестве универсального вектора атаки для беспрепятственного проникновения в окружающую среду для максимального воздействия. Организации должны снова выйти на передний план — чего они могут достичь только при полной видимости угрозы, исходящей от идентичности, и за счет упреждающего охвата уязвимых активов многофакторной идентификацией. Только таким образом они могут эффективно снизить риск». ***(Yaron Kassner. A Decade of Discussion and We're Still***

Not Thinking Laterally // CPO Magazine (https://www.cpomagazine.com/cyber-security/a-decade-of-discussion-and-were-still-not-thinking-laterally/). 06.12.2022).

***

«З початку листопада державні ІТ-структури Вануату були вимушені повністю призупинити свою діяльність — це відбулось одразу після початку роботи уряду в новому складі. Наразі відомо, що близько 70% урядових установ вже відновили роботу, втім хакерська атака завдала величезних збитків економіці країни. Серед основних незручностей: урядовці втратили доступ до поштових скриньок та рахунків, а громадяни Вануату не могли продовжувати терміни дії водійських посвідчень, сплачувати податки, зв'язуватись з екстреними службами.

Як пояснили експерти, регіони як Вануату є «ідеальною» мішенню для кібератак, оскільки вони не мають достатньо ресурсів для забезпечення захисту інформаційних систем на належному рівні, порівняно з можливостями урядових організацій Європи та США. У хакерській атаці на Вануату вже підозрюють кіберзлочинців, які називають себе BlackCat. Раніше зловмисники намагались здійснити ідентичні атаки в Італії та Флориді (США).

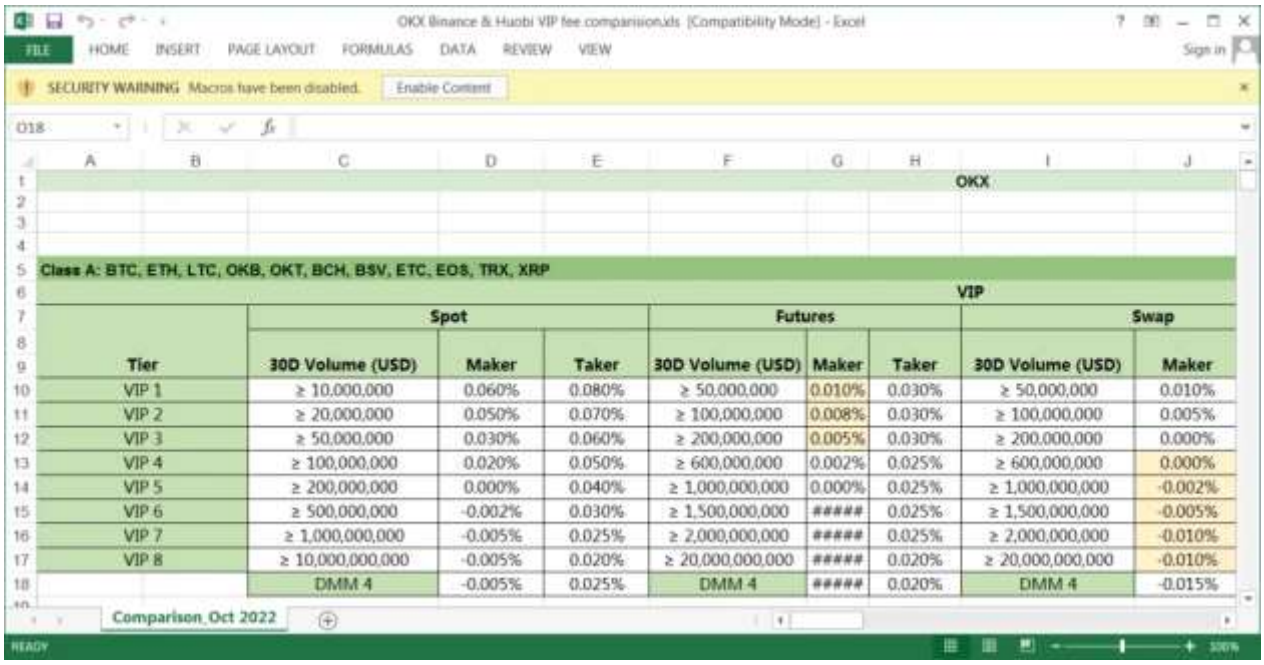
Нагадаємо, що наприкінці березня уряд Вануату підтримав ідею створення криптоострова, яку запропонував британський фахівець з нерухомості Ентоні Уелч. Острів Латаро розміром 300 гектарів мав стати новою криптостолицею світу. У 2017 році власники острова планували перетворити територію на заповідник дикої природи, щоб отримувати прибутки та захищати рідкісний вид крабів. Тоді така ідея нікого не зацікавила, тому Уелч «поставив ставку» на криптовалюти.

Окрім кібератак на ІТ-структури держав, криптовалютні шахраї зламують урядові соцмережі. Так на початку липня хакери отримали доступ до облікових записів армії Великобританії у Twitter та YouTube — все для розповсюдження скаму з метою крадіжки криптовалют. Тоді офіційний ютюб-канал British Army хакери перейменували на Ark Invest, видаливши всі попередні відео та опублікувавши декілька діпфейк-виступів Ілона Маска та Джека Дорсі. Під відео користувачів закликали інвестувати у шахрайські криптопроекти». ***(Масштабна***

хакерська атака зупинила роботу уряду цілої держави на місяць // No worries! (https://noworries.news/masshtabna-hakerska-ataka-zupynyla-robotu-uryadu-cziloyi-derzhavy-na-misyacz/). 12.12.2022).

***

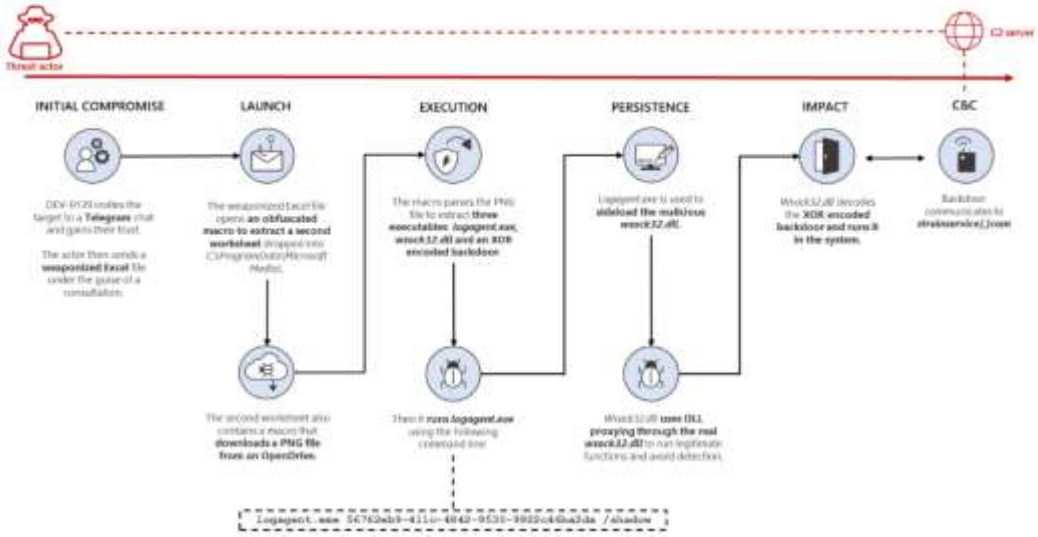
«Підрозділ безпеки компанії Microsoft у пресрелізі, опублікованому на сайті компанії, розкрив кібератаку, спрямовану на криптовалютні стартапи. Хакери завойовували довіру користувачів через чат у Telegram і надсилали Excel-файл під назвою «OKX Binance and Huobi VIP fee comparison. xls» — він містив шкідливий код, здатний віддалено отримати доступ до системи жертви.



Група розвідки кіберзагроз Security відстежила виконавця злому за ніком DEV-0139. Хакеру вдалося проникнути у групові чати у Telegram, маскуючись під представника криптоінвестиційної компанії. Він імітував обговорення торгових комісій з VIP-клієнтами великих бірж. Ціль шкідливого коду полягала в тому, щоб обманом змусити криптоінвестиційні фонди завантажити файл Excel.

Файл містив точну інформацію про структуру комісій найбільших криптовалютних бірж. З іншого боку, він мав у собі шкідливий макрос, який запускає інший аркуш Excel у фоновому режимі. Таким чином, зловмисник отримував віддалений доступ до зараженої системи жертви.

«…зловмисник має широкі знання про індустрію криптовалют і проблеми, з якими може зіткнутися цільова компанія. Він ставив запитання про комісійні структури, тобто комісії, які використовуються платформами криптовалютного обміну для торгівлі. Як і в багатьох інших компаній у цій галузі, найбільші витрати походять від комісій, які стягують біржі. Це дуже конкретна тема, яка демонструє, наскільки хакер обізнаний і добре підготовлений перед тим, як напасти на свою ціль» — повідомляють у своєму пресрелізі Microsoft.



Хоча Microsoft і не назвала ніяких конкретних підозрюваних, компанія з кібербезпеки Volexity також опублікувала свої висновки про атаку, зв’язавши її з північнокорейською хакерською групою Lazarus. За даними аналітиків, зловмисники lazarus Group використовують аналогічні шкідливі електронні таблиці порівняння комісійних зборів криптобірж для поширення шкідливої програми AppleJeus. Саме цю програму вони використовували в операціях із крадіжки цифрових активів.

Найвідоміше хакерське угруповування також підозрюється у допомозі уряду Північної Кореї у розробці зброї масового знищення — подейкують, що левова частка фінансування ядерної програми якраз складає крадена криптовалюта. До того ж Lazarus звинуватили у хакерських атаках на ізраїльську та японські криптобіржі». ***(Microsoft: хакери персонально почали полювати на великих власників криптовалюти // No worries! (https://noworries.news/microsoft-hakery-personalno-pochaly-polyuvaty-na-velykyh-vlasnykiv-kryptovalyuty/). 12.12.2022).***

***

«В последние несколько месяцев граждан Австралии резко осознали реальные последствия киберпреступлений. Все началось в сентябре 2022 года, когда гигант беспроводных услуг Optus объявил об утечке данных. Первоначальное раскрытие информации поступило от генерального директора, и она объяснила, что расследование нарушений все еще продолжается, но «некоторая» информация о клиентах была скомпрометирована. Через несколько дней это число выросло до 10 миллионов. После атаки клиенты были проинформированы о том, что их паспорта, водительские права и персональные данные были скомпрометированы, что превратило инцидент в худший случай в истории Австралии.

Тем не менее, всего несколько недель спустя граждане Австралии снова пострадали.

На этот раз нарушение касалось страхового гиганта Medibank. Когда о взломе было впервые объявлено, компания заявила, что никакие данные клиентов не были скомпрометированы. К сожалению, только через несколько дней выяснилось, что это заявление было очень оптимистичным. Фактически данные всех четырех миллионов клиентов оказались в руках злоумышленников.

Но это был не конец.

В конце октября было обнаружено еще одно нарушение, затронувшее коммуникационную платформу, используемую Министерством обороны Австралии, что поставило под угрозу информацию текущих и бывших сотрудников.

Это вызвало возмущение в Австралии. Внезапно данные 14 миллионов граждан (более половины населения) оказались в руках киберпреступников.

Граждане хотели знать, почему их данные были скомпрометированы и почему не была обеспечена безопасность для их защиты. Была ли это продолжительная и целенаправленная атака на страну? Разве компании, которым они доверили свои данные, не воспринимали киберугрозу всерьез?

Итак, какие именно ключевые проблемы подвергали риску такие большие массивы данных?

Правительство и политика

Одной из самых больших опасений клиентов Optus было то, что данные многих бывших клиентов были скомпрометированы. Причина этого в том, что правительство Австралии не требует от компаний удалять данные о бывших клиентах, которые они хранят. Вместо этого государственное законодательство о надзоре фактически поощряет поставщиков телекоммуникационных услуг хранить данные о своих клиентах как минимум в течение двух лет.

В Великобритании это строго запрещено из-за GDPR, где организации могут хранить персональные данные только не дольше, чем это необходимо для выполняемой задачи. В результате многие эксперты по кибербезопасности полагали, что последствия взлома были бы гораздо менее серьезными, если бы правительство больше сосредоточилось на конфиденциальности граждан, а не на слежке.

Кроме того, когда речь идет об организациях, хранящих данные о клиентах, системы безопасности довольно слабы. Организации должны собирать крайне конфиденциальную информацию о гражданах для предотвращения мошенничества, но когда дело доходит до хранения и защиты этих данных, конфиденциальности уделяется очень мало внимания. Шифрование часто рассматривается как инструмент, используемый злоумышленниками, и настоящие компании должны соблюдать государственное законодательство, которое требует от сотрудников правоохранительных органов наличия бэкдора для доступа к зашифрованным данным, что еще больше ставит под угрозу конфиденциальность потребителей.

Реагирование на инцидент

Еще одна проблема, которая была отмечена нарушениями, заключалась в том, что у австралийских организаций не было процесса, позволяющего быстро понять истинный масштаб нарушений. Это привело к тому, что была опубликована неточная информация о масштабах нарушений, а жертвы получили информацию по каплям.

Прошло два месяца, а информация по-прежнему очень туманна. Тем не менее, чем дольше расследуются нарушения, тем дольше люди подвергаются риску и тем больший ущерб наносят организации своей репутации.

Итак, что мы можем узнать из брешей, которые организации могут использовать для повышения своей безопасности?

Хороший пример плохого примера

Атаки в Австралии стали прекрасным примером очень плохой реакции на кибератаки.

Когда предприятия не могут подготовиться к атакам, они отказываются от своих полномочий, чтобы ограничить их воздействие. Похоже, именно это произошло и с Optus, и с Medibank. Вместо этого организациям следует подготовиться к атакам и сделать их важной частью своих стратегий кибербезопасности.

Организации должны уделять время не только повышению безопасности своих данных с помощью надежных уникальных пользовательских паролей, реализации MFA, использования управления привилегированным доступом (PAM) для защиты ключевых учетных записей, развертывания многоуровневой безопасности для предотвращения горизонтального перемещения и регулярного обучения сотрудников фишингу и киберпреступности, но они также должны отрепетировать свою реакцию на инциденты.

Кибератаки сегодня неизбежны, поэтому крайне важно иметь хорошо отработанный ответ, когда они действительно угрожают цифровым сетям. Выполняя учения по пожарной безопасности, организации смогут локализовать инцидент и намного быстрее понять его масштабы.

Недавние теракты в Австралии стали тревожным звонком

Недавние атаки привлекли внимание к кибербезопасности в Австралии. К счастью, страна сейчас принимает меры и реформирует прежние правила конфиденциальности данных, чтобы улучшить защиту и защиту.

Но на самом деле для этих изменений не должно было быть украдено половины данных страны.

Пусть это будет уроком для других предприятий и стран; когда дело доходит до кибератак, не существует иммунитета, и каждый является целью». ***(Jordan Schroeder. Crikey! Not Another One! Lessons Learned From Australia's Wave of Breaches // Techstrong Group Inc. (https://securityboulevard.com/2022/12/crikey-not-another-one-lessons-learned-from-australias-wave-of-breaches/). 09.12.2022).***

***

«У середині 2020 року головний інженер FTX вніс секретні зміни у програмне забезпечення біржі криптовалют. Завдяки зміні коду інвестфонд Alameda фактично мав необмежену кредитну лінію із депозитів клієнтів FTX.

Він змінив код, щоб звільнити інвестиційний фонд Alameda Research, який належить засновнику FTX Сему Бенкману-Фріду, від функції на торговій платформі, яка автоматично розпродала б активи Alameda, якби він втрачав занадто багато позичених грошей, повідомляє Reuters.

У примітці, що пояснює цю зміну, інженер Нішад Сінгх підкреслив, що FTX ніколи не повинна продавати позиції Alameda.

Це звільнення дозволило Alameda продовжувати позичати кошти у FTX незалежно від вартості застави, що забезпечує ці позики. Зміна коду привернула увагу Комісії з цінних паперів і бірж США, яка у вівторок звинуватила Бенкмана-Фріда у шахрайстві. Комісія з цінних паперів і бірж (SEC) заявила, що це налаштування означало, що Alameda мала «практично необмежену кредитну лінію». Крім того, мільярди доларів, які FTX таємно позичила Alameda протягом наступних двох років, не надходили з її власних резервів, а були депозитами інших клієнтів FTX, заявила SEC.

SEC і представник Bankman-Fried відмовилися коментувати цю історію для ЗМІ. Сінгх не відповів на кілька запитів про коментарі…». ***(Катерина Колонович. Секретна зміна коду дозволила FTX використовувати гроші клієнтів // Speka.Media (https://speka.media/sekretna-zmina-kodu-dozvolila-ftx-vikoristovuvati-grosi-klijentiv-p662zp). 14.12.2022).***

***

«Російський кримінальний торговець зброєю Віктор Бут повідомив про власні плани з порятунку іншого злочинця з рф Олександра Винника, якого звинуватили відмиванні $ 9 мільярдів через криптовалютну біржу BTC-e. Наразі криптошахрай перебуває у в'язниці США, де йому загрожує до 55 років позбавлення волі.

Як саме допомагатиме Виннику так званий «продавець смерті» Бут наразі невідомо, адже останній лише нещодавно повернувся з американської в'язниці. «Непроста ситуація навколо російського айтішника Олександра Винника, несправедливо затриманого в Греції. Давайте пам'ятати і думати про його повернення», — висловився громадянин країни-терориста Бут.

Учасники криптовалютної спільноти та обмануті інвестори BTC-e сподіваються, що Винник відповідатиме за свої вчинки перед законом США та відбуде своє покарання повною мірою. Саме таке майбутнє очікує на всіх російських злочинців…». ***(Ув'язненому засновнику BTC-e допомагатиме російський «продавець смерті» // No worries! (https://noworries.news/uvyaznenomu-zasnovnyku-btc-e-dopomagatyme-rosijskyj-prodavecz-smerti-2/). 14.12.2022).***

***

«Заканчивая 2022 год, мы в Security Boulevard хотели выделить самые популярные статьи года. Ниже представлен последний из нашей серии «Лучшее за 2022 год».

В 2022 году киберпреступность станет более угрожающей. Уровень киберпреступности растет с каждым годом, и ожидается, что в следующем году он достигнет своего пика. Говорят, что сегодня киберпреступность влияет на безопасность более 80% предприятий во всем мире. В основном это связано с ограниченными возможностями органов власти по отслеживанию кибератак, поскольку данный вид преступлений совершается с использованием виртуального мира.

Согласно статистике кибербезопасности, более половины кибератак совершаются с помощью программ-вымогателей. В статистике также говорится, что базы данных здравоохранения являются наиболее целевыми из-за их важности для бизнеса. Веб-сайты социальных сетей также используются для распространения вредоносных программ и вирусов или компрометации конфиденциальной информации.

В этом блоге обсуждаются важные тенденции и разработки в области киберпреступлений, такие как программы-вымогатели, конфиденциальность в Интернете и безопасность. Итак, приступим.

1. Программы-вымогатели: рост числа атак

В последние годы программы-вымогатели представляют серьезную угрозу для бизнеса во всем мире. После заражения это вредоносное ПО удерживает в заложниках ценные файлы в системе, шифруя их до тех пор, пока не будет выплачен определенный выкуп в виде биткойнов, переводов или любой другой формы цифровой валюты.

В настоящее время существует три типа программ-вымогателей:

Программа-вымогатель, которая шифрует файлы в системе.

Программа-вымогатель Locker блокирует экран устройства до тех пор, пока деньги не будут выплачены.

Программа-вымогатель Wiper удаляет файлы с жесткого диска.

Эксперты считают, что программы-вымогатели станут самой легкой формой киберпреступности в следующем году из-за растущей тенденции к криптовалютам. Ожидается, что в 2022 году он затронет более 8 миллионов пользователей или 10% всех пользователей Интернета.

2. Конфиденциальность в Интернете: угроза анонимности

Интернет предоставил различные способы общения и самовыражения. Однако киберпреступники злоупотребляют этой свободой, нарушая права отдельных лиц. Анонимность является одной из причин, по которой они это делают, поскольку она дает им возможность оставаться незамеченными после совершения незаконных действий в Интернете.

Конфиденциальность в Интернете окажется под угрозой в следующем году по следующим причинам:

я). Около 43% всех утечек данных связаны с малым и средним бизнесом. Цифры растут день ото дня. Только в 2021 году во всем мире было зарегистрировано 1862 утечки данных. Он превзошел как общий показатель 2020 года (1108 человек), так и предыдущий рекорд в 1506 человек, установленный в 2017 году.

ii). В первую пятерку наиболее целевых платформ входят популярные сайты социальных сетей, при этом Facebook занимает первое место с более чем 1 миллиардом взломанных записей.

III). Киберпреступники полагаются на существующие утечки данных для целевых организаций, потому что для них экономически выгодно использовать украденные имена пользователей и пароли в процессе вброса учетных данных для входа.

IV). Украденная информация также может быть продана в Интернете в виде торговых площадок утечки данных. Хакеры могут использовать социальную инженерию для кибератак, потому что многие пользователи все еще используют одни и те же пароли на разных платформах.

3. Безопасность: многочисленные угрозы через устройства IoT

IoT относится к интеллектуальным технологиям в таких устройствах, как бытовая техника, часы и другие устройства, которые выполняют различные функции, которыми можно управлять с помощью смартфона. В недавнем отчете указано, что во всем мире установлено около 35,82 миллиарда устройств IoT, а к 2025 году их число достигнет 75,44 миллиарда. Он выполнит множество задач дома или на рабочем месте. Наиболее важной особенностью этой технологии является подключение различных устройств, чтобы они могли работать вместе.

Однако эти устройства IoT также представляют серьезную угрозу конфиденциальности и безопасности людей. Два типа встроенных устройств IoT могут управлять другими электронными функциями в доме, а носимые устройства носят на теле.

Вот некоторые из причин, по которым безопасность будет под угрозой из-за этих устройств в следующем году:

i) Отсутствие протоколов безопасности в большинстве устройств IoT. Большинство производителей, производящих устройства IoT, не прикрепляют протоколы безопасности к своим устройствам из-за отсутствия знаний о том, как это работает. Это означает, что эти устройства более уязвимы для хакеров, что вызовет многочисленные проблемы с сохранением конфиденциальности в Интернете в следующем году.

ii) Отсутствие прозрачности. Известно, что компании используют различные технологии, не предоставляя пользователям возможность отказаться или узнать, какая информация о них собирается. Это приведет к случаям утечки данных, что может сделать личную информацию людей уязвимой для киберпреступников в следующем году.

iii) Ожидается, что хакеры будут продолжать атаковать устройства Интернета вещей, использующие незащищенные или устаревшие программные системы. Производители оборудования должны рассмотреть возможность внедрения протоколов безопасности в свои продукты, пока не стало слишком поздно. Это затруднит хакерам взлом устройств IoT и обеспечение безопасности личных данных в следующем году.

4. Онлайн-атаки: рост активности киберпреступников

Онлайн-атаки будут по-прежнему представлять угрозу в следующем году по следующим причинам:

i). Использование передовых технологий для совершения онлайн-атак. Киберпреступники используют новые методы для выполнения незаконных операций в Интернете, из-за чего правоохранительным органам сложно их выследить и узнать об их деятельности.

ii). Использование устройств, подключенных к Интернету вещей, для проведения онлайн-атак в следующем году увеличится из-за ограниченных протоколов безопасности, подключенных к этим устройствам.

iii). Использование искусственного интеллекта (ИИ) для совершения онлайн-атак в следующем году будет расти. Ожидается, что хакеры будут использовать эту технологию для нарушения работы компьютерных систем организаций, получения контроля над устройствами других пользователей и кражи конфиденциальных данных с их серверов.

5. Платформы социальных сетей: продолжение вопросов конфиденциальности

Ниже приведены основные платформы социальных сетей и то, как они будут использоваться в следующем году для угрозы конфиденциальности людей:

i). Facebook. Эта платформа представляет угрозу для безопасности своих пользователей в Интернете, поскольку она собирает информацию от третьих лиц, которые поддерживают рекламные кампании на этом веб-сайте. Затем компания использует собранные данные для целевой рекламы, что делает ее членов уязвимыми для онлайн-мошенничества и других киберпреступных действий.

ii). Instagram. Это приложение для обмена фотографиями собирает личную информацию пользователей и продает эти данные третьим лицам. Это представляет серьезную угрозу конфиденциальности отдельных лиц, поскольку киберпреступники могут легко использовать собранную информацию в злонамеренных целях в следующем году.

iii). Twitter. Киберпреступники могут использовать функцию прямого обмена сообщениями на этой платформе для нападения на конкретных людей из-за отсутствия мер конфиденциальности.

iv). Snapchat — взломанные сторонние приложения позволяют киберпреступникам собирать изображения и видео людей без их согласия. Это позволяет им легко ориентироваться на сообщения конкретных пользователей в следующем году на этой платформе.

v). Магазин приложений Google для Android. Киберпреступники могут использовать поддельные банковские приложения, названия игр, крипто-майнеры и вредоносное ПО в этом магазине в следующем году из-за слабых протоколов безопасности.

vi). Google Chrome. Этот браузер собирает информацию о действиях пользователей в Интернете и продает их третьим лицам, что упрощает хакерам кражу данных у конкретных пользователей.

vii). YouTube. В следующем году на эту платформу будет совершено больше кибератак из-за ограниченных протоколов безопасности, связанных с ее контентом. Хакеры могут использовать вредоносное ПО и методы фишинга с этого веб-сайта для доступа к данным отдельных лиц, которые они затем незаконно продают с целью получения прибыли.

viii). WhatsApp. Киберпреступники могут использовать это приложение для обмена сообщениями, чтобы заставить пользователей открывать вредоносные ссылки из-за ограниченных мер безопасности, которые оно использует при обработке сообщений, полученных пользователями.

6. Киберпреступные рынки: дальнейшее развитие рынков темной паутины

Ниже приведены основные рынки темной сети и то, как они будут использоваться в следующем году для угрозы конфиденциальности людей:

i). Dream Market — это одна из самых популярных торговых площадок в даркнете, позволяющая киберпреступникам продавать различные нелегальные товары и услуги.

ii). Точка- Киберпреступники используют эту российскую торговую площадку для продажи нелегальных товаров и услуг в даркнете.

iii). Рынок Hansa. Киберпреступники используют этот рынок для продажи утечек информации в следующем году из-за слабых протоколов безопасности.

iv). Пиратский рынок — это известный темный веб-рынок, который позволяет киберпреступникам торговать различными нелегальными товарами и услугами. Хакеры могут использовать этот веб-сайт для покупки вредоносного ПО в следующем году для запуска целевых атак против конкретных лиц.

Заключение

Как мы видели, киберпреступные рынки и платформы социальных сетей в следующем году будут представлять серьезную угрозу конфиденциальности пользователей. Эти платформы должны использовать новейшие меры

безопасности, чтобы защитить себя от онлайн-мошенничества и других киберпреступных действий». ***(Best of 2022: The Rise of Cybercrime – An Overview // Techstrong Group Inc. (https://securityboulevard.com/2022/12/the-rise-of-cybercrime-an-overview/). 26.12.2022).***

***

«Этот блог является частью нашего обзора за 2022 год, ретроспективы разведки, в которой освещаются наиболее важные тенденции прошлого года, а также обзор 2023 года.

ОСНОВНЫЕ ВЫВОДЫ

С 1 января по 30 ноября 2022 года Flashpoint зафиксировала в общей сложности 109 146 случаев вербовки инсайдеров, инсайдерской рекламы или общих дискуссий, связанных с инсайдерской деятельностью. Из них 22 985 были уникальными. Большинство этих постов были на средних англоязычных каналах Telegram.

Предупреждающие знаки в 2022 году соответствуют тем, которые наблюдались годами ранее. Потенциальные внутренние угрозы могут проявлять техническое и нетехническое поведение, прежде чем негативно повлиять на их организацию.

Ландшафт внутренних угроз

Чтобы увеличить свои шансы на успех, злоумышленники часто обращаются за помощью к недовольным или злонамеренным сотрудникам организаций, против которых они нацелены. В конце концов, зачем тратить ресурсы на обход мер безопасности, если вы можете заставить кого-то внутри обойти их за вас?

Таким образом, тактика вербовки инсайдеров стала чрезвычайно популярной среди хакеров, стремящихся взломать системы и/или совершить атаки программ-вымогателей. Вот что мы увидели в ландшафте инсайдерских угроз в 2022 году.

Распределение внутренних угроз

В этом году Flashpoint собрала и исследовала:

Всего 109 146 сообщений, рекламирующих инсайдерские услуги.

Всего 22 985 уникальных постов от лиц из незаконных и подпольных сообществ.

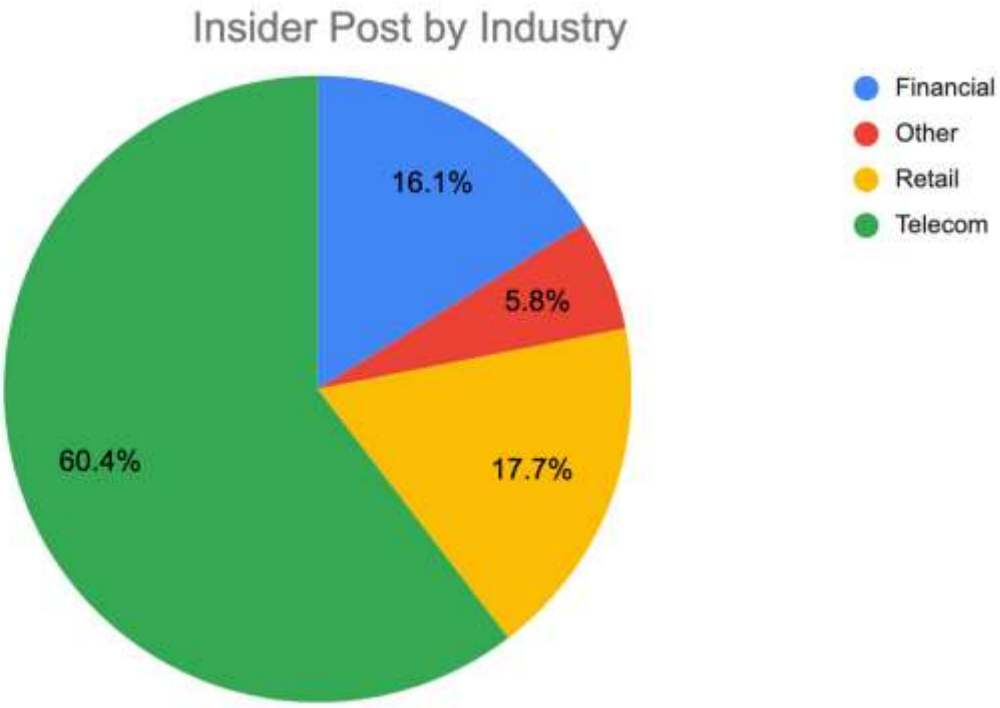
всего 3964 канала

всего 11 376 авторов

Если посмотреть на общее количество уникальных инсайдерских постов в 2022 году, количество выявленных инсайдерских постов с угрозами варьировалось от 1299 в феврале до 2585 в июле — в среднем 2090 постов в месяц. По оценке Flashpoint, рост с первого квартала 2022 года до конца года был в основном связан с общим ростом незаконных и подпольных сообществ. Например, в сообществах Telegram с апреля 2022 года по ноябрь 2022 года число активных пользователей увеличилось на 200 миллионов человек, а Flashpoint продолжает выявлять новые каналы и группы Telegram, связанные с внутренними угрозами, методами мошенничества, утечками данных и другим незаконным контентом.

Однако группа злоумышленников LAPSUS$ также может быть частично ответственна за рост инсайдерских угроз в Telegram. LAPSUS$ успешно привлекала инсайдеров к крупным операциям, которые могли предоставить доступ к корпоративным виртуальным частным сетям (VPN) или помочь обойти многофакторную аутентификацию.

С точки зрения активности внутренних угроз наибольшему риску подвергается организация, занимающаяся бизнесом в телекоммуникационной отрасли. Далее следуют розничные и финансовые организации:



Предупреждающие знаки внутренней угрозы

Потенциальные внутренние угрозы могут проявлять как техническое, так и нетехническое поведение, прежде чем негативно повлиять на их организацию. Хотя эти действия могут напрямую не указывать на сотрудника как на злонамеренного инсайдера, они могут послужить основой для мониторинга его

деятельности или проведения дополнительных расследований, чтобы определить, представляют ли они повышенный риск.

Нетехнические признаки инсайдерской деятельности

Ниже приведены нетехнические предупреждающие знаки, которые могут быть связаны с инсайдерами:

Финансовые трудности: значительные изменения в финансовых обязательствах, такие как увеличение долга, повышение цен или снижение заработной платы, могут побудить сотрудника стать внутренней угрозой. Инсайдеры могут продавать свои услуги другим субъектам угроз через форумы или чаты, или они могут создавать финансовые возможности для себя в своей организации.

Увольнение из компании: сотрудники, покидающие организацию из-за неблагоприятных обстоятельств, представляют повышенный риск инсайдерской угрозы.

Нестандартное рабочее время: субъекты могут использовать нетипичное рабочее время для создания инсайдерских угроз, потому что в это время работает меньше сотрудников службы безопасности. Следуя нетипичному графику, злоумышленники могут вести свою обычную работу в рабочее время, а в другое время заниматься противоправной деятельностью.

Низкая производительность: плохо работающие сотрудники могут страдать от неожиданных изменений в своей личной жизни или иметь проблемы со своим положением в организации. Это может привести к тому, что они будут действовать против своих компаний, притворяясь инсайдерами.

Необъяснимая финансовая выгода: сотрудники, получающие необъяснимую финансовую выгоду, могут проявлять признаки того, что они являются инсайдерами. Они могут активно получать средства за свою незаконную деятельность, дополняя свой обычный доход.

Необычные зарубежные поездки: Необычные и незарегистрированные зарубежные поездки могут указывать на то, что работник нанят или обслуживает иностранное государство или субъект, спонсируемый государством.

Технические признаки инсайдерской деятельности

Ниже приведены технические предупреждающие знаки, которые могут быть связаны с инсайдерами:

Нерегулярная деятельность: сотрудники, получающие доступ к данным за рамками своих должностных обязанностей, могут проверять пределы своего доступа, чтобы злоупотреблять своим положением.

Нерегулярные загрузки. Наиболее распространенные методы эксфильтрации основаны на том, что инсайдер сначала загружает конфиденциальные файлы локально. Скачивание необработанных данных и выполнение больших объемов загрузок является нерегулярным для большинства должностей и может указывать на активность внутренних угроз.

Несанкционированные устройства. Сотрудники, использующие для работы неавторизованные устройства, подвергаются большему риску потери или продажи этих данных, поскольку они находятся за пределами корпоративных сетей.

Защита от внутренних угроз

Следующие меры по смягчению последствий могут быть развернуты организациями для выявления внутренних предупреждающих признаков и пресечения действий внутренних угроз до того, как они нанесут ущерб организации.

Оценка угроз. Создание профилей угроз для сотрудников позволяет лучше осуществлять постоянный мониторинг и оценку рисков сотрудников предприятия, что в идеале помогает организациям выявлять внутренние угрозы до того, как они станут реальностью.

Проведение кампаний по повышению осведомленности о безопасности. Проведение кампаний по информированию об инсайдерских угрозах важно для борьбы с распространением инсайдерской информации. Включение кампаний по информированию об инсайдерских угрозах наряду с обучением безопасности может помочь привить культуру, которая выявляет злоумышленников и защищает от них.

Предотвращение потери данных. Инструменты предотвращения потери данных (DLP) предназначены для защиты конфиденциальных данных от потери, кражи и неправомерного использования. Организации могут использовать три основных инструмента DLP: на уровне конечной точки, сети и хранилища. Network DLP отслеживает все сетевые коммуникации, такие как электронная почта и передача файлов, чтобы предупредить о подозрительной активности. Инструменты Endpoint DLP отслеживают устройства конечных пользователей, включая ноутбуки, и защищают от злонамеренного использования данных. Инструменты Storage DLP отслеживают данные в состоянии покоя и могут использоваться с локальными и облачными архитектурами хранения.

Привлечение потенциальных внутренних угроз: привлечение сотрудников, которые демонстрируют признаки риска внутренних угроз, может позволить организации исправить проблему и предотвратить их причинение вреда организации.

Мониторинг поведения. Мониторинг поведения пользователей необходим для защиты от потенциальных внутренних угроз, поскольку он позволяет ИТ-специалистам и специалистам по информационной безопасности создавать базовые уровни активности и обнаруживать аномальную активность в масштабах всего предприятия.

Ситуация с внутренними угрозами в 2023 году

Аналитики считают, что в 2023 году группы вымогателей, вероятно, продолжат вербовать инсайдеров для помощи в своих кибератаках. Человеческая ошибка представляет собой серьезную угрозу безопасности для организаций, а сотрудники часто становятся мишенью злоумышленников как потенциально самое слабое звено в их системе безопасности.

Атаки с использованием социальной инженерии, такие как фишинг, являются распространенным методом злоумышленников для получения учетных данных и конфиденциальной информации инсайдера. Однако группы вымогателей, такие как LAPSUS$ и «LockBit», нанимают сотрудников, чтобы поставить под угрозу безопасность своей организации ради денежной выгоды. Эти группы получают

выгоду от того, что инсайдер действует от их имени, предоставляя первоначальный доступ и возможность проводить разведку корпоративной среды. Сотрудник получает финансовую выгоду и может утверждать, что предоставил доступ невольно.

Группы вымогателей часто транслируют свое намерение вербовать на своих каналах Telegram, сайтах утечки, форумах глубокой и темной сети (DDW) и других средах. Такие объявления позволяют сотрудникам связаться с ними, если они готовы работать в качестве сообщников.

Flashpoint также считает, что весьма вероятно, что Telegram останется самым популярным средством для идентификации инсайдеров и злоумышленников и начала работы друг с другом. Наши аналитики продолжат отслеживать, выявлять и присоединяться к каналам внутренних угроз в 2023 году, чтобы предоставить дополнительную информацию.

Отслеживайте и защищайте от внутренних угроз с помощью Flashpoint

Набор действенных интеллектуальных решений Flashpoint позволяет организациям заблаговременно выявлять и снижать кибер- и физические риски, которые могут поставить под угрозу людей, места и имущество. Чтобы раскрыть всю мощь аналитики угроз, начните работу с бесплатной пробной версии Flashpoint». ***(Flashpoint Year In Review: 2022 Insider Threat Landscape // Techstrong Group Inc. (https://securityboulevard.com/2022/12/flashpoint-year-in-review-2022-insider-threat-landscape/). 15.12.2022).***

***

«Ряд потрясінь 2022 року, серед яких і війна в Україні, створили сприятливі умови для активності багатьох кіберзлочинців. Місяцями зловмисники атакували державні установи, лікарні, криптовалютні компанії та багато інших організацій. Вартість витоку даних зросла до 4,4 мільйона доларів США, а успіх підштовхуватиме кіберзлочинців до ще більшої активності у 2023 році.

За підсумками року спеціалісти ESET підготували список з 10 найбільших кіберінцидентів з урахуванням завданої ними шкоди, рівня складності чи геополітичних наслідків. І хоча порядок у списку не має значення, спочатку зупинимося на атаках, спрямованих на Україну, які більше вплинули на глобальні ризики цифрової безпеки.

Україна під прицілом кібератак. Критична інфраструктура України знову стала ціллю кіберзлочинців. На початку повномасштабного російського вторгнення дослідники ESET тісно співпрацювали з CERT-UA над усуненням атаки, націленої на систему енергопостачання країни з використанням шкідливої програми для знищення інформації. Цю загрозу група кіберзлочинців Sandworm намагалася розгорнути на високовольтних електричних підстанціях. Шкідливе програмне забезпечення отримало назву Industroyer2 на честь загрози, застосованої групою для відключення електроенергії в Україні в 2016 році. Однак цього разу програма використовувалася у поєднанні з новою версією загрози CaddyWiper для знищення інформації, ймовірно, щоб приховати сліди групи та уповільнити реагування та відновлення контролю для операторів енергетичної компанії.

Ще більше загроз для знищення інформації. CaddyWiper був далеко не єдиним інструментом для знищення даних, виявленим в Україні безпосередньо перед або в перші кілька тижнів вторгнення росії. 23 лютого 2022 року телеметрія ESET зафіксувала іншу загрозу такого ж функціоналу із назвою HermeticWiper на сотнях машин у кількох організаціях в Україні. Наступного дня почалася друга руйнівна атака на українську урядову мережу з метою знищення даних, цього разу з використанням IsaacWiper.

Перебої в роботі Інтернету. За годину до російського вторгнення масштабна кібератака на комерційного супутникового провайдера Viasat призвела до призвела до перебоїв у доступі до Інтернету для тисяч людей в Україні та навіть в інших країнах Європи. Вважається, що метою атаки, під час якої був використаний неправильно налаштований VPN-пристрій для отримання доступу до розділу управління супутниковою мережею, було послабити комунікаційні можливості

українського командування в перші години вторгнення. Проте її наслідки відчули далеко за межами України.

Надзвичайне положення в Коста-Ріці через програми-вимагачі. Однією з найактивніших цього року була група програм-вимагачів Conti, доступ до використання яких за плату зловмисники-розробники надають іншим хакерам. Одну з таких атак було спрямовано на невелику південноамериканську державу Коста-Ріка. Як результат, в країні було оголошено надзвичайний стан, а уряд назвав атаку актом «кібертероризму». Група з тих пір зникла, хоча її учасники, ймовірно, просто перейшли до іншої активності для уникнення уваги правоохоронних органів.

Атаки на державні органи в США. Інші програми-вимагачі також були активними у 2022 році. У вересні Агентство з кібербезпеки та захисту інфраструктури США повідомило, що пов’язані з Іраном кіберзлочинці атакували муніципальну установу США та аерокосмічну компанію, використовуючи уразливість Log4Shell для поширення програм-вимагачів. Також варта уваги атака на уряд США в листопаді. Тоді організацію федеральної цивільної виконавчої влади було атаковано та розгорнуто в її мережі шкідливе програмне забезпечення для майнінгу криптовалют.

Крадіжка в розмірі 618 мільйонів доларів США з використанням Ronin Network. Цей сайдчейн Ethereum для гри Axie Infinity був створений в’єтнамським розробником блокчейн-ігор Sky Mavis. У березні з’ясувалося, що хакерам вдалося використати викрадені приватні ключі, щоб підробити зняття коштів на суму 173 600 Ethereum (592 мільйони доларів США) і 25,5 мільйонів доларів США через Ronin двома транзакціями. Крадіжка в розмірі 618 мільйонів доларів США за цінами березня стала найбільшою в історії криптокомпаній. З атакою пов’язана північнокорейська група кібрезлочинців Lazarus.

Група програм-вимагачів Lapsus$, яка за допомогою резонансних крадіжок даних змушує своїх жертв платити, з’явилася протягом 2022 року,. Серед її цілей – Microsoft, Samsung, Nvidia, Ubisoft, Okta і Vodafone. Одним з її методів є підкуп інсайдерів у компаніях та їхніх підрядників. Хоча деякий час група була відносно

неактивною, вона знову повернулася наприкінці року, атакувавши розробника Grand Theft Auto Rockstar Games. Кілька ймовірних членів групи були заарештовані у Великобританії та Бразилії.

Витік даних Міжнародного комітету Червоного Хреста. У січні організація повідомила про серйозний інцидент, у результаті якого були скомпрометовані особисті дані понад 515 000 жертв. У швейцарського підрядника були викрадені дані про осіб, розлучених зі своїми родинами через конфлікти, міграцію та катастрофи, зниклих безвісти та їхніх сімей, а також осіб, які перебувають під вартою. Під час атаки була використана уразливість у системі, на якій було не застосовано виправлення.

Новий витік даних в Uber. У 2016 році у компанії було викрадено дані про 57 мільйонів користувачів. У вересні цього року знову повідомлялося, що хакер, потенційно член групи Lapsus$, зламав електронну пошту та хмарні системи, сховища коду та внутрішній обліковий запис Slack. Кіберзлочинець націлився на зовнішнього підрядника Uber, найімовірніше, знайшовши їх корпоративний пароль у даркнеті.

Медичні дані у руках хакерів. Зловмисникам вдалося отримати доступ до даних 4 мільйонів клієнтів австралійського гіганта медичного страхування. Атака може призвести до збитків компанії на близько 35 мільйонів доларів США. Вважається, що кіберзлочинці, пов’язані з програмою-вимагачем REvil (також відомою як Sodinokibi), отримали облікові дані адміністратора, і це стало початковим вектором атаки. Жертви цієї атаки тепер стикаються з хвилею подальших спроб шахрайства з особистими даними.

Що б не трапилося у 2023 році, деякі уроки з цих 10 серйозних інцидентів можуть стати в нагоді користувачам під час посилення цифрового захисту своїх пристроїв та корпоративних мереж. Зокрема компаніям слід правильно налагодити свої процеси та операції, організувати тренінги з цифрової обізнаності для всіх співробітників та забезпечити багаторівневий захист корпоративної мережі за допомогою передових рішень з кібербезпеки». ***(Герман Богапов. Найбільші кібератаки спрямовані на енергетику й держустанови // HiTech.Expert***

(https://expert.com.ua/154636-najbilshi-kiberataki-spryamovani-na-energetiku-j-derzhustanovi.html). 28.12.2022).

***

«Представники НАТО вважають, що штучний інтелект виявляється палицею на два кінці у кібератаках.

«ШІ дозволяє автоматично сканувати мережі та відбивати атаки, а не робити це вручну. Однак це працює і у зворотний бік», — заявив помічник генерального секретаря НАТО Девід ван Віл, пише Euronews.

За його словами, штучний інтелект можна використовувати для злому мереж із використанням облікових даних та алгоритмів. На думку Девіда ван Віла, спроба підбору комбінацій є величезною проблемою, проте союзники прагнуть етично використати ШІ.

Помічник генсекретаря вважає, що альянс використовуватиме технологію для захисту своєї інфраструктури. Однак у НАТО не впевнені, що противник буде таким самим етичним користувачем ШІ…». ***(Руслан Сорока. У НАТО назвали кібератаки з використанням штучного інтелекту критичною загрозою // Speka.Media (https://speka.media/u-nato-nazvali-kiberataki-z-vikoristannya-stucnogo-intelektu-kriticnoyu-zagrozoyu-py4jqp). 27.12.2022).***

***

«…Кибератаки представляют собой новую угрозу для морского сектора. Хотя степень их воздействия еще не полностью осознана, они представляют собой постоянно меняющуюся угрозу, которая со временем будет только усиливаться. В отличие от морских пиратов, принимающих физическую форму, угроза из киберпространства невидима и использует множество способов сохранения анонимности, чтобы замести следы. Действуя независимо от национальных и географических границ, киберугрозы могут запускать свои атаки из любой точки мира и в любую точку мира.

Пока системы подключены к компьютерной сети, существует возможность их взлома. Чем более оцифрованными и автоматизированными становятся наши системы, тем больше шансов для проникновения и достижения целей злоумышленника.

Здесь описывается эволюция трех групп киберугроз: (1) национальные хакеры, (2) киберпреступники и (3) преступные организации, которые заручаются поддержкой хакеров.

Хакеры национального государства действуют от имени своего правительства, чтобы скомпрометировать целевые государства, организации или отдельных лиц, чтобы собрать разведданные или причинить вред. Они, как правило, хорошо обеспечены ресурсами, высококвалифицированы и не мотивированы денежной выгодой.

Хакеры из национальных государств были связаны с атаками на промышленные объекты, использующие операционные технологии (OT), также известные как промышленные системы управления. Системы OT включают в себя аппаратное и программное обеспечение, которое отслеживает и контролирует физические устройства и процессы, включая силовые установки, системы управления грузами и другие на борту судов. Кибератаки на системы OT могут привести к физическому повреждению инфраструктуры или нарушению работы основных служб. Сообщения об атаках на промышленные объекты с 2010 года демонстрируют постепенный рост изощренности и масштабов. Например, в 2015 и 2016 годах по отдельности были предприняты две кибератаки на энергосистему Украины, что привело к отключению электроэнергии на несколько часов. В 2017 году были отключены системы безопасности нефтегазового объекта в Саудовской Аравии,

Хакеры национальных государств также были связаны с развертыванием разрушительного вредоносного ПО. В 2017 году вредоносное ПО NotPetya распространялось через обновление программного обеспечения MeDoc, де-факто приложения для налогового учета в Украине. Как только NotPetya была запущена, она распространилась по всему миру без разбора, необратимо делая компьютеры и

файлы непригодными для использования. Морской сектор Юго-Восточной Азии понес сопутствующий ущерб, оказавшись в эпицентре этой атаки. Хотя атака не нанесла физического ущерба, последствия для судоходных линий и портов, таких как те, которыми управляет Maersk, одна из крупнейших судоходных компаний в мире, были разрушительными.

Киберпреступники компрометируют свои цели для получения денежной выгоды. В середине 2010-х годов распространение программ-вымогателей обогнало другие методы и стало доминирующим и наиболее прибыльным методом. Это включает взлом сетей, шифрование файлов на большом количестве компьютеров и требование выкупа за ключ дешифрования.

За последнее десятилетие киберпреступники быстро эволюционировали. С 2018 года вместо того, чтобы распространять программы-вымогатели без разбора, некоторые банды перешли к выбору важных целей в определенных секторах, таких как здравоохранение. Результат этой стратегии отражается в скачке стоимости собранных выкупов. Банда вымогателей под названием Ryuk добилась значительных успехов, собрав в 2019 году выкуп в размере 61 миллиона долларов. Ryuk известен своими нападениями на больницы, поскольку они более охотно платят выкупы, чтобы избежать задержек в лечении пациентов. Выбор ценных целей не всегда может привести к более высокой отдаче. Например, крупная финансовая организация, разумно инвестировавшая в свою киберзащиту, может оказаться непростой мишенью.

Киберпреступники стали более изощренными, чтобы преодолевать более сильную защиту. Схемы франчайзинга, предлагающие до 70% собранного выкупа, возникли для расширения круга талантливых партнеров. Также появилась экосистема специалистов, предлагающих уникальные услуги, например те, которые позволяют программам-вымогателям избежать обнаружения коммерческим антивирусным программным обеспечением.

Известно, что преступные организации, такие как торговцы наркотиками, заручаются помощью хакеров для расширения своих возможностей. В 2011 году хакеры вывели морской оборот наркотиков на новый уровень, когда

контрабандисты наркотиков наняли хакеров для взлома компьютеров в бельгийском порту Антверпен. Используя свой доступ к данным о перемещении контейнеров, контрабандисты наркотиков смогли (1) обнаружить контейнеры, которые им не принадлежали, но содержали кокаин, который они ранее спрятали, и (2) извлечь кокаин из этих контейнеров до того, как законные владельцы заявили о их фактический груз — бананы.

Какие основные инструменты управления используются в ответ на киберугрозы?

Инструменты управления, используемые в ответ на киберугрозы в морском секторе Юго-Восточной Азии, включают (1) международные конвенции для судовладельцев и операторов, (2) национальное законодательство по усилению кибербезопасности в критически важных инфраструктурах (включая морские порты) и (3) отраслевые соглашения. инвестиции и развитие потенциала.

В 2017 году Международная морская организация (ИМО) приняла резолюцию MSC.428(98). Эта резолюция требует, чтобы судовладельцы и операторы учитывали киберриски в своей системе управления безопасностью в рамках соблюдения Международного кодекса управления безопасностью. Администрациям флага было предложено обеспечить соответствие зарегистрированным судам и компаниям. Государства-члены ИМО, например, Соединенные Штаты через свою береговую охрану, также могут осуществлять контроль государства порта, чтобы налагать вышеупомянутые требования на компании с судами под иностранным флагом, которые заходят в их порты.

В поддержку реализации MSC.428(98) международные судоходные ассоциации, в том числе Балтийский и Международный морской совет, Ассоциация цифровых контейнерных перевозок и Международный морской форум нефтяных компаний, опубликовали несколько руководств. В апреле 2022 года Международная ассоциация классификационных обществ приняла два новых унифицированных требования, E26 и E27, чтобы обеспечить минимальные требования к киберустойчивости для судов нового класса, строительство которых заключено с 1 января 2024 года. E26 описывает безопасную интеграцию ИТ и ОТ.

систем в конструкцию судна, в то время как E27 касается системной целостности бортовых систем и оборудования. Подавляющее большинство коммерческих судов в мире строятся и проверяются на соответствие стандартам, установленным классификационными обществами.

Национальное законодательство Юго-Восточной Азии также заложило основу для повышения киберустойчивости в важнейших секторах, включая морской сектор. В Сингапуре Закон о кибербезопасности 2018 года установил правовую основу для надзора и поддержания национальной кибербезопасности. Он также предоставляет полномочия Комиссару по кибербезопасности издавать своды правил для регулирования мер, принимаемых владельцами критической информационной инфраструктуры для защиты своей инфраструктуры от киберугроз. Другие страны Юго-Восточной Азии, включая Малайзию, Таиланд, Индонезию, Филиппины и Вьетнам, также приняли аналогичные законы о кибербезопасности.

В Сингапуре Морское и портовое управление (MPA) несет ответственность как за осуществление контроля со стороны государства порта, так и за выполнение обязанностей Администрации флага судов, зарегистрированных в Сингапуре. Его миссия также включает в себя защиту своих морских интересов. В 2019 году MPA открыло свой Операционный центр морской кибербезопасности для раннего обнаружения, мониторинга и реагирования на кибератаки.

Какой основной вред кибератаки наносят заинтересованным сторонам в регионе?

Кибератаки представляют риск для региональных заинтересованных сторон, нарушая судоходные операции, торговлю и ставя под угрозу безопасность. Эффект кибератаки NotPetya на Maersk в 2017 году был разрушительным. 50 000 ноутбуков и 4000 серверов в 130 странах были недоступны в течение десяти дней, пока Maersk пыталась продолжить работу вручную. 17 из 76 принадлежащих Maersk контейнерных терминалов, эксплуатируемых APM Terminals, были закрыты или столкнулись с серьезным замедлением грузовых операций. В индийском порту Нхава-Шева пришлось выделить дополнительное место для хранения экспортных

контейнеров, застрявших из-за невозможности АРМ получить доступ к данным бронирования. А пирс 400 компании АРМ в порту Лос-Анджелеса был закрыт для прибывающих дальнобойщиков.

Кибератаки, в результате которых суда застревают в перегруженных точках, таких как Малаккский пролив и Сингапур, также могут нарушить мировую торговлю. Блокирование Суэцкого канала из-за случайного заземления Ever Given в 2021 году, хотя и не вызванное кибератакой, является хорошей иллюстрацией.

Кибератаки также могут поставить под угрозу безопасность на море. На сегодняшний день большинство кибератак в морском секторе были направлены на компрометацию портов и прибрежных корпоративных сетей, а не на захват судов или портового оборудования. Однако есть опасения по поводу крупных атак такого рода в будущем. Основой для беспокойства является (1) растущая связь и автоматизация, используемые на судах и в портах; (2) сообщения о кибератаках, затрагивающих бортовые системы, например, в 2019 году Береговая охрана США сообщила об инциденте на сверхбольшом контейнеровозе у порта Нью-Йорка, комментируя: «Хотя вредоносное ПО значительно ухудшило функциональность бортовой компьютерной системы, основные системы управления судном не пострадали», и; (3) усиливающаяся с 2010 года тенденция кибератак на промышленные объекты, которые, как и корабли, также использовать системы ОТ. Некоторые методы взлома, которые использовались для того, чтобы сбить с толку навигационные средства, также вызывают беспокойство. Подмена глобальной системы позиционирования (GPS) может привести к ложным данным GPS, что приведет к неточным навигационным решениям экипажа или автопилота, если они не будут дополнительно проверены.

Как развилась морская осведомленность для снижения киберугроз?

Осведомленность о киберугрозах в морском секторе Юго-Восточной Азии сейчас находится в зачаточном состоянии. Чтобы ускорить его разработку, необходимо создать центр обмена и анализа морской информации (ISAC), такой как Центр обмена и анализа информации Морской транспортной системы в США и NormaCyber в Норвегии. ISAC могут создать доверительную экосистему, в которой

участники могут делиться опытом, помогая менее опытным расти. ISAC также предоставляют действенную информацию об угрозах, оповещения, ранние предупреждения и непрерывный мониторинг через свои центры управления безопасностью. В этом регионе несколько доверенных объектов могут быть хорошо расположены, чтобы заполнить этот пробел. Они включают Центр объединения информации и Соглашение о региональном сотрудничестве по борьбе с пиратством и вооруженным ограблением судов в Азии, Центр обмена информацией, которые облегчают обмен информацией об угрозах морской безопасности. Обе организации могут использовать свои хорошо налаженные многосторонние связи и партнерские отношения с региональными военными, правоохранительными органами и частным сектором для обмена информацией об угрозах морской кибербезопасности». ***(Chan Yan Jau. CYBER-ATTACKS AS AN EVOLVING THREAT TO SOUTHEAST ASIA'S MARITIME SECURITY // The Asia Maritime Transparency Initiative and The Center for Strategic and International Studies (https://amti.csis.org/cyber-attacks-as-an-evolving-threat-to-southeast-asias-maritime-security/). 07.12.2022).***

***

«Волна мошенничества в период с июля по сентябрь привела к тому, что жители Новой Зеландии понесли прямые финансовые потери на общую сумму почти 9 миллионов долларов. Государственное агентство кибербезопасности CERT NZ призывает всех использовать это как предупреждение и принять меры для своей защиты в Интернете.

Последний ежеквартальный аналитический отчет CERT NZ показал, что, хотя количество инцидентов выросло на 3% по сравнению с предыдущим кварталом, финансовые потери выросли на 128%, что делает их самыми высокими потерями за квартал с момента начала регистрации в 2017 году.

Директор CERT NZ Роб Поуп сказал, что всплеск потерь вызывает обеспокоенность, но, надеюсь, он вдохновит новозеландцев на более безопасный онлайн.

«Несмотря на то, что большие суммы общих убытков легко ошеломляют, наши данные показывают, что большинство людей теряют от 100 до 500 долларов, что для большинства из нас является настоящим жалом в кармане. Мы хотим, чтобы новозеландцы обратили внимание на эти цифры и использовали их в качестве мотивации для быстрых и простых действий, которые не позволят им и их ванау стать следующей мишенью».

Согласно отчету CERT NZ, одной из причин больших убытков является увеличение несанкционированных денежных переводов, несанкционированного доступа и мошенничества с покупкой, продажей и дарением товаров. Эти типы инцидентов традиционно связаны с высоким уровнем потерь. Аналогичное снижение наблюдалось и в других типах инцидентов, таких как фишинг.

«С приходом праздничного сезона новозеландцы будут искать выгодные предложения в Интернете, и мошенники знают об этом», — сказал Поуп. «Мы просим всех быть осторожными, когда они совершают покупки в Интернете или просматривают онлайн-рынки, и с подозрением относятся ко всему, что кажется слишком хорошим, чтобы быть правдой».

«Людям также следует включить двухфакторную аутентификацию, так как это по-прежнему лучший способ предотвратить доступ злоумышленников к вашим учетным записям. Это включает в себя аккаунты в социальных сетях, а также банки».

В отчете Cyber Security Insights есть советы для новозеландцев выявлять мошенничество до того, как оно произойдет. CERT NZ надеется, что люди поделятся этими советами, когда они навещают Ванау и друзей летом, чтобы мы все могли избежать мошенничества в это Рождество.

Ключевая статистика:

2069 инцидентов, зарегистрированных в CERT NZ в третьем квартале 2022 г. (с 1 июля по 30 сентября 2022 г.)

Сообщается о прямом финансовом убытке в размере 8,9 млн долларов США.

314 человек потеряли от 100 до 1000 долларов.

12 человек потеряли более 10 000 долларов

7,5 млн долларов потеряно из-за мошенничества и мошенничества

Из них 4,8 миллиона были потеряны из-за несанкционированного перевода денег (обратите внимание, что это отличается от несанкционированного доступа к аккаунту).

Если вы считаете, что стали жертвой онлайн-мошенничества, свяжитесь с CERT NZ, а если вы потеряли деньги, немедленно обратитесь в свой банк.

CERT NZ получил наибольшее количество отчетов о покупке, продаже и пожертвовании товаров в Интернете за один квартал (375).

Большинство сообщений касалось покупки товаров, которые либо не были доставлены, либо были доставлены некачественные товары.

Количество поддельных интернет-магазинов растет, и их становится все труднее обнаружить.

Количество сообщений о несанкционированном доступе увеличилось на 28% по сравнению с 2021 годом.

Эти инциденты повлекли за собой финансовый убыток в размере 734 000 долларов США в третьем квартале». ***(Record Scam Loss Is A Call For NZers To Act On Cyber Security // Scoop Media (https://www.scoop.co.nz/stories/BU2212/S00084/record-scam-loss-is-a-call-for-nzers-to-act-on-cyber-security.htm). 07.12.2022).***

***

«… самые страшные истории о безопасности в 2022 году.

Уязвимость Log4Shell сеет хаос в течение 2022 года

Уязвимость Log4Shell продолжает сеять хаос в бизнесе спустя год после того, как она впервые потрясла индустрию безопасности. Обнаруженная в декабре 2021 года уязвимость нулевого дня удаленного выполнения кода (RCE) в регистраторе Java Log4j оказалась настолько серьезной из-за огромного количества приложений и сервисов, на которых она работает: Log4j используется миллионами компьютеров во многих организациях и лежит в основе множества интернет-сервисов. и приложений, включая Twitter, Microsoft и Amazon.

Критическая уязвимость Log4Shell с рейтингом 10/10, имеющая обозначение CVE-2021-44228 в Национальной базе данных уязвимостей NIST, относительно легко эксплуатируется, поскольку не требует привилегированного доступа для использования в атаках. Поэтому неудивительно, что всего через 24 часа после того, как она была раскрыта, исследователи из охранной фирмы Checkpoint зафиксировали почти 200 000 попыток использования этой проблемы. Через неделю после того, как Log4Shell стал достоянием общественности, киберпреступники и другие злоумышленники использовали эту уязвимость в рамках более чем 1,2 миллиона атак по всему миру.

Проблема с Log4Shell сохранялась вплоть до 2022 года. В феврале уязвимость использовалась спонсируемыми иранским государством злоумышленниками, нацеленными на правительство США. Еще в октябре 2022 года сообщалось, что группа, связанная с правительством Китая, использовала уязвимость для нападения на несколько организаций на Ближнем Востоке.

В ноябре компания Tenable, занимающаяся безопасностью, обнаружила, что, несмотря на исправление и устранение проблемы, до 72% фирм остаются уязвимыми для Log4Shell.

За массовым взломом Uber взялся печально известный Lapsus$

Uber столкнулся с одним из крупнейших нарушений безопасности года, когда злоумышленники смогли получить доступ к системам после того, как обманом заставили сотрудника передать данные.

Новость о взломе впервые сообщила New York Times в сентябре, причем сам злоумышленник сообщил изданию об инциденте. Вскоре после этого компания указала пальцем на хакерскую группу Lapsus$, которая нацелилась на другие технологические фирмы, включая Microsoft и Nvidia, как на инициаторов атаки.

Впоследствии семь человек были арестованы в марте полицией лондонского Сити, которая ведет международное расследование дела Lapsus$, а двое подростков предстали перед судом в апреле.

Uber заявил, что злоумышленнику удалось получить доступ к учетной записи подрядчика, рассылая спамом запросы многофакторной аутентификации. Uber

подозревает, что устройство подрядчика было заражено вредоносным ПО, что позволяет злоумышленникам красть учетные данные и продавать их в Интернете.

Используя украденные учетные данные, злоумышленники смогли получить доступ к некоторым внутренним системам Uber, включая сообщения Slack, финансовый инструмент для выставления счетов и панель инструментов, где исследователи безопасности сообщают об уязвимостях.

В Uber заявили, что данные клиентов не были скомпрометированы, но фирма быстро приступила к набору персонала, чтобы укрепить свою систему безопасности.

Программы-вымогатели продолжают поражать организации по всему миру

Программы-вымогатели продолжали разрушать организации по всему миру в 2022 году, особенно выделялись две атаки.

Первым был двойной удар по Коста-Рике, которая в течение года подверглась серии нападений. В апреле страна пострадала от кибератаки, нацеленной на важнейшую гражданскую инфраструктуру, предположительно совершенной российской группой Conti. Среди нарушенных услуг были международная торговля и сбор налогов, при этом пострадавшие организации были вынуждены полагаться на ручку и бумагу, чтобы добиться цели, а правительство в конечном итоге объявило чрезвычайное положение в стране.

В следующем месяце, как только страна начала вставать на ноги, страна подверглась новой атаке программы-вымогателя, на этот раз нацеленной на Фонд социального обеспечения Коста-Рики (CCSS), который управляет общественным здравоохранением. Более 30 000 медицинских приемов пришлось перенести после того, как группа вымогателей Hive, которая, как считается, имеет некоторые связи с первоначальными злоумышленниками, вывела из строя ИТ-системы в больницах и клиниках страны.

В целом атаки обошлись организациям, работающим в Коста-Рике, в сотни миллионов долларов США.

Второй крупный инцидент с программами-вымогателями в этом году произошел в октябре, когда австралийская страховая компания Medibank была

атакована группой программ-вымогателей, связанной с русскоязычным REvil. Когда компания отказалась платить выкуп, банда опубликовала конфиденциальные медицинские записи, включая имена клиентов, номера паспортов, даты рождения и информацию о требованиях. Злоумышленники даже разделили украденные данные клиентов на «плохие» и «хорошие» списки в зависимости от того, был ли диагноз связан с такими факторами, как наркомания или злоупотребление алкоголем.

Поскольку это такая прибыльная бизнес-модель с растущим числом предложений «как услуга» для аутсорсинга, программы-вымогатели не исчезнут в ближайшее время и будут продолжать угрожать бизнесу в 2023 году и далее.

Ограбления биткойнов происходят на криптовалютных биржах, платформах и личных кошельках

Кибер-злоумышленники всегда будут преследовать деньги, и криптовалюта не исключение. Более того, крипто-сделки не связаны с личностью людей, что делает их привлекательными для преступников.

В октябре сообщалось, что инвесторы потеряли более 3 миллиардов долларов (2,46 миллиарда фунтов стерлингов) из-за 125 взломов в 2022 году. По данным компании Chainalysis, занимающейся аналитикой блокчейнов, этот год, вероятно, превзойдет 2021 год как самый крупный год для взломов за всю историю наблюдений.

Среди крупных инцидентов 2022 года в начале года произошел взлом криптовалютной биржи Crypto.com, поддерживаемой Мэттом Дэймоном, в результате чего пострадали 483 пользователя. Сайт признал, что злоумышленники смогли украсть 35 миллионов долларов (28,7 миллиона фунтов стерлингов) несанкционированного снятия биткойнов и эфира в результате ограбления.

Затем, в феврале, злоумышленники украли 320 миллионов долларов (262 миллиона фунтов стерлингов) из протокола Wormhole — моста, связывающего блокчейны Ethereum и Solana. В следующем месяце сеть Ronin Network потеряла более 620 миллионов долларов (509 миллионов фунтов стерлингов) после того, как злоумышленник скомпрометировал закрытые ключи и организовал поддельные выплаты. Затем, в апреле, Beanstalk Farms — сеть для балансировки спроса и

предложения криптовалют — подверглась атаке, и было украдено 182 миллиона долларов (149 миллионов фунтов стерлингов) цифровой валюты.

В августе злоумышленники смогли взломать Nomad, программу, позволяющую пользователям обменивать токены из одной цепочки блоков в другую, похитив около 190 миллионов долларов (156 миллионов фунтов стерлингов) в биткойнах.

Российско-украинская война вызывает опасения кибератак

Эксперты по кибербезопасности начали предупреждать о риске широкомасштабных кибератак, исходящих из России, как только она вторглась в Украину в феврале 2022 года. Были распространены опасения, что российские хакеры попытаются скомпрометировать критически важную инфраструктуру, такую как электрические сети, и что эти атаки могут также быть нацелены на Украину. союзников, включая Великобританию и США.

В марте президент США Джо Байден предупредил предприятия критически важных секторов о необходимости быть начеку в связи с растущей киберугрозой со стороны России. Национальный центр кибербезопасности (NCSC) также предупредил, что вредоносная программа HermeticWiper использовалась против украинских организаций, и заявила, что она может повлиять на другие страны.

Но в целом атаки были ограниченными и простыми по своему масштабу, по крайней мере отчасти потому, что США и Европа перед войной предоставили Украине и другим странам Восточной Европы значительный опыт в области кибербезопасности.

Это не означает, что в первые дни конфликта не было никаких негативных последствий, и некоторые атаки вызвали сбои, особенно в работе коммуникационных услуг. Одна из первых кибератак на компанию широкополосного доступа Viasat 24 февраля началась примерно за час до начала вторжения России в Украину. NCSC заявил, что Россия «почти наверняка несет ответственность за атаку», которая затронула частных и коммерческих интернет-пользователей, ветряные электростанции в Центральной Европе и украинские военные, которые, как предполагается, были первоначально намеченной целью.

В марте крупнейшая в Украине компания фиксированной связи «Укртелеком» подверглась серьезной кибератаке, в результате которой услуги компании были отключены по всей стране.

Уязвимости ProxyNotShell в Microsoft Exchange досаждают администраторам

В 2021 году уязвимости ProxyShell и ProxyLogon в Microsoft Exchange доминировали в заголовках, отчасти потому, что их было очень легко использовать. Год спустя появилась новая пара уязвимостей, влияющих на Exchange Server, под общим названием ProxyNotShell.

Обнаруженные в сентябре исследователями безопасности из вьетнамской компании GTSC, два нулевых дня получили ряд попыток исправления, прежде чем Microsoft выпустила патч в ноябре. GTSC заявила в своем отчете, что она заметила использование обеих уязвимостей в дикой природе по крайней мере за месяц до публикации своих выводов, а позже Microsoft подтвердила, что уязвимости использовались в атаках.

Отслеживаемые как CVE-2022-41040 и CVE-2022-41082, уже использованные уязвимости используются одна за другой для повышения привилегий с помощью подделки запросов на стороне сервера (SSRF) для получения доступа к серверной части Microsoft Exchange PowerShell, а затем удаленное выполнение кода на уязвимом сервере.

Обе проблемы затрагивают версии Microsoft Exchange 2013, 2016 и 2019 и оцениваются как имеющие высокую серьезность с оценкой CVSSv3 8,8/10.

Даже сейчас эти недостатки вызывают мурашки по спине у администраторов Exchange Server, потому что, хотя злоумышленнику необходимо пройти аутентификацию, их очень легко использовать.

Взлом Okta подчеркивает пиар-сторону реагирования на инциденты

Когда Okta была взломана в январе 2022 года, пострадали сотни ее клиентов. Тем не менее, компания, которая предоставляет программное обеспечение для «единого входа» и управляет входом в систему для более чем 100 миллионов клиентов, только два месяца спустя, в марте, признала, что ее взломали через

стороннего поставщика услуг поддержки клиентов. Признание было сделано после того, как группа Lapsus$ заявила, что взломала фирму, опубликовав скриншоты.

Первоначально Okta опубликовала заявление, в котором говорилось, что утечка «была расследована и локализована», но признала, что скриншоты, опубликованные в Интернете, «связаны с этим январским событием». В нем также говорится, что «нет никаких доказательств продолжающейся вредоносной активности, помимо активности, обнаруженной в январе».

Однако по мере того, как беспокойство по поводу инцидента нарастало, фирма выпустила ряд блогов. В одном из них глава службы безопасности Okta Дэвид Брэдбери заявил, что хакеры получили доступ к компьютеру инженера службы поддержки, нанятого Sykes, частью Sitel Group, в течение пяти дней. Он сказал, что инцидент был «аналогичен уходу от вашего компьютера в кафе, когда незнакомец - в данном случае фактически - сел за вашу машину и использует мышь и клавиатуру».

Он подчеркнул, что доступ был ограничен, а сама Окта, однако, не была взломана.

Позже Okta признала, что «совершила ошибку», задержав раскрытие информации о нарушении. «В январе мы не знали масштабов проблемы с Sitel — только то, что мы обнаружили и предотвратили попытку захвата учетной записи и что Sitel наняла стороннюю судебно-медицинскую фирму для расследования», — заявили в компании. «В то время мы не понимали, что существует риск для Okta и наших клиентов. Мы должны получать более активную и принудительную информацию от Sitel».

Взлом Okta не только подчеркивает важность безопасности цепочки поставок, но и демонстрирует необходимость обеспечения прозрачности и ясности в случае инцидента. В эпоху роста числа кибератак клиенты понимают, что нарушения случаются, но они также ожидают быстрого и четкого ответа». ***(Kate O'Flaherty. The scariest cyber security horror stories of 2022 // Future US LLC (https://www.itpro.com/security/cyber-security/369758/the-scariest-cyber-security-horror-stories-of-2022). 22.12.2022).***

***

Діяльність хакерів та хакерські угруповування

«Дослідники компанії з кібербезпеки опублікували звіт «Споживчі кіберзагрози: прогнози на 2023 рік», у якому спрогнозували, які методи атак використовуватимуть хакери. Найбільшою загрозою аналітики вважають віртуальну реальність, де збільшиться кількість скаму та кібератак.

За словами дослідників, у 2023 році для втілення своїх планів хакери активніше використовуватимуть метавсесвіти, де легко видавати себе за будь-кого, приховуючи справжню особистість. Користувачів попередили про ймовірні шахрайські схеми, віруси, програми-вимагачі та фішинг. Також вважають, що кількість віртуальних злочинів ростиме зі збільшенням метавсесвітів, обсяг ринку яких до 2026 року досягне $ 50 мільярдів.

Експерти вважають, що насильство та сексуальні домагання стануть серйозною проблемою у віртуальній реальності. Наразі не існує механізмів, здатних на 100% захистити користувачів від ймовірних зловмисників. Втім, є випадки, коли за насильство у метавсесвіті злочинці все-таки отримували покарання. Так мешканця Південної Кореї засудили до 4 років ув'язнення через створення та розповсюдження у віртуальній реальності контенту сексуального характеру з неповнолітніми.

30-річний зловмисник спонукав неповнолітніх жертв фотографувати та знімати на відео свої оголені тіла й надсилати їх йому. За інформацією правоохоронних органів, південнокореєць знайомився з неповнолітніми у метавсесвітах, де приховував свою справжню особистість та вік. Після отримання бажаних медіа, він розповсюджував їх у віртуальній реальності.

Щодо NFT та криптовалюти, дослідники з безпеки назвали їх головними цілями хакерів. Вважають, що шахраї використовуватимуть будь-які методи, щоб заволодіти обліковими записами гравців метавсесвітів або спонукати їх до скамерських транзакцій. Тому користувачам порадили й надалі бути максимально

обережними у мережі». ***(Криптовалютні аналітики назвали метавсесвіти головною кіберзагрозою 2023 року // No worries! (https://noworries.news/kryptovalyutni-analityky-nazvaly-metavsesvity-golovnoyu-kiberzagrozoyu-2023-roku-2/). 01.12.2022).***

***

«Lapsus$ нацелился на некоторые из самых сложных компаний на планете», — сказал председатель CSRB и заместитель министра внутренней безопасности по вопросам политики Роберт Сильверс.

Сегодня Министерство внутренней безопасности США (DHS) объявило, что Наблюдательный совет по кибербезопасности (CSRB) рассмотрит недавние атаки, связанные с Lapsus$, глобальной хакерской группой, занимающейся вымогательством. Сообщается, что Lapsus$ использовал методы для обхода ряда широко используемых средств контроля безопасности и успешно проник в ряд компаний в различных отраслях и географических регионах. CSRB разработает практические рекомендации о том, как организации могут защитить себя, своих клиентов и своих сотрудников от таких атак. После завершения доклад будет передан президенту Байдену через министра внутренней безопасности Алехандро Н. Майоркаса и директора CISA Джен Истерли.

«Совет по обзору кибербезопасности быстро зарекомендовал себя как инновационная и устойчивая организация в экосистеме кибербезопасности, — сказал секретарь Алехандро Н. Майоркас. «При проверке Lapsus$ Правление будет опираться на уроки, извлеченные из своей первой проверки, и поделится практическими рекомендациями, чтобы помочь частному и государственному секторам повысить свою киберустойчивость».

CSRB — это беспрецедентная государственно-частная инициатива, объединяющая лидеров правительства и отрасли для проведения авторитетного сбора фактов и выдачи рекомендаций в связи со значительными инцидентами в области кибербезопасности. Первый обзор CSRB был посвящен уязвимостям, обнаруженным в конце 2021 года в широко используемой библиотеке

программного обеспечения с открытым исходным кодом Log4j. В июле 2022 года CSRB завершил этот обзор и опубликовал свой отчет, который включал 19 действенных рекомендаций для правительства и отрасли. CSRB не имеет регулирующих полномочий и не является правоприменительным органом. Его цель состоит в том, чтобы определить соответствующие извлеченные уроки для информирования будущих улучшений и лучшей защиты наших сообществ.

«Lapsus$ нацелился на некоторые из самых сложных компаний на планете», — сказал председатель CSRB и заместитель министра внутренней безопасности по вопросам политики Роберт Сильверс. «После крупных инцидентов Наблюдательный совет по кибербезопасности проводит авторитетную проверку фактов и выдает рекомендации, которые могут оказать непосредственное влияние на безопасность экосистемы. Совместными усилиями правительства и отрасли мы будем давать рекомендации о том, как отражать и реагировать на эти виды кибератак с вымогательством».

«Поскольку киберугрозы продолжают развиваться, крайне важно, чтобы все организации признали, что они не являются непреодолимыми», — сказала заместитель председателя CSRB Хизер Адкинс. «CSRB рассмотрит киберактивность Lapsus$, чтобы проанализировать их тактику и помочь организациям любого размера защитить себя».

«Субъекты Lapsus$ совершили наносящие ущерб вторжения в несколько важнейших секторов инфраструктуры, включая здравоохранение, государственные учреждения и критически важное производство», — сказала директор CISA Джен Истерли. «Диапазон жертв и разнообразие используемых тактик требуют, чтобы мы понимали, как субъекты Lapsus$ осуществляли свои злонамеренные действия в киберпространстве, чтобы мы могли снизить риск для потенциальных будущих жертв. Мы благодарим CSRB за проведение этой проверки, чтобы помочь усовершенствовать нашу коллективную киберзащиту».

CSRB был создан в соответствии с указом президента «Улучшение национальной кибербезопасности» для обеспечения продуманного подхода к извлечению уроков из киберинцидентов. Для получения дополнительной

информации посетите веб-сайт CISA.gov/CSRB№». ***(Cyber Safety Review Board to Conduct Second Review on Lapsus$ // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cyber-safety-review-board-to-conduct-second-review-on-lapsus/). 02.12.2022).***

***

«Редакція NoWorries не радить встановлення хакерських інструментів на ваші пристрої!

Розробники інструменту для встановлення джейлбрейку Apple повідомили, що їм вдалось зламати операційну систему iOS 16. Джейлбрейк ОС Apple вдалося успішно реалізувати завдяки виявленій вразливості під назвою checkm8 bootrom. Детальніше про це розповіли спеціалісти видання iDownloadBlog.

Хакер під ніком palera1n заявив, що джейлбрейк відтепер працюватиме і на iOS 16.1.1 та iPadOS 16. Джейлбрейк (jailbreak) — офіційно не підтримувана корпорацією Apple операція, яка дозволяє отримати доступ до файлової системи ряду моделей iPhone, iPod, iPad, Apple TV, Apple Watch та розширити базові можливості пристрою. Операція користується популярністю переважно серед власників iPhone.

Як пояснив хакер, для успішного джейлбрейку на нових версіях ОС Apple у користувача має бути смартфон або планшет на базі процесора A10 або новішого чипа.

За словами розробників інструменту для встановлення джейлбрейку, операцію з розширення базових налаштувань пристрою можливо зробити лише за відсутності пароля. Якщо ж пароль на екрані блокування був встановлений раніше, доведеться скинути пристрій до заводських налаштувань.

Нагадаємо, що один з найвідоміших хакерів у джейлбрейк-спільноті Джордж Хотц (він же Geohot), який став відомим завдяки зламу ігрової приставки Sony PlayStation 3 та випуску джейлбрейка для iPhone, відтепер працює на Ілона Маска. Наразі Хотц проходить 12-тижневий випробувальний термін, після якого Маск вирішить його подальшу долю у компанії. Перед відомим хакером поставлено 2

основних завдання: розв’язати проблеми з пошуковою системою Twitter та прибрати вікно авторизації, яке блокує доступ до пошуковика незареєстрованим користувачам.

Щодо фундаментальних змін у компанії Apple, представники корпорації планують дозволити користувачам встановлювати альтернативні додатки на iOS, які продукуватимуть сторонні гравці технорinку. Раніше користувачі iPhone та iPad могли завантажувати цифрові продукти лише з фірмового магазину App Store. Якщо компанія дозволить встановлювати інше програмне забезпечення на свої фірмові ґаджети, розробники зможуть обходити обмеження Apple і встановлену 30%-ву комісію». ***(Хакерам вдалось реалізувати джейлбрейк для iOS 16.1.1 та iPadOS 16 // No worries! (https://noworries.news/hakeram-vdalos-realizuvaty-dzhejlbrejk-dlya-ios-16-1-1-ta-ipados-16/). 14.12.2022).***

***

«Министерство внутренней безопасности США (DHS) заявило в пятницу, что Наблюдательный совет по кибербезопасности расследует недавние кибератаки, связанные с Lapsus$.

«Сообщается, что Lapsus$ использовал методы для обхода ряда широко используемых средств контроля безопасности и успешно проник в ряд компаний в различных отраслях и географических регионах», — говорится в сообщении DHS.

Хакерская группа, состоящая из нескольких членов по всему миру, совсем недавно была замешана в цифровом вторжении в компанию Uber Inc (UBER.N), занимающуюся заказом такси.

Также известно, что он проник в системы Nvidia Corp (NVDA.O), Microsoft Corp (MSFT.O) и Okta Inc (OKTA.O), службы аутентификации.

Совет по обзору кибербезопасности — это государственно-частный орган, который занимается инициативами по установлению фактов. Он служит для обзора основных киберсобытий и вынесения конкретных рекомендаций». ***(Department of Homeland Security to probe cyber attacks linked to Lapsus$ // Reuters***

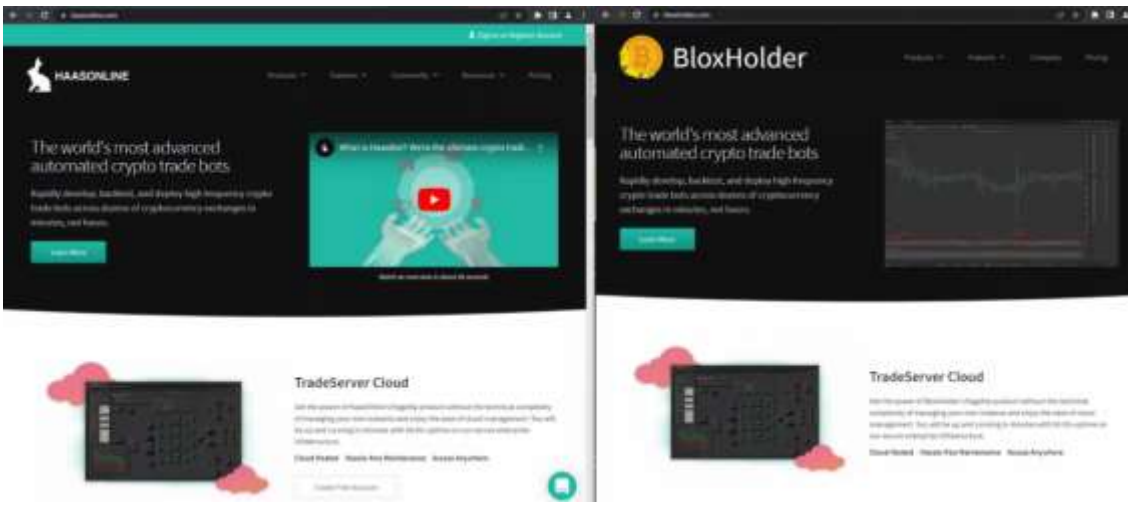
(https://www.reuters.com/world/us/department-homeland-security-probe-cyber-attacks-linked-lapsus-2022-12-02/?rpc=401&). 02.12.2022).

***

Вірусне та інше шкідливе програмне забезпечення

«Зловмисники із Північної Кореї розповсюджують вірус, який замаскований під бота для криптовалютної торгівлі - про це у своєму блозі повідомили IT-аналітики фірми Volexity. Йдеться про відоме хакерське угруповування Lazarus Group, яке вже неодноразово фігурувало у найбільших криптовалютних скандалах по всьому світі.

Дослідники стверджують, що нова хакерська кампанія розпочалася ще влітку 2022 року та тривала щонайменше до жовтня. У Volexity змогли виявити сайти-клони торгових ботів, які розповсюджували віруси для крадіжки цифрових активів.



Так, відомо, що сайт [bloxholder[.]com] поширює вірус під виглядом комерційного бота, схожого на сервіс HaasOnline. Шкідливий ресурс розповсюджує інсталятор Windows MSI під виглядом торгового робота BloxHolder. Насправді програма є вірусом AppleJeus, що пов’язаний із торговим клієнтом QTBitcoinTrader.

У жовтні 2022 року північнокорейські шахраї почали поширювати віруси у вигляді Excel-документу. Повідомляється, що xls-файл розміром 214 Кб під назвою «OKX Binance & Huobi VIP fee comparision. xls» містить макрос, який створює нові

файли на комп’ютері жертви. Як тільки вони будуть встановлені на ПК, вірус самостійно створює заплановане завдання для злому.

Примітно, що масштаби вкраденої криптовалюти досі залишаються незрозумілі. Проте, дослідники Volexity наголошують, що вірус від Lazarus Group — AppleJeus — здатен оновлюватися. Наприклад, в останній версії шкідливого ПЗ API-з'єднання шифруються за допомогою спеціального алгоритму, що ускладнює їхнє відстеження антивірусами на ПК.

На початку листопада ми розповідали, що північнокорейські хакери здійснили атаку на криптокомпанію в Ізраїлі. А в жовтні Lazarus Group проникли й на японські криптобіржі. Найвідоміше хакерське угруповування також підозрюється у допомозі уряду Північної Кореї у розробці зброї масового знищення — подейкують, що левова частка фінансування ядерної програми якраз складає крадена криптовалюта». ***(Хакери з Північної Кореї створили фейкове програмне забезпечення для крадіжки криптовалют // No worries! (https://noworries.news/hakery-z-pivnichnoyi-koreyi-stvoryly-fejkove-programne-zabezpechennya-dlya-kradizhky-kryptovalyut/). 06.12.2022).***

****

«Google TAG приписывает эксплойты спонсируемой государством APT37, также известной как Reaper

Хакеры, спонсируемые северокорейским государством, воспользовались уязвимостью нулевого дня в движке JavaScript браузера Microsoft Internet Explorer через документ Office, отправленный пользователям в Южной Корее.

Группа анализа угроз Google заявила, что обнаружила эксплойт в октябре после того, как несколько человек из Южной Кореи загрузили на VirusTotal копию вредоносного файла Word. Документ якобы является обновленной информацией о давке толпы на Хэллоуин, в результате которой погибло более 150 человек в районе Итхэвон в Сеуле.

APT37, также известная как Reaper, в первую очередь нацелена на Южную Корею, страну, с которой тоталитарный режим в Пхеньяне поддерживает

напряженное семидесятилетнее перемирие. Фирма по кибербезопасности Mandiant написала, что APT37, которая, по-видимому, активна по крайней мере с 2012 года, фокусируется на проведении шпионских кампаний как в государственном, так и в частном секторах.

Microsoft выпустила патч для нулевого дня в начале ноября.

Уязвимость CVE-2022-41128 находилась в движке JavaScript Internet Explorer — jscript9.dllприложении, которое Office использует для отображения HTML-контента. Google характеризует недостаток как неправильную компиляцию точно в срок, которая приводит к путанице типов переменных. Она похожа на другую уязвимость, CVE-2021-34480, которую исследователи Google выявили в 2021 году.

По словам Google, эта северокорейская группа угроз ранее использовала нулевые дни Internet Explorer. Использование Internet Explorer через канал Office имеет свои преимущества, поскольку оно не зависит от выбора пользователем браузера по умолчанию. Google также не требует связывания эксплойта с другим, чтобы выйти из изолированной программной среды расширенного защищенного режима Internet Explorer.

Вредоносный документ загружал шаблон файла форматированного текста, который, в свою очередь, извлекал удаленный HTML-контент, но только в том случае, если пользователи отключили параметр защищенного просмотра Office. В конечном итоге исследователи Google не восстановили окончательную полезную нагрузку кампании, но в прошлом APT37 поставляла различные имплантаты, которые «злоупотребляют законными облачными сервисами в качестве канала C2 и предлагают возможности, типичные для большинства бэкдоров».

Агентство по кибербезопасности и безопасности инфраструктуры добавило уязвимость нулевого дня IE в свой каталог известных эксплуатируемых уязвимостей в ноябре и приказало федеральным гражданским агентствам исправить ошибку к 9 декабря». ***(Mihir Bagwe. North Korean Hackers Look to Internet Explorer Zero Days // Information Security Media Group, Corp. (https://www.govinfosecurity.com/north-korean-hackers-look-to-internet-explorer-zero-days-a-20651). 07.12.2022).***

***

«По словам Fortinet, операторы Zerobot быстро обновили вредоносное ПО с помощью эксплойта для распространения

Новый ботнет использует уязвимости в большом количестве сетевого оборудования и сетевых камер с упором на оборудование, произведенное в Восточной Азии.

Среди целевых устройств — три типа маршрутизаторов марки Totolink производства гонконгской компании Zioncom и различные камеры китайской компании Hikvision. Ботнет, названный Zerobot фирмой по кибербезопасности Fortinet, также использует уязвимость, обнаруженную в тепловизионных камерах американской компании Teledyne FLIR.

Zerobot также использует уязвимости программного обеспечения, в том числе Spring4Shell, уязвимость в широко используемой платформе Java Framework с открытым исходным кодом Spring Framework, что повышает шансы ботнета на успех. Родитель Spring, VMWare, выпустила патч в марте.

Всего ботнет использует 21 уязвимость. Судя по всему, его операторы приобрели два из них у 0day.today — веб-сайта, предположительно предназначенного для образовательных целей, который продает эксплойты за криптовалюту.

Как только Zerobot заражает устройство, он загружает скрипт для дальнейшего распространения, пишет Fortinet. Компания впервые наблюдала за ботнетом 18 ноября, когда он содержал только основные функции. 24 ноября операторы ботнета обновили вредоносное ПО, включив в него модуль самораспространения.

«За очень короткое время он был обновлен за счет обфускации строк, модуля копирования файлов и модуля распространения эксплойта, которые усложнили его обнаружение и увеличили возможность заражения большего количества устройств», — пишет Кара Лин, исследователь Fortinet.

Исследователи выбрали название Zerobot, основываясь на том, как ботнет сохраняет себя на зараженных устройствах, используя имя файла zero.

Как это работает

После заражения Zerobot копирует себя на устройствах Windows в папку автозагрузки с именем файла FireWall.exe. В Linux есть три пути к файлам: %HOME%, /etc/init/и /lib/systemd/system/.

После инициализации Zerobot использует IP-протокол WebSocket для доступа к своему серверу управления и контроля. Команды включают:

- ping: Heartbeat, поддержание соединения;
- атака: запуск атаки для различных протоколов: TCP, UDP, TLS, HTTP и ICMP;
- стоп: Остановить атаку;
- update: установить обновление и перезапустить Zerobot;
- enable_scan: Сканировать открытые порты и начать распространять себя через эксплойт или взломщик SSH/Telnet;
- disable_scan: отключить сканирование;
- команда: запуск команды ОС cmd в Windows и bash в Linux;
- kill: убить программу ботнета.

Чтобы пользователи не могли нарушить работу программы Zerobot, она устанавливает модуль AntiKill, который перехватывает любой сигнал, отправленный для завершения процесса». ***(Prajeet Nair. Novel Botnet Dubbed 'Zerobot' Targets Slew of IoT Devices // Information Security Media Group, Corp. (https://www.govinfosecurity.com/novel-botnet-dubbed-zerobot-targets-slew-iot-devices-a-20658). 08.12.2022).***

***

«Поставщик шпионского ПО в Испании был связан со схемой эксплуатации нулевого дня, которая затронула Windows, а также браузеры Chrome и Firefox с 2018 по 2021 год.

Variston IT, базирующаяся в Барселоне, публично позиционирует себя как охранная фирма. Инструмент эксплуатации не рекламируется на его веб-сайте, и неясно, кому именно фирма предоставляла это шпионское ПО.

Испанское шпионское ПО использовало автоматическое сканирование Защитника Windows в эксплойте с нулевым щелчком

Структура эксплуатации была описана Группой анализа угроз Google в недавнем сообщении в блоге. Хотя Variston IT не рекламирует шпионское ПО и не заявляет о нем, исследователи Google представили маркеры, обнаруженные в его коде, включая скрипт, подписанный компанией.

Фреймворк Heliconia нацелен на ряд уязвимостей, которые были исправлены Google, Microsoft и Mozilla с начала 2021 по 2022 год. Основываясь на версиях Firefox, в которых присутствует уязвимость, исследователи полагают, что шпионское ПО могло использоваться как уже в конце 2018 года. Система сканирования уязвимостей Google «Safe Warnings» теперь будет обнаруживать и предупреждать о среде эксплуатации при переходе к онлайн-файлам, которые ее содержат, как и последние обновления Защитника Windows.

Обнаружение уязвимости произошло через анонимный отчет в программу поощрения ошибок Chrome. Обновление Защитника Windows особенно важно, поскольку компонент «Heliconia Soft» шпионского ПО использует ошибку в более старых версиях, которая позволяет использовать эксплойт без щелчка, поскольку Защитник автоматически сканирует входящий вредоносный PDF-файл. Ошибка рендерера Chrome требует открытия вредоносного файла или URL-адреса в браузере, как и цепочка эксплойтов Firefox (которая может работать как в Linux, так и в Windows, хотя версия для Windows содержит уникальный элемент выхода из песочницы).

В анализе не было предложено конкретное окно уязвимости, но эксплойт Firefox предназначен для использования уязвимости, присутствующей в версиях браузера с 64 по 68. Firefox 64 был выпущен в декабре 2018 года, что делает его самым ранним известным моментом, когда есть доказательства того, что инфраструктура эксплуатации жизнеспособна в дикой природе (Firefox 69 был

выпущен в сентябре 2019 года). Исследователи Google говорят, что они не нашли прямых доказательств того, что оно использовалось, но то, что продолжительность времени, в течение которого шпионское ПО было доступно, в сочетании с тем, что оно, по-видимому, исходило от поставщика эксплойтов, указывает на то, что кто-то, вероятно, использовал его в какой-то момент.

Variston IT отрицает связь с инфраструктурой эксплуатации

Хотя название компании фигурирует в коде среды эксплуатации, ИТ-директор Variston Ральф Вегнер ответил на запросы СМИ, заявив, что компания «была бы удивлена», если бы такой элемент был обнаружен в дикой природе. Коммерческие шпионские организации обычно пытаются замести следы, утверждая, что они продают только законным правительствам в правоохранительных целях, но кажущееся отрицание компанией того, что продукт даже принадлежит им, вызывает еще больше вопросов, чем обычно, о том, когда и где он использовался.

Исследователи Google отмечают, что рынок коммерческих программ-шпионов процветает и может быстро выйти из-под контроля. И это несмотря на общественное внимание, уделяемое израильской группе NSO за последние два года, и предпринятые против нее юридические действия, включая санкции. Как показало шпионское ПО Pegasus NSO, более продвинутые из этих фирм часто продают инфраструктуру эксплуатации с основными эксплойтами нулевого дня для ОС или приложений для обмена сообщениями, которые неизвестны и исправлены до того, как они были использованы в дикой природе в течение нескольких месяцев. Исследователи Google также выпустили предупреждение и статью о Pegasus, которая использовала нулевой день в iMessage для взлома устройств iOS, не требуя от пользователя открывать вредоносное сообщение или даже щелкать что-либо вообще. Apple с тех пор исправил эту уязвимость, но Pegasus остается доступным и, как предполагается, все еще используется во многих странах с репрессивными правительствами.

И, как показывают предыдущие предупреждения Google об угрозах, NSO Group — не единственный игрок, скрывающийся на рынке инфраструктур

эксплуатации. Исследователи опубликовали аналогичный отчет об угрозе для итальянской RCS Lab, которая предоставляет шпионские инструменты, нацеленные на устройства Android и iOS. Инструменты этого поставщика требуют нажатия на ссылки вредоносных программ в сообщениях, но представляют больший риск, чем обычно, поскольку группа, по-видимому, работает с локальными интернет-провайдерами, когда это возможно, чтобы отключить мобильное соединение цели, а затем отправить сообщение с вредоносным ПО с инструкциями по его повторному включению.

Другой игрок на рынке шпионского ПО, Candiru, также базируется в Израиле. Этот поставщик предоставил платформу эксплуатации, основанную на уязвимости нулевого дня в браузере Chrome, которую, по словам Google, она исправила. До патча вредоносное ПО было нацелено на журналистов в Ливане, Турции, Йемене и Палестине.

Крис Клементс, вице-президент по архитектуре решений Cerberus Sentinel, отмечает, что многие из этих поставщиков шпионского ПО являются просто первоначальными брокерами доступа, которые пытались добавить видимость легитимности, работая с правительствами: «Коммерческие поставщики шпионского ПО работают в пространстве, которое в любом другом контексте неотличимо от киберпреступности. Эксплойты, которые они разрабатывают, и функции наблюдения за их продуктами действительно по определению являются вредоносными программами. Эти организации часто защищают себя от юридических последствий, заявляя, что продают свои инструменты только для этического использования правительствами и правоохранительными органами; однако эти утверждения неоднократно оказывались неверными для некоторых поставщиков шпионского ПО. На самом деле единственная разница между этими организациями и поставщиками программ-вымогателей как услуг и брокерами начального доступа в даркнете заключается в их целевых клиентах и уровне полировки их продукта. К сожалению, часто мало контроля над тем, чтобы эти компании придерживались заявленных этических стандартов в отношении того, кому они продают и на кого ориентируются их продукты. Поскольку эти продукты

профессионально разработаны для коммерческого рынка, они часто столь же удобны для пользователя, сколь чрезвычайно эффективны в компрометации своих целей, используя эксплойты нулевого дня или почти нулевого дня, которые практически не имеют защиты. В конечном счете, человек или организация, на которые нацелены такие инструменты, мало что могут сделать, чтобы защитить себя, и эти инструменты используются относительно экономно по сравнению с другими вредоносными программами массового рынка. В результате они могут долгое время оставаться незамеченными защитниками и производителями. Однако общий совет, который будет полезен, заключается в том, чтобы всегда обновлять свои устройства и программное обеспечение с помощью исправлений безопасности, режим блокировки «для ограничения вашего воздействия за счет некоторых удобств и функциональности». ***(Scott Ikeda. "Commercial Spyware" Vendor Linked to Exploitation Framework Using Zero-Days in Chrome, Firefox and Windows // CPO Magazine (https://www.cpomagazine.com/cyber-security/commercial-spyware-vendor-linked-to-exploitation-framework-using-zero-days-in-chrome-firefox-and-windows/). 07.12.2022).***

***

«Group-IB обнаружила около трех десятков групп российских хакеров, распространяющих вредоносное ПО для кражи информации по модели «стилер как услуга». Инфостилер — это разновидность вредоносного ПО, которое собирает учетные данные, хранящиеся в браузерах, номера платежных карт и учетные данные криптокошелька, и отправляет их на серверы, контролируемые злоумышленниками.

По данным исследователей, за первые семь месяцев 2022 года группы угроз заразили 890 000 пользовательских устройств информационными программами, получив 50 миллионов паролей. Эта цифра на 80% больше, чем в предыдущий период.

Кроме того, злоумышленники также удалили 2 117 626 523 файла cookie (+74%), 113 204 криптокошелька (+216%) и 103 150 кредитных карт (+81%).

Российские хакеры используют вредоносное ПО Raccoon и Redline infostealer для получения сохраненных учетных данных

Группа по защите от цифровых рисков Group-IB обнаружила, что 34 группы российских хакеров развернули вредоносные программы Raccoon и Redline infostealer для сбора паролей от Steam, Roblox, Amazon, PayPal, а также информации о криптовалютных кошельках и кредитных картах. PayPal и Amazon являются наиболее уязвимыми: 16% и 13% украденных данных исходят от двух интернет-гигантов.

Кроме того, в отчете было обнаружено, что российские хакеры координировали свои действия по взлому русскоязычных групп Telegram, в которых в среднем было 200 активных участников, в основном актеры низкого уровня, ранее участвовавшие в Classiscam.

Несмотря на использование русского языка в качестве языка общения, они нацелены на жертв в 111 странах, в основном в США, Бразилии, Индии, Германии и Индонезии.

Самая популярная вредоносная программа-инфостилер, используемая российскими хакерами

Исследователи Group-IB оценили Redline как самую популярную вредоносную программу: 23 из 34 групп используют этот вариант. Вредоносное ПО Raccoon infostealer было далеко вторым, его использовали всего восемь групп, в то время как пользовательские программы для кражи информации имеют только три выделенные группы.

Тем не менее, администраторы групп предоставляют своим работникам похитители информации как Redline, так и Raccoon и претендуют на долю украденных данных или прибыли. Некоторые группы используют до трех вариантов вредоносного ПО для кражи информации, а другие — только один.

Работники киберпреступности могут арендовать вредоносное ПО из даркнета всего за 150-200 долларов в месяц.

Низкий барьер входа способствовал распространению вредоносного ПО для кражи информации.

Исследователи Group-IB объяснили, что приток киберпреступников в Classiscam с тысячами преступников вынудил злоумышленников изобретать больше способов заработать деньги с помощью киберпреступности, что привело к распространению вредоносного ПО для кражи информации. Кроме того, команда обвинила низкий барьер входа в рост распространения вредоносного ПО для кражи информации.

«Новичкам не нужно обладать продвинутыми техническими знаниями, так как процесс полностью автоматизирован и единственная задача работника — создать файл со стилером в боте Telegram и направить на него трафик, — написали они. «Однако для жертв, чьи компьютеры заражены стилером, последствия могут быть катастрофическими».

Российские хакеры создали иерархию после окончания Classiscam, и эта практика видна даже в их технологическом мастерстве. Например, процесс координации является высокоавтоматизированным: боты генерируют вредоносный контент, общаются между участниками и выполняют бухгалтерские задачи от их имени.

Тем не менее, «работники» по-прежнему выполняют низкоуровневые задачи, такие как направление трафика на вредоносные сайты для распространения вредоносных программ с использованием различных методов, таких как публикации в социальных сетях, видео на YouTube и зараженные файлы. Этот процесс включает в себя добавление вредоносных ссылок в обзоры видео на YouTube, поддельные розыгрыши и лотереи в социальных сетях, а также различные файлы NFT, чтобы заманить жертв к загрузке вредоносного ПО для кражи информации. Ссылки обычно направляют жертв на поддельные веб-сайты, выдающие себя за популярные бренды, чтобы завоевать доверие жертв и повысить вероятность загрузки вредоносного ПО.

В случае успеха российские хакеры продают украденные учетные данные на торговых площадках даркнета с прибылью. По оценкам Group-IB, рыночная стоимость украденных журналов и данных кредитных карт составила примерно 5,8 млн долларов.

Исследователи Group-IB призвали пользователей, сохраняющих пароли в браузерах, воздержаться от этой практики. Кроме того, им следует регулярно очищать файлы cookie своего браузера и избегать загрузки и установки подозрительного программного обеспечения.

«Этот тип вредоносных программ часто доставляется через зараженные документы Office, которые запускают сценарии PowerShell, и показывает, почему анализ угроз на основе поведения так важен для организаций», — отметил Шон Сербер, вице-президент по архитектуре и стратегии решений в Tanium». ***(Alicia Hope. Russian Hackers Steal 50 Million Passwords From 111 Countries Using Infostealer Malware // CPO Magazine (https://www.cpomagazine.com/cyber-security/russian-hackers-steal-50-million-passwords-from-111-countries-using-infostealer-malware/). 01.12.2022).***

***

«Согласно отчету Verizon о расследовании нарушений данных за 2022 год, офисные документы и электронная почта по-прежнему являются проверенными способами, с помощью которых киберпреступники доставляют вредоносную полезную нагрузку для получения доступа к сетям организаций. Злоумышленники могут скрывать вредоносный код, вредоносные макросы и небезопасные гиперссылки в общих файлах и доставлять их своим жертвам по электронной почте или через веб-приложения, что дает им возможность распространяться по всей ИТ-инфраструктуре организации.

Именно это обнаружили исследователи вредоносного ПО из HP Wolf Security при расследовании недавних кибератак на отели в Латинской Америке.

Вредоносное ПО OpenDocument нацелено на отели

Кампания началась с того, что злоумышленники отправили жертвам поддельное электронное письмо с запросом на бронирование с вредоносным вложением, выдававшим себя за регистрационный документ гостя. В этой конкретной кампании автор угрозы злоупотребил текстовым форматом OpenDocument (.odt).

OpenDocument — это формат файла на основе XML, используемый распространенными пакетами программного обеспечения для обработки текстов с открытым исходным кодом, включая Apache OpenOffice, LibreOffice и Microsoft Office. Киберпреступники используют это программное обеспечение для распространения вредоносных программ, которые обходят защиту конечных точек.

Это еще более опасно, чем текущее вредоносное ПО, часто встречающееся в файлах Microsoft Office, — оно загружает полезную нагрузку трояна удаленного доступа (RAT), используя объекты связывания и внедрения (OLE). Подобные методы на основе OLE, такие как CVE-2021-40444 и Folina, также были замечены в злоупотреблении документами Microsoft Office.

Анализ OpenDocument и AsyncRAT

Исследовательская группа OPSWAT изучила вредоносное вложение электронной почты и обнаружила связанный объект «webnar.info/internet/1.doc», который загружает и запускает вредоносный файл Excel.

Как только пользователь открывает вложение и разрешает ему обновлять поля со ссылками на другие файлы, загруженный файл Excel запрашивает, чтобы пользователь разрешил макросы. Принятие макросов активирует цепочку заражения.

В результате полезная нагрузка вредоносного ПО устанавливает AsyncRAT, позволяя хакерам удаленно отслеживать и контролировать зараженные устройства через безопасное и зашифрованное соединение.

Воздействие файловых угроз

Как только злоумышленник получает контроль над зараженными устройствами, он может проникнуть в сеть дальше и скомпрометировать серверы организации и другую критически важную инфраструктуру, поставив под угрозу операции всего бизнеса. Они могут получить доступ и украсть конфиденциальную личную информацию (PII, PHI, финансовые отчеты), подвергая организацию риску нарушения нормативных требований и штрафов. Финансово мотивированные хакеры могут блокировать пользователей от их систем, продавать украденные данные или удерживать их в заложниках с помощью атаки программ-вымогателей.

Как защитить свою организацию от этого вредоносного ПО с высокой степенью уклончивости

Существует много способов, с помощью которых организации могут защитить себя от угроз, связанных с файлами, от использования технологий нулевого доверия до применения более строгих политик в отношении разрешенных типов файлов.

По состоянию на 10 июля 2022 года традиционные антивирусные ядра, используемые программным обеспечением для сканирования вредоносных программ, не смогли обнаружить эту угрозу. Технология мультисканирования использует несколько антивирусных ядер, чтобы увеличить скорость обнаружения и сократить время обнаружения вспышек. Если целевая организация использует только одну антивирусную программу для защиты от кибератак, существует высокая вероятность компрометации.

Еще одна технология нулевого доверия, которую могут развернуть организации, — глубокое обезвреживание и реконструкция контента (CDR), обеспечивающая расширенную защиту от угроз, связанных с файлами. Как показано на снимке экрана ниже, Deep CDR обнаруживает, очищает и нейтрализует угрозы, заложенные в файле, в том числе вредоносный объект OLE, используемый во вредоносном ПО AsyncRAT, используемом в кампании, нацеленной на латиноамериканские отели.

Deep CDR работает, идентифицируя URL-адреса в файлах XML, которые указывают на серверы злоумышленника, и заменяя их безвредным хеш-фрагментом (#). Когда пользователь открывает вложение, объект OLE не может загрузить и запустить вредоносное ПО RAT. Обезвреженные файлы больше не представляют угрозы для вашей корпоративной сети.

В то время как кампания вредоносного ПО AsyncRAT нацелена на отели, которые хранят и обрабатывают PII для тысяч гостей, только представьте, что подобная кампания может сделать с критически важными инфраструктурными сетями, такими как больницы, государственные учреждения, службы экстренной помощи и другие. Методологии вредоносных программ и атак будут постоянно

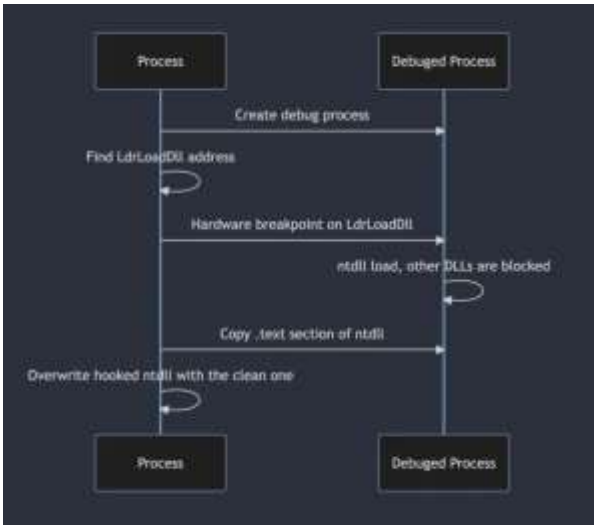
развиваться, но защита от файловых угроз с помощью этих технологий и элементов управления с нулевым доверием — это простой первый шаг к уменьшению поверхности атаки и предотвращению распространения злоумышленников на инфраструктуру организации». ***(George Prichici. Cybercriminals Leverage File-Based Attacks to Infiltrate Critical Networks // Techstrong Group Inc. (https://securityboulevard.com/2022/12/cybercriminals-leverage-file-based-attacks-to-infiltrate-critical-networks/). 16.12.2022).***

***

«Cymulate, поставщик платформы для оценки состояния кибербезопасности, поделился методом, получившим название Blindside, который позволяет вредоносному ПО обходить некоторые платформы обнаружения и реагирования на конечных точках (EDR) и другие системы мониторинга/контроля.

Майк ДеНаполи, директор по техническому обмену сообщениями в Cymulate, сказал, что исследователи компании обнаружили, что, используя точки останова для внедрения команд для выполнения неожиданных, нежелательных или злонамеренных операций, становится возможным создать чистую версию файла ntdll, в которой отсутствуют ловушки, которые есть на многих платформах EDR. полагаться на выявление этих типов атак. Он отметил, что после создания можно скопировать память чистой ntdll в существующий процесс таким образом, чтобы отцепить все ранее перехваченные системные вызовы.

Техника Blindside, по сути, использует методы, используемые для отладки программного обеспечения, вместо выполнения произвольного кода. При первом создании процесса автоматически загружается ntdll.dll. Точка останова блокирует загрузку дополнительных dll, перехватывая LdrLoadDLL для создания процесса, в котором только ntdll находится в автономном, неподключенном состоянии.



Киберпреступники становятся все более искусными в методах и изощренных атаках, которые обходят средства защиты кибербезопасности. По словам ДеНаполи, командам по кибербезопасности крайне важно регулярно проверять, могут ли имеющиеся у них платформы кибербезопасности обнаруживать новые типы угроз по мере их развития. К сожалению, слишком много команд по кибербезопасности развертывают платформу по принципу «установил и забыл», что делает их организацию менее защищенной, чем они ожидают, добавил он.

Даже если лишь небольшой процент киберпреступников обладает навыками, необходимыми для разработки этих атак, у них нет недостатка в механизмах, позволяющих им делиться созданным ими кодом с другими киберпреступниками.

ДеНаполи отметил, что в ближайшие месяцы кибербезопасность станет более сложной задачей, поскольку регулирующие органы, такие как Комиссия по ценным бумагам и биржам (SEC), требуют от организаций раскрывать нарушения и подробно описывать, какие шаги они предприняли для повышения безопасности своей ИТ-среды. В результате организации больше не смогут игнорировать какие-либо недостатки используемых ими платформ кибербезопасности, добавил он.

Хорошо это или плохо, нет никаких сомнений в том, что руководители высшего звена уделяют кибербезопасности больше внимания, чем когда- либо. Проблема в том, что многие из них не понимают всех нюансов. Выбрасывание денег на кибербезопасность не всегда дает ожидаемый результат по мере развития методов и тактик. Платформы, которые сегодня используются для успешного

предотвращения атак, могут нуждаться в расширении для борьбы с новыми классами угроз по мере их появления.

Тем временем киберпреступники наверняка продолжат оттачивать свои навыки. Киберпреступники теперь организованы в синдикаты, что позволяет им специализироваться в различных областях. По мере того, как каждая из этих команд совершенствует свои навыки, сотрудникам правоохранительных органов становится все труднее идентифицировать всех членов того или иного синдиката. В результате кибербезопасность превращается в бесконечную битву, в которой невозможно победить в каждом отдельном сражении. Скорее, цель состоит в том, чтобы выиграть как можно больше сражений, сводя к минимуму радиус взрыва, когда что-то в конечном итоге пойдет не так». ***(Michael Vizard. Cymulate Identifies Cyberattack Technique That Evades EDR Platforms // Techstrong Group Inc. (https://securityboulevard.com/2022/12/cymulate-identifies-cyberattack-technique-that-evades-edr-platforms/). 21.12.2022).***

***

Програми-вимагачі

«Сегодня Федеральное бюро расследований (ФБР) и CISA выпустили совместный бюллетень по кибербезопасности (CSA) #StopRansomware: Cuba Ransomware, чтобы предоставить сетевым защитникам тактики, методы и процедуры (TTP) и индикаторы компрометации (IOC), связанные с кубинским вымогателем. В ходе расследований ФБР эти TTP и IOC были выявлены совсем недавно, в августе 2022 года. Этот CSA обновляет бюллетень ФБР за декабрь 2021 года: индикаторы компрометации, связанные с программой-вымогателем Cuba. Основные обновления включают в себя:

ФБР выявило резкое увеличение как числа скомпрометированных организаций США, так и сумм выкупа, требуемых злоумышленниками-вымогателями Кубы.

С весны 2022 года кубинские злоумышленники-вымогатели расширили свои TTP.

Отчеты третьих сторон и открытых источников указывают на возможную связь между участниками программы-вымогателя Cuba, участниками программы RomCom Remote Access Trojan (RAT) и участниками программы-вымогателя Industrial Spy.

ФБР и CISA призывают сетевых защитников пересмотреть совместный CSA и применить включенные меры по смягчению последствий. См. StopRansomware.gov для получения дополнительных рекомендаций по защите, обнаружению и реагированию на программы-вымогатели». ***(#StopRansomware: Cuba Ransomware // CISA (https://www.cisa.gov/uscert/ncas/current-activity/2022/12/01/stopransomware-cuba-ransomware). 01.12.2022).***

***

«…Вымогательство со стороны операторов программы-вымогателя на Кубе принесло преступной группировке 60 миллионов долларов, по оценке федерального правительства США в предупреждении о том, что число американских организаций, ставших жертвами атак этой банды, удвоилось за последний год.

Операторы Кубы активно нацелены на критически важные сектора инфраструктуры, включая финансовые учреждения, правительственные здания, сектор здравоохранения, производство и информационные технологии. Банда представляет собой еще одну группу программ-вымогателей, в которой злоумышленники крадут данные, прежде чем покинуть системы со злонамеренным шифрованием, а затем сливают данные, чтобы попытаться заставить непокорных жертв заплатить. Банда получила свое название благодаря расширению .cuba, которое она добавляет к зашифрованным файлам, и своему пристрастию к революционно-китчевым произведениям искусства.

Нет никаких признаков того, что группа имеет какую-либо связь с одноименной страной, говорится в совместном бюллетене ФБР и Агентства по кибербезопасности и безопасности инфраструктуры.

ФБР обнаружило кубинских вымогателей, скомпрометировавших более 100 организаций по всему миру. Среди их жертв было правительство Черногории, которое в августе отключило несколько правительственных веб-сайтов и служб в ходе того, что официальные лица характеризуют как целенаправленную кибератаку.

Последнее предупреждение является продолжением предупреждения ФБР от декабря 2021 года, в котором сумма вымогательства с Кубы оценивается в 43,9 миллиона долларов.

По словам двух агентств, группа изменила свои методы за последние полгода, отметив сообщения о очевидной связи между участниками программы-вымогателя Cuba и участниками RomCom RAT и участниками программы-вымогателя Industrial Spy.

Агентства ссылаются на отчет Palo Alto Networks, в котором говорится, что Куба использует RomCom для управления и контроля и что примерно в мае Куба начала продавать свои данные на онлайн-рынке Industrial Spy для продажи украденных данных.

Агентства также сообщают, что программа-вымогатель Industrial Spy имеет явное сходство по конфигурации с программой-вымогателем Cuba, а в отчете о компрометации иностранной медицинской компании отмечается, что Куба развернула RomCom RAT.

В отчете Пало-Альто говорится, что Куба использовала CVE-2022-24521 в драйвере Windows Common Log File System для кражи системных токенов и повышения привилегий, использовала сценарий PowerShell для разведки, развернула инструмент под названием KerberCache для взлома билетов Kerberos в автономном режиме через Kerberoasting и использовал CVE-2020-1472, чтобы получить административные привилегии.

Предупреждение также предупреждает, что Куба использовала дроппер, который записывает драйвер ядра в файловую систему под названием ApcHelper.sys, которая нацелена на продукты безопасности и завершает их работу. Дроппер не был подписан, но драйвер ядра был подписан с использованием сертификата, найденного в утечке LAPSUS NVIDIA». ***(Prajeet Nair. Cuba Ransomware Targeting Critical Infrastructure, Feds Warn // Information Security Media Group, Corp. (https://www.govinfosecurity.com/cuba-ransomware-targeting-critical-infrastructure-feds-warn-a-20620). 02.12.2022).***

***

«Государственные органы и частный сектор пострадали от атаки на поставщика ИТ-услуг

Атака программы-вымогателя на стороннего поставщика ИТ-услуг в Новой Зеландии затронула несколько правительственных учреждений по всей стране, в том числе министерство юстиции и национальный орган здравоохранения.

Управление уполномоченного по вопросам конфиденциальности заявило, что «ведется срочная работа», чтобы понять все последствия инцидента. Сторонним поставщиком является Mercury IT, чья страница LinkedIn описывает его как малый бизнес, базирующийся в Веллингтоне. Он предоставляет широкий спектр ИТ-услуг клиентам по всей Новой Зеландии, согласно одностраничному веб-сайту на домене компании.

Новости об инциденте начали просачиваться в общественность после того, как частная медицинская страховая компания Accuro из Веллингтона проинформировала клиентов в четверг об инциденте у стороннего поставщика, который мог повлиять на личные данные ее 34 000 клиентов.

Представитель Управления уполномоченного по вопросам конфиденциальности сообщил Information Security Media Group, что ИТ-отдел Mercury постоянно стоит за этой чередой перебоев в обслуживании.

Национальный центр кибербезопасности Новой Зеландии, министерство здравоохранения Новой Зеландии и министерство юстиции опубликовали во вторник отдельные заявления, подтверждающие инцидент.

Государственные службы здравоохранения работают в обычном режиме, но врачи в некоторых районах страны не имеют доступа к реестру наследственных сердечных заболеваний или услугам по уходу за близкими. Приблизительно 8 500 записей о тяжелой утрате и 5 500 записей в регистре сердечных заболеваний недоступны.

Также пострадали шесть других регулирующих органов в области здравоохранения, услуги которых предоставляются Mercury IT. В их число входят Совет оптометристов и оптометристов Новой Зеландии, Совет хиропрактики, Совет ортопедов, Совет психологов Новой Зеландии, Совет диетологов и Совет физиотерапевтов Новой Зеландии.

Министерство юстиции сообщает, что инцидент, по-видимому, повлиял на доступ примерно к 14 500 записям, касающимся перевозки умерших людей, и примерно к 4000 вскрытий.

The New Zealand Herald сообщила, что некоторые организации частного сектора также могут быть затронуты, в том числе лоббистская организация Business NZ. Онлайн-домен организации в настоящее время отображает одностраничный веб-сайт, на котором указано, что он «в настоящее время находится на обслуживании». ***(Mihir Bagwe. Ransomware Attack in New Zealand Has Cascading Effects // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ransomware-attack-in-new-zealand-has-cascading-effects-a-20636). 06.12.2022).***

***

«Банда вымогателей Ragnar Locker раскрыла конфиденциальные данные бельгийского полицейского подразделения, приняв их за муниципалитет Звейндрехт.

Бельгийские СМИ назвали эту утечку данных одним из крупнейших разоблачений государственной службы в истории страны, в результате которого также были разоблачены люди, сообщавшие о преступлениях. Таким образом, воздействие может повлиять на деятельность и расследования правоохранительных органов, подвергая опасности свидетелей и предупреждая подозреваемых.

Банда вымогателей раскрыла отчеты о расследовании бельгийской полиции

Банда вымогателей с двойным вымогательством опубликовала украденную информацию на своем сайте утечки данных «имя и позор» в даркнете.

Утечка данных включает конфиденциальную информацию, такую как отчеты о расследованиях, судимости, тысячи номерных знаков, штрафы за нарушение правил дорожного движения, личные дела, телефонные исследования и файлы преступлений, включая изображения жестокого обращения с детьми. Утечка также выявила записи дорожных камер, которые могли раскрыть местонахождение людей в определенное время, тем самым нарушив их конфиденциальность и поставив под угрозу их безопасность.

Другие просочившиеся конфиденциальные данные включают имена, номера телефонов, а также метаданные абонентов и SMS людей, находящихся под тайным полицейским расследованием. Эта информация может предупредить подозреваемых о продолжающихся расследованиях, что позволит им уничтожить улики и устранить потенциальных свидетелей.

По сообщениям местных бельгийских СМИ, банда вымогателей раскрыла данные за 18 лет, собранные бельгийским полицейским подразделением с 2006 по сентябрь 2022 года. Хотя утечка затронула небольшое бельгийское полицейское подразделение, она может затронуть тысячи граждан.

«Эта атака показывает серьезные последствия кибератак: люди, которые сообщили о преступлениях или злоупотреблениях, потенциально могут получить утечку своих личных данных в Интернете. Уголовные расследования могут быть скомпрометированы, а уязвимым лицам может быть причинен реальный вред», — сказал Оливер Пинсон-Роксбург, генеральный директор Defense.com.

По словам Пинсона-Роксбурга, организации, хранящие конфиденциальные данные, нуждаются в надежной киберзащите для защиты своей деятельности и жизни людей. В противном случае могут возникнуть «опасные для жизни ситуации», что приведет к подрыву доверия населения к таким организациям.

Бельгийская полиция винит в этом человеческий фактор

Полицейское подразделение Zwijndrecht в Антверпене, Бельгия, преуменьшило значение инцидента, обвинив его в человеческой ошибке.

Марк Снелс, начальник полиции Звейндрехта, сообщил местному СМИ VRT, что данные были связаны с административной сетью, содержащей данные о персонале, такие как списки сотрудников и фотографии сотрудников. Однако он признал, что утечка данных содержала конфиденциальную информацию, хотя обычно ее «стараются выкладывать только в профессиональную сеть».

Снелс также охарактеризовал изображение жестокого обращения с детьми, по ошибке включенное в кеш информации, украденной бандой вымогателей Ragnar Locker, как «очень болезненное».

Банда вымогателей Ragnar Locker потребовала выкуп от бельгийской полиции

Начальник полиции Звейндрехта подтвердил, что банда вымогателей потребовала вымогателей, чтобы скрыть утечку данных, но местное отделение полиции отклонило запрос. Однако Снелс не раскрыл сумму, которую банда вымогателей Ragnar Locker потребовала в качестве выкупа.

Между тем, бельгийская полиция начала уведомлять лиц, пострадавших от утечки данных, и начала расследование инцидента со взломом.

Эксперты считают, что банда вымогателей нацелилась на плохо защищенную конечную точку Citrix как на начальный вход в полицейские сети. Другие источники утверждают, что злоумышленник получил доступ к сети, подобрав пароль.

Тем не менее, уязвимость высокой степени серьезности (CVSS v3 8.1) CVE-2022-27511 в функции управления доставкой приложений Citrix Server (ADM)

может позволить злоумышленнику сбросить пароль администратора во время перезагрузки устройства.

Будучи небольшим полицейским управлением, полицейскому подразделению Zwijndrecht, возможно, не хватало опыта для устранения критических уязвимостей в своих системах, что привело к нынешнему затруднительному положению.

«Эта последняя атака, в ходе которой была атакована слабозащищенная конечная точка Citrix, подчеркивает необходимость того, чтобы предприятия защищали каждую область своей цифровой инфраструктуры, иначе злоумышленники, такие как Рагнар Локер, воспользуются преимуществом», — сказал Пинсон-Роксбург.

Однако бельгийское полицейское подразделение не раскрыло, как банда вымогателей проникла в его системы, сославшись на продолжающееся расследование.

Ragnar Locker, впервые обнаруженный в апреле 2020 года, представляет собой группу вымогателей программ-вымогателей, нацеленную на компьютеры с Windows и Linux.

В марте 2022 года ФБР выпустило экстренное предупреждение о группе программ-вымогателей, которая нацелилась как минимум на 52 объекта в 10 объектах критической инфраструктуры в секторах производства, энергетики, финансовых услуг, правительства и информационных технологий.

«Атака банды вымогателей Ragnar Locker идет по проторенному пути группы, преследуя органы государственного сектора и раскрывая конфиденциальные данные», — добавил Пинсон-Роксбург. «Правительственные организации должны знать об угрозе, которую представляет эта конкретная группа. Только в этом году они нацелились на греческого оператора природного газа Air Portugal и несколько инфраструктурных организаций в США». ***(Alicia Hope. Ransomware Gang Hacks Belgian Police Unit While Targeting Municipality, Leaks Investigation Reports // CPO Magazine (https://www.cpomagazine.com/cyber-security/ransomware-gang-hacks-belgian-police-unit-while-targeting-municipality-leaks-investigation-reports/). 09.12.2022).***

***

«Trend Micro Incorporated (TYO), мировой лидер в области решений для кибербезопасности, прогнозирует, что в ближайшие годы группы программ-вымогателей будут все чаще атаковать серверы Linux и встроенные системы. В последнем отчете Trend Micro за 2022 год зафиксирован двузначный рост числа атак на эти системы в годовом исчислении в первом полугодии 2022 года.

В Катаре решения Trend Micro обнаружили и заблокировали более 2,1 миллиона почтовых угроз, предотвратили более 2,2 миллиона вредоносных URL-атак и 14 512 URL-хостов. Кроме того, было выявлено и остановлено более 3 миллионов атак вредоносных программ.

Обнаружение атак со стороны программы-вымогателя как услуги (RaaS) резко возросло в первой половине 2022 года. Крупные игроки, такие как LockBit и Conti, были обнаружены с 500-процентным увеличением в годовом исчислении и почти удвоили количество обнаружений за шесть месяцев соответственно. Модель RaaS принесла значительную прибыль разработчикам программ-вымогателей и их филиалам.

Согласно данным, Trend Micro заблокировала 63 миллиарда угроз в первом полугодии 2022 года, в первом полугодии было на 52% больше угроз, чем за тот же период 2021 года, а в тройку лидеров вошли правительство, производство и здравоохранение нацелены на вредоносное ПО.

В отчете также подчеркиваются сохраняющиеся риски удаленной и гибридной среды работы и обучения. Благодаря решениям Trend Micro Smart Home Network (SHN) компания Qatar заблокировала более 1,8 миллиона входящих и исходящих атак SHN и предотвратила 21 824 события SHN, чтобы хакеры могли нацеливаться на домашние устройства или контролировать их с целью запуска вредоносного ПО, получения конфиденциальной информации, перехвата сообщений или запуска внешних атак.

Асад Араби, управляющий директор Gulf Cluster, Trend Micro, сказал: «Несмотря на то, что предприятия в Катаре успешно справляются с современным

ландшафтом угроз, расширяющаяся поверхность атаки заставляет службы безопасности быть более бдительными, чем когда-либо. Последние результаты полугодового отчета содержат важную информацию об укреплении цифровой инфраструктуры организации, которую можно улучшить за счет интеграции многоуровневой унифицированной платформы кибербезопасности, которая защищает от будущих угроз».

Каждый день появляются новые группы программ-вымогателей. В первой половине 2022 года самым заметным был Черный Баста. Несмотря на то, что предприятия малого и среднего бизнеса являются более популярной мишенью, многие злоумышленники предпочитают крупные корпорации. Эксплуатация уязвимостей — распространенный вектор атаки программ-вымогателей. Неисправленные уязвимости вносят свой вклад в растущую поверхность цифровых атак, которую многие организации пытаются защитить, поскольку гибридные рабочие места расширяют их ИТ-среду. Более двух пятых глобальных организаций (43%) считают, что это «выходит из-под контроля».

Кроме того, видимость в облаке имеет решающее значение, учитывая постоянный риск, исходящий от третьих сторон, использующих такие методы, как облачный майнинг криптовалюты и облачное туннелирование, для использования неправильно настроенных сред. Злоумышленники часто используют последние для размещения фишинговых веб-сайтов или маршрутизации вредоносного трафика». ***(TYO detects nearly 11 million cyber security threats in Qatar // Trade Arabia (https://www.tradearabia.com/news/IT_404149.html). 12.12.2022).***

***

«Trend Micro Incorporated, мировой лидер в области решений для кибербезопасности, прогнозирует, что в ближайшие годы группы программ-вымогателей будут все чаще атаковать серверы Linux и встроенные системы. В последнем отчете Trend Micro за 2022 год зафиксирован двузначный рост числа атак на эти системы в годовом исчислении в первом полугодии 2022 года.

В Омане решения Trend Micro обнаружили и заблокировали более 1,8 миллиона почтовых угроз и предотвратили более 1,47 миллиона вредоносных атак через URL-адреса и 10 914 хостов URL-адресов. Кроме того, выявлено и остановлено более 1,4 млн атак вредоносных программ.

«Оманские предприятия доблестно боролись с быстро меняющимся ландшафтом угроз, однако проблемы с защитой расширяющейся поверхности атак остаются, — сказал Асад Араби, управляющий директор Gulf Cluster, Trend Micro. «Для защиты цифровой среды важно внедрить многоуровневую кибербезопасность. Самый последний полугодовой отчет — это важный ресурс, который поможет организациям найти более разумный и мощный подход к будущим вызовам безопасности в цифровой сфере»…». ***(Trend Micro safeguards Oman from over 5.7 million cyber security threats // Muscat Media Group (https://timesofoman.com/article/124375-trend-micro-safeguards-oman-from-over-57-million-cyber-security-threats). 12.12.2022).***

***

Програми-трояни

«Поддельные программы-вымогатели — не первый Wiper, нацеленный на удаление систем Windows в России

Российские компьютерные сети атакует новый троянец, который претендует на роль программы-вымогателя, но на самом деле предназначен для того, чтобы стирать системы и оставлять их без возможности восстановления.

Вредоносное ПО было названо CryWiper московской фирмой по кибербезопасности «Лаборатория Касперского», которая утверждает, что недавно обнаружила вредоносный код в дикой природе.

«На первый взгляд эта вредоносная программа выглядит как программа-вымогатель: она модифицирует файлы, добавляет.cryк ним расширение, уникальное для CryWiper, и сохраняет файл README.txtc примечанием о выкупе, в котором содержится адрес биткойн-кошелька, контактный адрес электронной

почты создателей вредоносной программы. и идентификатор заражения», — сообщается в нем.

Но все это — уловка, поскольку «файл, измененный CryWiper, не может быть восстановлен до исходного состояния — никогда», — говорится в нем. «Поэтому, если вы видите записку о выкупе и ваши файлы имеют новое расширение.CRY, не спешите платить выкуп: это бессмысленно».

Ежедневная российская газета «Известия» сообщает, что системы «мэрий и судов» входят в число организаций, зараженных поддельным вымогателем, который требует 0,5 биткойна — 8050 долларов США — за ключ дешифрования.

«Вайперы особенно опасны, так как восстановить работоспособность скомпрометированной инфраструктуры зачастую невозможно», — говорит Олег Скулкин, руководитель отдела цифровой криминалистики и реагирования на инциденты сингапурской компании по кибербезопасности Group-IB. «Злоумышленники часто не имеют финансового вознаграждения в качестве своего способа действий, а это означает, что их основная мотивация не состоит в том, чтобы жертва платила выкуп за восстановление своих файлов».

CryWiper — последний из длинной линейки новых вайперов, дебютировавших в преддверии и после военного вторжения России в Украину 24 февраля.

«Появление еще одного вайпера, замаскированного под программу-вымогатель, не стало неожиданностью, — говорит Скулкин.

И это не первая вредоносная программа Wiper, нацеленная на Россию. Например, через несколько дней после вторжения России группа исследователей безопасности MalwareHunterTeam сообщила, что обнаружила в дикой природе несколько версий нацеленного на Россию вредоносного ПО под названием RURansom. В нем говорится, что вредоносное ПО было разработано для проверки того, что зараженная система имеет российский IP-адрес, прежде чем запускать полезную нагрузку.

CryWiper протирает окна в России

CryWiper — это 64-битный исполняемый файл для операционной системы Windows.

«Изучив образец вредоносного ПО, мы выяснили, что этот троянец, хотя и маскируется под программу-вымогатель и вымогает деньги у жертвы за «расшифровку» данных, на самом деле не шифрует, а целенаправленно уничтожает данные в пораженной системе», — исследователи «Лаборатории Касперского». Об этом в своем блоге сообщают Федор Синицын и Янис Зинченко. «Более того, анализ программного кода троянца показал, что это была не ошибка разработчика, а его первоначальный замысел».

В частности, троянец предназначен для перезаписи большинства файлов «псевдослучайно сгенерированными данными».

Он предназначен для шифрования типов файлов, которые не требуются для работы ОС. «Вредоносное ПО сосредоточено на базах данных, архивах и пользовательских документах», — сообщает «Лаборатория Касперского».

Как сообщает «Лаборатория Касперского», CryWiper включает в себя ряд возможностей:

Использует планировщик заданий для запуска вайпера каждые 5 минут;

Передает имя зараженной системы на командно-контрольный сервер и должен получить команду для продолжения, прежде чем он начнет стирать зараженную систему;

Останавливает несколько баз данных, сервер Exchange и веб-службы Active Directory, «иначе доступ к некоторым файлам будет заблокирован и их невозможно будет повредить»;

Удаляет теневые копии файлов на диске «C», чтобы затруднить восстановление;

Отключает удаленные подключения к системе через протокол удаленного рабочего стола, хотя цель этого «не совсем ясна», но может быть предназначена для того, чтобы заставить группы реагирования на инциденты получить физический доступ для восстановления зараженных систем.

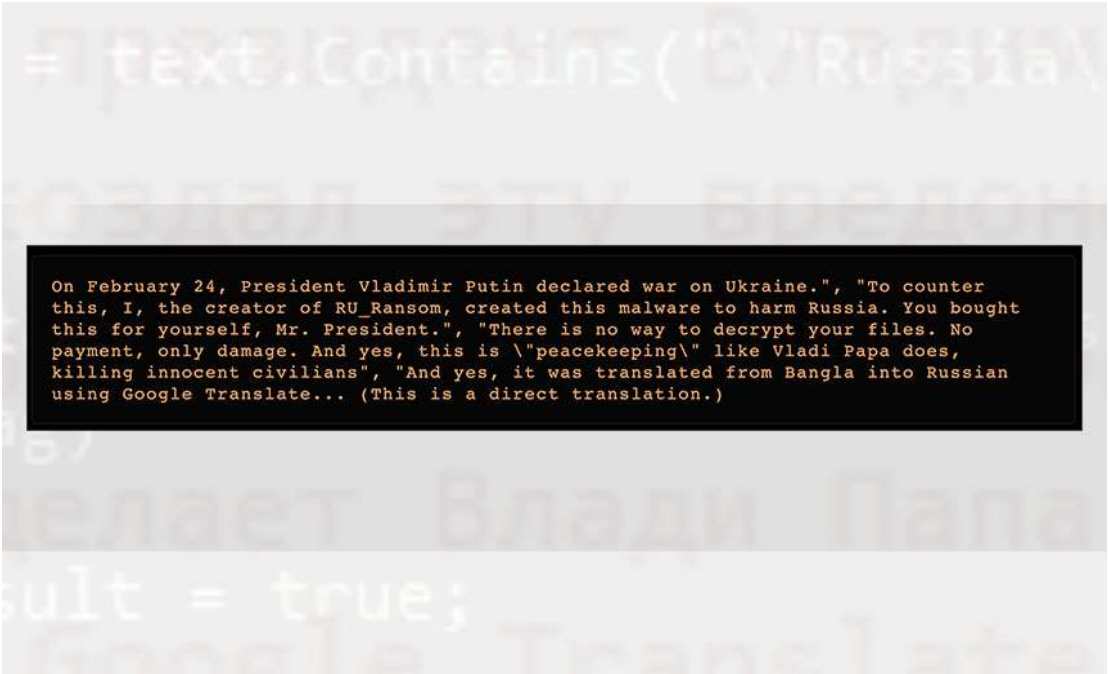
Несколько дворников в этом году

До этого года вредоносное ПО Wiper оставалось относительно редким, но, тем не менее, могло быть чрезвычайно разрушительным. Возьмем, к примеру, NotPetya, программу-вайпер, которую западные спецслужбы приписывают российской военной разведке и которая использовалась против Украины в 2017 году. Фальшивая программа-вымогатель вышла из-под контроля, в конечном итоге причинив коммерческий ущерб примерно в 10 миллиардов долларов по всему миру.

В прошлом году «такие атаки вспыхнули с новой силой», — говорит Скулкин. Варианты были выставлены группами, связанными или связанными как с Россией, так и с Украиной.

«На украинские организации нападали, например, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper и DoubleZero, в то время как хактивисты регулярно атаковали российские организации с помощью программ-вымогателей, основанных на исходных кодах Conti и LockBit, которые просочились в публичное пространство, наряду с законными инструментами, такими как BitLocker. и DiskCryptor», — говорит он.

Поскольку российско-украинская война идет уже девятый месяц, а мирных переговоров не предвидится, вполне вероятно, что в дикой природе будут замечены новые дворники.



Переведенная заметка удалена вредоносной программой RURansom wiper, которая нацелена только на системы в России (Источник: Trend Micro)». ***(Mathew J. Schwartz. Fresh CryWiper Wiper Malware Aims to Destroy Russian Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/fresh-crywiper-wiper-malware-aims-to-destroy-russian-data-a-20627). 05.12.2022).***

***

«Новий вірус-троян Godfather («Хрещений батько») активно шириться планетою, атакуючи криптогаманці та онлайн-банкінг. Фахівці з цифрової безпеки зафіксували атаки на понад 400 мобільних програм для Android, пише finextra.com.

За даними ресурсу, хакери використовують Godfather для атак на користувачів криптовалютних і банківських застосунків. Постраждали вже власники Android-пристроїв із 16 країн. Серед жертв трояна — 94 провайдери криптовалютних гаманців, 215 банківських установ та 110 криптообмінників у Туреччині (31), Іспанії (30), Канаді (22), Франції (20), Німеччині (19), Великій Британії (17) та США (49).

Для обману жертв Godfather генерує якісні вебпідробки. Вірус підставляє їх на екрани Android-смартфонів, коли користувач відкриває цільові програми. За допомогою трояна хакери крадуть облікові дані та обходять двофакторну автентифікацію.

Фахівці із сингапурської компанії Group-IB виявили у трояні код, який не дозволяє йому атакувати користувачів, які розмовляють російською або однією з мов, які використовували у колишньому Радянському Союзі.

«Поява Godfather підкреслює здатність учасників загроз редагувати та оновлювати свої інструменти, щоб підтримувати їхню ефективність, попри зусилля постачальників засобів виявлення та запобігання зловмисному програмному забезпеченню оновлювати свої продукти. Зловмисники можуть повернутися до вихідного коду, оновити застарілі типи зловмисного програмного забезпечення та багатьма способами зробити їх ще небезпечнішими. З таким інструментом, як

Godfather, зловмисники обмежені лише своєю здатністю створювати переконливі вебфейки для певної програми». ***(Кіра Іванова. Троян «Хрещений батько» атакував криптогаманці та банки по всій планеті // Speka.Media (https://speka.media/n4903-pn2k1p). 25.12.2022).***

***

Фішингові атаки

«Недавний всплеск сообщений о компрометации деловой электронной почты на основе SMS (BEC) может указывать на более широкую тенденцию, связанную с всплеском фишинговых атак с помощью текстовых сообщений.

«Фишинговые мошенничества широко распространены среди SMS-угроз, и теперь BEC-атаки также становятся мобильными», — говорится в сообщении в блоге Trustwave, в котором указывается, что в 2022 году в Федеральную комиссию по связи США поступило в три раза больше нежелательных текстовых сообщений, чем в 2019 году.

«В этом году мы наблюдаем тенденцию постепенного перехода BEC на мобильные устройства. Мы называем это компрометацией бизнес-текста», — сказал Сай Патрик Харр, генеральный директор SlashNext, которая опубликовала отчет, показывающий 50-процентное увеличение атак на мобильные устройства, при этом мошенничество и кража учетных данных возглавляют список полезной нагрузки.

«Мобильные устройства менее защищены, и на мобильных устройствах гораздо проще скрыть данные об отправителе. Самая популярная тактика, которую мы наблюдаем, заключается в том, что киберпреступники отправляют эти сообщения новым сотрудникам, которые не так хорошо знакомы с процессами компании и хотят хорошо выполнять свою работу», — сказал Харр.

«BEC часто работает с помощью социальной инженерии, и переход на мобильные устройства — это естественная эволюция», — сказал Бад Брумхед, генеральный директор Viakoo. «Многие организации проходят всестороннее

обучение фишинговым атакам по электронной почте и используют автоматизированные решения для борьбы со спамом; текстовые сообщения могут обойти обе эти защиты из-за присущего людям доверия к своим мобильным устройствам».

Отмечая, что убытки от BEC-атак во всем мире превысили 43 миллиарда долларов и что «мошенники становятся все более изощренными в своих приманках», исследователи Trustwave заявили: «Ход и природа BEC-атак в SMS аналогичны электронной почте, где злоумышленники обычно выдают себя за руководителей компаний», когда злоумышленники делают «законный запрос, например, запрос на банковский перевод, отправку копии отчета об устаревании или изменение счета заработной платы».

«Атаки BEC всегда будут здесь, пока они остаются прибыльными. Помните, что киберпреступность и киберпреступность как услуга — это индустрия с оборотом в триллион долларов, подпитываемая фишингом, а BEC — главная собака атак на основе электронной почты», — сказал Мика Аалто, соучредитель и генеральный директор Hoxhunt.

Рабочая группа по борьбе с фишингом (APWG) заявила, что мошенничество с подарочными картами доминировало в схемах во втором квартале 2022 года, а в отчете FTC за декабрь 2020 года говорится, что четверть потребителей, потерявших деньги в результате мошенничества, расплачивались подарочной картой, чаще всего от Target, Google. Play, Apple, eBay и Walmart.

Атаки обычно начинаются с электронного письма, когда злоумышленники запрашивают номер мобильного телефона жертвы — у них также есть множество способов получить номер, в том числе через утечку данных, социальные сети, сайты поиска людей и мошенничество с портами. Мошенничество с переносом — это мошенничество, при котором злоумышленники изображают из себя жертв и передают или «портируют» номер телефона жертвы другому поставщику услуг. «Чтобы эта афера сработала, злоумышленникам необходимо исследовать и собирать информацию о своей цели, используя общедоступные записи, платформы социальных сетей, утечки данных или слежку», — говорится в сообщении

Trustwave. «Как только о цели будет собрано достаточно данных, злоумышленники свяжутся с поставщиком услуг мобильной связи жертвы, выдавая себя за жертву, и попытаются передать номер жертвы на мобильный телефон, принадлежащий злоумышленнику».

Затем, получив контроль над номером телефона, мошенники могут «сбросить пароли жертвы на своих сервисах и платформах», говорят исследователи. «Все уведомления и предупреждения о входе в систему, обычно получаемые телефоном цели, теперь будут приниматься телефоном, контролируемым злоумышленником».

Переходя от BEC-атаки к SMS-атаке, субъекты угроз получают ряд преимуществ, говорится в сообщении блога, в том числе ограничение предоставляемой ими информации, которую можно отследить, более активное взаимодействие, «обеспечивающее немедленную связь между мошенниками и жертвами» и доставку как «в случае мошенничества с подарочными картами отправка изображений подарочных карт происходит быстро, что позволяет злоумышленникам легко достичь своей цели».

В отчете SlashNext отмечается, что Smishing и мобильные атаки не привлекали внимание специалистов по безопасности, пока серия громких нарушений, в том числе в Uber, Twilio и Cloudflare, не побудила их к действию. «В настоящее время количество мобильных фишинговых атак растет: 83% организаций сообщают, что угрозы для мобильных устройств растут быстрее, чем угрозы для других устройств, согласно Verizon Mobile Security Index 2022», — говорится в отчете. Эти инциденты, тем не менее, «демонстрируют рост фишинговых SMS-атак», которые успешно собирают учетные данные в начале цепочки атак, чтобы спровоцировать нарушение.

«Эти атаки были хорошо спланированы и осуществлены», — говорится в отчете SlashNext. «Пользователям трудно идентифицировать их, а это означает, что организации не могут полагаться на обучение сотрудников, чтобы остановить атаки с помощью SMS и других каналов связи».

Брумхед утверждал, что «взлом SIM-карты по-прежнему слишком прост; операторы мобильной связи по-прежнему остаются самым слабым звеном,

поскольку слишком многие их сотрудники поддаются методам социальной инженерии, позволяющим перенести мобильную учетную запись на другую SIM-карту».

По его словам, несмотря на то, что пользователи все лучше используют MFA, биометрию и другие средства защиты, «без прекращения взлома SIM-карт количество атак BEC будет продолжать расти».

«Постоянная прибыльность BEC-атак доказывает, что поведением сотрудников в области кибербезопасности пренебрегают и неправильно управляют подходом к обеспечению безопасности, основанным на соблюдении нормативных требований», — сказал Аалто. «Культура безопасности нуждается в реформировании, которое начинается с преобразования человеческого уровня в актив, который при наличии подходящего обучения и платформы дополняет основы защиты, обнаружения и реагирования структуры NIST». ***(Teri Robinson. Mobile BEC Attacks on the Rise // Techstrong Group Inc. (https://securityboulevard.com/2022/12/mobile-bec-attacks-on-the-rise/). 13.12.2022).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«25-річному Ніколасу Тругліа загрожує до 18 місяців тюремного ув'язнення за те, що він брав участь у схемі, внаслідок якої у блокчейн-консультанта Майкла Трепіна у 2018 році викрали 22 мільйони доларів у криптовалюті.

Стверджується, що злочинці попросили Ніколаса конвертувати токени, вкрадені у Трепіна, у біткоїн. Сторона звинувачення описує Ніколаса як учасника чималої кримінальної групи, що використовує техніку SIM-свопінгу (способу перенесення номерів з телефону жертви на SIM-картки під контролем шахраїв) з метою обкрадання представників криптоіндустрії.

Після власного приватного розслідування Трепін фактично сам вказав владі на можливих викрадачів його активів. Тругліа — єдиний із групи, кому висунуто кримінальні звинувачення, а також потенційне відшкодування збитків на 80 мільйонів доларів.

18 місяців — це лише півтора роки в'язниці. Такий короткий термін за такий крадіжку може бути пов'язаний з аутизмом Ніколаса. Адвокат шахрая заявив, що аутизм ускладнює розуміння наслідків у реальному світі для Ніколаса». ***(Криптовалютному шахраю дали лише півтора роки в'язниці за крадіжку $ 22 мільйонів у криптовалюті // No worries! (https://noworries.news/kryptovalyutnomu-shahrayu-daly-lyshe-pivtora-roky-vyaznyczi-za-kradizhku-22-miljoniv-u-kryptovalyuti/). 03.12.2022).***

***

«У Румунії, Молдові та Швеції провели масштабні обшуки. Шукали міжнародну групу, яка відмивала десятки мільйонів євро на комп'ютерному шахрайстві, використовуючи підставні компанії з Гонконгу та Ізраїлю.

Викрили організовану групу, яка спеціалізувалася на незаконній діяльності з відмивання коштів, одержаних злочинним шляхом. Вони діяли у період з лютого 2018 року по січень 2021 року на території Румунії, Болгарії, Польщі та Угорщини.

Злочинці займалися комп'ютерним шахрайством щодо фірм і компаній у Європі, Австралії, Північній Америці, Південній Америці, Азії.

Також вони виманювали кошти у громадян ЄС під прикриттям венчурних інвестицій. У схемі брали участь громадяни України, Молдови та Швеції. Вони переїжджали до Румунії для створення підставних компаній. На їхнє ім'я відкривалися банківські рахунки, через які потім відмивалися кошти.

У справі наклали арешт на активи вартістю понад п'ять мільйонів доларів. При цьому обсяг транзакцій, які підлягають кримінальному переслідуванню, перевищує 70 мільйонів євро». ***(У Румунії, Молдові та Швеції обшуки: ловили комп'ютерних шахраїв, які відмивали мільярди євро // UA.NEWS***

(https://ua.news/ua/world/v-rumynyy-moldove-y-shvetsyy-obysky-lovyat-kompyuternyh-moshennykov-otmyvayushhyh-myllyardy-evro). 07.12.2022).

***

«Прокуратура США раскрывает дела xDedic Criminal Marketplace

Захваченная в 2019 году торговая площадка способствовала мошенничеству на сумму более 68 миллионов долларов, говорят ФБР и IRS

Конфискация правоохранительными органами США в 2019 году криминального онлайн-рынка приносит дивиденды прокуратуре, разворачивающей судебное преследование обвиняемых мошенников, которые предположительно получили скомпрометированные учетные данные с сайта.

Прокуратура обнародовала четыре обвинительных заключения, обвиняющих трех граждан Нигерии и одного жителя Великобритании в сговоре с целью кражи личной информации американцев с целью получения мошеннического возмещения налогов.

Судебные преследования являются последним событием многолетних усилий по привлечению к ответственности пользователей и администраторов торговой площадки xDedic. Вскоре после захвата сайта в 2019 году представители ФБР и IRS подсчитали, что сайт способствовал мошенничеству на сумму более 68 миллионов долларов по всему миру. Испанские власти арестовали обвиняемого администратора сайта Александру Хабасеску, гражданина Молодова, на Канарских островах в марте и экстрадировали его в США 21 ноября.

Хабасеску предъявлено обвинение по двум пунктам уголовного обвинения в заговоре с целью незаконного использования устройств несанкционированного доступа и в хранении более 15 устройств несанкционированного доступа. Если его признают виновным, ему грозит до 15 лет лишения свободы.

Прокурор США Роджер Б. Хандберг из Среднего округа Флориды в понедельник объявил об аресте четырех обвиняемых в мошеннической схеме налогового мошенничества: Акинолы Тейлор, Олайеми Адафин и Олакунле

Ойебанджо в Лондоне 30 ноября и Казима Оланреваджу Рунсеве в Мальмё, Швеция, 1 декабря.

Тейлор и Рунсев якобы получили скомпрометированные учетные данные от xDedic.

В случае признания виновным предполагаемых участников заговора о налоговом мошенничестве каждому грозит до 20 лет лишения свободы за мошенничество с использованием электронных средств плюс, возможно, дополнительные штрафы». ***(Prajeet Nair. US Prosecutors Unspool xDedic Criminal Marketplace Cases // Information Security Media Group, Corp. (https://www.govinfosecurity.com/us-prosecutors-unspool-xdedic-criminal-marketplace-cases-a-20633). 06.12.2022).***

***

«Борьба с онлайн-мошенничеством Интерпола привела к аресту около 1000 киберпреступников и возвращению цифровых и финансовых активов на сумму почти 130 миллионов долларов.

«Всего в результате операции было задержано 975 человек и раскрыто более 1600 дел. Кроме того, было заблокировано почти 2800 банковских счетов и счетов с виртуальными активами, связанных с незаконными доходами от финансовых преступлений в Интернете», — сообщил Интерпол.

В операции с 28 июня по 23 ноября участвовали правоохранительные органы не менее 30 стран со всех континентов.

Операция Интерпола HAECHI III посадила известных киберпреступников за решетку

Операция HAECHI III была нацелена на различные онлайн-преступления, такие как голосовой фишинг, мошенничество в романтических отношениях, секс-вымогательство, мошенничество с инвестициями и отмывание денег, связанное с незаконными азартными играми в Интернете.

В результате операции было опубликовано 95 уведомлений, в том числе «красные уведомления» на двух беглецов. Южнокорейский дуэт разыскивался в

связи с глобальной схемой Понци, включая хищение 28 миллионов евро у 2000 южнокорейцев. Двое подозреваемых были арестованы в Греции и Италии в ходе пятимесячной операции.

Индийское и австралийское национальные центральные бюро Интерпола (NCB) также арестовали подозреваемых киберпреступников, которые выдавали себя за сотрудников правоохранительных органов и убеждали жертв перевести 159 000 долларов США с помощью подарочных карт, криптовалюты и финансовых учреждений.

Киберпреступники убедили свои цели в том, что их личные данные были украдены и использованы для совершения преступлений, связанных с наркотиками. Затем они проинструктировали жертв перевести свои деньги и виртуальные активы на «доверительный счет», чтобы очистить себя от предполагаемых преступлений.

Индийский NCB провел обыски в колл-центрах подозреваемых в Нью-Дели и Нойде, задержал киберпреступников и собрал любопытные доказательства, в том числе четыре криптовалютных кошелька. Власти конфисковали 25,83 биткойна, 37 000 долларов, хранящихся в нескольких цифровых кошельках, и банковский счет с еще 37 000 долларов у одного из подозреваемых киберпреступников.

Точно так же Интерпол вернул 1,25 миллиона долларов, украденных в результате мошенничества с компрометацией деловой электронной почты (BEC) в Ирландии.

По словам генерального секретаря Интерпола Юргена Штока, успех операции стал результатом следования за деньгами и трансграничного сотрудничества правоохранительных органов через Интерпол. Сток подчеркнул необходимость лишить киберпреступников их незаконных доходов, отметив, что операция позволила странам достичь этой цели.

HAECHI III — это третья операция международного органа по сотрудничеству правоохранительных органов, направленная против киберпреступников за пределами страны. В ноябре 2021 года HAECHI II позволил правоохранительным органам арестовать 1000 киберпреступников и вернуть 27

миллионов долларов. В мае 2021 года операция HAECHI I с участием 40 правоохранительных органов Азиатско-Тихоокеанского региона привела к взысканию с киберпреступников 83 млн долларов.

Новые тенденции в области преступности и Протокол быстрого реагирования по борьбе с отмыванием денег

В ходе операции Интерпол запустил Протокол быстрого реагирования по борьбе с отмыванием денег (ARRP), позволяющий странам запрашивать и помогать другим в борьбе с доходами от преступлений.

С января ARRP помог странам вернуть более 120 миллионов долларов от киберпреступников, причастных к различным цифровым злоупотреблениям в Интернете. Кроме того, операция помогла Интерполу раскрыть 16 новых криминальных тенденций, в том числе варианты мошенничества в романтических отношениях и секс-вымогательства, а также использование зашифрованных приложений для обмена сообщениями для продвижения поддельных криптокошельков.

Открытия помогут правоохранительным органам в борьбе с киберпреступниками, причастными к такой деятельности по всему миру». ***(Alicia Hope. INTERPOL Arrested Almost 1,000 Cybercriminals and Recovered $130 Million in Global Operation // CPO Magazine (https://www.cpomagazine.com/cyber-security/interpol-arrested-almost-1000-cybercriminals-and-recovered-130-million-in-global-operation/). 06.12.2022).***

***

«Органи правопорядку Китаю заарештували 63 особи, які звинувачуються у відмиванні грошей. Використовуючи криптовалюти, банді вдалося «відмити» близько $ 1,7 млрд. Злочинці привернули увагу влади цього літа, коли Департамент громадської безпеки помітив дивні транзакції на великі суми і передав інформацію поліції.

Зібравши докази, група з 230 співробітників поліції провела розшукові заходи у 17 провінціях, автономних регіонах та містах. В результаті їм вдалося знайти та заарештувати 63 підозрюваних, у яких було вилучено понад $ 18,5 млн.

Банда організувала незаконну діяльність у травні минулого року. Її члени допомагали китайським та закордонним злочинцям відмивати гроші, отримані від організації нелегальних онлайн-казино, фінансових пірамід та інших шахрайських схем. Кошти виводилися за допомогою криптовалюти. Для проведення операцій залучалося багато найманих працівників (дропів) по всій країні, які отримували винагороду за успішні транзакції.

Організаторів незаконного бізнесу заарештовано, вони перебувають під вартою». ***(У Китаї провели наймасштабніший арешт криптовалютних шахраїв // No worries! (https://noworries.news/u-kytayi-provely-najmasshtabnishyj-aresht-kryptovalyutnyh-shahrayiv/). 11.12.2022).***

***

«США конфіскують 48 вебсайтів у межах боротьби з кібератаками. Мережа сайтів влаштовувала мільйони DDoS-атак по всьому світу.

Міністерство юстиції оголосило, що США конфіскували десятки інтернет-доменів і висунули звинувачення шістьом особам у злочині. Сайти використовували для запуску мільйонів DDoS-атак по всьому світу. Атаки DDoS (скорочено від distributed-denial-of-service) спрямовують величезні обсяги непотрібного інтернет-трафіку на сайт або комп'ютерну мережу, щоб вивести їх з ладу, повідомляє Bloomberg.

На думку експертів з кібербезпеки, DDoS-сервіси за наймом часто називають себе «інструментами стресу» або «завантажувача», які нібито пропонують людям спосіб перевірити стійкість сайтів та сервісів, якими вони керують. Насправді послуги часто використовують для переслідувань, вимагання та злочинних дій.

Одним із популярних способів застосування сервісів є переміщення конкурентів у відеогрі офлайн. Також служби DDoS використовували, щоб вимагати від сайтів новин видалення небажаних статей або шантажувати компанії з

приводу припинення атак». ***(Катерина Колонович. США накрили мережу сайтів, які влаштовували DDoS-атаки // Speka.Media (https://speka.media/ssa-nakrili-merezu-saitiv-yaki-vlastovuvali-ddos-ataki-9q64wv). 15.12.2022).***

***

«Скандально відомого засновника криптовалютної біржі FTX, через банкрутство якої інвестори втратили мільярди вкладень, арештували на Багамських островах. Згідно з даними правоохоронних органів, затримання колишнього мільярдера стало можливим завдяки обвинувальному акту, який виніс Фріду прокурор Південного округу Нью-Йорка.

Наразі вирішуються питання, пов'язані з екстрадицією Сема Бенкмана-Фріда у США. Також вже сьогодні SBF постане перед судом у столиці Багамських островів, Нассау.

Офіційний обвинувальний акт прокурор Даміан Вільямс пообіцяв оприлюднити найближчим часом. Втім, вже зараз колишнього мільярдера звинувачують у шахрайстві та змові з використанням електронних засобів, шахрайстві з цінними паперами та відмиванні грошей. Комісія з цінних паперів та бірж США (SEC) також підготувала окремий обвинувальний акт, що стосується порушень закону про цінні папери США.

Раніше ходили чутки, що Бенкман-Фрід підкупив демократів США і саме тому залишався на свободі. Таку теорію підтримав навіть Ілон Маск, припустивши, що реальна сума спонсорських вкладень Фріда у Демократичну партію навіть більша за $ 1 мільярд.

Експерти з правових питань наголосили: якщо федеральний уряд висуне проти Бенкмана-Фріда звинувачення в шахрайстві з використанням електронних засобів або банків, то існує висока ймовірність того, що підприємця буде засуджено на довічний термін, без можливості звільнення під заставу…». ***(Сем Бенкман-Фрід арештований і може отримати довічний термін // No worries! (https://noworries.news/sem-benkman-frid-areshtovanyj-i-mozhe-otrymaty-dovichnyj-termin/). 13.12.2022).***

***

«Міністерство юстиції США повідомило, що колега найрозшукуванішої криптошахрайки Руджі Ігнатової зізнався у викраденні близько $ 4 мільярдів інвесторських коштів.

Карл Грінвуд був співзасновником криптовалюти OneCoin разом із так званою криптокоролевою Руджею Ігнатовою, яка досі перебуває у федеральному розшуку. Грінвуд та Ігнатова заснували фінансову піраміду OneCoin, яку вони та їх офшорна компанія OneCoin Ltd просували під виглядом криптовалюти.

Ігнатова обіцяла інвесторам зробити OneCoin найпопулярнішою віртуальною валютою у світі, закликаючи користувачів переводити власні заощадження на інвестиційні рахунки OneCoin.

Як стало відомо, Грінвуда заарештували в Таїланді ще у 2018, а потім екстрадували до США, де він досі перебуває під арештом. Наразі йому висунуто обвинувачення в організації фінансової піраміди та обмані інвесторів. Дізнавшись, що прокуратура Південного округу Нью-Йорка (SDNY) починає посилено боротися з фінансовими злочинами, Карл Грінвуд вирішив у всьому зізнатися. Його спільницю досі не знайдено. Влітку Ігнатову внесли у список 10 найбільш розшукуваних криптошахраїв.

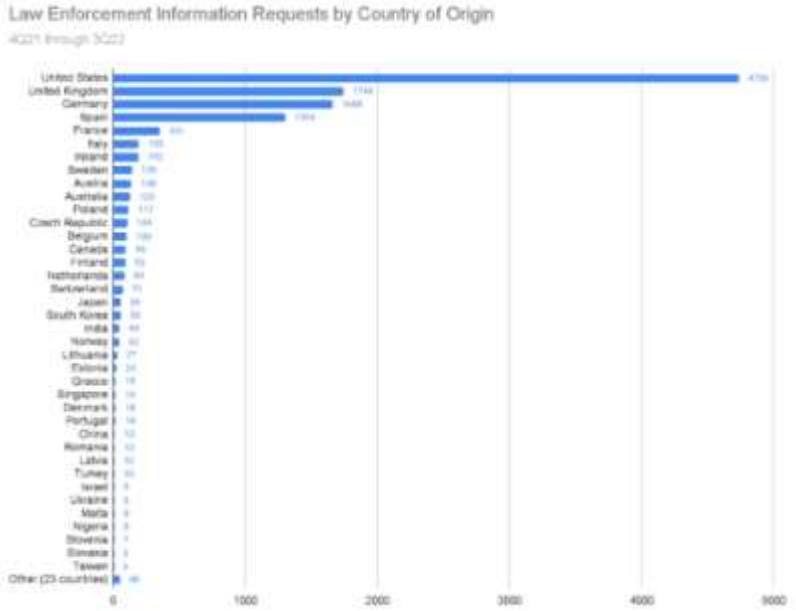
Вважають, що Руджа Ігнатова тепер може бути чоловіком. Про це свідчить низка ескізів, які ілюструють ймовірні зміни у зовнішності горезвісної бізнеследі. Правоохоронці припускають, що Ігнатова могла вдатися до таких хитрощів, щоб уникнути арешту за свої махінації.

Також існують припущення, що Руджа Ігнатова може переховуватися в Дубаї. Журналісти BBC стверджують, що Ігнатова нібито купила віллу в ОАЕ вартістю 20 мільйонів доларів, де, ймовірно, живе упродовж останніх п’яти років. BBC також виявила, що вона уклала багатомільйонну угоду з королівським шейхом Еміратів Саудом бін Фейсалом Аль Касімі». ***(Один із розробників криптовалюти OneCoin зізнався в обмані на $ 4 мільярди // No worries!***

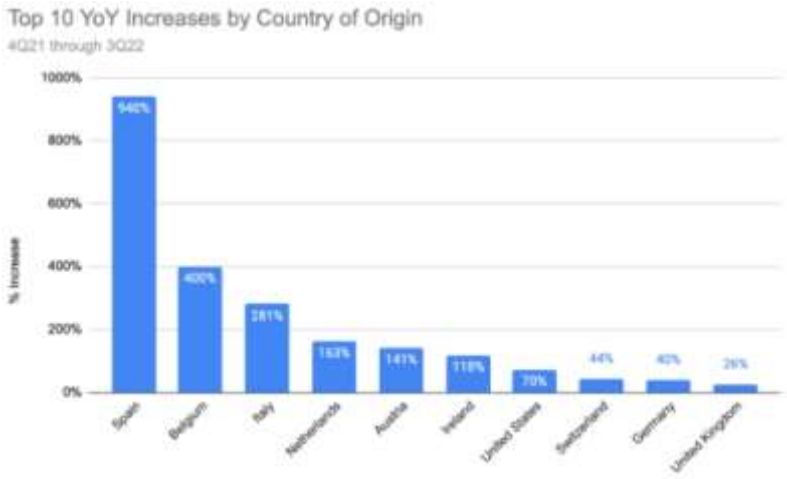
(https://noworries.news/odyn-iz-rozrobnykiv-kryptovalyuty-onecoin-ziznavsya-v-obmani-na-4-milyardy/). 17.12.2022).

***

«Згідно зі звітом Coinbase, з 1 жовтня 2021 року до 30 вересня 2022 року криптовалютна біржа отримала 12 320 запитів на розкриття інформації про клієнтів від правоохоронних органів — таким чином Coinbase стала криптоплатформою, яка більше за інших співпрацює з правоохоронцями.



«Від часу торішнього звіту кількість запитів збільшилася більш ніж удвічі. Ми пов’язуємо це із поєднанням нашого власного розширення та загального збільшення інтересу правоохоронних та регуляторних органів до криптоіндустрії», — прокоментував головний юрист Coinbase Пол Гревал. Найбільше біржа співпрацювала з правоохоронцями США, Великої Британії, Німеччини, Іспанії та Франції.



Серед європейських країн, які почали активніше звертатись до Coinbase цьогоріч — Іспанія, Бельгія, Італія, Нідерланди, Австрія, Велика Британія. «Запити можуть включати судові повістки, постанови, ордери на обшук або інші офіційні юридичні процедури. Ми зобов'язані на них відповідати, якщо вони законні відповідно до фінансових та інших чинних правил», — наголосив Гревал.

Деякі учасники криптоспільноти вважають, що Coinbase надмірно прагне задовольнити вимоги регуляторів, при цьому ігноруючи потреби власних клієнтів. Таку точку зору підтримує і колишній працівник американських спецслужб Едвард Сноуден. На конференції Camp Decrypt 2022 програміст попередив спільноту про небезпеку, яку несе за собою онлайн-простір — за його допомогою корпорації та уряди країн збирають дані користувачів для своїх цілей. Як вважає програміст, благородної мети у цьому немає». ***(За 12 місяців Coinbase 12 320 разів взаємодіяла з правоохоронцями // No worries! (https://noworries.news/za-12-misyacziv-coinbase-12-320-raziv-vzayemodiyala-z-pravoohoronczyamy-2/). 13.12.2022).***

***

«Международные правоохранительные органы уничтожили около 50 так называемых загрузочных DDoS-сайтов. И семи из их предполагаемых администраторов были предъявлены обвинения..

Эти службы отказа в обслуживании, также известные как стрессеры, нанимают DDoS-атак. Они утверждают, что являются законными инструментами тестирования производительности, но, как вы можете себе представить, их часто используют во зло.

И ФБР говорит, что операторы прекрасно знали, для чего они используются…». ***(Richi Jennings. Operation PowerOFF: DDoS Sites Denied Service (by US, UK, Europol) // Techstrong Group Inc. (https://securityboulevard.com/2022/12/operation-poweroff-ddos-richixbw/). 16.12.2022).***

***

«Цифровая трансформация и облачные вычисления значительно расширили современную поверхность атаки, которая теперь охватывает рассредоточенные среды, распределенные рабочие нагрузки и активы, разбросанные по разным местам. Одна только защита периметра не может обеспечить 100%-ную защиту организаций в этой сложной среде угроз. В результате организации, полагающиеся исключительно на традиционную защиту периметра, подвергаются значительно большему риску и страдают от последствий.

Исследование, проведенное The Enterprise Strategy Group (ESG), показало, что за последние два года более трех четвертей опрошенных организаций (76 %) подверглись атаке программ-вымогателей, а две трети (66 %) испытали хотя бы одну цепочку поставок программного обеспечения. атака. Опрос лишь подтверждает то, что большинству из нас уже известно: масштабы и масштабы этой волны преступлений, связанных с программами-вымогателями, беспрецедентны, и организации регулярно несут значительные убытки.

Все больше технологических лидеров, инвесторов и потребителей требуют перемен. Организациям необходимо снизить риск и повысить устойчивость к атакам в облаке. Внедрите нулевое доверие — стратегию безопасности, основанную на допущении нарушений и минимальных привилегий.

Наше мышление должно измениться

В последние месяцы крупная национальная сеть больниц подтвердила, что была вынуждена закрыть несколько служб обслуживания пациентов в нескольких штатах после атаки программы-вымогателя. Служба скорой помощи в Нью-Йорке признала, что атака программы-вымогателя затронула до 318 000 пациентов. А

Коллегия адвокатов штата Джорджия заявила, что нарушение привело к потере личных данных сотрудников.

В этих примерах нет ничего уникального. Нарушения такого рода сейчас — обычное дело, особенно в облаке. Некоторые из известных облачных уязвимостей, появившихся в недавнем прошлом, включают неправильно настроенное облачное хранилище, слабую панель управления, незащищенные сегменты S3, небезопасные API и несанкционированный доступ — и это лишь некоторые из них. Тем не менее, почти половина из 1000 опрошенных ESG специалистов в области ИТ и безопасности заявили, что не верят, что их взломают. Некоторым такое отношение может показаться ошеломляющим — несмотря на растущие потери от программ-вымогателей, организации по-прежнему верят, что они невосприимчивы, — но важно отметить, что изменение мышления, похоже, происходит. Все большее число руководителей высшего звена придерживаются принципа нулевого доверия и концепции «предполагать нарушение».

Мы должны предположить нарушение

При нулевом доверии одним из наиболее реалистичных и эффективных способов защиты конфиденциальных данных и других бизнес-активов является признание неизбежности нарушений. В современном гиперподключенном гибридном мире облачная безопасность будет по-прежнему подвергаться растущим атакам. Мы не должны забывать, что облачные вычисления по-прежнему основаны на программном обеспечении, и по этой причине уязвимости будут использоваться. Нарушения просто обязаны произойти. Хорошая новость заключается в том, что организации могут свести к минимуму свое влияние, внедрив технологии, которые автоматически изолируют нарушения, такие как сегментация с нулевым доверием. Сегментация с нулевым доверием изолирует злоумышленников и сдерживает распространение программ-вымогателей и брешей в гибридной поверхности атаки.

Кроме того, другие инструменты нулевого доверия, такие как многофакторная проверка подлинности (MFA) и единый вход (SSO), помогают сократить первоначальную поверхность атаки и снизить подверженность рискам с самого начала.

Начните с ясной картины

Сегодня защита сложных и распределенных сред означает повышение уровня видимости в облаке. Например, аналитики безопасности долгое время опасались теневых ИТ, практики добавления сотрудниками неавторизованных приложений, поскольку это применимо к облаку. Борьба с этой проблемой начинается с понимания того, что включает в себя уязвимости. Различные гибридные и мультиоблачные развертывания создают пробелы в видимости рабочих нагрузок приложений, что затрудняет отслеживание поведения. Это создает «слепые зоны» безопасности в рассредоточенных архитектурах, что в конечном счете усложняет защиту предприятия.

Организациям нужны инструменты, которые обеспечивают полную видимость и понимание уязвимых путей, которые злоумышленники могут использовать в своей гибридной ИТ-системе для получения доступа во всей организации. Эта информация помогает специалистам по безопасности определить, где в первую очередь внедрять архитектуру с нулевым доверием.

Сегментируй и властвуй

Ключевой стратегией предотвращения превращения атак в катастрофы является сегментация, один из основных компонентов нулевого доверия. В отличие от традиционной защиты периметра, целью сегментации является не предотвращение нарушений.

Сегментация обеспечивает дополнительную защиту приложений и данных, ограничивая доступ только тем, что необходимо для предотвращения распространения атак на критически важные активы, тем самым ограничивая их воздействие.

Сегментация изолирует скомпрометированные системы во время атаки и ограничивает перемещение злоумышленников по сети. Это не только не позволяет злоумышленникам обнаружить и украсть важную информацию, но и ограничивает распространение программ-вымогателей. Поскольку облачные среды очень распределены, сегментация является важной частью обеспечения устойчивости в гибридной среде.

Возвращаясь к опросу ESG: 75% респондентов, отнесенных к категории продвинутых пользователей, заявили, что считают, что специализированные инструменты сегментации имеют решающее значение для нулевого доверия. Кроме того, организации, применяющие сегментацию в рамках своей стратегии нулевого доверия, экономят в среднем 20,1 млн долларов США на простоях приложений и ежегодно избегают пяти киберкатастроф. Сегментация является основой отказоустойчивой архитектуры безопасности и имеет первостепенное значение для снижения рисков в облаке.

Zero-Trust — золотой стандарт

За последние два года принцип нулевого доверия быстро стал золотым стандартом кибербезопасности, и отрасль с этим согласна. Например, девять из десяти респондентов в опросе ESG сообщили, что нулевое доверие было одним из трех главных приоритетов безопасности на предстоящий год, а 33% заявили, что это их главный приоритет кибербезопасности.

По мере того, как все больше предприятий интегрируют свои облачные экосистемы и экосистемы центров обработки данных, а внедрение гибридных и мультиоблачных стратегий расширяется, прозрачность среды становится еще более важной для организационной устойчивости. Группы безопасности не могут защищать или защищаться от того, чего они не видят.

В нынешних условиях разрушительных атак программ-вымогателей единственный способ, которым организации могут повысить устойчивость в облаке, — это нулевой уровень доверия. «Никогда не доверяй, всегда проверяй» — именно так организации могут и впредь уравновешивать гибкость, обеспечиваемую облаком, с требованиями безопасности клиентов и заинтересованных сторон. Атаки программ-вымогателей не исчезнут в ближайшее время, но это не означает, что каждая атака или взлом в облаке должны иметь катастрофические последствия для бизнеса и эксплуатации». ***(PJ Kimer. Zero-Trust: Restoring Resilience in the Cloud // Techstrong Group Inc. (https://securityboulevard.com/2022/12/zero-trust-restoring-resilience-in-the-cloud/). 16.12.2022).***

***

«В мире громких эксплойтов смарт-контрактов разработчики и другие заинтересованные стороны часто направляют свое внимание на безопасность в одном направлении; а именно, они, как правило, сосредотачиваются на коде в цепочке, но часто пренебрегают безопасностью фреймворка. При написании смарт-контрактов такая оплошность может иметь серьезные негативные последствия для безопасности. Небезопасные фреймворки или языки могут незаметно создавать уязвимости при компиляции или добавлении проверок кода. Крошечная ошибка на периферии, когда организация дважды не проверяет доверительные отношения между своим приложением и базовой структурой, может привести к катастрофическим финансовым потерям.

Эксплуатация в реальном мире: червоточина

Возможно, одним из самых ярких примеров неудачной защиты инфраструктуры в последнее время является взлом червоточины стоимостью 350 миллионов долларов в начале 2022 года. Эта атака была прямым результатом использования небезопасной и устаревшей функции в устаревшей версии Solana. Протокол Wormhole позволил объединить различные активы в сети между сетью Solana и другими популярными сетями, такими как Ethereum. Поскольку Solana не совместима с цепочками EVM, связующее решение требовало индивидуальной реализации как для Solana, так и для Ethereum, и каждая из них должна была беспрепятственно взаимодействовать друг с другом. Как оказалось, реализация моста в Solana работала на Solana 1.7.0 (исходник), что позволяло использовать небезопасную команду load_instruction_atметод. Хотя с тех пор этот метод устарел, как показано на рис. 1, мы можем понять, как работал эксплойт, сославшись на отчеты того времени.

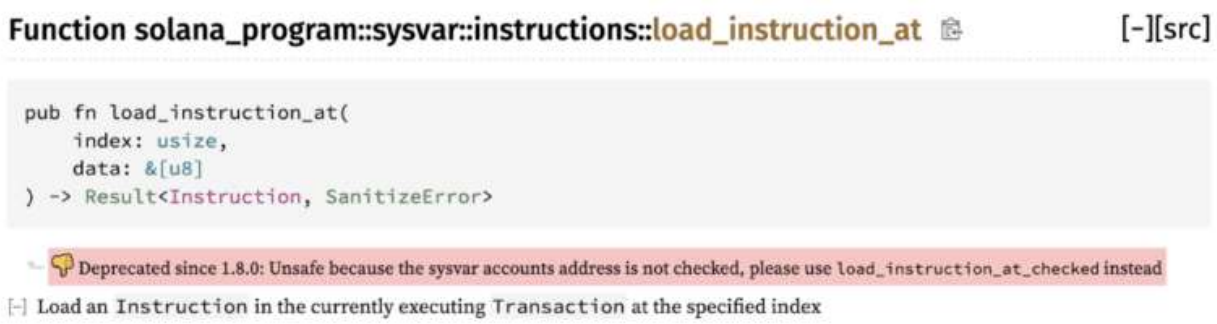


Рисунок 1: load_instruction_at устарел после Solana 1.7.0

В Solana sysvar — это жестко заданный адрес учетной записи, который можно вызвать для доступа к определенным данным состояния. Например, контракт может выполнить вызов учетной записи SysvarC1ock11111111111111111111111111111111, чтобы считать время.

Wormhole использовала метод load_instruction_at для проверки того, что пользователь ввел правильную учетную запись sysvar. Поведение происходило в следующем порядке:

Вызывается verify_signatures с учетной записью sysvar, контролируемой пользователем.

Проверьте учетную запись sysvar с помощью load_instruction_at, чтобы убедиться, что инструкция соответствует ожидаемому идентификатору учетной записи sysvar.

Использовал проверенную системную переменную, чтобы убедиться, что у учетной записи есть разрешение на чеканку упакованного ETH в Solana.

Однако, как оказалось, злоумышленник мог подделать любой адрес в качестве учетной записи sysvar, используя уязвимый метод. До атаки червоточины Солана объявила устаревшим метод load_instruction_at, заменив его на load_instruction_at_checked, который проверял бы, что предложенный адрес был реальной учетной записью sysvar.

В то время как команда Wormhole сделала фиксацию, исправляющую эту проблему, и через несколько недель отправила фиксацию в свой репозиторий GitHub, злоумышленник смог использовать уязвимость, чтобы подделать контролируемую пользователем учетную запись sysvar, за несколько часов до того, как Wormhole получила возможность интегрироваться. которые меняются в

цепочке. Злоумышленник создал программу с инструкцией, которая должна пройти необходимую проверку, и использовал ее, как если бы это была действующая учетная запись sysvar, чтобы обойти требуемую проверку подписи. Поскольку мост Соланы использовал «успешную» проверку подписи, чтобы определить, есть ли у пользователя разрешение на выпуск (или разблокировку) обернутого ETH (WETH) в цепочке получателя, злоумышленник смог полностью слить контракт своего обеспечения WETH.

Как мы исправляем ошибки

Взлом червоточины стал возможен в результате того, что команда разработчиков внесла изменения безопасности фреймворка в общедоступный репозиторий GitHub перед развертыванием исправления в рабочей среде. На самом деле злоумышленник воспользовался проектом всего через несколько часов после того, как разработчики отправили патч на GitHub.

Саму фиксацию разработчики обозначили как простое обновление номера версии [Источник] с текстом «Обновить Solana до 1.9.4» [Источник]. Однако это «простое» обновление сопровождалось множеством добавлений и удалений в кодовой базе, как показано на рис. 2. Несоответствие между простым описанием фиксации и обширными изменениями могло побудить злоумышленника обратить пристальное внимание и заметить обновление безопасности, которое команда разработчиков отправила на GitHub, но не на смарт-контракты в сети.

Рисунок 2: Обновление безопасности было похоронено вместе со многими другими изменениями в одном коммите.

Wormhole мог бы поступить в этой ситуации по-другому, чтобы предотвратить возникновение этой проблемы. Команда разработчиков должна была использовать локальную фиксацию, содержащую исправления безопасности, для обновления программ на Солане перед отправкой обновлений в общедоступный репозиторий. Однако это решение делает одно важное предположение: уязвимый протокол — это централизованная компания с определенной структурой управления и четкими внутренними частными каналами связи, где это действие может быть легко скоординировано между руководством и разработчиками. В этом случае команда Wormhole соответствует этим критериям, но это не всегда применимо ко всем проектам Web3, связанным с критическими обновлениями безопасности.

Автоматическое исправление: широко применимое решение

Чаще всего экосистемы в Web3 децентрализованы, а уязвимые ресурсы, лежащие в основе протоколов, находятся вне прямого контроля разработчиков. Следовательно, нам нужен протокол для обработки критических с точки зрения безопасности обновлений децентрализованных сетей. Go Ethereum (geth), ведущая реализация протокола ethereum, является прекрасным примером базовой технологии с широкими последствиями для безопасности. Geth поддерживает примерно 75% всех узлов Эфириума; таким образом, эксплуатация критической уязвимости безопасности в реализации geth в реальных условиях будет иметь катастрофические последствия для протокола Эфириума и, соответственно, для всей криптоэкосистемы.

Компания Geth изложила свою политику раскрытия информации в документе о раскрытии уязвимостей. Компания следует принципу «тихого исправления», вводя две 4-8-недельные задержки между выпуском исправления для критической уязвимости, раскрытием того, что исправление связано с безопасностью, и, наконец, публикацией результатов уязвимости. Этот подход сочетает в себе прозрачность и безопасность. Мы настоятельно рекомендуем аналогичный подход для основных технологий, которые требуют установки исправлений пользователями или разработчиками и могут иметь серьезные последствия, если

злоумышленник обнаружит уязвимость системы безопасности платформы до того, как пользователи интегрируют исправления.

Как этого избежать, используя доверительную экосистему

Wormhole исправила уязвимость, обновив свою версию Solana и переключившись на load_instruction_at_checked в коммите 7edbbd. Чтобы снизить риск подобных атак, организации, заботящиеся о безопасности, должны использовать современные библиотеки разработки и по возможности использовать самые последние версии программного обеспечения. Будьте дисциплинированы в проверке объявлений о том, что в проектах не рекомендуются небезопасные методы, поскольку разработчики часто не подчеркивают это в деталях обновления. Кроме того, обратите особое внимание на предупреждения об устаревании во время компиляции и при чтении документации.

Кроме того, такие проекты, как компилятор Solidity, поддерживают исторические списки известных ошибок, которые вы можете сопоставить с версиями, используемыми в вашей организации. Этот шаг служит защитой от человеческих ошибок во время первоначального просмотра документации. Хотя это и требует дополнительного времени, двойная проверка доверительных зависимостей здесь может снизить уязвимость вашей организации к этому типу атак.

На отраслевом уровне мы выступаем за более широкое внедрение прозрачных объявлений и ведения записей в экосистеме разработки Web3. Такие проекты, как Solana и другие, имеют возможность четко предупреждать пользователей, когда они обнаруживают потенциально критические уязвимости в базовой структуре или языке. Мы считаем, что эти проекты несут этическое обязательство по прямому и своевременному раскрытию информации о проблемах безопасности фреймворка, учитывая широко распространенную экосистему доверия, в которой они участвуют». ***(Web3 Trust Dependencies: A Closer Look at Development Frameworks & Tools // Techstrong Group Inc. (https://securityboulevard.com/2022/12/web3-trust-dependencies-a-closer-look-at-development-frameworks-tools/). 14.12.2022).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Щорічний захід Pwn2Own, організований Zero Day Initiative (ZDI), проходив у Торонто (Канада). По суті, це дослідницька конференція, в рамках якої хакери можуть продемонструвати свої здібності щодо злому комерційних продуктів. Згодом усі дані передаються виробникам для того, щоб ті «латали дірки».

У рамках Pwn2Own хакери виявили різні вразливості в мережевих накопичувачах (NAS) HP, NETGEAR, Synology, Sonos, TP-Link, Canon, Lexmark та Western Digital, але найшвидше їм вдалося зламати Samsung Galaxy S22.

Команди хакерів STAR Labs та Chim вже в перший день Pwn2Own знайшли дві дірки у безпеці Galaxy S22, які дозволили отримати повний доступ до телефону. У другий день заходу хакери з групи Pentest Limited ще раз зламали телефон, а на третій день Galaxy S22 зламали вчетверте, причому рекордно швидко — лише за 55 секунд.

Важливо, що на всіх пристроях, наданих для злому в рамках Pwn2Own, встановлюються всі останні оновлення — це одна з вимог конкурсу». ***(Білі хакери зламали Samsung Galaxy S22 за 55 секунд // No worries! (https://noworries.news/bili-hakery-zlamaly-samsung-galaxy-s22-za-55-sekund/).*** 10.12.2022).

***

«Коммуникационные навыки CISO никогда не были более важными. Организации сталкиваются с беспрецедентными рисками кибербезопасности, не последним из которых являются уязвимости программного обеспечения, которые могут превратиться в кошмарные атаки на цепочку поставок.

Главные события последних двух лет, такие как атака SUNBURST и обнаружение уязвимости Log4J, привлекли внимание к тому, какое влияние проблемы с цепочками поставок программного обеспечения могут оказать на многие компании.

Такие события с высоким уровнем риска также показывают, почему организациям так важно сосредоточиться на повышении безопасности своих цепочек поставок программного обеспечения и управлении уязвимостями. И чтобы добиться этого, директорам по информационной безопасности и другим руководителям по безопасности необходимо знать, как эффективно общаться с теми людьми, которые во многих случаях принимают ключевые стратегические решения: членами высшего руководства и советом директоров.

Важным компонентом обсуждения является знание того, какие вопросы поднять с руководителями предприятий. Вот несколько ключевых вопросов, которые следует рассмотреть:

Знаем ли мы нашу позицию риска? Организациям трудно обеспечить достаточную безопасность, если у них нет четкого понимания рисков, с которыми они сталкиваются. Им необходимо иметь контроль над всеми своими сторонними зависимостями, а также видимость и контекст для всего их программного обеспечения.

Насколько мы готовы к защите от атак на цепочку поставок программного обеспечения и насколько мы уверены в своей способности быстро закрыть окно атаки на новые уязвимости? Такие инциденты, как получившие широкое распространение атаки на такие компании, как SolarWinds и Kaseya, должны привлечь внимание высшего руководства, поскольку они могут оказать огромное влияние на бизнес.

Готовы ли мы к предстоящим требованиям по соблюдению требований? В 2021 году Белый дом издал указ об улучшении национальной кибербезопасности, который требует от продавцов программного обеспечения предоставлять федеральным агентам по закупкам спецификации программного обеспечения (SBOM) для каждого программного приложения, и есть некоторые предположения,

что это требование в конечном итоге станет тем, что компании потребуют от своих сторонних партнеров.

Как только директора по информационной безопасности узнают, какие вопросы обсуждать, как им на самом деле общаться с советами директоров и высшим руководством? Во-первых, говорите на языке, который они могут понять и понять. Руководители службы безопасности никогда не должны перегружать бизнес-аудиторию техническим жаргоном, который сбивает их с толку.

Бизнес-лидеры хотят, чтобы все объяснялось лаконично и в привычных для них терминах. Использование технического жаргона и акронимов не будет работать, и если директора по информационной безопасности будут делать это, они рискуют быстро потерять аудиторию.

Один из терминов, с которым совет директоров и топ-менеджеры, безусловно, может иметь отношение, — это рентабельность инвестиций (ROI). Начальники службы безопасности должны быть готовы показать, какие результаты приносят инвестиции в инструменты и услуги безопасности. Именно здесь хорошо иметь набор показателей, которые могут продемонстрировать ценность решений по обеспечению безопасности, таких как сканеры уязвимостей.

Хорошие примеры метрик включают среднее время обнаружения (MTTD), которое измеряет, сколько времени требуется группе безопасности для обнаружения уязвимости; среднее время исправления (MTTR), которое измеряет количество времени, которое требуется команде для устранения уязвимости программного обеспечения в среде организации; и время, потраченное на исправление программного обеспечения.

Еще одна хорошая практика при общении с советами директоров и высшим руководством — открыто говорить о рисках, не прибегая к страху, неуверенности и сомнениям. Бизнес-лидеры не хотят слышать истории о том, что может пойти не так; им нужны предложения о том, как предотвратить инциденты, не мешая производительности сотрудников…». ***(Enhancing CISO Communication with Boards and C-Suites in 2023 // Techstrong Group Inc.***

(https://securityboulevard.com/2022/12/enhancing-ciso-communication-with-boards-and-c-suites-in-2023/). 15.12.2022).

***

«Rezilion, поставщик платформы управления уязвимостями, поделился списком основных уязвимостей, обнаруженных в 2022 году. В отчете предлагается, чтобы организации рассмотрели их до начала Нового года, если они еще этого не сделали. Эти уязвимости включают в себя:

Pwnkit –CVE-2021-4034, уязвимость повышения привилегий в файле pkexec пакета Linux Policykit.

Dirty Pipe — CVE-2022-0847, серьезная уязвимость повышения привилегий, которая использует механизм PIPE в Linux для записи в привилегированный существующий кеш страниц.

Spring4Shell –CVE-2022-22965, уязвимость нулевого дня удаленного выполнения кода (RCE), вызванная ошибкой в механизме, который использует предоставленные клиентом данные для обновления свойств объекта в приложении Spring MVC или Spring WebFlux.

NimbusPWN — CVE-2022-29799 (обход пути) и CVE-2022-29800, пара уязвимостей, которые можно объединить в цепочку для повышения привилегий с помощью потока в networkd-dispatcher в ядре Linux.

Dirty Cred — две CVE: CVE-2021-4154 и CVE-2022-2588, набор локальных уязвимостей повышения привилегий, способных обходить проверки разрешений учетных данных ядра.

ProxyNotShell — CVE-2022–41040 и CVE-2022–41082, пара уязвимостей RCE, нацеленных на серверы Microsoft Exchange. Text4Shell или ACT4Shell — CVE-2022-42889, критическая уязвимость удаленного выполнения кода (RCE), которая злоупотребляет функциональностью интерполяции текста Apache Commons в подстановке строк.

Spooky SSL — CVE-2022-3603 и CVE-2022-3786, пара уязвимостей, которые могут активировать RCE при определенных обстоятельствах.

Офри Узан, исследователь безопасности в Rezilion, сказал, что, хотя каждая из этих уязвимостей может по-разному влиять на организации, скорость их обнаружения будет только увеличиваться по мере проведения дополнительных исследований. По ее словам, организациям также следует исходить из того, что в 2023 году будет обнаружено больше уязвимостей нулевого дня.

После раскрытия уязвимости Spring4Shell в конце 2021 года осознание потенциального воздействия уязвимостей, безусловно, возросло. Хотя эта уязвимость, возможно, не была такой смертельной, как предполагалось вначале, все больше организаций пересмотрели свои возможности реагирования на инциденты, когда осознали, насколько они зависят от сторонних программных компонентов для создания приложений. На самом деле, в большинстве организаций есть много возможностей для улучшения, отметил Оузан.

В идеале ИТ-команды и специалисты по кибербезопасности должны применять передовые методы DevOps к процессам управления инцидентами, которые фокусируются на симптомах, указывающих на назревающее нарушение работы службы. Общая цель состоит в том, чтобы исправить проблемы задолго до того, как возникнет реальная проблема. Автоматическое применение исправлений приложений должно быть частью этих усилий. Можно утверждать, что чем больше организации привыкают реагировать на внезапные инциденты, тем более рутинным становится весь процесс. Мышечная память, которую организация в конечном итоге развивает, также позволяет ей стать более устойчивой, что снижает общий уровень стресса. Такой подход обеспечивает дополнительное преимущество, заключающееся в снижении уровня выгорания, с которым могут столкнуться члены группы управления инцидентами в ИТ, что, в свою очередь, снижает текучесть кадров.

С точки зрения кибербезопасности трудно предсказать, что принесет 2023 год, но чем сложнее становится ИТ-среда, тем больше времени требуется для решения проблем». ***(Michael Vizard. Report Surfaces Top Vulnerabilities of 2022 // Techstrong Group Inc. (https://securityboulevard.com/2022/12/report-surfaces-top-vulnerabilities-of-2022/). 22.12.2022).***

***

«CVE-2022-37958 — это уязвимость в механизме безопасности SPNEGO NEGOEX в Windows, выпущенная Microsoft 13 сентября 2022 года с оценкой CVSS 7,5.

Однако 13 декабря произошло несколько интересных событий вокруг уязвимости:

Корпорация Майкрософт выпустила следующее обновление редакции : серьезность, влияние и рейтинг CVSS изменены с «Раскрытие важной информации» на «Критическое удаленное выполнение кода».

Было опубликовано доказательство концепции (PoC) эксплуатации уязвимости: первое сообщение в твиттере написала Валентина Пальмиотти, известная как chompie1337:

Очевидно, эти события связаны друг с другом, и причина, по которой Microsoft переклассифицировала уязвимость, заключается в том, что исследователь безопасности Red Hat Валентина Пальмиотти (chompie1337) доказала, что уязвимость может привести к удаленному выполнению кода.

Чтобы лучше понять уязвимость, давайте рассмотрим некоторые основные понятия.

GSSAPI

GSSAPI расшифровывается как Generic Security Service Application Programming Interface.

GSSAPI предоставляется поставщиками средств защиты в виде библиотек, которые можно использовать для разработки приложений. Каждое приложение, которое хочет использовать механизм безопасности, будет использовать независимый от поставщика GSSAP. Затем, если он захочет заменить реализацию безопасности, его нужно будет переписать.

СПНЕГО

SPENGO означает простой и защищенный механизм согласования GSSAPI.

SPNEGO — это псевдомеханизм GSSAPI, который согласовывает выбор технологии безопасности для программного обеспечения клиент-сервер.

Он используется, когда клиентское приложение хочет подключиться к удаленному серверу, однако оно не знает, какой протокол аутентификации поддерживает сервер.

SPNEGO определяет, какие общие GSSAPI доступны на каждой стороне (клиент и сервер), выбирает один из них, а затем отправляет ему все дальнейшие операции безопасности.

SPNEGO будет работать только в том случае, если и на стороне сервера, и на стороне клиента включена конфигурация SPNEGO, и после настройки аутентификации SPNEGO завершит свою работу.

Протоколы приложений Microsoft, использующие SPNEGO

Список неполный, и можно обнаружить другие протоколы, использующие механизм SPNEGO.

Общая файловая система Интернета (CIFS)/блок сообщений сервера (SMB)

HTTP

CredSSP, который используется протоколом удаленного рабочего стола (RDP).

Расширения удаленного вызова процедур

Облегченный протокол доступа к каталогам (LDAP)

СПНЕГО НЕГОЭКС

NEGOEX, что означает расширенное согласование, расширяет возможности SPNEGO.

Когда SPNEGO выбирает NEGOEX, процесс согласования основывается не только на том факте, что и клиент, и сервер поддерживают механизм безопасности, он добавляет пару сообщений метаданных для каждого согласованного механизма безопасности.

Метаданные содержат информацию о конфигурациях доверия механизма безопасности, поэтому SPNEGO более гибок при использовании NEGOEX.

CVE-2022-37958

Критическая уязвимость удаленного выполнения кода перед аутентификацией, которая влияет на широкий спектр протоколов и потенциально может быть заражена червем.

Когда NEGOEX включен, злоумышленник может использовать любой протокол приложения Windows, использующий аутентификацию, и через протокол получить доступ к протоколу NEGOEX и удаленно выполнить код. Уязвимость оценивается как критическая во всех категориях, кроме «сложности использования», которая оценивается как высокая из-за того, что для успешного использования уязвимости требуется несколько попыток.

Подвержен ли я уязвимости?

Вы будете подвержены уязвимости, если выполняются следующие условия:

Ваша система работает на Windows.

У вас есть клиентские приложения и серверное программное обеспечение, использующие SPNEGO, и включен механизм NEGOEX.

У вас не установлено сентябрьское исправление Microsoft (или более поздняя версия).

Исправление

Для устранения уязвимостей необходимо установить последние обновления Microsoft, выпущенные с 13 сентября…». ***(Yotam Perkal. Everything you need to know about the SPNEGO NEGOEX CVE-2022-37958 // Techstrong Group Inc.***

(https://securityboulevard.com/2022/12/everything-you-need-to-know-about-the-spnego-negoex-cve-2022-37958/). 17.12.2022).

***

«ИТ-директора используют экономический спад как причину для консолидации инструментов Zscaler

Джей Чаудри, председатель и главный исполнительный директор Zscaler

По словам генерального директора Джей Чаудри, Zscaler заключила крупные многолетние многоцелевые сделки, поскольку экономический спад побуждает клиентов искать замену дорогим устаревшим точечным продуктам.

По словам Чаудхри, поставщик облачной безопасности из Сан-Хосе, штат Калифорния, говорит, что клиенты все чаще покупают безопасный веб-шлюз, частный доступ и цифровые продукты компании в виде единого пакета. Но более крупные сделки означают, что теперь для их закрытия обычно требуется год, а не девять месяцев, поскольку клиенты подвергают транзакцию дополнительной проверке и проверке, говорит финансовый директор Ремо Канесса.

«Я считаю, что периоды неопределенности могут послужить катализатором перемен», — говорит Чодри инвесторам во время телефонной конференции по доходам в четверг. «ИТ-директора говорят мне, что они используют эту сложную среду, чтобы стимулировать изменения и устранять технический долг устаревших точечных продуктов, которые дорого покупать и эксплуатировать».

По данным Canessa, за последний год Zscaler увеличила количество клиентов, которые ежегодно тратят на компанию не менее 1 миллиона долларов, на 55% с 224 год назад до 348 сегодня. Компания также добавила 128 клиентов в финансовом квартале, закончившемся 31 октября, которые планируют тратить 100 000 долларов США на Zscaler каждый год, доведя эту цифру до 2 217, говорит Канесса.

«Клиенты расширяют свои обязательства перед нами, от целевого варианта использования до гораздо более широкого подхода, ориентированного на платформу», — говорит Канесса инвесторам во время телефонной конференции по прибыли. «В нашем портфеле возможностей мы активно работаем над большим количеством многолетних и многокомпонентных возможностей, чем у нас было раньше».

«Существует давление на консолидацию затрат и упрощение»

По словам Чаудхри, для заключения сделок с семизначной суммой требуется как взаимодействие с ИТ-директором заказчика или другим членом высшего руководства, так и серьезное экономическое обоснование, которое может быть представлено финансовому директору. Zscaler увеличил количество оценок бизнес-ценности, которые он проводит для клиентов, и обычно предлагает рентабельность инвестиций более 200%, учитывая, сколько точечных продуктов он заменяет.

По словам Чаудри, крупные сделки все чаще должны проходить через финансовых директоров и генеральных директоров клиентов для утверждения, особенно по мере того, как экономические препятствия усиливаются.

Чаудхри говорит, что Zscaler и его партнеры преуспели в формировании прочных связей на высшем уровне и позиционировании платформы как части бюджета ИТ-директора, а не как части бюджета безопасности, поскольку у первого больше денег. По словам Чаудхри, безопасность обычно составляет довольно небольшую часть общего ИТ-бюджета, курируемого ИТ-директором, и тесное сотрудничество с ИТ-директорами позволило Zscaler получить справедливую долю общего ИТ-бюджета.

«Существует давление на консолидацию затрат и упрощение», — говорит Чодри. «Хотя клиенты не будут начинать большие новые проекты, проекты, которые можно реализовать без больших инвестиций, уже выполняются».

С технологической точки зрения, Чаудхри говорит, что предложение компании по защите данных набирает обороты, учитывая опасения клиентов по поводу утечки данных и того, что сотрудники работают из любого места. По словам Чаудри, в прошлом квартале компания Zscaler представила новую службу

предотвращения потери данных, которая автоматически классифицирует неструктурированные данные без предварительной настройки.

Zscaler также недавно интегрировала технологию автоматизации рабочих процессов ShiftRight в свое предложение по защите данных, чтобы значительно сократить время разрешения дел, упростив организациям управление потенциальными рисками и инцидентами. В ближайшие месяцы компания интегрирует возможности, приобретенные у ShiftRight в сентябре за 25,6 млн долларов, в области своей платформы, не связанные с защитой данных.

«Преимущество Zscaler заключается в том, что с точки зрения затрат, безопасности и удобства пользователей — это лучшая платформа, — говорит Канесса. «Нам нужно найти выход из этой макросреды, продолжать работать, и мы чувствуем, что все само о себе позаботится»…» ***(Michael Novinson. Zscaler CEO: 'Uncertainty Can Act as a Catalyst for Change' // Information Security Media Group, Corp. (https://www.govinfosecurity.com/zscaler-ceo-uncertainty-act-as-catalyst-for-change-a-20605). 01.12.2022).***

***

«Компания Panther недавно опубликовала свой второй ежегодный отчет «Состояние SIEM», в котором приняли участие 285 штатных специалистов по кибербезопасности, каждый из которых работает в команде, которая в настоящее время использует платформу управления информацией и событиями безопасности (SIEM), включая инженеров по безопасности, аналитиков и архитекторы. Цель сравнительного анализа состояния SIEM — получить представление о том, что видят специалисты по обеспечению безопасности, их проблемы, разочарования и то, что они хотят улучшить.

49% считают, что их SIEM покрывает менее половины их данных безопасности.

SIEM — это важная часть инфраструктуры безопасности организации, и для эффективной работы она должна охватывать все данные безопасности. Если SIEM покрывает только часть данных безопасности организации, он не сможет

обеспечить комплексную защиту, необходимую для защиты сетей и систем организации. Кроме того, если SIEM не имеет полного представления о данных безопасности организации, он не сможет определить потенциальные угрозы и уязвимости, которые могут поставить организацию под угрозу.

«В отчете этого года также показано, как устаревшие SIEM-системы сдерживают работу специалистов по безопасности, делая их работу более сложной и менее приятной», — сказал Джек Наглиери, генеральный директор и основатель Panther. «Команды безопасности используют эти инструменты, даже если они не могут обеспечить необходимый масштаб и гибкость, поскольку сталкиваются с новыми и возникающими угрозами — проблемы, с которыми мы с моей командой также столкнулись, работая в таких компаниях, как Amazon и Airbnb».

Адекватная безопасность сегодня зависит от наличия надежного конвейера данных, структурированных данных и рабочих процессов, ориентированных на облако. Специалисты по безопасности осознают статичность традиционных платформ SIEM, и многие обеспокоены их будущим. Многие из сегодняшних поставщиков SIEM разработали свое текущее решение более десяти лет назад и не сильно изменили свой подход за последнее десятилетие». ***(Alicia Hope. Report Finds 49% Of Security Practitioners Believe Their SIEM Covers Less Than Half of Their Security Data // CPO Magazine (https://www.cpomagazine.com/cyber-security/report-finds-49-of-security-practitioners-believe-their-siem-covers-less-than-half-of-their-security-data/). 06.12.2022).***

***

«Opera анонсувала новий набір інструментів безпеки для свого блокчейн-браузера. Web3 Guard — набір функцій, який має захистити інтернет-користувачів від зловмисних децентралізованих програм (DApps), фішингових атак та хакерів. У компанії запевнили, що нова система безпеки не збиратиме жодних персональних даних.

Web3 Guard сканuватиме вебсторінки на наявність ознак експлойту. Денні Яо, старший менеджер із продуктів Web3 в Opera, зазначив: «На сьогодні Web3

Guard надає користувачам вчасну інформацію для того, щоби вони не лише усвідомлювали потенційні ризики, які існують на цей час в інтернеті, але й поступово знайомилися з типами небезпек, властивих саме для Web3».

Нові інструменти безпеки криптографічного браузера також містять засіб перевірки шкідливих адрес. Крім того, у браузері є можливість увімкнення HTTPS — це гарантує, що сайти, які відвідують користувачі, використовують надійні методи шифрування.

«Відомі браузери, якими сьогодні користуються більшість людей, не створені для роботи зі складністю Web3… З нашим Opera Web3 зі спеціальними функціями безпеки ми робимо величезний стрибок вперед. Тепер люди зможуть користуватися Web3-програмами безпечніше», — наголосив Яо.

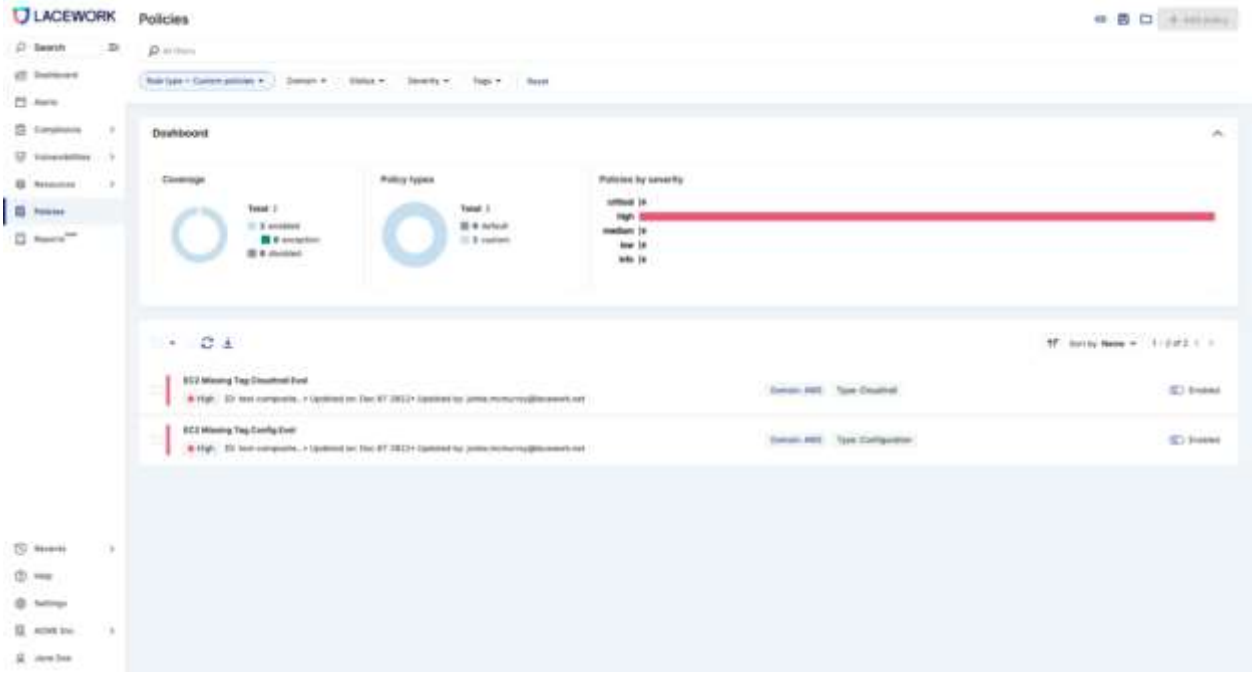
Раніше стало відомо, що браузер Opera отримає функцію створення NFT. Користувачі зможуть завантажувати в блокчейн зображення та інші медіафайли, миттєво перетворюючи їх на невзаємозамінні токени. Послуга надаватиметься безкоштовно. Команда Opera впевнена, що новий інструмент дозволить новачкам вивчати можливості блокчейну. Крім того, митці отримають у розпорядження найпростіший спосіб створення NFT». ***(Opera покращила безпеку для власників криптовалют // No worries! (https://noworries.news/opera-pokrashhyla-bezpeku-dlya-vlasnykiv-kryptovalyut/). 16.12.2022).***

***

«Lacework добавила в свою платформу дополнительные возможности управления состоянием безопасности в облаке (CSPM), чтобы можно было создавать подробные настраиваемые политики с использованием языка запросов Lacework (LQL) для обеспечения соответствия конфигураций конкретным требованиям организаций.

Кроме того, компания добавила поддержку тестов Center of Internet Security (CIS) наряду с сотнями других дополнительных элементов управления, написанных командой Lacework Labs.

Наконец, Lacework также добавила возможность создавать настраиваемые отчеты, охватывающие несколько облачных учетных записей.



Кейт Маклин, старший директор по маркетингу продуктов Lacework, сказала, что предложение Lacework CSPM предназначено для упрощения выявления неправильных конфигураций облачных сервисов. Первоначально доступная для рабочих нагрузок, развернутых на Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform (GCP), Маклин сказал, что платформа Lacework уникальна тем, что она изначально разработана для поддержки нескольких платформ облачных вычислений.

LQL позволяет создать, например, политику для общедоступного сегмента хранилища или базы данных, предварительно определив, какие условия и поведение разрешены. Группы кибербезопасности могут устанавливать оповещения о состоянии для конкретных облачных конфигураций и получать оповещения каждый раз, когда ресурс не соответствует определенной политике. Такой подход позволяет группам по кибербезопасности использовать LQL для определения набора детальных политик для нескольких облачных платформ, каждая из которых имеет уникальный набор ресурсов, которые необходимо защитить, отметил Маклин.

По словам Маклина, по мере того, как все больше рабочих нагрузок развертывается в нескольких облаках, Lacework обосновывает необходимость

централизованного подхода, который в конечном итоге помогает снизить общую стоимость безопасности, поскольку устраняет необходимость развертывания и настройки отдельных сред безопасности для каждого облака.

Сегодня большинство организаций развертывают рабочие нагрузки в нескольких облаках. Тем не менее, большинство групп по кибербезопасности все еще пытаются наверстать упущенное в своих возможностях сделать эти рабочие нагрузки такими же безопасными, как и те, которые выполняются в локальных ИТ-средах. В основе всей этой облачной небезопасности лежит способ предоставления облачной инфраструктуры. Разработчики, практически не имеющие опыта в области кибербезопасности, обычно предоставляют облачные ресурсы, а затем развертывают приложения. Это означает, что почти наверняка будут допущены ошибки.

Напротив, большинство развертываний приложений в локальных ИТ-средах обрабатывается централизованной командой, которая обычно проверяет параметры на наличие неправильных конфигураций. Многие организации, развертывающие приложения в облаке, еще не смогли определить и поддерживать аналогичный набор лучших практик. Правда в том, что в спешке, чтобы уложиться в сроки развертывания приложений, многие разработчики пропускают (или, по крайней мере, минимизируют) количество времени, которое должно быть посвящено обеспечению облачной безопасности. Затем группы кибербезопасности просят обнаружить все потенциальные неправильные конфигурации, которые могли быть непреднамеренно созданы этими разработчиками. Проблема, конечно, в том, что многим из них все еще не хватает инструментов, необходимых для достижения этой цели.

Так или иначе, в наступающем году проблемы с облачной безопасностью встанут на передний план. Осталось только определить, какая часть усилий по обеспечению безопасности этих рабочих нагрузок будет направлена на упреждение, а не на реагирование постфактум на неизбежное нарушение». ***(Michael Vizard. Lacework Stiffens Cloud Security Posture Management // Techstrong***

Group Inc. (https://securityboulevard.com/2022/12/lacework-stiffens-cloud-security-posture-management/). 19.12.2022).

***

«В этом сообщении блога мы подводим итоги нашего разговора 30 августа 2022 года с AWS и Lacework. Мы говорим о миграции в облако, модернизации приложений, а затем о применении безопасности для модернизации приложений, таких как распределенные архитектуры. Мы надеемся, что вы найдете информацию ценной. Давайте начнем…

Во-первых, давайте рассмотрим путь внедрения облака. Это путь, который обычно выбирают наши клиенты, когда они либо мигрируют, либо создают собственные облачные приложения.

Основываясь на опыте миллионов бизнес-клиентов, AWS рассматривает переход организаций к облаку в четыре этапа. Первый этап мы называем «этап проекта». На этом этапе компании обычно экспериментируют с новыми проектами, запускают рабочие нагрузки на AWS, измеряют и оценивают облако. Как правило, это делается на основе проекта за проектом.

Второй этап – «основной этап». На этом этапе организации начинают определять основные конструкции, такие как сетевое подключение и управление идентификацией и доступом. Они могут увидеть преимущества облака и включить в него важные компоненты, такие как платформы наблюдения и безопасность.

Третий этап больше ориентирован на миграцию. Компании начинают масштабировать внедрение облака AWS и увеличивать свое присутствие в облаке. На этом этапе компании обычно разрабатывают стратегию модернизации приложений. Они выяснят, какие приложения будут перенесены и как они будут модернизированы, будь то контейнеры или бессерверные решения, Kubernetes, ECS и EKS.

Четвертый и последний этап часто называют этапом «переосмысления» или этапом «оптимизации облачных операций». Именно здесь организации начинают в полной мере использовать преимущества облака. Они ускоряют выход на рынок,

используя технологии, которые они разрабатывали на третьем этапе, такие как бессерверные модели, микросервисы, контейнеризация и другие облачные технологии и архитектуры.

Теперь, когда мы определили четыре этапа модели внедрения облачных технологий и, надеюсь, вы чувствуете себя с ней более комфортно, возникает вопрос… с чего начать этот путь? Традиционно важно понимать свой инвентарь ИТ; что у вас есть, что можно перенести в облако, а что можно удалить. Обратите внимание, что если оно больше не представляет ценности для бизнеса, вам может потребоваться полностью удалить приложение.

Как только вы получите четкое представление о своих приложениях и определите, какие из них лучше подходят для облака, вы должны перенести или повторно разместить их. Обычно «повторный хостинг» — это перенос приложения в более современную среду для экономии средств или повышения производительности; то, что мы называем движением подъема и смещения. Это упрощает операции и предоставляет вам минимальные жизнеспособные компоненты того, что вы делаете с облаком.

«Переплатформа» — это когда вы изменяете инфраструктуру, которую использует приложение. Например, если вы взяли одно из ваших существующих приложений, а затем существующий компонент приложения и переместили его в управляемую службу. В базовой бизнес-логике нет радикальных изменений.

«Рефакторинг» — это когда вы перестраиваете приложение, чтобы воспользоваться преимуществами современных облачных сервисов и архитектур. Когда вы переходите к распределенным архитектурам посредством рефакторинга, вам нужна скорость. Вам нужно использовать гибкость DevOps, и вы хотите оптимизировать свои механизмы доставки программного обеспечения, которые включают в себя автоматическую безопасность, тестирование на соответствие, а затем и то, и другое необходимо для запуска кода в производство безопасным и совместимым способом.

«Выкуп» — это, как правило, то, о чем мы думаем, как о покупке. Вы берете приложения, которые вы использовали, и заменяете их приложениями SAS.

Почему это важно?

В мире DevOps мы объединяем безопасность и соответствие требованиям и придумываем DevSecOps. Организации хотят убедиться, что в части сборки вашего механизма, а также в операционной среде или среде выполнения вы выявляете уязвимости, соответствие требованиям и неправильные конфигурации до того, как они станут критическими проблемами в вашей операционной среде.

Большинство людей, вероятно, знают о модели общей ответственности Amazon Web Services (AWS), и в модели общей ответственности AWS несет определенную ответственность за базовую инфраструктуру, на которую вы размещаете свои данные, свои приложения и свои рабочие нагрузки. Клиенты несут ответственность за то, что они размещают в облаке, что мы называем «ИТ-безопасность в облаке». Мы рассматриваем различные поддомены программного обеспечения и пытаемся подумать о том, как они на самом деле охватывают пять основных блоков NIST Cybersecurity Framework.

Скажем, вы находитесь на пути миграции в облако. Как выглядит хорошая программа для облачной безопасности? И прежде чем мы что-нибудь построим, как выглядит этот фундамент? Существуют ли требования соответствия, которых мы должны придерживаться? Есть ли географические границы?

Существуют ли отношения со сторонними организациями или интеграции со сторонними организациями, которые нам необходимо учитывать? На данный момент многие из этих вопросов уже должны были быть решены.

Например, из чего на самом деле состоит контейнер? Вы по-прежнему должны защищать контейнеры, как и обычный сервер, но вы должны защищать их по-другому. Если у вас есть три разных приложения, которые размещены в одной части инфраструктуры, у вас есть свой хост, и, кроме того, у вас будет операционная система Docker, а затем вы можете разместить несколько контейнеров. Кроме того, каждый из этих разных контейнеров будет иметь свои собственные приложения, свои собственные библиотеки приложений и свои собственные конфигурации Docker.

Как мы защищаем весь хост? У вас есть сами контейнеры, но хост все еще находится в корне, на сервере, который нуждается в защите. Очень популярный способ запуска контейнеров сегодня — это Kubernetes, потому что он действительно хорошо справляется с управлением несколькими контейнерами эффективным способом, автоматизируя множество процессов запуска и остановки контейнеров.

Когда вы попадаете в среду AWS, у вас есть несколько различных вариантов управления контейнерами. Вы можете создавать собственные хосты с помощью Amazon Elastic Compute Cloud (EC2). Вы запускаете инстанс EC2, создаете хост Docker или хост Kubernetes, а затем размещаете все свои контейнеры на этих инстансах EC2.

Так что же на самом деле происходит, когда ваши контейнеры работают? Как узнать, что с контейнером происходит что-то плохое или вредоносное? Как убедиться, что ваше виртуальное частное облако (VPC) настроено правильно? Мы постоянно видим это, когда кто-то настраивает VPC, и не всегда обращает на это внимание. Возможно, они используют настройки по умолчанию, и они открывают порты для всего мира, а не ограничивают определенный диапазон IP-адресов. И, наконец, уязвимы ли ваши библиотеки? Когда мы используем контейнеры в облаке, мы склонны предлагать им точечные решения. И, возможно, мы хотим использовать решения, которые мы всегда использовали локально. Это не всегда работает из-за сложности облака.

Еще одна вещь, о которой вы должны помнить при управлении безопасностью контейнеров в облаке, — это ограниченные ресурсы. Когда у вас есть до 50 облачных учетных записей в многооблачных средах, с которыми вы работаете, как вы можете отслеживать свои облачные рабочие нагрузки? У вас есть обзор ваших контейнеров, чтобы понять, что происходит?

Вот где действительно может помочь подход безопасности облачных контейнеров Lacework. Платформа данных Lacework Polygraph® Data Platform может помочь вам визуализировать все контейнеры в вашей среде безопасности. И вы не только создаете контейнеры, в которых могут быть уязвимые библиотеки, но

и запускаете уязвимые библиотеки в производственной среде. Возможность иметь полную видимость всех контейнеров, разбросанных по вашей среде во время выполнения и в рабочей среде, — это очень важно.

Есть важные вопросы по защите контейнеров: защищаете ли вы всю сеть вокруг них? А как насчет ваших политик IAM, которые вы установили в отношении контейнеров? Вы слишком вседозволительны? Или у вас есть MFA для всех ваших пользователей? Просто иметь возможность анализировать, что происходит в вашей облачной среде, и представлять это вам с помощью подхода, основанного на поведении, а не на основе правил, является ключевым фактором.

Мы принципиально подходим к безопасности и облачной безопасности как к проблеме данных. Мы принимаем вызовы API и получаем действия пользователей из облака. А из рабочей нагрузки мы получаем информацию о запусках приложений, запущенных процессах, сетевом поведении и конфигурациях. Оттуда мы анализируем данные и понимаем, что для вас нормально, а что нет.

Важно расширять возможности групп безопасности и инструментов, в которых они работают. Принуждение операционной группы к использованию облака и инструмента облачных операций обычно не работает. Поэтому у нас есть множество различных интеграций с командами JIRA, такими как Slack, где люди могут работать в том инструменте, который им наиболее удобен.

Хотя технология контейнеров является ведущей инновацией для обеспечения ИТ-операций более отказоустойчивой и гибкой средой, в ваш подход необходимо включить безопасность». ***(Moving Containers: Uncovering Challenges. Finding Solutions // Techstrong Group Inc. (https://securityboulevard.com/2022/12/moving-containers-uncovering-challenges-finding-solutions/). 19.12.2022).***

***

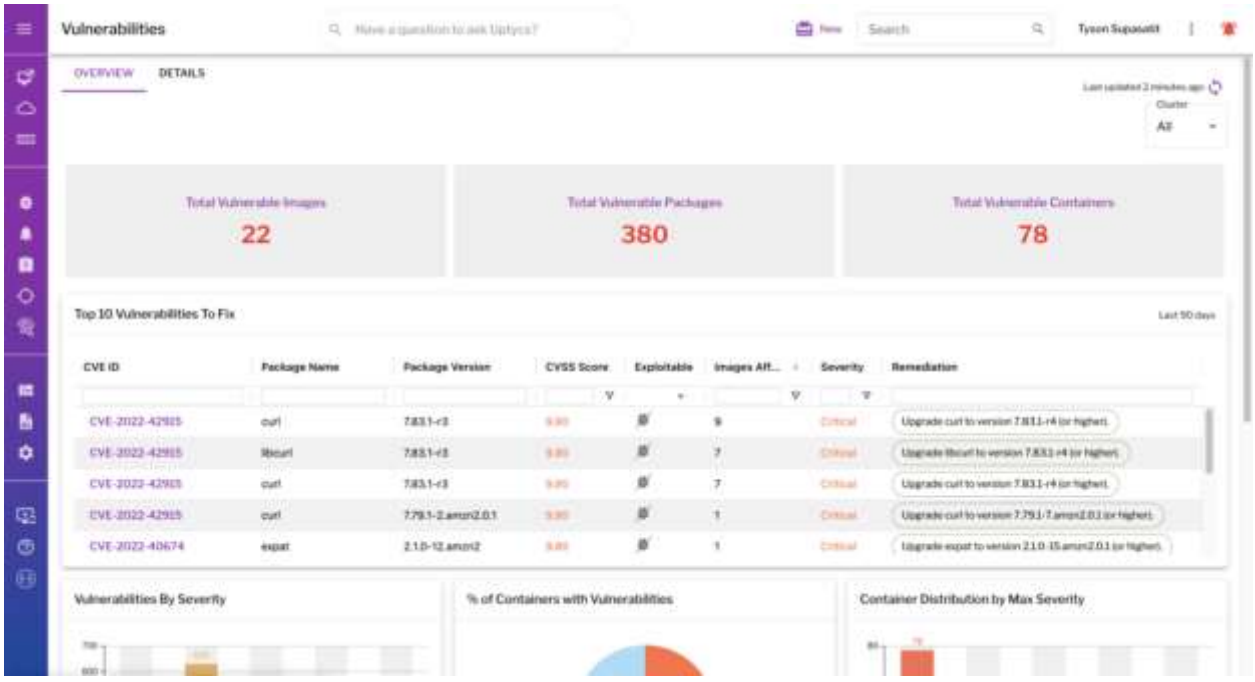
«Uptycs добавила к своей платформе возможность безагентного сканирования, которая объединяет возможности облачной платформы защиты приложений (CNAPP) и решения расширенного обнаружения и реагирования (XDR) в одном предложении.

В зависимости от варианта использования группы кибербезопасности часто вынуждены выбирать разные платформы кибербезопасности при выборе между агентскими и безагентскими подходами.

Джек Рериг, технологический евангелист Uptycs, сказал, что последняя версия платформы Uptycs позволяет полностью сканировать неуправляемые облачные рабочие нагрузки для обнаружения таких рисков, как неправильные конфигурации, нарушения политик, открытые секреты, уязвимости и вредоносное ПО.

С другой стороны, он отметил, что организации могут использовать подход на основе агентов, чтобы воспользоваться возможностями исправления и блокировки, основанными на поведении обнаруженного вредоносного ПО.

По словам Рерига, подход Uptycs к предоставлению этих возможностей будет собирать нормализованные данные телеметрии таким образом, чтобы их можно было легко запрашивать независимо от того, установлен ли агент. Он добавил, что эта возможность позволяет снизить уровень разногласий, которые часто возникают, когда команды по информационной безопасности, DevOps и ИТ-операции пытаются сотрудничать. Каждой команде предоставляется доступ к одним и тем же данным для облегчения совместной работы, отметил Рериг.



Уже давно ведутся споры о преимуществах безагентных и агентных подходов к кибербезопасности. Агенты предоставляют командам по кибербезопасности

больший контроль, в то время как безагентные подходы не требуют дополнительных затрат на ИТ-среду. Однако сегодня участились ситуации, когда разработчики самостоятельно развернули рабочую нагрузку в облаке без установки какого-либо агентского программного обеспечения, поэтому безагентный подход позволяет группам кибербезопасности оценивать состояние безопасности этих неуправляемых рабочих нагрузок путем сканирования интерфейсов прикладного программирования (API).

Неясно, в какой степени группы кибербезопасности смогут убедить разработчиков добавить еще одного агента к рабочим нагрузкам приложений, которые уже инструментированы с использованием широкого спектра агентов мониторинга. Во многих случаях безагентный подход является путем наименьшего сопротивления при попытке поощрения внедрения лучших практик DevSecOps. Чем меньшее влияние платформа кибербезопасности оказывает на темпы разработки и развертывания приложений, тем более восприимчивы к ней команды DevOps.

«Независимо от подхода, Uptycs теперь является универсальным магазином для решения обоих подходов к кибербезопасности, когда многие организации стремятся сдержать расходы за счет сокращения числа поставщиков кибербезопасности, которые им необходимо привлечь», — отметил Рериг. Он добавил, что Uptycs достигла этой цели, предоставив возможности CNAPP и XDR на одной платформе, а не требуя от групп кибербезопасности развертывания и управления двумя отдельными средами. Uptycs постоянно отслеживает конечные точки, парк серверов и облачные ресурсы через единый интерфейс, доступный для всех в ИТ, отметил Рериг.

Большинству организаций необходимо пересмотреть свои стратегии кибербезопасности, поскольку угрозы продолжают увеличиваться в объеме и сложности. Задача состоит в том, чтобы найти наиболее экономичный способ достижения этой цели, не идя ни на какие компромиссы, которые впоследствии могут аукнуться организацией». ***(Michael Vizard. Uptycs Adds Agentless Scanning to Integrated Cybersecurity Platform // Techstrong Group Inc.***

(https://securityboulevard.com/2022/12/uptycs-adds-agentless-scanning-to-integrated-cybersecurity-platform/). 20.12.2022).

***

«Служба управления исходным кодом Microsoft GitHub поможет предотвратить случайное встраивание секретов разработчиками в общедоступные репозитории кода. Новый бесплатный сервис сообщит вам, если вы сделали что-то, чего делать не следовало..

Например, закрытые ключи или токены доступа к базе данных. Легко случайно зарегистрироваться, не подумав. Но это не то, что вы хотите, чтобы злоумышленник обнаружил. Это большая проблема.

Естественно, бесплатного обеда не бывает. GitHub хочет, чтобы вы обновились до премиум-версии сервиса. В сегодняшнем выпуске SB Blogwatch мы смотрим дареному коню в зубы…». ***(Richi Jennings. GitHub Secret Scanning is now Free (as in Beer) // Techstrong Group Inc. (https://securityboulevard.com/2022/12/github-secret-scanning-free-richixbw/). 19.12.2022).***

***

«Вы позволите заблуждениям помешать вам принять инструмент, который может помочь вашей команде безопасности работать лучше всего? За десять лет создания решений для мониторинга безопасности я понял, что службам безопасности необходим общий стратегический подход к обнаружению, чтобы защитить свою организацию. Тем не менее, я обнаружил, что многие не решаются отказаться от процессов, к которым они привыкли, несмотря на то, что они уже не так эффективны, как раньше. Обнаружение как код — отличный общий подход к обнаружению угроз и реагированию на них, но многие могут не захотеть его применять из-за того, что слышали: его сложно реализовать, он замедляет работу команд и является просто модным словечком. Но что, если вера в эти заблуждения помешала вам внедрить действительно полезный инструмент для вашей команды?

Вот пять распространенных заблуждений относительно обнаружения как кода и того, во что вместо этого должны верить специалисты по безопасности.

Что такое обнаружение как код?

Обнаружение как код сочетает в себе преимущества разработки программного обеспечения с функциональностью обнаружения поведения, которое может привести к взлому. В долгосрочной перспективе обнаружение как код обеспечит устойчивость, надежность и стандартизацию обнаружения и реагирования. Это также по своей функции заставляет службы безопасности по умолчанию автоматизировать работу, работать в большем масштабе и повышать эффективность команды.

Но действительно ли обнаружение как код предлагает преимущества, выходящие за рамки текущих инструментов, которые вы используете? Вот пять заблуждений, в которые, как мы видели, верят службы безопасности, и правда об этом.

Заблуждение: Обнаружение как код — это только написание логики обнаружения на языке программирования.

Правда: Существует заблуждение, что единственное, что может предложить обнаружение как код, — это то, что оно поощряет написание обнаружений на универсальном языке программирования, а не на проприетарном языке кодирования. Но обнаружение как код гораздо шире и предлагает структуру для управления логикой обнаружения точно так же, как инженеры-программисты управляют кодом. Использование языка программирования для логики обнаружения не является обязательным требованием для успешной реализации рабочих процессов обнаружения как кода.

Заблуждение: детектирование как код сложно реализовать.

Правда: команды безопасности, привыкшие к определенным инструментам, могут не захотеть переходить на новый подход из-за необходимости перехода, развертывания и изучения новой платформы. Да, обнаружение как код может быть сложно реализовать с технологической точки зрения, если ваш поставщик SIEM не поддерживает его. Однако, если ваша SIEM предоставляет инструменты командной

строки, поддержку и учебные пособия для включения обнаружения в виде кода, внедрение может быть на удивление простым.

Заблуждение: обнаружение как код замедляет работу команды.

Правда: не потребуется ли команде безопасности больше времени, чтобы написать код и создать все эти обнаружения и рабочие процессы? Перевод любой команды на новый рабочий процесс требует времени, чтобы привыкнуть к нему, и команды должны со временем наращивать мышечную память, чтобы работать эффективно. Долгосрочная окупаемость инвестиций в структурированный, технически обоснованный процесс управления обнаружением приведет к более качественному содержанию обнаружения и экономии времени инженерами по обнаружению и аналитиками безопасности.

Заблуждение: «обнаружение как код» — это просто модное слово поставщика.

Правда: В наши дни многие поставщики ссылаются на обнаружение как на код как на преимущество. Это просто модное словечко и еще один прыжок в моду «все как код» или они действительно предлагают вашей команде что-то стоящее? Важно точно понимать, что поставщик предлагает для своего решения «обнаружение как код». Проанализируйте, действительно ли это решение соответствует широко распространенным платформам не только для реализации обнаружения как кода, но и будет ли это решение работать с вашей существующей инфраструктурой (например, системами контроля версий и CI/CD).

Заблуждение: писать код слишком сложно.

Правда: Наконец, для тех, кто еще не выучил язык кодирования — и, возможно, даже для тех, кто его изучил — существует еще одно заблуждение, что научиться программировать слишком сложно. Как специалисты по безопасности, мы уже знакомы с Python как языком сценариев для анализа локальных журналов. Основы Python может изучить каждый, и это отличный способ расширить свои знания в области программирования и повысить уровень своих способностей к анализу данных безопасности. В Интернете есть множество отличных ресурсов, классов и учебных пособий для изучения основ Python». ***(Jack Naglieri. 2023***

Debunking 5 Myths About Detection-as-Code // Techstrong Group Inc. (https://securityboulevard.com/2022/12/debunking-5-myths-about-detection-as-code/). 21.12.2022).

***

«После приобретения Reposify в начале этого года CrowdStrike сегодня добавила технологию управления внешней поверхностью атаки (EASM) к платформе CrowdStrike Falcon.

Технический директор CrowdStrike Майкл Сентонас сказал, что CrowdStrike Falcon Surface первоначально будет доступен как отдельный модуль, прежде чем возможности EASM будут более глубоко встроены в основную платформу кибербезопасности компании. В то же время CrowdStrike интегрировала Crowdstrike Falcon Surface со своим предложением CrowdStrike Falcon Intelligence Recon.

Во второй половине следующего года компания интегрирует CrowdStrike Falcon Surface с CrowdStrike Falcon Spotlight, модулем управления исправлениями, и CrowdStrike Falcon Discover, инструментом мониторинга.

Общая цель состоит в том, чтобы обеспечить комплексный подход с использованием единого агента для управления кибербезопасностью. По словам Сентонаса, такой подход в конечном итоге снизит затраты за счет устранения необходимости для групп кибербезопасности интегрировать несколько точечных продуктов.

По словам Сентонаса, CrowdStrike приобрела Reposify, чтобы получить доступ к механизму сканирования поверхности атаки, который, по мнению компании, был быстрее и точнее, чем конкурирующие платформы. Организации всех размеров борются с кибербезопасностью, потому что они потеряли видимость своей среды; Он добавил, что технология EASM упрощает сканирование сетей для обнаружения всех возможных атакуемых поверхностей.

По словам Сентонаса, после обнаружения становится возможным применять политики безопасности и устранять уязвимости с помощью различных модулей, составляющих платформу CrowdStrike.

CrowdStrike сочетает набор собственных разработок с платформами, приобретенными за последний год, для расширения платформы CrowdStrike Falcon. Falcon использует алгоритмы машинного обучения и другие формы искусственного интеллекта (ИИ), а также индикаторы атак, глубокую видимость ядра, настраиваемые индикаторы компрометации (IoC) и поведенческую блокировку для защиты ИТ-сред.

Общая цель состоит в том, чтобы предоставить набор основных возможностей, которые специалисты по кибербезопасности могут легко расширить, добавив дополнительные модули, например, специально для защиты контейнеров.

Неясно, насколько организации объединяют инструменты кибербезопасности в рамках своих усилий по снижению затрат на кибербезопасность. Тем не менее, во времена экономической неопределенности всегда возникает необходимость сократить расходы. Проблема, как всегда, заключается в том, что организациям придется заранее потратить немного денег на приобретение новой платформы, чтобы впоследствии сократить расходы за счет устранения необходимости в других продуктах и услугах.

Независимо от подхода к кибербезопасности, поверхность атаки, которую необходимо защищать, продолжает расширяться. В эпоху Интернета вещей (IoT) к сети подключается не только больше устройств и платформ, но и развертывается больше типов приложений. Большинство групп кибербезопасности не смогут идти в ногу со скоростью расширения ИТ-среды без помощи алгоритмов машинного обучения.

Тем временем атаки на эти ИТ-среды будут только увеличиваться в объеме и изощренности. К сожалению, шансы на то, что группы кибербезопасности смогут бороться с этими угрозами с помощью существующих устаревших инструментов и платформ, ничтожны». ***(Michael Vizard. CrowdStrike Adds Attack Surface Management Module // Techstrong Group Inc. (https://securityboulevard.com/2022/12/crowdstrike-adds-attack-surface-management-module/). 15.12.2022).***

***

«EE запустила новое приложение для кибербезопасности, предназначенное для обеспечения расширенной онлайн-безопасности и большего спокойствия для клиентов.

EE Cyber Security на базе Norton™ поможет клиентам лучше защитить свои устройства и цифровую идентификацию с помощью одной простой в использовании услуги. Запуск является частью пути EE к тому, чтобы стать наиболее ориентированным на клиента технологическим брендом в

Великобритании, подчеркивая его стремление представлять новые продукты и услуги, выходящие за рамки возможностей подключения.

Являясь частью BT Group, клиенты EE получают выгоду от существующей команды BT, состоящей из более чем 3000 специалистов по безопасности, которые помогают защитить свою сеть и клиентов от кибератак, а также онлайн-инструментов безопасности, которые помогают защитить их и их семью в Интернете. Тем не менее, угроза онлайн-безопасности сохраняется: 41% британских потребителей признают, что им трудно оставаться в безопасности в Интернете, а 80% особенно обеспокоены тем, что их личные данные могут быть украдены и использованы.

Чтобы защитить потребителей от новых онлайн-угроз, EE заключила партнерское соглашение с Norton™, мировым лидером в области кибербезопасности потребителей, для запуска EE Cyber Security Powered by Norton™.

С момента запуска услуга доступна исключительно для мобильных клиентов EE с ежемесячной оплатой через два пакета: EE Cyber Security Duo, предназначенный для защиты до 2 устройств, и EE Cyber Security Multi для защиты до 15 устройств. Они обеспечивают клиентам:

- Темный веб-мониторинг. Мониторинг личной информации клиентов в даркнете, включая адреса электронной почты, номера банковских счетов, номера кредитных карт, номера телефонов, номер водительских прав, и уведомлять их, если они будут обнаружены.

- Мониторинг социальных сетей. Отслеживает учетную запись клиента на самых популярных сайтах социальных сетей и уведомляет их о подозрительной активности, такой как изменения настроек их учетной записи, необычные входы в систему и опасные ссылки в их сообщениях.

- Безопасность устройства. Предлагает защиту в режиме реального времени для устройств Windows™ PC, Mac® или Android™* от программ-вымогателей, вирусов, шпионских программ, вредоносных программ и других онлайн-угроз. Он также отслеживает и помогает блокировать несанкционированный трафик, а также

помогает защитить личную и финансовую информацию клиентов, когда они находятся в сети.

- Безопасность СМС. Помогает идентифицировать текстовые сообщения с небезопасными ссылками и уведомляет клиентов, чтобы они не подвергали риску свою личную информацию. Он без проблем работает на устройствах Android и iOS.

- Табель успеваемости. Предоставляет сводку обо всех действиях, предпринятых службой для защиты клиента, его устройства и информации, хранящейся на нем, за последние 30 дней.

- Менеджер паролей NortonTM. Предоставляет клиентам инструменты для более безопасного создания паролей и управления ими в одном месте.

Доступно по гибкому 30-дневному скользящему плану: EE Cyber Security Duo можно добавить к любому тарифному плану мобильной связи с ежемесячной оплатой всего за 2 фунта стерлингов в месяц, а EE Cyber Security Multi можно добавить к любому тарифному плану мобильной связи с ежемесячной оплатой всего за 5 фунтов стерлингов в месяц.

Запуск EE Cyber Security Powered by Norton™ произошел после того, как новое исследование показало, что более трети (37%) британских потребителей испытывают повышенное беспокойство по поводу мошенничества в Интернете во время оживленного периода праздничных покупок — Рождества, Дня подарков и январских распродаж. Исследование показало, что почти четверть (24,5%) покупали товары в интернет-магазинах, которыми они никогда не пользовались и о которых никогда не слышали в прошлом, при этом почти каждый третий (29,4%) признается, что ранее откладывал свои обычные предостережения, чтобы обеспечить хорошую покупку. сделка за период.

Чтобы помочь клиентам понять, находится ли их личность в Даркнете, который часто используется в качестве рынка для украденных личных данных, EE также запустила бесплатную ежегодную онлайн-проверку через веб-сайт EE. Новая ежегодная проверка личности EE на базе услуг NortonTM предоставляет клиентам простой и быстрый способ узнать, был ли их адрес электронной почты раскрыт в даркнете. Все, что нужно сделать клиентам, это посетить ee.co.uk/security/cyber-

security, нажать «проверить мою электронную почту», войти в свою учетную запись My EE, ввести свой адрес электронной почты и запустить сканирование. Клиенты могут проверять один адрес электронной почты в год, и после завершения сканирования они не только получат результаты, но и получат советы и рекомендации о том, как обеспечить более надежную защиту своих данных в будущем». ***(Ray Sharma. EE Launches New Cyber Security Application Powered by Norton // The Fast Mode (https://www.thefastmode.com/technology-solutions/29371-ee-launches-new-cyber-security-application-powered-by-norton). 12.12.2022).***

***