**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

№ 10 (жовтень)

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.– №10 (жовтень) . – 244с.

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.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2022
© Національна бібліотека України імені В.І. Вернадського, 2022

ЗМІСТ

Стан кібербезпеки в Україні 4
Правове забезпечення кібербезпеки в Україні 7
Кібервійна проти України 7
Міжнародне співробітництво у галузі кібербезпеки 11
Коронавірус COVID-19 та питання кібербезпеки 15
Світові тенденції в галузі кібербезпеки 17
Сполучені Штати Америки та Канада 71
Країни ЄС та Великобританія 102
Індія 121
Австралія 124
Інші країни 127
Кібервійни та протидія зовнішній кібернетичній агресії 139
Кіберзахист критичної інфраструктури 150
Кіберзахист закладів охорони здоров'я 156
Захист персональних даних 161
Кібербезпека Інтернету речей 181
Кіберзлочинність та кібертероризм 183
Діяльність хакерів та хакерські угруповування 197
Вірусне та інше шкідливе програмне забезпечення 204
Фішингові атаки 224
Операції правоохоронних органів та судові справи проти кіберзлочинців 231
Технічні аспекти кібербезпеки 232
Виявлені вразливості технічних засобів та програмного забезпечення 234
Технічні та програмні рішення для протидії кібернетичним загрозам 235

«…3 жовтня, у Комітеті цифрової трансформації під головуванням Олександра Федієнка відбулась робоча нарада щодо кібербезпеки країни. Про це повідомляє пресслужба Комітету Ради.

Участь у заході взяли представники РНБО, СБУ, СЗРУ, МЗС, Мінюсту, Держспецзв'язку та НКЕК.

Основна увага була приділена реєстрації IP-адрес на окупованих територіях, оскільки росія намагається вкрасти українські IP-адреси шляхом їх реєстрації на своїх юридичних осіб, не резидентів України.

Наразі до RIPE NCC звернулись власники IP-адрес з т.о. територій України, щоб отримати погодження на закріплення їх власності за російськими юридичними особами.

Це питання важливе, оскільки зволікання із вживанням відповідних заходів з боку України збільшує ризики для стабільності роботи інтернету в регіоні.

Учасники наради напрацювали механізми з обмеження операцій трансферу з суб'єктів–резидентів України на будь-яких інших. Також до RIPE NCC планується направити лист з переліком заходів для вирішення даної проблеми та задля захисту українських власників IP-адрес, які опинилися на окупованих територіях». ***(РФ намагається вкрасти українські IP-адреси: Комітет Ради провів нараду щодо кібербезпеки країни // 4studio (https://4studio.com.ua/novyny/rf-namagayetsya-vkrasty-ukrayinski-ir-adresy-komitet-rady-proviv-naradu-shhodo-kiberbezpeky-krayiny/). 05.10.2022).***

***

«Вперше в Україні почав діяти навчальний курс «Програма стратегічного лідерства для українських управлінців у сфері кібербезпеки SJC-2022». Курс призначений для підвищення рівня професійної підготовленості керівників державного та приватного секторів, політиків, які залучені до створення спільних стратегічних рішень з питань кібербезпеки.

Про початок курсу повідомив Апарат Ради національної безпеки і оборони України.

Програма стратегічного лідерства складається з шести модулів, кожен з яких є унікальним. Для навчання було відібрано 43 керівники з державного та приватного секторів, які працюють у сфері кібербезпеки. Реалізація програми стала платформою, де вони зможуть обмінюватися досвідом, розвивати стратегічне мислення та ухвалювати нелінійні, асиметричні рішення для посилення національних кібербезпекових спроможностей.

«Ми живемо у важкі часи, коли одночасно з військовим вторгненням в нашій країні відбувається перша у світі кібервійна. І лише тому, що ми змогли об'єднатися, ми не просто стримуємо ворога в кіберпросторі, а й здобуваємо перевагу. Держава, критична інфраструктура, кіберволонтери з усього світу та бізнес виступили єдиним фронтом, і саме це стало ключовим і вирішальним у нашій боротьбі», – сказала керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук, відкриваючи перший день занять.

Вона також зазначила, що загроза не зменшується, очікується ескалація, атаки на критичну інфраструктуру, енергетичний сектор тощо. І, за її словами, саме мудрість, стратегічне лідерство і взаємодія, які покладені в основу цієї програми, є умовами забезпечення стійкості нашої держави у кіберпросторі.

Програма розроблена Глобальним центром взаємодії в кіберпросторі спільно з кращими міжнародними експертами та за підтримки Національного координаційного центру кібербезпеки». ***(В Україні започатковано навчальну програму стратегічного лідерства для управлінців у сфері кібербезпеки // Інформаційне агентство АрміяInform (https://armyinform.com.ua/2022/10/11/v-ukrayini-zapochatkovano-navchalnu-programu-strategichnogo-liderstva-dlya-upravlinciv-u-sferi-kiberbezpeky/). 11.10.2022).***

***

«Глава Держспецзв'язку України Юрій Щиголь заявив, що понад 90% хакерських атак виявляються успішними через людський фактор: хтось не оновив корпоративне програмне забезпечення, встановив легкий пароль тощо. У Держспецзв'язку нагадали, що одна із найпотужніших кібератак рф на українського телеком-провайдера сталась через скомпрометований обліковий запис співробітника компанії...

Очільник Держспецзв'язку зазначив, що з початку року урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зафіксувала понад 1700 кібератак. І головними мішенями хакерів ставали державні та місцеві органи влади, сфера телекомунікацій, фінансовий сектор, енергетичний сектор, сектор безпеки та оборони, логістика.

В усіх цих організаціях працюють звичайні українці, які не завжди опікуються питаннями кібербезпеки. І саме вони отримують найбільше листів від російських хакерів, що містять шкідливе програмне забезпечення або мають на меті викрасти їхні облікові дані». ***(Илона Завальнюк. 90% кібератак успішні через людський фактор – Держспецзв'язку // processer.media (https://processer.media/ua/90-kiberatak-uspishni-cherez-ljudskij-faktor-derzhspeczv-yazku/). 18.10.2022).***

***

«У межах Місяця кібербезпеки в Україні Держспецзв'язку створила спеціальний сайт cybermonth.cip.gov.ua, на якому можна знайти корисну інформацію з кібербезпеки для всіх груп користувачів інтернету, в тому числі – тих, хто планує зробити кібербезпеку своєю професією.

У розділі «Для абітурієнтів та студентів» ви знайдете інформацію про реформу освіти у сфері кібербезпеки та систему професійних стандартів, яку започатковує в Україні Держспецзв'язку. Такий підхід відповідає найкращим міжнародним практикам і сприятиме підвищенню інституційної спроможності України до кіберзахисту.

Мета реформи

Подолати розрив між знаннями, навичками, кваліфікаціями випускників та вимогами роботодавців;

дати інструменти для професійного середовища та закладів вищої освіти, щоб можна було швидко адаптувати навчальні програми до вимог часу;

запровадити в Україні професії у сфері кіберосвіти, які відповідають найкращим світовим практикам та сучасним реаліям;

створити систему кваліфікаційних центрів, у яких кожен фахівець зможе отримати незалежне підтвердження своїх знань, навичок та кваліфікацій відповідних професіям;

спростити процедуру нострифікації сертифікатів, які видають інші країни та впливові міжнародні організації;

дати простий та зручний інструмент роботодавцям для побудови кар'єрного шляху для своїх співробітників.

У межах реформи в Україні запроваджується система професійних стандартів – компетенцій, знань, умінь та навичок, які необхідні фахівцю для відповідності певній посаді. Цей підхід враховує досвід Європейської рамки кваліфікації та американської Стратегічної освітньої ініціативи у сфері кібербезпеки та відповідає стандартам в ЄС та США.

Нові професії з кібербезпеки

У Державному класифікаторі професій з'являтимуться нові професії з кібербезпеки та інформаційної безпеки; а експерти від держави, сектору освіти та ринку розробляють для них відповідні професійні стандарти. Уже додані нові професії (загалом їх – 17) і розроблені професійні стандарти під шість із них. Професійні стандарти для інших – у розробленні. Також планується подальше розширення Державного класифікатора професій.

Стандарти слугуватимуть орієнтиром закладам вищої освіти для адаптації відповідних освітніх програм у межах спеціальності "кібербезпека" під потреби ринку. Навіть студенти в межах однієї спеціальності розумітимуть, які саме знання, компетенції, навички для них пріоритетні, щоб згодом мати змогу обійняти певну посаду.

Також завдяки стандартизації роботодавці та самі фахівці зможуть будувати кар'єрний шлях, розуміючи, які саме додаткові тренінги та навчання потрібно пройти людині на посаді, щоб підвищити її професійну кваліфікацію.

Крім того, в межах реформування в Україні буде запроваджена система незалежних центрів кваліфікації: де як випускники, так і досвідчені фахівці зможуть отримати підтвердження відповідності своїх знань конкретним посадам або пройти просту процедуру нострифікації чинних сертифікатів, виданих іноземними установами (CISA, наприклад).

Кіберобізнаність і стійкість

25 жовтня у межах місяця Кібербезпеки в ЄС на спеціальній сесії CONNECT University (DG CONNECT) «Кіберобізнаність і стійкість: досвід України» заступник голови Держспецзв'язку Олександр Потій розповідатиме про роль обізнаного суспільства у забезпеченні кіберстійкості країни та розвиток кадрового потенціалу України в галузі кібербезпеки…». ***(Герман Богапов. Україна реформує освіту у сфері кібербезпеки // HiTech.Expert (https://expert.com.ua/153201-ukra%d1%97na-reformuye-osvitu-u-sferi-kiberbezpeki.html). 24.10.2022).***

***

Правове забезпечення кібербезпеки в Україні

«Верховна Рада» ухвалила в цілому проєкт закону №7607 «Про внесення змін до деяких законів України щодо формування та реалізації державної політики у сфері захисту критичної інфраструктури». Він визначає, що функції уповноваженого органу з питань захисту критичної інфраструктури України виконуватиме «Державна служба спеціального зв'язку та захисту інформації України» («Держспецзв'язку»).

Цей документ – закономірний крок держави в напрямку посилення стійкості критичної інфраструктури країни. Попередній варіант законодавства передбачав створення окремого органу, який відповідатиме за ці завдання. Реалізація ухвалених змін дасть можливість без створення нового органу забезпечити формування та реалізацію державної політики у сфері критичної інфраструктури та зекономити державні кошти.

Від 2020 року на «Держспецзв'язку» була покладена функція формування переліку та реєстру об'єктів критичної інформаційної інфраструктури. Створення реєстру об'єктів критичної інформаційної інфраструктури – необхідна умова для аналізу рівня захисту таких об'єктів та проведення роботи з його посилення там, де він може бути недостатнім. Після ухвалених законодавчих змін служба забезпечить створення повного ланцюжка захисту: формування реєстру об'єктів критичної інформаційної інфраструктури, наповнення реєстру об'єктів критичної інформаційної інфраструктури та подальшу щоденну роботу з посилення стійкості таких об'єктів і держави загалом». ***(«Держспецзв'язку» стане уповноваженим органом з питань захисту критичної інфраструктури // Компьютерное Обозрение (https://ko.com.ua/derzhspeczv_yazku_stane_upovnovazhenim_organom_z_pitan_zahistu_kritichnoyi_infrastrukturi_ukrayini_142414). 21.10.2022).***

***

Кібервійна проти України

«Кіберфахівці Служби безпеки України з початку повномасштабного вторгнення нейтралізували майже 3,5 тис. кібератак на електронні системи центральних органів влади та об'єктів критичної інфраструктури України.

З них 1650 кіберзагроз виявили в режимі «реального часу». Більшість російських атак мали на меті або знищити цифрові сервіси, або дестабілізувати роботу підприємств енергетичної і транспортної галузей. Про це повідомила СБУ 3 жовтня.

До організації і проведення диверсій причетні російські спецслужби й підконтрольні їм хакерські угруповання.

«У Полтавській області Служба безпеки знешкодила групу хакерів, яка діяла в інтересах РФ. Зловмисники планували здійснити серію потужних кібератак на електронні системи владних інституцій та об'єкти енергетики. До складу злочинного угруповання входили четверо хакерів, які спеціалізувалися на проведенні DDos-атак на цифрові інформаційні ресурси. За це вони одержали гроші через заборонені платіжні системи РФ», – зазначили в прессслужбі.

Проте кіберпідрозділи СБУ викрили цей задум на етапі підготування, ідентифікували російських організаторів і затримали безпосередніх «виконавців».

«Ще одне хакерське угруповання нейтралізовано у Львові. За вказівкою окупантів хакери масово зламували активні облікові записи інтернет-користувачів з України та Євросоюзу. Таким чином вони мали доступ до персональних даних громадян. За даними слідства, агресор використовував зламані акаунти для поширення дезінформації щодо суспільно-політичної ситуації в Україні та ЄС нібито від імені пересічних людей», – повідомила СБУ.

Організатору прокремлівської групи хакерів повідомили про підозру й тримають під вартою». ***(СБУ знешкодила тисячі кібератак: подробиці // Gazeta.ua (https://gazeta.ua/articles/np/_sbu-zneshkodila-tisyachi-kiberatak-podrobici/1114067). 03.10.2022).***

***

«Кіберполіція ідентифікувала понад 14 500 російських військових, які брали участь у вторгненні в Україну.

У перші дні повномасштабної війни розгорнули автономні центри для комунікації з іншими силами забезпечення безпеки й оборони, повідомив начальник Департаменту кіберполіції Юрій Виходець.

«Наші працівники змінили вектор роботи на протидію кібератакам на державні органи й приватний сектор, виявлення та реагування на антиукраїнську пропаганду в інтернеті, ідентифікацію колаборантів, розробку систем і механізмів для збирання інформації з відкритих джерел про військовослужбовців РФ», – сказав він.

Також зафіксували участь 170 членів незаконних збройних формувань у бойових діях і фінансуванні війни.

Попередили майже 400 кібератак на українські інформаційні ресурси.

Провели понад 1400 обшуків. За цей час виявили близько 800 випадків онлайн-шахрайства. Викрили 23 осіб, які створювали й розповсюджували незаконний контент за участю дітей. Від їхніх дій постраждали 48 неповнолітніх». ***(Україна «вираховує» російських окупантів: дані скількох уже відом // Gazeta.ua (https://gazeta.ua/articles/life/_ukrayina-virahovuye-rosijskih-okupantiv-dani-skilkoh-uzhe-vidomi/1114765). 07.10.2022).***

***

«В Україні розпочався п’ятий місячник кібербезпеки. Вперше в умовах війни. Головна тема – кібервійна з Росією.

Місячник стартував з інформаційної платформи для студентів. Окрім офлайн публіки, до події онлайн приєдналися понад 50 освітніх закладів. Представники

кіберполіції, держспецзв'язку та Міністерства оборони презентували, що можуть запропонувати молодим спеціалістам.

Заступник голови Держслужби спецзв'язку та захисту інформації України Олександр Потій наголошує, що на ринку зараз дефіцит якісних кваліфікованих кадрів. Тому їх потрібно поповнювати.

Нині держава потребує кіберфахівців аж у 30 професіях цього напрямку. Зокрема, необхідні розробники, тестувальники й аналітики. Триває створення кібервійська. Це підтверджують й у Міністерстві оборони.

– Кібервійська існують, вони діють. І сьогодні внесені законопроекти, проекти рішень парламенту та уряду будуть тільки допомагати цьому процесу, – наголошує заступник міністра оборони України з питань цифрового розвитку Олег Гайдук.

Цьогоріч місячник кібербезпеки налічуватиме майже 30 подій. Це – сесії, хакатони, виставки та конкурси. Мета – показати молоді, що зараз країні дуже потрібні їхні знання та бажання працювати на безпеку держави». ***(Єгор Ромахло. Україні потрібні воїни Інтернету – стартував п'ятий місячник кібербезпеки // Факти ICTV (https://fakty.com.ua/ua/videos/ukrayini-potribni-voyiny-internetu-startuvav-pyatyj-misyachnyk-kiberbezpeky/). 07.10.2022).***

***

«Євросоюз виділив Україні 29 млн євро для протидії РФ у кіберпросторі та цифровому просторі. Про це повідомляє Державна служба спеціального зв'язку та захисту інформації за підсумками другого раунду Діалогу з кібербезпеки між Україною та ЄС.

19 млн євро млн євро буде спрямовано на підтримку стійкої цифрової трансформації.

«ЄС виділив Україні 29 млн євро для посилення її стійкості у протидії загрозам у кіберпросторі та цифровому просторі. З цієї суми 10 млн євро використано для закупівлі обладнання та програмного забезпечення для цифрової безпеки, та надання іншої відповідної підтримки, а решта 19 млн євро призначена для підтримки стійкої цифрової трансформації», – йдеться у заяві відомства.

У ході зустрічі представники України та Євросоюзу обговорили нинішній ландшафт кіберзагроз, зокрема кібератаки на критичну інформаційну інфраструктуру України, які розпочалися ще до нападу Росії у лютому». ***(Николай Шелудько. Євросоюз виділив Україні 29 млн євро на посилення кібербезпеки // Процес (https://processer.media/ua/ievrosojuz-vidiliv-ukraini-29-mln-ievro-na-posilennya-kiberbezpeki/). 05.10.2022).***

***

«З початку повномасштабної російської агресії Європейський Союз підтримав кібербезпеку в Україні із загальним бюджетом – 10,778 млн євро, виконавцем проекту є Академія електронного врядування з Естонії (eGA).

Про це повідомляє представництво ЄС в Україні.

«Ми є свідками того, що кіберпростір також є місцем битви. Європейський Союз підтримує Україну в убезпеченні її кіберпростору, який має значний вплив на стабільність країни та життя її громадян. Цифрові послуги та надання дистанційних

послуг є наразі життєво важливими», – зазначив голова представництва Матті Маасікас.

Зазначається, що ЄС підтримує платформу безпечного обміну даними «Трембіта» та управління державними реєстрами, зокрема виявлення та нейтралізацію можливих кіберзагроз. Крім того, надається підтримка захисту критичної інфраструктури та державних даних, включаючи заміну знищеного обладнання. А також ЄС надає засоби захисту, які дозволяють оперативному персоналу підтримувати та зберігати критичну державну інфраструктуру.

Проект "Підтримка ЄС для посилення кібербезпеки в Україні" триває з березня 2022 року по лютий 2023 року.

Війна в Україні та кібербезпека:

За перші 4 місяці 2022 року кількість загроз для викрадення інформації зросла на 12%. При цьому найбільше зростання було у підкатегоріях шпигунського та шкідливого банківського програмного забезпечення. Зокрема кількість шпигунських програм у цей період зросла на близько 18%.

6 вересня 2022 року президент України Володимир Зеленський повідомив, що завдяки професіоналізму українських ІТ-фахівців і допомозі іноземних партнерів, зокрема таких компаній, як Amazon, українські веб-ресурси та бази даних були захищені від потужних атак, які здійснювалися з території РФ та Білорусі в перші дні повномасштабного вторгнення.

Платформа хмарних обчислень Amazon Web Services допомогла українським міністерствам та приватним компаніям перенести понад 10 петабайт (10 млн гігабайт) даних на безпечні сервери після вторгнення Росії в Україну.

ІТ-фахівці проаналізували вплив війни в Україні на кібербезпеку.

Аналітики ESET повідомили, що хакери використовують LinkedIn і WhatsApp під час атак на оборонну галузь країн Європи. ***(Дмитро Петровський. Євросоюз підтримав кібербезпеку в Україні на суму понад 10 мільйонів євро // УНІАН (https://www.unian.ua/economics/finance/yevrosoyuz-pidtrimav-kiberbezpeku-v-ukrajini-na-sumu-ponad-10-milyoniv-yevro-12017985.html?_gl=1*ygvbp6*_ga*MTM1MTcwNDUxOS4xNjY0MTk1MTc4*_ga_JLSK4Y8K67*MTY2Njc4MTE1NS4zLjEuMTY2Njc4MjMzNS42MC4wLjA.*_ga_DENC12J6P3*MTY2Njc4MTE1Ni4zLjEuMTY2Njc4MjMzNS42MC4wLjA.). 20.10.2022).***

***

«Війна іде не тільки на полі бою, але і в кіберпросторі та вочевидь вона не скінчиться навіть після знищення ворожої армії. Тому наша країна як ніколи раніше потребує фахівців із кібербезпеки та кіберзахисту, які зможуть чинити гідний опір ворогу на кіберфронті.

У межах місяця кібербезпеки «Державна служба спеціального зв'язку та захисту інформації України» («Держспецзв'язку») створила спеціальний сайт cybermonth.cip.gov.ua, де можна знайти корисну інформацію з кібербезпеки для всіх груп користувачів інтернету, в тому числі – тих, хто планує зробити кібербезпеку своєю професією.

Так у розділі «Для абітурієнтів та студентів» розміщено інформацію про реформу освіти у сфері кібербезпеки та систему професійних стандартів, яку

започатковує «Держспецзв'язку». Вважається, що це сприятиме підвищенню інституційної спроможності України до кіберзахисту…» ***(«Держспецзв'язку» започатковує в Україні реформу освіти у сфері кібербезпеки // Компьютерное Обозрение (https://ko.com.ua/derzhspeczv_yazku_zapochatkovuye_v_ukrayini_reformu_osviti_u_sferi_kiberbezpeki_142439). 25.10.2022).***

***

«…компанія Microsoft в минулу п'ятницю виявила атаку хакерської групи на транспортні та логістичні компанії в Україні та Польщі за допомогою нового виду програмного забезпечення з вимогою викупу.

Дослідники виявили, що хакерські атаки дуже схожі на попередні атаки кіберкоманди, пов'язаної з російським урядом, яка порушила роботу урядових установ України.

Жертви нової програми-вимагача, названої «Prestige», збігаються з жертвами іншої кібератаки, яка знищувала дані за допомогою шкідливого програмного забезпечення «FoxLoad» або «HermeticWiper», наголошує Microsoft.

«Prestige» працює шляхом шифрування даних жертви та залишає записку з вимогою викупу, в якій говориться, що дані можуть бути розблоковані тільки після придбання інструменту для дешифрування, повідомили в Microsoft.

У кількох випадках дослідники відзначили, що хакери отримували адміністраторський контроль над системами жертв до розгортання програми-вимагача, що свідчить про те, що вони викрали їх облікові дані раніше і чекали слушного моменту.

«Розгортання програм-вимагачів в масштабах підприємства не є поширеним явищем в Україні, і ця активність не була пов'язана з жодною з 94 активних груп, які відстежує Microsoft», - зазначають дослідники». ***(Microsoft: Україна та Польща стали мішенню нової кібератаки // Компьютерное Обозрение (https://ko.com.ua/microsoft_ukrayina_ta_polshha_stali_mishennyu_novoyi_kiberatak i_142367). 17.10.2022).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Україна та Європейський Союз 29 вересня провели в Польщі другий раунд Діалогу з питань кібербезпеки, де передусім обговорювалося протистояння зловмисній кібердіяльності Росії.

…про це у вівторок повідомила Державна служба спеціального зв’язку та захисту інформації України.

Зокрема ЄС висловив солідарність із Україною, яка нині протистоїть кіберзагрозам, спрямованим на знищення її критичної інфраструктури, та запевнив у готовності й надалі надавати підтримку.

Сторони обмінялися думками щодо поточних загроз, серед усього – численних кібератак проти критичної інформаційної інфраструктури України, які розпочалися ще до початку повномасштабного вторгнення у лютому і тривають донині.

Представники України та ЄС обговорили актуальні інституційні та правові зміни в контексті кібербезпеки, зокрема в європейській Директиві про безпеку мереж та інформаційних систем, а також зусилля Києва з узгодження власного законодавства в цій сфері з правом Євросоюзу.

ЄС запевнив, що продовжуватиме надавати політичну, фінансову та матеріальну підтримку Україні для посилення її кіберстійкості. Учасники домовилися про подальше посилення своїх зусиль заради забезпечення кібербезпеки.

Зазначається, що ЄС уже виділив Україні 29 мільйонів євро для посилення стійкості в протидії кіберзагрозам. Із них 10 мільйонів євро було використано для закупівлі обладнання й програмного забезпечення, а решта – призначені для підтримки стійкої цифрової трансформації.

Додаткова підтримка у сфері кіберзахисту надається через Європейський механізм підтримки миру». ***(Україна та ЄС провели другий раунд діалогу з питань кібербезпеки // Європейська правда (https://www.eurointegration.com.ua/news/2022/10/4/7148061/). 17.10.2022).***

***

«Министерский комитет по кибербезопасности Совета сотрудничества стран Персидского залива (ССЗ) провел свое первое заседание в штаб-квартире Генерального секретариата ССАГПЗ в Эр-Рияде.

На встрече присутствовали руководители специализированных учреждений по кибербезопасности в странах ССЗ и Генеральный секретарь ССАГПЗ д-р Найеф Аль-Хаджраф. Саудовскую Аравию представляло Национальное управление кибербезопасности.

Собравшиеся обсудили рабочие документы, представленные странами ССЗ, которые направлены на укрепление сотрудничества в области кибербезопасности на уровне стран Персидского залива посредством нескольких инициатив, связанных с развитием сектора кибербезопасности.

Руководители учреждений обсудили несколько вопросов, представляющих взаимный интерес, в области кибербезопасности, в том числе проведение совместных учений по кибербезопасности в странах ССАГПЗ, чтобы активизировать обмен информацией и опытом и внести вклад в развитие сектора». ***(GCC Cybersecurity Ministerial Committee Holds First Meeting in Riyadh // H H Saudi Research and Marketing LTD (https://english.aawsat.com/home/article/3947116/gcc-cybersecurity-ministerial-committee-holds-first-meeting-riyadh). 23.10.2022).***

***

«Сингапур и Германия подписали соглашение о признании своей соответствующей системы рейтинга кибербезопасности для умных потребительских товаров, включая умные колонки, домашних роботов и

центры домашней автоматизации. Член ЕС является второй страной, сделавшей это после Финляндии.

Агентство кибербезопасности Сингапура (CSA) заявило в четверг, что подписало соглашение с Федеральным управлением информационной безопасности Германии (BSI) о взаимном признании ярлыков кибербезопасности, выданных обеими странами.

Согласно договору, продукты, выпущенные с маркировкой BSI, будут считаться соответствующими Уровню 2 схемы маркировки кибербезопасности CSA.

Сингапурская модель маркировки оценивает и классифицирует интеллектуальные устройства по четырем уровням на основе количества звездочек, каждая из которых указывает на дополнительный уровень тестирования и оценки, через который прошел продукт. Например, первый уровень указывает, что продукт соответствует базовым требованиям безопасности, таким как обеспечение уникальных паролей по умолчанию и предоставление обновлений программного обеспечения, в то время как продукт четвертого уровня прошел структурированные тесты на проникновение в утвержденных сторонних тестовых лабораториях и соответствует требованиям третьего уровня.

Продукты с рейтингом уровня 2 и выше будут признаны немецким BSI.

Взаимное признание будет применяться к потребительским устройствам Интернета вещей (IoT), включая интеллектуальные телевизоры, интеллектуальные игрушки, трекеры здоровья, интеллектуальное освещение и интеллектуальные термостаты.

Первоначально соглашение не распространялось на некоторые продукты, такие как интеллектуальные дверные замки, общие вычислительные устройства, такие как компьютеры и смартфоны, а также детекторы огня, газа и воды, которые были разработаны для запуска любых приложений без заранее определенной цели, говорится в сообщении CSA.

Государственное агентство Сингапура заявило, что будет работать с BSI над добавлением дополнительных категорий продуктов в соответствии с двусторонним соглашением.

Азиатская страна подписала аналогичный договор с Финляндией в октябре 2021 года, при этом потребительские продукты IoT, имеющие маркировку кибербезопасности последней, считаются соответствующими сингапурским требованиям уровня 3, и наоборот.

Такие соглашения сэкономили производителям интеллектуальных устройств не только деньги и время, которые они в противном случае потратили бы на дублированные испытания, но и предоставили им доступ к новым рынкам.

По состоянию на октябрь 2022 года сингапурские знаки кибербезопасности получили более 200 продуктов. CSA получило более 300 заявок на лейблы.

Подключенные медицинские устройства будут оцениваться на предмет гигиены безопасности

Схема маркировки страны в четверг была расширена за счет включения медицинских устройств, которая была запущена в сотрудничестве с Министерством здравоохранения (МЗ), Управлением медицинских наук (HSA) и Интегрированными информационными системами здравоохранения (IHIS).

Такие устройства все чаще подключаются к больницам и домашним сетям, но могут причинить физический вред в случае атаки IoT, заявил старший государственный министр Министерства связи и информации Сингапура Джанил Путучер.

Выступая в четверг на конференции Singapore International Cyber Week, министр сказал, что медицинские устройства, такие как мониторы ЭКГ и кардиостимуляторы, становятся умнее, поскольку медицинские компании и специалисты используют технологии для улучшения своих возможностей по сбору данных о пациентах, проведению терапии или индивидуальной терапии.

Однако расширение возможностей подключения означало повышенные риски кибербезопасности и могло поставить под угрозу личную информацию пациентов, клинические данные или протоколы лечения, что в конечном итоге повлияло на результаты лечения пациентов.

Путучеар сказал: «Когда мы думаем об устройствах IoT, на первое место выходят удобство и эффективность, но не обязательно безопасность и безопасность пользователей. Отсутствие надежной защиты IoT может представлять серьезные риски. Многие потребительские IoT-устройства содержат кеш потребительских данных. и информация, которая в случае утечки может поставить под угрозу конфиденциальность потребителей.

«В более серьезных случаях взлом IoT может привести к серьезным физическим повреждениям и даже к риску для жизни», — сказал он, указывая на уязвимость, обнаруженную в 2017 году Управлением по санитарному надзору за качеством пищевых продуктов и медикаментов США в кардиостимуляторах, которая позволяла изменять функции устройства и истощать его батарея.

Расширение сингапурской схемы маркировки кибербезопасности для включения медицинских устройств будет стимулировать производителей разрабатывать такие продукты с учетом кибербезопасности.

Схема маркировки будет применяться к медицинским устройствам, которые обрабатывают данные о состоянии здоровья или могут подключаться к другим устройствам, системам и службам.

Включая четыре уровня рейтинга, каждый уровень будет указывать на дополнительный уровень тестирования и оценки, которому подвергся продукт. Уровень 1 означал, что медицинское устройство соответствует базовым нормативным требованиям, которые в настоящее время соответствуют требованиям регистрации медицинских устройств, утвержденным HSA.

Базовые требования к кибербезопасности для уровня 1 схемы маркировки включают требования, которым должны соответствовать медицинские устройства для регистрации в HSA. Следовательно, все медицинские изделия, зарегистрированные HSA, будут считаться соответствующими Уровню 1 схемы маркировки кибербезопасности.

Продукты, которым присвоены уровни от 2 до 4, должны будут соответствовать «расширенным» требованиям кибербезопасности, таким как требования к устройствам и данным. Устройства в этих категориях, возможно, должны будут пройти независимые сторонние тесты, согласно CSA, в котором говорится, что более подробная информация будет предоставлена позже.

Правительственное агентство заявило, что в течение следующего месяца будут проведены официальные консультации с производителями медицинского оборудования, а также с ассоциациями, чтобы собрать отзывы о предлагаемых требованиях уровней 2–4. Они будут включать сроки реализации». ***(Eileen Yu. Singapore, Germany to mutually recognise IoT cybersecurity labels // ZDNET, A Red Ventures company (https://www.zdnet.com/article/singapore-germany-to-mutually-recognise-iot-cybersecurity-labels/). 20.10.2022).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Пандемия COVID-19 остается свежей в нашей памяти, поскольку она затронула многие аспекты нашей жизни. Киберпространство не является исключением. Из-за настоятельной необходимости оставаться в безопасности людям приходилось создавать альтернативные методы работы, учебы, общения и доступа к услугам. Однако в этот период киберпреступники также удвоили свои усилия по использованию ситуации.

В отчете о преступности в Интернете за 2020 год зафиксирован ущерб на сумму более 4,2 миллиарда долларов, связанный с киберпреступлениями. Наиболее часто регистрируемыми преступлениями являются фишинговые атаки и вымогательство. COVID-19 угрожал не только жизням, но и кибербезопасности — последняя не сильно изменилась после пандемии.

Следовательно, компании рискуют операционными и финансовыми потерями, если они не планируют и не защищают себя от возможных кибератак. В этой статье мы анализируем влияние COVID-19 на кибербезопасность и обсуждаем проверенные методы обеспечения безопасности и конфиденциальности в Интернете.

Переход на цифровую работу после COVID-19

Цифровая трансформация предполагает использование цифровых технологий во многих аспектах организационной деятельности. Несмотря на неуклонный рост внедрения цифровых технологий, COVID-19 ускорил цифровую трансформацию. Чтобы сохранить производительность, предприятия должны были адаптироваться и расти в цифровом пространстве.

На сегодняшний день переход на цифровые технологии стал необходимостью для многих предприятий, чтобы удовлетворить постоянно растущие потребности потребителей. Кроме того, необходимо создать противоэпидемический план по отраслям для поддержания эффективности.

Киберугроза для малого и среднего бизнеса

Киберпреступность существует уже давно. Однако пандемия вызвала всплеск этой практики. Вопреки распространенному мнению, что затронуты только крупные предприятия, киберугрозы затрагивают малые и средние предприятия (МСП). Согласно отчету Keeper and Ponemon State of SMB Cybersecurity за 2018 год, малые предприятия составляют 67% жертв киберпреступлений. Виной всему отсутствие эффективных стратегий кибербезопасности.

Фишинговые атаки

Фишинг — это форма онлайн-мошенничества, при которой преступники притворяются, что им доверяют или пользуются хорошей репутацией, чтобы обманом заставить своих жертв раскрыть важную и личную информацию. Такие данные включают данные кредитной карты, номера социального страхования, дни рождения, адреса проживания, данные для входа в систему и т. д. В зависимости от цели и используемого носителя фишинговые атаки можно классифицировать следующим образом:

● Целевой фишинг

Злоумышленники нацеливают фишинговые электронные письма на конкретных людей или компании, чтобы украсть информацию или установить вредоносное ПО.

● Китовый фишинг

Китобойный промысел — более целенаправленная форма целевого фишинга. Здесь целями обычно являются владельцы бизнеса или влиятельные лица.

● смишинг и вишинг

Смишинг осуществляется с помощью текстовых сообщений, а вишинг — с помощью голосовых вызовов или аудиосообщений.

Вредоносное ПО

Вредоносное ПО — это сокращение от вредоносного программного обеспечения. Он включает в себя различное программное обеспечение или программы, предназначенные для кражи, эксплуатации, заражения или нанесения вреда устройствам и сетям.

Программы-вымогатели

Здесь вредоносное ПО может использоваться для блокировки или шифрования файлов жертвы до тех пор, пока жертва не заплатит выкуп за их восстановление. Злоумышленники добиваются этого с помощью фишинговых писем. Из-за этих атак предприятия рискуют потерять файлы или значительную сумму денег.

Подготовка сотрудников к возможным кибератакам

Помимо последствий для конфиденциальности данных, компании рискуют значительными финансовыми потерями.

Поэтому, независимо от размера, предприятия должны быть готовы к возможным кибератакам. Вот несколько советов, как оставаться впереди в киберпространстве:

Инвестируйте в инструменты кибербезопасности и персонал

Инвестирование в кибербезопасность начинается с обеспечения актуальности всего программного обеспечения компании. Регулярные обновления программного обеспечения — это простой и экономичный способ предотвращения кибератак. Операционные системы предлагают регулярные обновления, чтобы не отставать от постоянно меняющихся стратегий кибератак. Он закрывает некоторые лазейки, через которые мошенники могут получить доступ.

Внедрение многофакторной аутентификации (MFA)

МФА обеспечивают дополнительный уровень защиты от кибератак. В дополнение к обычным паролям, MFA требуют других данных, уникальных для авторизованного пользователя. Это затрудняет доступ хакеров к важным файлам.

Регулярно делайте резервные копии

Резервные копии хороши, особенно в случае атак программ-вымогателей. Желательно иметь несколько защищенных копий ценных документов онлайн и офлайн.

Регулярные напоминания и тренинги по кибербезопасности для сотрудников

Организуйте учения и аварийные учения для ваших сотрудников. Расскажите им, как выявлять атаки, защищаться от них и быть в курсе новых тенденций в области кибербезопасности.

Четыре способа преодоления кризисов кибербезопасности компаниями

Нарушение может иметь разрушительные последствия для бизнеса. Однако время никого не ждет. Уместно вернуться к нормальной жизни и продолжить как можно скорее. Вот способы преодоления кризисов кибербезопасности.

Используйте свой план киберстрахования

Это также известно как страхование киберответственности. Он защищает бизнес от кибератак и взломов и помогает компенсировать понесенные убытки.

Переключиться на безопасные резервные копии

Крайне важно использовать безопасные резервные копии, поскольку некоторые из них могут быть скомпрометированы. Возьмите за привычку регулярно создавать резервные копии данных в нескольких и безопасных местах.

Оценить стратегии кибербезопасности

Сделайте критическую и объективную оценку ваших текущих стратегий безопасности. Найдите лазейки и внесите соответствующие коррективы. Кроме того, обратитесь за помощью к эксперту в оценке и обновлении стратегий кибербезопасности, чтобы ограничить ущерб.

Приспособиться к плану обеспечения непрерывности бизнеса

Создайте и обновите план обеспечения непрерывности бизнеса. В зависимости от степени повреждения принять меры для продолжения работ. Некоторые из них могут включать ограничение электронной почты, использование большего количества документов и т. д.

Вывод

Количество случаев киберпреступности резко возросло с начала пандемии. Потеря данных, судебные иски, потеря партнеров или клиентов и финансовые потери — это лишь некоторые из последствий кибератак…» ***(Paul Cawthon. Cybercrime after COVID-19 // TechTarget, Inc. (https://www.datasciencecentral.com/cybercrime-after-covid-19/). 13.10.2022).***

***

Світові тенденції в галузі кібербезпеки

«Не секрет, что пандемия во многих отношениях послужила катализатором, ускорив потребность в лучших технических специалистах, поскольку компании удваивают цифровизацию. Однако в этой войне за таланты индустрия кибербезопасности проигрывает.

В отрасли кибербезопасности уже много лет наблюдается острая нехватка талантов — результат постоянной борьбы с привлечением и удержанием квалифицированных сотрудников. В сочетании со сложным характером операций по обеспечению безопасности за последние пару лет ресурсы были истощены, что привело к дополнительной нагрузке на и без того облагаемых налогом специалистов по кибербезопасности и подорвало цифровую трансформацию в Азии.

Недавнее исследование, проведенное Trellix, показало, что многие специалисты по кибербезопасности во всем мире разочарованы ограниченной поддержкой развития навыков, а также отсутствием признания того добра, которое они приносят обществу. Еще более примечательно то, что треть нынешней рабочей силы планирует сменить профессию в будущем, что ясно указывает на то, что волна Великой отставки еще не достигла своего пика в индустрии кибербезопасности.

Затем в центре внимания находятся организации, работающие на местах, и возникает вопрос: смогут ли они привлечь лучших специалистов, которые им нужны, чтобы они могли оцифровывать, не попадая в поле зрения злонамеренных хакеров?

Сегодняшняя рабочая сила хочет значимой работы

Сегодня во многих заголовках преобладает изменение ожиданий сотрудников в результате трансформации рынка труда, когда молодые технические специалисты увольняются с работы в поисках более душевной работы. В конечном счете, люди теперь ищут работу, где они могут конструктивно использовать свои навыки и таланты для достижения большей цели.

Таким образом, карьера в области кибербезопасности — это палка о двух концах: она может быть эффективной и полезной, но в то же время чрезвычайно сложной и требовательной.

Сотрудники SecOps имеют дело с постоянным потоком сигналов тревоги, поэтому неудивительно, что кибербезопасность часто воспринимается как отрасль с высокими ставками и высоким уровнем стресса. Кроме того, поскольку их технологический стек рассредоточен по множеству инструментов, выявление атак по векторам может стать сложной задачей для специалистов по кибербезопасности.

Тем не менее, в индустрии кибербезопасности не все так скучно — есть сотрудники из разных слоев общества, которые преуспевают в профессиональном плане, а также находят личное удовлетворение. Ключом к этому являются работодатели, которые должны поставить людей в основу своих методов обеспечения безопасности и культуры на рабочем месте, чтобы привлечь в отрасль умных и мотивированных работников.

Когда дело доходит до таланта, качество может превзойти количество

Если это еще не очевидно, поиск талантов в области кибербезопасности является не только локальным, но и глобальным приоритетом.

В том же отчете, упомянутом ранее, мы обнаружили, что 85% специалистов по кибербезопасности считают, что нехватка рабочей силы влияет на способность их организации защищать все более сложные информационные системы и сети.

На этом фоне организации должны делать больше для расширения поиска талантов. Не менее важным, чем наем новых кандидатов, будет повышение квалификации существующей рабочей силы, как с помощью технических

возможностей, так и таких компетенций, как способность к обучению и сотрудничество. Важность этого нельзя недооценивать: ИТ-команды старшего руководства, включая директора по информационным технологиям (CIO), должны быть в курсе новейших инструментов безопасности и быть осведомленными о быстро меняющихся тенденциях в отрасли, чтобы они могли предоставлять сотрудникам возможности для оттачивать свои навыки.

Как бы пугающе ни звучала индустрия кибербезопасности с внешней точки зрения, сотрудники, которые приобретают критические навыки межличностного общения, имеют большие шансы на эффективную адаптацию и продвижение по карьерной лестнице. Например, более половины респондентов в нашем исследовании считают критическое мышление и работу в команде качествами, которые были наиболее полезными для их роли. Это способности, которые действительно можно изучить и улучшить с течением времени.

Агентство кибербезопасности Сингапура возглавляет новую национальную инициативу SG Cyber Talent, взращивая талантливых энтузиастов кибербезопасности с самого раннего возраста. Хотя предоставление таких возможностей является отличной стратегией для привлечения молодых талантов в отрасль, создание надежного источника знаний в области кибербезопасности займет много времени. Владельцы бизнеса должны действовать сейчас, иначе они рискуют проиграть своим конкурентам.

XDR расширяет свою поддержку для организаций всех размеров

Умные организации понимают, что просто нанять больше сотрудников не может быть единственным решением. Киберугрозы будут только увеличиваться в количестве и сложности, что заставит организации внедрять инновации и использовать более эффективные технологические инструменты.

Откройте для себя расширенное обнаружение и реагирование (XDR) — платформу, которая позволяет организациям любого размера упростить свои системы безопасности и снизить рабочую нагрузку на персонал. Использование этого инструмента немедленно дает сотрудникам больше передышки и времени для эффективного и действенного выполнения своих обязанностей.

Это достигается тремя способами.

Во-первых, XDR объединяет несколько решений безопасности на одной платформе, а это означает, что конечные точки, электронная почта, сети и облако могут быть легко подключены. Таким образом, имея более полную картину своей экосистемы безопасности, группы SecOps смогут лучше адаптироваться и защищать свою поверхность атаки.

Во-вторых, автоматизируя рабочие процессы с помощью искусственного интеллекта и машинного обучения, XDR помогает повысить квалификацию человека. Расширенный интеллект упрощает прогнозирование атак и быстрое обнаружение угроз, а также координацию корректирующих действий и автоматических ответов в режиме реального времени. Другими словами, XDR всегда работает, так что работникам не нужно.

Наконец, XDR предоставляет встроенные экспертные знания, в их распоряжении несколько оборонительных сборников, предлагающих тактику и контрмеры. Экосистема разработана с использованием лучших в своем классе

аналитических данных, предоставляя командам SecOps все знания, необходимые им для принятия оптимальных решений в области кибербезопасности — до, во время и после атаки.

В конечном счете, индустрия кибербезопасности предлагает душевную и целеустремленную карьеру, к которой сегодня стремится большинство талантов, но это может стать возможным только в том случае, если организации готовы инвестировать в новые технологии, которые помогут упростить безопасность и вывести ее за пределы того, что есть сегодня.

Таким образом, решение готово, и предприятиям пора взглянуть на более широкую картину». ***(Muhammad Zulhusni. Hacking the shortage in cybersecurity talent // Tech Wire Asia (https://techwireasia.com/2022/10/hacking-the-shortage-in-cybersecurity-talent/). 14.10.2022).***

***

«За последние четыре года (в период с августа 2022 г. по август 2019 г.) количество поисковых запросов в Интернете по запросу «обучение сотрудников кибербезопасности» выросло на 114%. В результате организации делают шаг в правильном направлении, чтобы улучшить соблюдение требований кибербезопасности среди своих сотрудников. Дополнительные данные показали значительное увеличение «обучения по вопросам кибербезопасности» на 66% за тот же период.

Всплеск спроса на обучение по вопросам кибербезопасности происходит на фоне постоянной нехватки навыков в области кибербезопасности, что говорит о том, что работодатели обращают внимание на то, чтобы вся их рабочая сила была более осведомлена о кибербезопасности, чтобы снизить вероятность кибератак. Исследование рынка труда в области кибербезопасности в Великобритании показало, что половина (51%) всех предприятий частного сектора отмечают недостаток базовых технических навыков в области кибербезопасности, что составляет около 697 000 предприятий.

Согласно недавним выводам Interisle, количество фишинговых атак увеличилось на 61% в прошлом году и составило более одного миллиона атак. С ростом числа фишинговых атак неудивительно, что поисковые запросы, связанные с «обучением сотрудников по вопросам фишинга», за последние четыре года выросли на 72%. Тем не менее, также интересно, что поисковые запросы по фразе «моделирование фишинга для сотрудников» за тот же период выросли на 62%. Это показывает, что организации признают важность обучения сотрудников фишинговым атакам и их тестирования, чтобы убедиться, что они поняли курс обучения.

Вызывает тревогу тот факт, что недавний отчет IBM о стоимости утечки данных показал, что средняя глобальная стоимость утечки данных увеличилась до 4,35 млн долларов США в 2022 году, что на 2,6% больше, чем в 2021 году. Цена несоблюдения требований и жертвы утечки данных слишком высока., особенно с учетом отчета, показывающего, что человеческий фактор был причиной 21% взломов.

Джейсон Стирланд, технический директор DeltaNet International, прокомментировал: «Хотя обучение, безусловно, не заменит квалифицированных специалистов по кибербезопасности, эти статистические данные подчеркивают необходимость повышения общей осведомленности сотрудников в области кибербезопасности. Организации не могут просто полагаться на профессионалов в области кибербезопасности для защиты инфраструктуры бизнеса и защиты своих данных. Обучение сотрудников — это шаг в правильном направлении, но работа еще далеко не завершена. Например, тестирование сотрудников с помощью сообщений, имитирующих фишинг, является неотъемлемой частью процесса обучения. В результате ИТ- и HR-подразделения могут понять, какие сотрудники могут представлять повышенный риск и, следовательно, нуждаются в дальнейшем обучении и поддержке.

«Сотрудники по всем направлениям, от отдела кадров до финансового отдела, имеют доступ к критически важным данным, поэтому жизненно важно обучить всех в бизнесе вопросам осведомленности о кибербезопасности, от понимания того, как обнаруживать попытки фишинга до предотвращения утечки данных. Кибербезопасность — это не только проблема для ИТ-специалистов и специалистов по безопасности в организациях; это проблема отдела кадров. Обучение сотрудников обучению осведомленности о кибербезопасности должно обновляться ежегодно в рамках программы обучения соблюдению требований в организации и не должно откладываться до тех пор, пока не произойдет утечка данных.

Исследование Всемирного экономического форума показало, что 59% кибер-руководителей заявили, что им будет сложно реагировать на инцидент кибербезопасности из-за нехватки навыков в их команде. Из-за нехватки навыков в области кибербезопасности организации по-прежнему будут подвергаться риску при защите своей инфраструктуры.

Джейсон продолжил: «Несмотря на то, что предприятия должны иметь надежные системы безопасности, во всей компании должна существовать корпоративная культура для снижения рисков. Кроме того, кибербезопасность требует ответственности от всех сотрудников, и работники поймут это только в том случае, если они будут обучены ее важности и знают, как действовать.

«За последний год организации по всему миру столкнулись с тем, что сотрудники возвращаются на рабочие места, ориентируются на офисных, удаленных и гибридных работников. К сожалению, многие предприятия забывают о важности обучения своих гибридных и удаленных сотрудников передовым методам кибербезопасности, что ослабляет устойчивость организации к любым нарушениям безопасности. ИТ- и HR-специалисты должны выявлять любые пробелы в навыках в организации и обеспечивать, чтобы все сотрудники понимали свою роль в защите инфраструктуры организации и защите ее данных». ***(Jason Stirland. CYBERSECURITY SKILLS SHORTAGE A GROWING CONCERN FOR PRESSURED FIRMS // theHRDIRECTOR (https://www.thehrdirector.com/business-news/security/cybersecurity-skills-shortage-growing-concern-pressured-firms/). 13.10.2022).***

***

«…З 15 по 17 листопада компанія Softprom – найбільший Cyber Security Distributor в Україні, на території Східної та Центральної Європи, Західної та Центральної Азії проводить Online Security Forum.

SECURITY FORUM – FUELED BY CYBER BRAVERY

Ми не говоримо багато, ми надаємо можливість дізнатися про актуальне, брати участь у професійному нетворкінгу та обмінятися досвідом з колегами:

Master-classes & use-cases. Учасникам представлять основні методи та підходи у роботі з технологіями у дії. Скористайтеся демонстраціями та чек-листами при подальшому налаштуванні та запуску рішень.

Eyes to eyes communication. Можливість забронювати тет-а-тет зустріч зі спікерами, представниками вендорів та іншими експертами.

Програма заходу. На Security Forum 2022 не буде «класичних» доповідей. Фокус на практичні майстер-класи та тестування, комунікаціях online…

Буде корисно кібервоїнам, IT спеціалістам та Фахівцям з Інформаційної безпеки, CISO та CIO, CRMO та CEO, Founder'ам IT-компаній та Інтеграторів. Участь безплатна, необхідна попередня реєстрація.

Захід підтримали світові лідери у сфері IT технологій та IT Безпеки. Серед генеральних партнерів компанії Rapid7, VMware, Imperva, Forcepoint, Logsign, OPSWAT, Sycope, Citrix, CrowdStrike, Senhasegura…». ***(Online Security Forum 2022 – Реєстрація відкрита // Компьютерное Обозрение (https://ko.com.ua/online_security_forum_2022_reyestraciya_vidkrita_142337). 12.10.2022).***

***

«У рамках головування Чеської Республіки в Раді ЄС регіон Височина організував конференцію «Цифрове партнерство для кібербезпеки та стійкості в регіонах» у співпраці з Міністерством закордонних справ Чеської Республіки…

Окрім гостей та лекторів із Чехії, на конференцію прибули експерти з Тайваню, Естонії, Франції, Румунії, Вірменії, Грузії, Молдови, Азербайджану та України.

Україну на заході представляли представники IT-спільноти із Закарпатської області. Про це зазначалося на сайті Закарпатської ОВА.

Основну увагу конференція зосередила на впливі геополітичних ситуацій на кібербезпеку та нових загрозах, з якими зараз мають справу експерти з країн ЄС. Грузія, Молдова та особливо Україна, які з початку російського вторгнення стикаються з масовими кібератаками на установи державного управління, були дуже зацікавлені у налагодженні співпраці, але особливо в обміні перевіреною практикою виявлення кібератак. «Зловмисники все ще на кілька кроків попереду тих, хто захищає організацію, і цю прогалину дуже важко подолати. Досі важко забезпечити достатній потенціал для розбудови кібербезпеки та стійкості – це були центральні теми конференції. Потрібно знати, що тенденція до зростання здатності налагоджувати партнерські стосунки на національному чи міжнародному рівнях є дуже позитивною, що призводить саме до підвищення стійкості до кібератак.

Головною перевагою широко представленої міжнародної зустрічі став обмін досвідом між європейськими лідерами у цій сфері та представниками країн Східного партнерства, обмін досвідом у розбудові потенціалу у сфері кібербезпеки та стійкості на регіональному рівні, а також як зміцнення міжнародного партнерства з можливістю обміну новими відкритими інструментами для державного управління. Наприклад, йшлося про залучення експертів, їх адекватну оцінку та підвищення привабливості сфери для жінок. Фахівці з Тайваню прочитали лекції про створення централізованої безпеки лікарні, а експерти з Естонії представили свій шлях поступового створення власної цифрової компанії». ***(Закарпаття представило Україну на міжнародній конференції з кібербезпеки у Чехії // ТОВ «Голос Карпат» (https://goloskarpat.info/society/63459d56626cf/). 11.10.2022).***

***

«Страхование кибер-ответственности не является универсальной общей политикой, которая может применяться ко всем типам бизнеса. У каждой организации есть выбор в отношении того, какие типы покрытия киберответственности ей необходимы для защиты от злонамеренных атак, таких как программы- вымогатели или вредоносное ПО, и знание волновых эффектов, которые может оказать атака на все, от конфиденциальных данных клиентов до непрерывности бизнеса, важно для определения того, как чтобы сделать этот выбор.

Прежде чем сокращать покрытие по полису страхования ответственности за кибербезопасность, чтобы сэкономить премиальные доллары, убедитесь, что вы понимаете взаимосвязь между различными элементами покрытия и то, как они применяются к современной кибератаке.

Ниже вы найдете пример сценария, демонстрирующий, какие части покрытия киберстрахования могут быть вызваны гипотетическим событием кибербезопасности.

Сценарий: платежная система подверглась атаке программы-вымогателя, которая полностью отключила ее сеть, не позволяя ей проводить платежи для своих пользователей. Кроме того, конфиденциальные финансовые данные пользователей, которые сохранили свою платежную информацию в компании, могут быть скомпрометированы, хотя полный масштаб еще не известен. Злоумышленники потребовали большой выкуп за восстановление важных данных, необходимых для возобновления работы сети, но не упомянули о статусе каких-либо конфиденциальных данных клиентов.

Ниже описано, какие конкретные части полиса страхования кибербезопасности будут активированы этим событием и как политика может реагировать после того, как событие прошло.

Сетевая безопасность

Покрытие сетевой безопасности следует рассматривать как важный компонент полиса страхования кибербезопасности для большинства организаций, особенно для тех, в отношении которых действует конфиденциальность финансовой информации и данных. В этом гипотетическом сценарии сбой сетевой безопасности привел к атаке программы-вымогателя, которая отключила сеть компании.

Сетевая безопасность покрывает расходы первой стороны (т. е. расходы, понесенные непосредственно в результате киберинцидента). Это покрытие обычно включает такие элементы, как:

Юридические расходы

ИТ-криминалистика

Переговоры и оплата запроса программы-вымогателя

Восстановление данных

Уведомление о нарушении для потребителей

Консультации по связям с общественностью

Эти элементы вступают в действие после взлома и охватывают несколько областей реагирования. Как только страховая компания признает нарушение, инициируется скоординированное реагирование, которое включает получение рекомендаций от адвоката по нарушениям в сочетании с выводами специалистов по ИТ-криминалистике.

В большинстве случаев адвокат по взлому нанимает собственного стороннего консультанта по ИТ-криминалистике для проведения независимого расследования, которое включает анализ причины, происхождения и масштаба инцидента, а также любые рекомендации по исправлению сети/системы. Менеджер по кибервымогательству также может быть задействован для согласования требования выкупа и способа оплаты от имени компании.

Тем временем адвокат по взлому и ИТ-криминалисты также оценят состояние данных компании, чтобы определить, были ли они украдены или раскрыты неправомерно, включая конфиденциальную или личную информацию о ее клиентах.

Если команда ИТ-криминалистов подтвердит компрометацию конфиденциальных данных, советник по взлому проанализирует юридические обязательства компании по уведомлению своих клиентов, государственных органов и агентств кредитного мониторинга. Таким образом, команде по связям с общественностью будет поручено общаться со средствами массовой информации или клиентами в отношении инцидента, его воздействия и последующего реагирования.

В конце концов, должно быть принято решение о том, платить или нет требование о выкупе. Решение об оплате взвешивается с учетом таких факторов, как общая стоимость восстановления украденных данных из резервных копий и прогнозируемых затрат, связанных с любой формой перерыва в работе при восстановлении данных.

В этом гипотетическом сценарии считается, что в интересах компании отказаться от выплаты огромного выкупа и вместо этого инициировать восстановление данных из резервных копий таким образом, чтобы критически важные процессы компании возобновились как можно быстрее. насколько это возможно, что позволяет возобновить обработку платежей через несколько часов. Также было установлено, что лишь небольшая часть конфиденциальных данных клиентов была потенциально скомпрометирована.

Реагирование на политику страхования кибербезопасности: после инцидента

Теперь, когда инцидент с программой-вымогателем устранен в оперативном смысле, его влияние все еще необходимо учитывать в нескольких других областях политики.

Прерывание работы сети

Покрытие сбоев в работе сети позволяет компании возместить упущенную прибыль, фиксированные расходы и другие дополнительные расходы, понесенные из-за отключения сети в результате события кибербезопасности.

В этом случае покрытие возмещает компании, занимающейся обработкой платежей, доход, который она упустила, когда не смогла провести платежи во время атаки программы-вымогателя из-за сбоя сети.

Ошибки и упущения

Компания по обработке платежей зависит от облегчения платежей для своих клиентов. Атака программы-вымогателя отключила ее сеть, в результате чего компания не смогла выполнить свои договорные обязательства по предоставлению этой услуги своим пользователям, что, в свою очередь, означало, что розничные торговцы и поставщики не могли принимать определенные формы оплаты от своих клиентов во время атаки, что, вероятно, стоило им дохода.

Именно здесь вступает в действие покрытие ошибок и упущений (E&O). E&O покрывает претензии, возникающие в результате ошибок при выполнении или невыполнении ваших услуг. Покрытие касается заявлений о халатности или нарушении контракта и может включать расходы на юридическую защиту в результате судебного процесса или любых споров со стороны его клиентов.

Ответственность за конфиденциальность

Поскольку обработчику платежей доверяют чрезвычайно конфиденциальную финансовую и личную информацию, защита конфиденциальности имеет важное значение. Когда эта информация скомпрометирована, клиенты, безусловно, подвергаются риску, но компания также несет ответственность.

Покрытие ответственности за конфиденциальность защищает компанию от ответственности, связанной с кибер-инцидентом или нарушением закона о конфиденциальности, а также от любых нормативных расследований, проводимых правительствами и правоохранительными органами.

Если групповой иск (и возможное урегулирование) возникнет у клиентов, чьи данные были скомпрометированы, ответственность за конфиденциальность защитит платежную систему. То же самое относится к любым судебным расходам, штрафам или взысканиям, вытекающим из регулирующего расследования, проводимого правительством или правоохранительными органами.

Потребности в страховании кибербезопасности уникальны для каждой организации

В приведенном выше гипотетическом сценарии платежная система смогла не только смягчить непосредственный ущерб, причиненный атакой программы-вымогателя, и найти наиболее выгодное решение, но и возместить финансовые потери от простоя сети, защитив себя от обязательств, возникающих в результате потенциальных судебных разбирательств. и расследования.

Тем не менее, это всего лишь пример сценария того, как определенные части политики киберответственности могут реагировать на нарушение. У каждой

организации есть свои требования и обязательства, которые следует учитывать при разработке надежной политики, обеспечивающей адекватный уровень защиты на всех фронтах». ***(Dan Burke. How a Cyber Attack Triggers Multiple Parts of a Cyber Security Insurance // An Assurex Global & IBN Partner (https://woodruffsawyer.com/cyber-liability/cyber-attack-triggers/). 03.10.2022).***

***

«Сегодняшние заголовки ясно показывают, что конфиденциальность и кибербезопасность вышли за рамки вопросов ИТ и соблюдения законодательства и теперь являются экологическими, социальными и управленческими (ESG) ориентирами, жизненно важными для рыночной капитализации и стоимости акционеров.

Для понимания масштаба вопроса важно уточнить терминологию. На высоком уровне конфиденциальность данных касается личной информации, которую компании собирают, используют и передают, а также того, как они сообщают о своей практике. Кибербезопасность, с другой стороны, касается того, что компании делают для защиты личных и важных для бизнеса данных и поддержания устойчивости. Конфиденциальность и кибербезопасность практически не регулировались до 2018 года, когда вступил в силу Общий регламент Европейского союза (ЕС) о защите данных. В настоящее время существует более 150 стран с законами о защите данных.

Конфиденциальность и кибербезопасность в основном затрагивают области, выходящие за рамки правового поля. Проблемы с конфиденциальностью привели к потере рыночной капитализации публичных компаний в размере 1,4 триллиона долларов в первом и втором кварталах 2022 года. В 2021 году киберпреступления обошлись нашей мировой экономике в 6 триллионов долларов, и ожидается, что к 2025 году эта цифра увеличится до 10,5 триллионов долларов. и кибербезопасность были бы страной, они были бы третьим по величине ВВП после США (ВВП 20,89 трлн долларов) и Китая (ВВП 14,72 трлн долларов). Недавно Министерство юстиции США указало, что будет проводить новую политику добивается одобрения корпоративных программ соответствия на уровне руководителей высшего звена и дала понять, что будет ожидать, что генеральные директора будут ручаться за корпоративные программы соответствия. Кроме того, недавнее уголовное осуждение директора по информационной безопасности (CISO) за утечку данных привело к тому, что некоторые комментаторы призвали к ответственности советы директоров, а не директоров по информационной безопасности.

Сообщество инвесторов следит за тем, что делают советы директоров. Консультанты по доверенности, такие как Institutional Shareholder Services (ISS), незаметно оценивают компании по их кибербезопасности и конфиденциальности с помощью управленческого аспекта оценки ESG. Крупнейшие глобальные инвесторы недавно поставили кибербезопасность на второе место по степени озабоченности ESG, а Bloomberg сообщил в 2021 году, что его обзор документов SEC за последние пять лет «показывает растущую тенденцию компаний, явно классифицирующих свое соблюдение правил конфиденциальности данных и добровольных стандартов в качестве экологических требований», социальные и управленческие (ESG) вопросы».

Рамки для отчетности ESG содержат рекомендации по конфиденциальности и киберотчетности. Глобальная инициатива по отчетности (GRI), надежный ресурс для отчетности ESG многих компаний, выпустила специальный «Стандарт конфиденциальности клиентов», в котором говорится, что о нарушениях конфиденциальности клиентов следует сообщать в рамках управления рисками предприятия.

Кроме того, инвесторы активно участвуют в надзоре за кибербезопасностью и конфиденциальностью. Один многонациональный инвестор, управляющий активами на сумму 10 триллионов долларов, сообщил, что взаимодействует с компаниями для повышения вовлеченности совета директоров. Например, в нем сообщалось: «В ходе взаимодействия с фармацевтической компанией мы обсудили надзор совета директоров за рисками кибербезопасности и внимание руководства к раннему обнаружению, а не к тому, что оно считало недостижимой целью полного предотвращения».

8 апреля 2021 года FTC призвала советы директоров «создать команду заинтересованных сторон», которые могут «... привнести другой взгляд на проблемы». По данным FTC, помимо директора по информационным технологиям (CIO) и директора по информационной безопасности, в команду, которая отчитывается перед советом директоров, должны входить нетехнические лидеры, такие как генеральный директор, финансовый директор и главный юрисконсульт.

FTC также рекомендовала советам директоров пересмотреть структуру своих комитетов, чтобы обеспечить надзор совета директоров за кибербезопасностью либо на уровне комитета по аудиту, либо через отдельный комитет, занимающийся вопросами кибербезопасности. В связи с этим FTC отметила, что «независимо от того, как организация структурирует свои обязанности по надзору за киберрисками, ключевым выводом является то, что киберриски должны быть приоритетом в зале заседаний совета директоров. Надзор на уровне совета директоров помогает гарантировать, что угрозы кибербезопасности, средства защиты и ответные меры привлекают внимание высших эшелонов власти и получают ресурсы, необходимые для правильного выполнения работы».

FTC также рекомендовала советам директоров регулярно проводить брифинги по кибербезопасности: «Когда дело доходит до безопасности, члены совета директоров должны быть в курсе, но исследования показывают, что многие из них не в курсе».

9 февраля 2022 года SEC выпустила предлагаемое правило, которое требует от инвестиционных консультантов и зарегистрированных инвестиционных компаний принять письменные политики кибербезопасности и подготовить письменные отчеты для контроля совета директоров. «Предлагаемое правило 38a-2 потребует, чтобы совет директоров фонда, включая большинство его независимых директоров, первоначально утвердил политику и процедуры фонда в области кибербезопасности, а также рассмотрел письменный отчет об инцидентах в области кибербезопасности и существенных изменениях в кибербезопасности фонда. политики и процедуры, которые… необходимо будет готовить не реже одного раза в год».

Согласно SEC, «надзор за советом директоров не должен быть пассивной деятельностью», и призвала советы получать и читать письменные отчеты.

Комиссия по ценным бумагам и биржам отметила, что «необходимые письменные отчеты… предоставят директорам фондов информацию, необходимую для того, чтобы задавать вопросы и искать соответствующую информацию об эффективности программы и ее реализации, а также о том, есть ли у фонда достаточные ресурсы в отношении вопросов кибербезопасности, включая доступ к экспертизе в области кибербезопасности».

В марте 2022 года SEC предложила еще одно правило, описывающее ее намерение требовать от публичных компаний раскрытия информации о том, есть ли в их советах члены с опытом работы в области кибербезопасности. SEC объяснила обоснование этого предлагаемого нового требования о раскрытии информации, заявив: «Кибербезопасность уже является одним из главных приоритетов многих советов директоров, а инциденты с кибербезопасностью и другие риски считаются одной из самых больших угроз для компаний. Соответственно, инвесторы могут счесть важным раскрытие информации о том, обладают ли какие-либо члены правления знаниями в области кибербезопасности, поскольку они считают свои инвестиции в владельца регистрации, а также свои голоса на выборах директоров владельца регистрации».

29 июля 2022 года Департамент финансовых услуг штата Нью-Йорк предложил внести поправки в свои правила, налагающие обязательства на банки и страховые советы. В случае доработки предложенное правило потребует утверждения советом директоров политик кибербезопасности, которые охватывают (как минимум): «(а) информационную безопасность; (б) управление данными и их классификация; и конфиденциальность клиентов».

Ситуация с судебными процессами в США против публичных компаний претерпевает изменения. В статье под названием «Личная ответственность директоров, пренебрегающих кибербезопасностью» один автор заметил, что «в последние месяцы среди юристов истцов начала проявляться тенденция подавать производные иски акционеров, связанные с инцидентами кибербезопасности, — теперь адвокаты все чаще подают иски конкретно на основании сбоев, связанных с обязанностью надзора». Обзор судебных досье выявил более 73 производных исков акционеров, поданных против публичных компаний в США в связи с предполагаемой утечкой данных или нарушением конфиденциальности.

На международном уровне доски все чаще находятся в центре внимания глобальных руководств по кибербезопасности и конфиденциальности. Например, в Национальном центре кибербезопасности Соединенного Королевства (NCSC) есть комплект инструментов кибербезопасности для советов, который содержит «ресурсы, предназначенные для поощрения важных дискуссий по кибербезопасности между советом и его техническими экспертами». Проект закона ЕС о цифровой операционной устойчивости был одобрен Европейским советом и Европейским парламентом и в настоящее время готов к предварительным переговорам. В случае его принятия будут установлены обязательства для «руководящих органов» финансовых учреждений, в том числе требование о том, что «члены руководящего органа должны на регулярной основе проходить специальную подготовку для получения и поддержания в актуальном состоянии достаточных

знаний и навыков для понять и оценить риски ИКТ и их влияние на деятельность финансовой организации».

Датский центр кибербезопасности (CFCS) опубликовал в декабре 2019 года руководство по кибербезопасности для советов директоров, в котором подчеркивается, что, хотя руководство должно взять на себя ведущую роль в определении приоритетов кибербезопасности, на советы директоров возложены обязанности по надзору в отношении оценки рисков, уязвимостей, планов, процессов и готовности, а также а также культура и люди. Австралийская комиссия по ценным бумагам и инвестициям недавно опубликовала ключевые вопросы для совета директоров организации.

Комиссия по финансовым услугам Маврикия направила циркулярное письмо советам директоров компаний, предоставляющих финансовые услуги, в котором напомнила им об их обязанности контролировать деятельность руководства по снижению киберрисков.

Внимание к конфиденциальности и кибербезопасности, вероятно, только возрастет, учитывая огромное количество данных, которые ежедневно генерируются во всем мире. Каждую секунду 127 новых подключенных устройств подключаются к сети, что составляет 11 миллионов новых подключенных устройств ежедневно. По оценкам, в 2022 году мир будет производить и потреблять 94 зеттабайта данных. Чтобы представить это число в перспективе, за одним зеттабайтом стоит 21 ноль.

Таким образом, среда кибербезопасности и конфиденциальности повысила уровень подотчетности в управлении корпоративными рисками и в советах директоров. Важно обеспечить повышенное взаимодействие, чтобы гарантировать, что применение инвестиций соответствует существенным угрозам, влияющим на организации». ***(Dominique Shelton Leipzig, Chris Hetner, Steve Roycroft. Resilience Requires a Modern Path to Board-Level Cyber, Privacy and Data Risk Governance // Nasdaq, Inc. (https://www.nasdaq.com/articles/resilience-requires-a-modern-path-to-board-level-cyber-privacy-and-data-risk-governance). 13.10.2022).***

***

«Поскольку граждане, правительства и предприятия больше, чем когда-либо, зависят от цифровой связи, одной из самых насущных отраслевых проблем в этом десятилетии является кибербезопасность.

Хотя эта проблема уже некоторое время находится в общественном сознании, все еще существует большой разрыв в восприятии между руководителями организаций, которые положительно относятся к своей киберустойчивости, и руководителями службы безопасности, которые этого не делают. Реальность такова, что киберпреступность не показывает никаких признаков замедления, создавая риски для всех аспектов общества. В 2021 году количество атак программ-вымогателей выросло на 150%, и более 80% экспертов говорят, что этот рост теперь угрожает общественной безопасности. Эти статистические данные демонстрируют серьезность и распространенность киберпреступности сегодня. Вопрос заключается в том, что, поскольку мы сосредоточены на глобальном восстановлении и новой эре экономического роста, как нам защититься от киберугроз?

В последние месяцы мы стали свидетелями беспрецедентного внимания политики к угрозе кибератак и устойчивости к цифровым технологиям благодаря тому, что они были отмечены в Отчете о глобальных рисках ВЭФ за 2022 год и коммюнике G7, в котором было зафиксировано официальное соглашение правительств «работать вместе для обмена опытом и минимизации киберугроз». риски». Для того, чтобы воплотить в жизнь амбициозные проекты по охвату цифровыми технологиями, устойчивости, улучшению показателей здоровья, обороне и многому другому для экономики завтрашнего дня; киберустойчивость является ключевым строительным блоком и средством реализации.

Негативные финансовые последствия, связанные с киберпреступностью, носят сейсмический характер и не могут быть устойчивыми для экономики в долгосрочной перспективе. Ни для кого не секрет, что передовые технологии, такие как искусственный интеллект (ИИ), машинное обучение (МО) и Интернет вещей, являются ключевыми строительными блоками для будущего прогресса, но, возможно, по иронии судьбы, именно эти технологии могут открыть новые возможности для киберпреступников. Конечной задачей будет обеспечение безопасности таких технологий и обеспечение более устойчивых и долгосрочных решений угроз, исходящих от киберпреступников. Экономическая перебалансировка будет справедливой только в том случае, если эти инструменты будут доступны для всех организаций и предприятий. Чтобы воплотить это видение в жизнь, потребность в сотрудничестве и поддержке между государственным и частным секторами как никогда актуальна.

Киберподдержка малого и среднего бизнеса жизненно важна для экономики в целом

Малые и средние предприятия (МСП) составляют основу местной экономики, но при этом подвержены высокому риску. МСП рассматриваются как ключевой аспект торговли и логистики, партнерских сетей и цифровых экосистем, однако все чаще становятся объектом кибератак. Исследования показывают, что 43% кибератак совершаются против малого бизнеса, по сравнению с 18% всего несколько лет назад. Примечательно, что недавние отчеты WEF показывают, что 88% респондентов обеспокоены киберустойчивостью малых и средних предприятий в их экосистеме.

Крайне важно, чтобы мы работали над поддержкой и защитой таких предприятий, особенно когда мы стремимся построить более устойчивые и сбалансированные общества. МСП, в отличие от других предприятий, часто нуждаются и имеют право на большую государственную поддержку и поддержку. Правительства, которые признают МСП неотъемлемой частью действительно процветающего общества, расширят возможности и обеспечат наибольший экономический прогресс. Помощь этим небольшим организациям в защите от постоянно растущей угрозы кибербезопасности должна стать приоритетом для специалистов по стратегии восстановления в государственном секторе на ближайшие месяцы и годы.

Сейчас как никогда важно, чтобы инфраструктура государственного сектора повышала устойчивость бизнеса, помогая выявлять, защищать, обнаруживать кибератаки, реагировать на них и восстанавливаться после них, а также обеспечивать быстрый возврат к полноценной работе. Даже при наличии надежной киберзащиты

компании не могут избежать всех киберкатастроф и их неблагоприятного воздействия на данные, конфиденциальность и доверие.

Поэтому ключевой задачей должна быть разработка стратегии киберустойчивости, которая может предвидеть и быстро восстанавливаться после значительных сбоев. Настоящим испытанием должно стать то, насколько быстро и беспрепятственно организации смогут вернуться к «обычному бизнесу». Одним из важнейших компонентов такой устойчивости является создание и проведение тщательных учебных мероприятий по кибербезопасности среди сотрудников. Это не только готовит сотрудников к выявлению рисков и соблазнов безопасности, но также повышает осведомленность и усиливает потребность в командной работе, навыках и сотрудничестве во всей организации.

Передовые технологические решения являются движущей силой цифровой трансформации. Они предлагают всем нам яркое и захватывающее цифровое будущее. Однако расширенные возможности также создают новые проблемы кибербезопасности, предоставляя киберпреступникам больше возможностей отключить критически важную инфраструктуру и вызвать огромные потрясения на уровне общества. Кибербезопасность должна быть в центре внимания лидеров государственного сектора и бизнеса. Комплексная стратегия кибербезопасности, которая работает совместно с правительствами и отраслью, является ключевым компонентом восстановления предприятий, национальной экономики и граждан во всем мире после пандемии…». ***(Mohammed Amin. Cybersecurity can turbocharge the economy // World Wide Worx (https://gadget.co.za/cybersecurity1/). 24.10.2022).***

***

«Кибербезопасность, возможно, даже важнее, чем замки, сейфы и стены для защиты современного бизнеса. Об этом сообщили члены Специальной группы по кибербезопасности (SIGCyber) Южноафриканского института практиков в области информационных технологий (IITPSA).

В заявлении, посвященном международному Месяцу осведомленности о кибербезопасности, который проводится каждый октябрь, члены IITPSA SIGCyber отметили, что интеллектуальная собственность, данные и системы для бизнеса имеют значительную ценность. Это делает их мишенью для киберпреступников.

По их словам, для борьбы с риском киберпреступности киберпреступность должна быть главным приоритетом, и необходимы дополнительные кампании по развитию навыков и повышению осведомленности.

Брайан Бакстер, CRO в Wolfpack Information Risk, говорит: «Ключевые активы для бизнеса известны как их «драгоценности короны». Это ценные активы, компрометация которых вызовет наибольшие сбои в бизнесе. Системы и данные информационных технологий составляют значительную часть драгоценностей короны организации. Это могут быть коммерческая тайна, интеллектуальная собственность, данные компании или клиента, а также операционные и финансовые системы».

«Все ценное привлекает внимание преступников, и киберпространство не исключение. Организованная киберпреступность представляет собой самую большую угрозу и является прибыльным и растущим бизнесом. Распространенными

угрозами являются программы-вымогатели, утечки данных, вредоносное ПО и фишинг.

Многие организации имеют основы кибербезопасности, но им не хватает формальных рамок для управления киберрисками и их снижения. Некоторые оставляют ключевые области без внимания, что означает, что «киберврата» остаются широко открытыми, что делает их привлекательной мишенью», — говорит Бакстер.

Он отмечает, что затраты на восстановление после физических или кибер-инцидентов могут быть намного выше, чем затраты на предотвращение таких событий. Поскольку потери из-за утечки данных могут исчисляться миллионами, многие затраты поддаются количественной оценке, но долгосрочный ущерб репутации и доверию клиентов или акционеров оценить труднее.

«Реальные угрозы, такие как кража со взломом, вандализм, пожар и наводнение, хорошо изучены. Деньги тратятся на заборы, сигнализацию, охрану, обнаружение и тушение пожаров для защиты физических активов. Такую же должную осмотрительность необходимо применять для защиты ценных виртуальных драгоценностей короны», — говорит Бакстер.

Бакстер говорит, что все организации должны сделать кибербезопасность своим бизнес - приоритетом. «Необходимо провести оценку киберриска, чтобы определить основные состязательные угрозы для драгоценностей короны. Необходимо внедрить соответствующие меры контроля и постоянно контролировать их эффективность», — советует он.

«Это обеспечит удержание и доверие клиентов, продемонстрировав, что вы цените их бизнес и данные. Это обеспечит устойчивость операций, финансовую стабильность и защитит интересы акционеров».

Приоритет кибербезопасности

Профессор Линн Футчер из Университета Нельсона Манделы, Школы ИТ, Центра исследований в области информации и кибербезопасности, говорит, что кибербезопасность больше нельзя считать второстепенной задачей, которую нужно решать после того, как будут выполнены другие более высокие приоритеты.

Она говорит: «Новые и развивающиеся угрозы кибербезопасности требуют изменения мышления каждого. Слишком часто мы слышим, как люди перекладывают ответственность на других, говоря: «кибербезопасность не входит в мои обязанности, это техническая проблема», «хакеры не нацелены на малый и средний бизнес», «у нас есть надежные пароли и программное обеспечение для защиты от вирусов для защиты нас от утечки данных», «мы соблюдаем отраслевые правила, поэтому мы в безопасности», «моя личная информация представляет ценность только для меня — никому другому она не понадобится».

Профессор Футчер предупреждает: «Всего один инцидент кибербезопасности может иметь разрушительные последствия, будь то финансовые, репутационные или связанные с конфиденциальностью. Рост киберпреступности вызывает растущую озабоченность организаций, правительств и общества в целом, усугубляемую беспрецедентным дефицитом навыков кибербезопасности, который существует как во всем мире, так и в Южной Африке. Этот пробел в навыках кибербезопасности можно эффективно устранить только совместными усилиями всех участников,

включая отдельных лиц, научные круги, организации и правительства по всему миру».

По ее словам, ведущие организации как на местном, так и на международном уровне могут сыграть ключевую роль в объединении этих ролевых игроков для решения вопросов кибербезопасности и связанных с этим проблем.

«Эти организации включают Международную федерацию обработки информации (IFIP), Ассоциацию вычислительной техники (ACM), Ассоциацию аудита и контроля информационных систем (ISACA) и IITPSA, и это лишь некоторые из них. Поэтому для нас как ИТ-специалистов важно взаимодействовать с этими организациями и играть свою роль в решении многих проблем кибербезопасности в Южной Африке».

От самого слабого звена до человеческого брандмауэра

Профессор Керри-Линн Томсон, также из Университета Нельсона Манделы, Школы ИТ, Центра исследований в области информации и кибербезопасности Школы ИТ Университета Нельсона Манделы, говорит, что, хотя людей часто называют «самым слабым звеном» в системе безопасности цепочки, можно утверждать, что их следует рассматривать как неотъемлемую часть защиты от кибербезопасности — человеческий брандмауэр — посредством культивирования культуры кибербезопасности.

Она отмечает, что в 2015 году была предложена Национальная концепция кибербезопасности Южной Африки, в которой говорится: «Для эффективного решения вопросов кибербезопасности разумно, чтобы гражданское общество, правительство и частный сектор сыграли свою роль в обеспечении культуры кибербезопасности в Южной Африке. Критически важным для этого является развитие культуры кибербезопасности, в которой игроки понимают риски серфинга в киберпространстве».

Профессор Томсон говорит: «Для создания этой социальной культуры кибербезопасности жизненно важно, чтобы отдельные пользователи технологий знали о кибербезопасности и обладали навыками, необходимыми для безопасного поведения и защиты себя и других в сети.

Чтобы заложить основу для этого, необходимо продвигать программы и кампании по повышению осведомленности о кибербезопасности для всех людей, выходящих в интернет, независимо от их возраста. Однако эти кампании по повышению осведомленности о кибербезопасности должны быть не только предоставлением информации, но и должны быть адаптированы к возрасту и нацелены на конкретные угрозы для различных возрастных групп. Например, киберзапугивание для детей младшего возраста по сравнению с кражей личных данных и финансовым мошенничеством для взрослых».

Она добавляет: «Эти кампании по повышению осведомленности о кибербезопасности должны опираться на поведенческие теории, такие как теория социального обучения и социокультурная теория, вместе с педагогически обоснованными образовательными принципами в попытке воплотить осведомленность в действиях. Это делает подход и направление развития социальной культуры кибербезопасности действительно междисциплинарными».

Преодоление разрыва в навыках кибербезопасности за счет сотрудничества

Доктор Мафувафуване, руководитель практики по решениям и стратегии безопасности в Logicalis SA, считает, что развитие навыков и обучение необходимы для борьбы с растущей эпидемией киберпреступности.

«Нет никаких сомнений в том, что кибербезопасность является обязанностью каждого. Технологии изменили почти все аспекты нашей жизни. По мере того, как мы продолжаем охватывать революцию 4IR, теперь мы контролируем наш домашний Интернет вещей (IoT) с помощью смартфонов или голоса. То, как мы общаемся, учимся и работаем, построено на сложных технологиях. Тем временем правительство продолжает внедрять концепцию умного города, которая делает город потрясающим и подключенным к беспроводной сети».

«Но задумывались ли вы когда-нибудь о безопасности, необходимой для защиты всего, от умного дома до умного города, от кибератак? Индустрия кибербезопасности отчаянно нуждается в людях из всех слоев общества, которые думают о карьере в сфере технологий, но мы должны сначала освоить цифровые навыки, чтобы гарантировать, что никто не останется без внимания», — говорит Мафувафуване.

«Общественность все еще пытается понять быстро развивающийся цифровой мир. Кому-то трудно перестраховаться в Интернете, если у него нет полного понимания того, как все связано. Отсутствие у них понимания того, как лучше всего использовать технологии, делает их уязвимыми перед киберпреступниками», — говорит он.

Борьба с киберпреступностью требует индивидуальной осведомленности и растущей армии специалистов по кибербезопасности, говорит он, отмечая, что Cybersecurity Ventures прогнозирует, что к 2025 году во всем мире будет открыто 3,5 миллиона вакансий в области кибербезопасности, что на 350% больше, чем за восемь лет.

Мафувафуване говорит: «Благодаря сотрудничеству между государственным сектором, частным сектором и академическими кругами мы можем создать учебную программу по кибербезопасности, которая состоит из подробных технических материалов и бизнес-стратегии. Курсы могут быть предложены во многих форматах, включая практические лаборатории. Некоторый контент также может быть создан для использования покровителем технологий, чтобы легко помочь обычным гражданам быть кибер-умными во время восстания 4IR». ***(Cybersecurity as important as physical security to protect the 'crown jewels' of business // Engineering News (https://www.engineeringnews.co.za/article/cybersecurity-as-important-as-physical-security-to-protect-the-crown-jewels-of-business-2022-10-20). 20.10.2022).***

***

«Сокращение бюджетов, нехватка персонала и значительные риски, связанные с устаревшими решениями в области кибербезопасности — эти и другие причины объясняют, почему центры управления безопасностью (SOC) и руководители службы безопасности (CSO) рассматривают более эффективные и безопасные системы с оптимизированным количеством инструментов и уровней.

Ключевым моментом для организаций гражданского общества является нахождение золотой середины между крупными решениями в области кибербезопасности и большим количеством специализированных нишевых функций кибербезопасности, которые требуются этим предприятиям.

Ключевые проблемы

В отчетах указывается, что с мая 2022 года технологические стартапы уволили почти 27 000 сотрудников, однако даже до сегодняшних сокращений бюджета и персонала в секторе кибербезопасности уже существовала хроническая нехватка кадров. Согласно исследованиям, «спрос на специалистов по кибербезопасности продолжает превышать предложение».

Недостаток персонала и навыков имеет ощутимые последствия в сфере кибербезопасности — неправильно настроенные системы, оценка рисков и управление ими, которые либо выполняются в спешке, либо пропускаются, медленное время восстановления, оставляющее системы незащищенными, и неспособность справиться со всеми активными угрозами для сети. Короче говоря, команды SOC все больше недоукомплектованы и перегружены работой — и все это при растущей волне все более изощренных атак.

Кроме того, устаревшие устаревшие решения могут сделать сети еще более уязвимыми. Конечно, есть отрасли, в которых старое означает мудрее, но в кибербезопасности устаревшие решения часто не поспевают за меняющимся ландшафтом угроз и не могут быть легко интегрированы с обновленными инструментами. Кроме того, они часто имеют сложные процессы настройки и обслуживания, которые делают управление, исправления или обновления сложными и непрактичными. Согласно отчетам, на незакрытые уязвимости и рискованные сервисы приходится 82% успешных атак.

Текущий ландшафт угроз только растет. Эра гибридной работы побудила предприятия принять все большее количество SaaS и веб-инструментов для устранения последствий децентрализованной рабочей среды — приложений для обмена сообщениями, обмена файлами, CRM и т. д. Как показали недавние взломы Google Drive и Dropbox, быстро растет число новых векторов атак, которые могут использовать злоумышленники. Эта тенденция, вероятно, сохранится только по мере разработки новых SaaS и веб-инструментов для оптимизации современного рабочего места, а политики удаленной работы дают сотрудникам возможность доступа к конфиденциальным приложениям с неуправляемых и сторонних устройств. Короче говоря, многие компании гораздо более уязвимы, чем они думают.

Большая палатка против ниши

Недоукомплектованные и перегруженные SOC-команды теперь сталкиваются с новым препятствием: перегрузкой системы. По мере того, как кибератаки становятся все более изощренными и частыми, количество инструментов киберзащиты, на которые полагаются специалисты по безопасности, постоянно растет. Отчеты показывают, что некоторые организации используют в среднем до 45 различных инструментов для обеспечения безопасности своих сетей.

Эти узкоспециализированные инструменты безопасности могут быть эффективными в борьбе с растущими изощренными киберугрозами, но их огромный объем сам по себе является проблемой, поскольку ими часто сложно управлять;

заставляя аналитиков тратить время на переключение между инструментами. Это приводит к задержке анализа инцидентов и обслуживания системы безопасности. Кроме того, разрозненный характер этих решений означает, что аналитики не могут получить целостное представление о проблемах или быстро реагировать на нарушения. Те, кто использовал более 50 инструментов, оценили себя как на 8% менее способных обнаружить атаку и на 7% менее быстро реагирующих на попытки ее устранения. Из-за нехватки персонала SOC также трудно сохранить опыт, необходимый для эффективного использования этих многочисленных систем.

Тем не менее, устаревшие решения для кибербезопасности не обязательно являются лучшей альтернативой. Может показаться выгодным иметь множество инструментов защиты на одной платформе, но точные ответы нишевых решений на растущий ландшафт угроз могут быть потеряны. Другими словами, эти универсальные решения не всегда могут справиться с растущей сложностью угроз. 40% специалистов по кибербезопасности заявили, что их текущая стратегия кибербезопасности, скорее всего, устареет всего через два года, а 37% заявили, что это произойдет через три года.

Середина земли

Чтобы эффективно бороться с вызовами кибербезопасности следующего поколения, ОГО необходимо создать эффективную золотую середину. Эта потребность отрасли только усугубляется текущим экономическим спадом, который вынуждает многие SOC сокращать бюджеты, предлагая наиболее эффективные решения для защиты уязвимых систем.

Хитрость для поставщиков кибербезопасности будет заключаться в том, чтобы предлагать сбалансированное количество решений, которые эффективно охватывают ряд векторов угроз — не настолько много, чтобы они потеряли фокус, но достаточно, чтобы клиенты могли меньше полагаться на громоздкое количество продуктов безопасности. В долгосрочной перспективе более оптимизированные системы кибербезопасности SaaS могут не только облегчить командам SOC наем, обучение и удержание своих команд, но и фактически снизить их рабочую нагрузку. Поставщики также должны стремиться к созданию простых в развертывании и управлении интегрированных решений, которые точно вписываются в существующие системы клиентов и беспрепятственно взаимодействуют с их стандартными операционными системами и бизнес-процессами. Это гарантирует, что как члены группы безопасности, так и общий персонал могут легко и без проблем использовать преимущества. В том же духе, поставщики должны предоставлять инструменты и услуги, которые укрепляют возможности команды SOC, предлагая спасательный круг для групп, которые недоукомплектованы и перегружены работой. Они могут поддерживаться автоматизированными платформами на основе машинного обучения и искусственного интеллекта и реальными экспертами по кибербезопасности в управляемой службе SOC, чтобы упростить анализ и устранение волны вредоносной активности, угрожающей компаниям.

В связи с нехваткой знаний в отрасли и сегодняшними экономическими проблемами необходимо ускорить внедрение современных оптимизированных и упорядоченных наборов решений для кибербезопасности; однако в дальнейшем они

наиболее целесообразны для эффективных, действенных и надежных команд SOC». ***(Motti Elloul. Why CSOs Are Decluttering Their Cybersecurity Toolboxes // Cyber Defense Media Group (https://www.cyberdefensemagazine.com/why-csos/). 23.10.2022).***

***

«Октябрь является всемирно признанным месяцем осведомленности о кибербезопасности. Это происходит в то время, когда ежедневно объявляется о новых утечках данных и краже личных данных. Что касается бизнеса, то 76% организаций сообщают, что за последние два года они подвергались атакам программ-вымогателей.

Тема 2022 года: «Видишь себя в киберпространстве? Это попытка привлечь больше людей к профессиям ИТ-безопасности. Но что это означает на практике?

Чтобы получить представление, Digital Journal поговорил с Дэвидом Антелизом, старшим техническим директором Skybox Security.

По словам Антелиз, поддержание кибербезопасности в воображении общественности необходимо для защиты услуг и организаций. Период осведомленности о кибербезопасности 200 – ключевой способ сделать это.

Антелиз говорит: «Месяц осведомленности о кибербезопасности в октябре этого года служит напоминанием о том, что надежда уже на горизонте, несмотря на то, как быстро развиваются субъекты угроз. Согласно анализу угроз Skybox Research Lab, в 2021 году было опубликовано 20 175 новых уязвимостей по сравнению с 18 341 в 2020 году».

Эти цифры вызывают тревогу. Антелиз говорит: «Это наибольшее количество уязвимостей, о которых когда-либо сообщалось за один год, и самый значительный рост по сравнению с прошлым годом с 2018 года. Первоначальные исследования показывают, что 2022 год также приведет к значительному увеличению числа уязвимостей, особенно тех, которые влияют на критически важную инфраструктуру».

Для решения этих проблем нужны новые подходы. Как отмечает Антелиз: «Мир видел, как традиционный подход к кибербезопасности, основанный на точечных продуктах, непреднамеренно создавал разрозненность и опасные пробелы в видимости. Злоумышленники знают, что многие организации отстают от установки исправлений и по-прежнему полагаются на традиционные подходы к управлению уязвимостями, основанные на оценках CVSS, поэтому они научились использовать уязвимости, оцененные как менее критические, для проведения своих атак».

Что нужно учитывать, Антелиз рекомендует: «Сегодня организации должны начать развиваться в направлении радикально более гибкой архитектуры безопасности. Чтобы повысить общую эффективность кибербезопасности, зрелые организации используют расширенную приоритизацию на основе рисков, которая включает анализ угроз, информацию об активах и моделирование, чтобы определить, что действительно подвержено атаке».

В красноречивом заключительном комментарии Антелиз заявляет: «На самом деле, почти половина организаций, в которых не было нарушений в 2021 году, использовали подход, основанный на оценке рисков.

Напротив, 48% организаций, в которых не было нарушений, применяли подход, основанный на оценке рисков. Это представляет собой ситуацию большей зрелости в областях видимости и контекста поверхности атаки, моделирования атаки, анализа подверженности, оценки риска, оценки уязвимости». ***(Tim Sandle. New approaches to cybersecurity are the only way out of the security wormhole // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/tech-science/new-approaches-to-cybersecurity-are-the-only-way-out-of-the-security-wormhole/article). 24.10.2022).***

***

«Нулевое доверие представляет собой самый большой сдвиг в отрасли за последнее время. Gartner ожидает, что расходы на нулевое доверие увеличатся более чем вдвое до 2025 года и составят 1,674 миллиарда долларов. Правительство США также обязало все федеральные агентства перейти к нулевому доверию к 2024 году. Национальному институту стандартов и технологий (NIST) также было поручено разработать сценарий для частного сектора.

Концепция нулевого доверия проста: ничему не доверяйте, все проверяйте. Хотя принцип нулевого доверия представляет собой совершенно новую философию для отрасли, специалисты по безопасности обнаружили, что его развертывание очень сложно, а простых готовых решений не существует. Раньше организации выстраивали защитный периметр вокруг своей сети, проверяли все, что проходит, а затем предоставляли доступ, привилегии и неявное доверие ко всему, что происходит внутри сети. Отрасли необходимо перенастроить все существующие инструменты, чтобы включить эту новую архитектуру безопасности.

Традиционных периметров безопасности, таких как внутренние и внешние, доверенные и недоверенные, уже недостаточно для отражения сегодняшних все более профессиональных и хорошо организованных киберпреступников. Вместо того, чтобы предполагать, что средства защиты организации будут отражать все атаки, нулевой уровень доверия признает, что атаки всегда будут проходить внутри защитного периметра. Чтобы установить действительно современную кибербезопасность, организациям необходимо расширить свои традиционные периметры безопасности и шлюзы. Мы должны заменить их системами, которые требуют аутентификации перед предоставлением любого уровня доступа, за которым следует тщательный контроль доступа даже для аутентифицированных пользователей. Поскольку атаки могут скрываться где угодно, маскируясь под что угодно, группы безопасности должны строго охранять и редко предоставлять доступ.

Плюсы нулевого доверия легко сложить. По данным IBM, нулевой уровень доверия снижает стоимость утечки данных на 43%. Illumio также сообщает, что сегментация с нулевым доверием экономит почти 40 часов в неделю и предотвращает в среднем пять киберкатастроф в год в типичной организации.

Нулевое доверие зависит от непрерывной проверки; мы никогда не берем на себя личность и никогда не предоставляем автоматический доступ. Прежде чем кому-либо будет предоставлен доступ к чему-либо (например, приложениям, данным, сетям), необходимо пройти проверку. Если исходить из того, что некоторые

атаки будут успешными, устранение нарушений становится важнейшей опорой кибербезопасности. Такие меры, как сегментация сети и доступ с минимальными привилегиями, предотвращают распространение атак и ограничивают ущерб одной областью.

Нулевое доверие позволяет организациям обнаруживать реальные и существующие угрозы при их появлении, а также использует аналитику угроз для предупреждения о входящих и запланированных атаках в режиме реального времени. Предполагается, что некоторые атаки настолько искусно спланированы, что они неизбежно заставят организации и их консультантов выделить больше ресурсов для оперативной разведки угроз. Однако немногие организации среднего размера имеют внутренние ресурсы, необходимые для мониторинга входящих и будущих угроз. Без этой автоматизированной аналитики угроз, поддерживаемой глобальной командой аналитиков, компании становятся все более уязвимыми для целого ряда угроз, таких как хорошо организованные и профессиональные атаки программ-вымогателей.

Малым и средним организациям необходимо перейти к нулевому доверию, поскольку существующие решения в области кибербезопасности, разработанные с учетом потребностей крупных компаний, оказались малопригодными. Недавнее исследование показало, что компании с небольшими группами безопасности продолжают сталкиваться с рядом уникальных проблем, подвергающих эти организации большему риску, чем крупные предприятия; 94 % говорят, что у них есть барьеры в поддержании уровня безопасности из-за нехватки квалифицированного персонала службы безопасности (40 %), чрезмерного ручного анализа (37 %) и все более удаленной рабочей силы (37 %).

Но, поскольку это влияет на весь набор защитных инструментов, специалисты по безопасности считают внедрение нулевого доверия сложным. Им может потребоваться добавить инструменты для сегментации, управления идентификацией и доступом, мониторинга сети и даже обнаружения и реагирования. Им также потребуется перенастроить существующие инструменты, чтобы они отражали новую архитектуру безопасности. Добавление расширенного обнаружения и реагирования (XDR) также может стать важной частью реализации нулевого доверия. Некоторые решения XDR предлагают анализ поведения пользователей, управление уязвимостями и аналитику угроз.

Чтобы заставить работать принцип нулевого доверия, многим организациям потребуется провести капитальный ремонт всего отдела кибербезопасности, поскольку нынешняя команда безопасности может не иметь навыков, опыта или персонала. И им может потребоваться нанять дополнительный персонал или услуги. В течение любого переходного периода группы безопасности должны практиковать строго контролируемое управление изменениями, поскольку злоумышленники никуда не денутся. Компании, особенно те, у которых ограниченные ресурсы кибербезопасности, а также федеральные агентства, испытывают все более острую потребность во внедрении нулевого доверия. Но его эффективность как в краткосрочной, так и в среднесрочной перспективе будет зависеть от высокого уровня планирования и управления». ***(Bruno Darmon. Zero-trust has changed***

cybersecurity forever // SC Media (https://www.scmagazine.com/perspective/zero-trust/zero-trust-has-changed-cybersecurity-forever%EF%BF%BC). 31.10.2022).

***

«Раньше многие организации нажимали кнопку отключения звука всякий раз, когда возникали дискуссии о кибербезопасности, но это молчание нарушается все чаще, поскольку все больше предприятий становятся жертвами хакеров и испытывают последствия, которые сказываются на их прибыли таким образом, что они требуют делиться информацией с регулирующими органами. Но в правила Комиссии по ценным бумагам и биржам вносятся изменения, которые принесут новые стандарты того, как сообщать о позиции безопасности в большинстве предприятий.

В начале 2022 года SEC выступила с предложением внести поправки в свои правила кибербезопасности, в которых изложены новые способы сообщения и раскрытия инцидентов безопасности. SEC утверждает, что хочет лучше информировать инвесторов о стратегии управления рисками организаций и киберуправлении, но для некоторых организаций это предложение может показаться еще одной нормативной нагрузкой.

Чтобы понять 129-страничное предложение, полезно разбить его на три основных аспекта, которые оно охватывает:

● Управление. Правила требуют прозрачности в отношении того, как организации инвестируют средства, и уделяют кибербезопасности приоритетное внимание среди своих бизнес-функций. Это требует раскрытия опыта совета директоров в области кибербезопасности, чтобы инвесторы могли сделать свои собственные выводы об уровне приоритетности кибербезопасности в этой организации и о способности совета давать рекомендации ИТ-директору, директору по информационной безопасности и другим заинтересованным сторонам в области безопасности.

● Управление рисками: сегодня у инвесторов нет точки отсчета для определения киберриска в качестве точки данных при оценке компаний, в которые следует инвестировать, поэтому требование сообщать о стратегии и управлении рисками кибербезопасности может повысить ценность тех компаний, у которых есть четкая политика и процедуры в отношении кибербезопасности. управление рисками. Компании, которые отстают, должны инвестировать в улучшение своей программы управления киберрисками.

● Инциденты кибербезопасности: в соответствии с новыми правилами организации должны будут сообщать в SEC об инцидентах кибербезопасности, которые имеют существенное значение для их операционных результатов, и предлагать обновленную информацию о предыдущих инцидентах. Сообщение о взломе может быть риском для репутации компании, курса акций и многого другого, но то, как оно обрабатывается, также может помочь этим факторам. В настоящее время сообщается о многих инцидентах, даже если организация хочет держать их в секрете, поэтому это требование не слишком обременительно, но становится упреждающей задачей, в которую компании должны инвестировать, чтобы убедиться, что их стратегия раскрытия информации готова на всякий случай.

Несколько простых шагов помогут вашей организации подготовиться к новым требованиям или подготовиться к следующему квартальному отчету:

● Оценка приоритета кибербезопасности. Новые требования призваны дать инвесторам представление о том, какое место кибербезопасность занимает в списке дел организации. Посмотрите на состав доски, чтобы увидеть, где находится опыт кибербезопасности, или есть ли необходимость подготовиться к новым требованиям. Кроме того, инвестиции в этот опыт повышают ценность за счет повышения устойчивости организации.

● Оцените свой подход к управлению рисками: узнайте, какие политики и процедуры кибербезопасности регулируют рабочие процессы, потому что они не только хороши для снижения рисков, но и показывают, что постоянное совершенствование станет показателем, который захотят увидеть инвесторы. Знание действующих политик и процедур кибербезопасности и демонстрация инвестиций, направленных на минимизацию рисков, свидетельствует о приоритете кибербезопасности в организации.

● Оцените свою программу реагирования на инциденты. Как известно, есть два типа организаций — те, которые были взломаны, и те, которые еще не знают об этом. Имея это в виду, организации могут инвестировать в создание программы упреждающего реагирования на инциденты. Наличие плана со сценариями для различных случаев, а также подготовленных заявлений о раскрытии информации может облегчить кризисное управление, и выполнение этого до требования SEC поможет организации лучше реагировать, когда инцидент действительно происходит.

● Установите уровень уверенности. Одним из ключей к правилам, предложенным SEC, является возможность количественной оценки успеха стратегии кибербезопасности организации — ее управления рисками, реагирования на инциденты и общего руководства. Инвестиции в инструменты и решения, которые могут дать некоторую уверенность в уровне выполнения управления рисками, являются лучшим доказательством для инвесторов, чем письменные политики или рабочие журналы инцидентов.

Инциденты, связанные с безопасностью, являются сегодня фактом деловой жизни, но реакция организации на инциденты и ее обработка раскрытия информации могут иметь большое значение. Новые требования SEC закрепляют на бумаге то, во что многие компании, как государственные, так и частные, уже должны были инвестировать». ***(Gordon Lawson. How to Prepare for New SEC Cybersecurity Disclosure Requirements // Wired Business Media (https://www.securityweek.com/how-prepare-new-sec-cybersecurity-disclosure-requirements). 31.10.2022).***

***

«Сегодняшние лидеры в области безопасности сталкиваются с растущими угрозами кибербезопасности со всех сторон, и с каждым годом это обходится им все дороже из-за сложности, облачных и несоответствующих требованиям. Согласно Отчету о затратах на утечку данных за 2022 год, затраты на утечку данных в Индии выросли до 176 миллионов в 2022 году, что на 25% больше, чем за последние два года. Выявление и пресечение этих утечек занимает больше

времени. Слишком много угроз. Слишком много разрозненных инструментов кибербезопасности. Слишком мало специалистов по кибербезопасности. Ясно одно: сегодняшние лидеры в области кибербезопасности должны не только помочь остановить сегодняшние угрозы, но и опережать завтрашние.

За последние два года методы ведения бизнеса и управления командами изменились. Все ваши данные, все ваши приложения и все ваши пользователи находятся повсюду. Компании все больше полагаются на облачные технологии. Это сделало традиционный подход к безопасности, основанный на разрешительных документах, неэффективным. После запуска 5G в Индии и вариантов использования и реализации, которые он принесет; пользователи должны быть готовы к возможности непредвиденных угроз и рисков кибербезопасности. Ситуация усугубляется по мере того, как ИТ-среды становятся все более рассредоточенными — с распространением устройств, пользователей и технологий — директора по информационной безопасности ссылаются на такие проблемы, как невозможность сократить разрозненность, отсутствие контроля над активами приложений и данных, а также фрагментированность инфраструктуры безопасности. Директорам по информационной безопасности необходимо принять единый подход, чтобы добиться большей прозрачности,

Этот месяц осведомленности о кибербезопасности — отличная возможность для организаций переоценить свои процессы кибербезопасности и укрепить свою цифровую защиту. От банковского дела до производства и за его пределами экстремальная цифровизация ускорила слияние виртуального и физического в каждой отрасли и вызвала полное переосмысление цифрового доверия. Чтобы построить более устойчивое будущее, предприятия начинают заглядывать внутрь себя, выявлять и устранять бреши в безопасности.

Подготовка к следующей волне угроз кибербезопасности

Поскольку угрозы кибербезопасности растут с каждым днем, компании не могут позволить себе не инвестировать в надежный процесс кибербезопасности, включая мониторинг, анализ угроз и упреждающее тестирование безопасности. Чтобы подготовиться к новой волне угроз кибербезопасности и оставаться на шаг впереди, ниже приведены некоторые способы, которыми компании могут подготовиться.

Переведите свою защиту в наступление с нулевым доверием. Сегодня многие службы безопасности строят сети на основе «меньшего доверия», а не нулевого доверия. Чтобы решить эту проблему, нам нужно смотреть на сети через призму злоумышленника и вести себя так, как если бы наша среда была скомпрометирована и подверглась атаке. Основное внимание следует уделять обнаружению, поиску угроз, тщательному изучению связей и отношений, а также внедрению и использованию искусственного интеллекта и аналитики.

Практикуйте готовность: то, как ваша команда реагирует в критический момент, может иметь решающее значение для количества времени и денег, потерянных в ответ на кибератаку. Разрабатывайте сценарии, регулярно тестируйте их и думайте не только о технических компонентах. Чтобы обеспечить максимальную готовность, симуляционные тесты должны стать стандартной

практикой реагирования на инциденты — сталкиваясь с атаками до того, как они произойдут, мы можем лучше реагировать.

Уменьшите сложность с помощью открытой архитектуры. Для подключения фрагментированных облачных сред компаниям следует применять открытый и комплексный подход к обеспечению безопасности. Платформы безопасности, основанные на открытых технологиях и обеспечивающие тесную интеграцию между инструментами, также должны быть рассмотрены предприятиями.

Подготовьтесь к квантово-безопасной криптографии: несмотря на то, что технологии стремительно развиваются в направлении квантовых вычислений, наряду с преимуществами, которые они подразумевают, они влияют на кибербезопасность. Квантовые вычисления смогут дестабилизировать даже современную инфраструктуру кибербезопасности. Хотя квантовых вычислений еще нет, квантово-безопасную криптографию лучше всего развертывать при медленной миграции в тандеме с традиционными криптографическими протоколами.

Инвестируйте в автоматизацию, искусственный интеллект и новые технологии: в недавнем исследовании Cost of Data Breach организации, которые полностью внедрили искусственный интеллект и автоматизацию безопасности, сократили расходы в среднем на 3,05 миллиона долларов. Для выявления угроз искусственный интеллект (ИИ) и машинное обучение (МО) могут анализировать модели поведения пользователей и операций.

Получите видимость с точки зрения злоумышленника: постоянно тестируйте средства защиты и проверяйте средства управления против автоматизированной красной команды. Это даст группам безопасности не только представление о том, где злоумышленник может нанести удар, но и доказательство воздействия и ущерба, которые могут возникнуть в случае их нападения. Получайте мгновенную и постоянную информацию о неизвестных и неуправляемых активах, на которые могут нацеливаться хакеры. Расставьте приоритеты по уязвимостям, которые хакеры нанесут первыми.

Киберпреступники всегда будут находить новые способы адаптации и использования технологий, чтобы избежать обнаружения, поэтому предприятиям и правительствам необходимо параллельно строить свою технологическую защиту и армии кибер-воинов. Сегодня полем битвы является кибербезопасность, и независимо от характера бизнеса, которым занимается компания, инвестиции в навыки и технологии в области кибербезопасности — это то, что обеспечит ее выживание.

Подготовка к 2023 году

Поскольку мир все больше полагается на цифровые технологии, актуальность и важность кибербезопасности в 2023 году будет продолжать стремительно расти. Организациям необходимо знать о связанных с ними киберрисках, поскольку они вкладывают большие суммы в технологии, независимо от того, делают ли они это. для инноваций или по необходимости. Вместе с новыми и постоянно меняющимися задачами приходят и экстраординарные возможности. Компании больше не могут отрицать, что кибербезопасность вышла за рамки простого вопроса для специалистов по безопасности и ИТ — теперь это основной бизнес-риск, к которому должна быть привлечена вся компания, чтобы подготовиться к нему и отреагировать

на него. Организации, стремящиеся наиболее эффективно позиционировать себя для следующего технологического развития, должны будут применять неустанный и упреждающий подход к созданию перспективных оборонительных возможностей». ***(Viswanath Ramaswamy. The next wave of cybersecurity threats: Are you ready? // Bennett, Coleman & Co. Ltd. (https://timesofindia.indiatimes.com/blogs/voices/the-next-wave-of-cybersecurity-threats-are-you-ready/). 31.10.2022).***

***

«Кибербезопасность — одна из самых быстрорастущих областей технологий, при этом глобальные расходы увеличиваются на 12–15 % в годовом исчислении. В этом секторе также существует нехватка кадров: по оценкам, глобальная нехватка рабочей силы составляет 3,5 миллиона человек, что сдерживает рост этой отрасли.

Женщины составляют только 24% специалистов по кибербезопасности. Тем не менее, они несут ответственность за наиболее важную работу в этой области, от основания компаний по обеспечению безопасности до определения корпоративной и государственной политики, руководства инициативами DEI и представления себя и своих компаний в советах директоров и глобальных организациях по безопасности.

Поощрение женщин, влияющих на кибербезопасность, может продемонстрировать разным женщинам во всем мире, что у них есть путь к лидерству и успеху в этой захватывающей и расширяющейся области. Поступая таким образом, мы можем двигаться к большей справедливости и вдохновлять еще больше выдающихся женщин, подобных этим, на достижения в этой области, а также наделяя кибербезопасность разнообразными талантами, необходимыми для достижения успеха…» ***(Alaina Percival. Women To Watch In Cybersecurity // Forbes (https://www.forbes.com/sites/alainapercival/2022/10/26/women-to-watch-in-cybersecurity/?sh=3c48486d30e6). 26.10.2022).***

***

«По мере того, как все больше компаний переживают цифровую трансформацию и продолжают хранить информацию о потребителях в облаке, риски кибербезопасности вызывают все большую озабоченность у веб-пользователей, компаний и онлайн-покупателей.

Согласно исследованию приоритетов безопасности Foundry за 2022 год, в котором приняли участие почти 900 опрошенных лидеров безопасности по всему миру, 90% считают, что их организации недостаточно делают для устранения рисков кибербезопасности.

Атаки на кибербезопасность не новы, но хакеры становятся все более изощренными и все чаще атакуют университеты и больницы. крупный бизнес и критическая инфраструктура.

Растущая проблема, с которой сегодня сталкиваются компании, заключается в том, что технологические угрозы развиваются слишком быстро, чтобы сотрудники службы кибербезопасности успевали за ними. Добавьте к этому тот факт, что во многих компаниях не хватает сотрудников в отделах кибербезопасности, и многие предприятия оказываются очень уязвимыми для кибератак.

«Если у вас не хватает персонала, никто не может просматривать каждое предупреждение», — сказал Боб Брэгдон, старший вице-президент и управляющий директор CSO Foundry Worldwide.

Когда дело доходит до борьбы с угрозами безопасности, когда они сталкиваются с такой нехваткой, 45 % ИТ-руководителей полагаются на существующий персонал, который берет на себя больше обязанностей, в то время как 45 % используют технологии автоматизации, а 42 % передают свои функции безопасности на аутсорсинг.

Специалисты по безопасности, опрошенные Foundry, согласились с тем, что автоматизация является ключевым инструментом для улучшения реагирования на инциденты и поддержания квалифицированного персонала службы безопасности. Например, 34% компаний изучают технологию SOAR (Security Orchestration, Automation, and Response), которая сочетает в себе возможности человека и машины для обработки отчетов об инцидентах.

Человеческая ошибка

Foundry обнаружил, что ошибки сотрудников остаются основным фактором, вызывающим опасения в отношении ИТ-безопасности: 34% респондентов заявили, что незлонамеренные ошибки пользователей были основной причиной инцидентов кибербезопасности, хотя в 2021 году этот показатель снизился с 44%. уязвимости системы безопасности (28%), неисправленные уязвимости программного обеспечения (26%) и нарушения цепочки поставок программного обеспечения, на долю которых приходится 17% инцидентов.

Руководителям службы безопасности трудно убедить всю или часть своей организации в серьезности рисков кибербезопасности, и они изо всех сил пытаются найти и удержать подходящих сотрудников службы безопасности для обеспечения безопасности своей организации.

Кроме того, лидеры в области безопасности сообщают, что их организации не вкладывают достаточно средств в технологии, людей или бюджет для надлежащего устранения рисков безопасности, и что вопросы безопасности часто отходят на второй план при разработке приложений. В отчете говорится, что обучение кибербезопасности также отсутствует на всех уровнях персонала.

По данным Foundry, когда дело доходит до выделения денег на кибербезопасность, крупные предприятия тратят около 122 миллионов долларов, а малые предприятия тратят около 16 миллионов долларов, при этом средний годовой бюджет безопасности составляет 65 миллионов долларов.

Заглядывая в будущее, 51% респондентов заявили, что средства защиты конечных точек для ноутбуков, настольных компьютеров и серверов в настоящее время находятся в разработке, чтобы предотвратить будущие риски безопасности. Обучение по вопросам безопасности также находится на повестке дня: 46% респондентов планируют больше инвестировать в обучение.

Более пятой части (22%) лидеров в области безопасности планируют обновить свои существующие технологии, в том числе улучшить многофакторную аутентификацию, а 21% планируют обновить технологии резервного копирования и восстановления данных.

Между тем, 32% изучают технологии нулевого доверия, подход к ИТ-системам, при котором сеть автоматически не доверяет устройству только потому, что оно используется внутри компании. По данным Foundry, более 20% предприятий планируют внедрить технологии нулевого доверия по сравнению с 13% в прошлом году». ***(Jada Jones. Cybersecurity leaders are having a hard time keeping companies secure, and there's no easy solution // ZDNET, A Red Ventures company (https://www.zdnet.com/article/cybersecurity-leaders-are-having-a-hard-time-keeping-companies-secure-and-theres-no-easy-solution/). 06.10.2022).***

***

«Модель зрелости нулевого доверия CISA представляет собой структуру для организаций государственного и частного секторов, предназначенную для усиления усилий по предотвращению несанкционированного доступа к технологической инфраструктуре и информационным ресурсам.

Модель зрелости с нулевым доверием (ZTMM), разработанная Агентством кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности США, является относительно новой и входит в число многих других аналогичных моделей зрелости, касающихся кибербезопасности.

В какой-то момент организациям потребуется проводить аудит кибербезопасности, особенно с учетом того, что CISA ZTMM и другие структуры нулевого доверия набирают обороты по мере того, как организации внедряют методы и рекомендации нулевого доверия, а правительство начинает предписывать использование нулевого доверия.

Почему важны аудиты зрелости кибербезопасности с нулевым доверием

Чтобы поддерживать нулевое доверие, необходимо активно управлять политиками и процедурами. Невыполнение периодических проверок планов и процедур кибербезопасности, а также отсутствие регулярного тестирования этих ресурсов может увеличить риск несанкционированных кибератак.

Аудиты соответствия требованиям нулевого доверия являются важной частью усилий организации по соблюдению моделей нулевого доверия и соответствующих стандартов кибербезопасности. Они обеспечивают объективные гарантии того, что организации имеют политику, процедуры, обученный персонал, образованных сотрудников и поддерживающее высшее руководство. Аудиты также показывают, что организации установили формальные средства контроля для обеспечения соблюдения руководящих принципов и спецификаций. Наконец, аудиты обеспечивают безопасную работу ИТ-инфраструктуры, а если нет, то позволяют быстро выявлять и устранять аномалии.

Контроль нулевого доверия для аудиторских расследований

Документ ZTMM следует семи базовым критериям нулевого доверия, определенным в специальной публикации NIST (SP) 800-207 (2020) «Архитектура нулевого доверия», каждый из которых можно рассматривать как элемент управления. Однако каждый элемент управления может быть расширен до более подробных элементов управления, которые касаются аспектов базовых критериев.

Например, третий критерий гласит: «Доступ к отдельным корпоративным ресурсам предоставляется на основе каждого сеанса». Ниже приведены

дополнительные средства контроля, которые могут поддерживать базовый контроль в рамках аудиторского расследования:

Доступ к ресурсам организации определяется политикой.

Доступ к организационным ресурсам регулируется рядом процедур.

Доступ ко всем ресурсам основан на индивидуальной потребности сотрудника в информации.

Доступ к ресурсам зависит от роли сотрудника в организации.

Доступ к ресурсам предоставляется на основе каждого сеанса, в зависимости от роли сотрудника и необходимости знать.

Завершение сеанса прекращает дальнейший доступ к ресурсам, если не инициирован новый сеанс.

Доступ к ресурсам предоставляется с помощью многоэтапного процесса, включающего идентификатор пользователя и многофакторную аутентификацию (MFA).

До отказа в доступе может быть предпринято не более трех неудачных попыток доступа, и он должен быть восстановлен администратором безопасности.

Пароли доступа пользователей должны обновляться каждые 60 дней.

Методы аутентификации пользователей должны пересматриваться каждые шесть месяцев и обновляться по мере необходимости.

Лучшие практики подготовки к аудиту с нулевым доверием

Наиболее важными элементами подготовки к аудиту являются общая подготовка и документация. Эти шаги включают следующее:

Обеспечить одобрение руководства и финансирование аудита.

Создать аудиторскую группу для взаимодействия с аудиторами.

Оцените возможности и опыт аудиторов с точки зрения аудита вопросов кибербезопасности.

Познакомьтесь с моделью нулевого доверия.

Понимание соответствующих стандартов кибербезопасности и лучших практик.

Подготовьте план аудита.

Защищать печатные и электронные доказательства, включая политики и процедуры; планы кибербезопасности; скриншоты различных функций кибербезопасности; записи различных действий, таких как исправление и обновление правил брандмауэра; и отчеты об испытаниях системы.

Предоставить копии предыдущих оценок, аудитов и других аналитических отчетов.

Обеспечьте рабочее место для аудиторов.

Контрольный список аудита модели зрелости с нулевым доверием CISA

В документе ZTMM приведены подробные сведения о действиях, которые могут выполняться по мере того, как организации развивают свои возможности нулевого доверия на трех конкретных этапах — традиционном, расширенном и оптимальном — с использованием пяти столпов развития нулевого доверия: идентификация, устройство, сеть/среда, приложение. нагрузка и данные.

В следующем контрольном списке представлены общие сведения о предлагаемых средствах контроля аудита и примеры доказательств с

использованием ZTMM в качестве основы. Три этапа и пять столпов встроены в стол». ***(Paul Kirvan. How to conduct a cybersecurity audit based on zero trust // TechTarget (https://www.techtarget.com/searchsecurity/tip/How-to-conduct-a-cybersecurity-audit-based-on-zero-trust). 10.2022).***

***

«Совокупность многих факторов увеличивает вероятность кибератаки на вашу цепочку поставок. Поскольку количество векторов атак резко возросло, киберпреступники, воюющие правительства и другие субъекты угроз стали более активно атаковать цепочки поставок. Эти киберугрозы становятся более серьезными, когда цепочки поставок уже находятся в кризисе — в отчете, опубликованном Accenture за май 2022 года, говорится, что сбои в цепочках поставок привели к потерям в размере 112 миллиардов евро (0,9 процента ВВП) только в еврозоне. В зависимости от последствий войны в Украине эти потери могут возрасти до 920 миллиардов евро (7,7 процента ВВП) в следующем году.

Хуже того, масштабная цифровая трансформация, дающая сектору цепочки поставок инструменты, позволяющие лучше справляться с подрывной нормой, предоставляет киберпреступникам все больше возможностей для проникновения в компании. Вот почему платформы кибербезопасности цепочки поставок должны идти в ногу с развивающимися киберугрозами и обеспечивать постоянное покрытие всех векторов атак. Нет лучшего ресурса для создания такого типа устойчивости, чем рабочая сила, осведомленная о кибербезопасности, включая каждого сотрудника.

Кибербезопасность необходима для устойчивости цепочки поставок

Согласно опросу руководителей цепочек поставок, проведенному McKinsey, 93% говорят, что предпринимают шаги, чтобы сделать свои цепочки поставок более устойчивыми. И тем не менее, по данным Gartner, всего 21% руководителей цепочек поставок считают свои сети «очень устойчивыми».

Компании могут улучшить этот статус-кво, обеспечив защиту каждого звена цепочки поставок от киберугроз, что означает внедрение комплексного решения по повышению осведомленности о кибербезопасности в масштабах всей компании и сотрудничество с партнерами, чтобы сделать то же самое.

Поскольку современные цепочки поставок сильно взаимосвязаны, угроза одному партнеру (например, стороннему поставщику) представляет угрозу для всей цепочки поставок. Это одна из причин, по которой 90 % специалистов по цепочкам поставок считают, что технология обеспечения прозрачности имеет первостепенное значение — компаниям необходимо постоянно знать, что происходит в цепочке поставок, и это особенно важно, когда речь идет о состоянии их кибербезопасности.

Цепочки поставок сталкиваются с большим количеством киберрисков, чем когда-либо

Недавний отчет NCC Group показал, что количество кибератак на цепочки поставок увеличилось на 51 процент в период с июля по декабрь 2021 года, при этом менее трети лиц, принимающих решения в области кибербезопасности, заявили, что они «полностью уверены», что смогут быстро и эффективно отреагировать на одну из таких атак. Компании четко осознают, что это неприемлемый уровень риска.

Респонденты заявили, что планируют увеличить свои бюджеты на кибербезопасность в среднем на 10 процентов в 2022 году. Согласно отчету Verizon о расследовании утечек данных за 2022 год (DBIR), атаки на цепочки поставок «резко увеличились» по сравнению с предыдущим годом. «От широко разрекламированных атак на критическую инфраструктуру до массовых нарушений цепочек поставок, — говорится в отчете, — финансово мотивированные преступники и гнусные государственные деятели редко, если вообще когда-либо, выходят из положения так, как они делали это в течение последних 12 месяцев».

Глобальная интеграция цепочек поставок привела к чрезвычайно высокому уровню риска для третьих сторон. Как поясняет Национальный институт стандартов и технологий (NIST), одними из основных рисков цепочки поставок являются «сторонние поставщики услуг или поставщики — от услуг по уборке до разработки программного обеспечения — с физическим или виртуальным доступом к информационным системам, программному коду или интеллектуальной собственности». NIST также называет «сторонние хранилища данных или агрегаторы данных» потенциальными векторами атак. Одна из причин 90 процентов руководителей цепочек поставок говорят, что в ближайшие три года они планируют регионализацию, так это то, что они обеспокоены рисками для третьих сторон, создаваемыми географически распределенными партнерами. Исследователи DBIR подчеркивают «взаимосвязанный характер реальных сред при обсуждении нарушений цепочки поставок и третьих сторон».

Кибербезопасность должна быть неотъемлемой частью стратегии управления рисками любой цепочки поставок, но эта стратегия не может быть ограничена четырьмя стенами вашей компании. Важно не только заручиться поддержкой заинтересованных сторон для разработки надежной платформы кибербезопасности среди ваших сотрудников. Вы должны сделать то же самое с вашими партнерами. Как отмечает DBIR, «одно ключевое нарушение цепочки поставок может привести к самым разным последствиям». Однако более трети компаний заявляют, что они не контролируют регулярно меры кибербезопасности своих поставщиков.

Как осведомленность о кибербезопасности может защитить цепочки поставок

Одной из наиболее устойчивых тенденций в области кибербезопасности является роль человека в обеспечении безопасности организаций. DBIR 2022 года сообщает, что 82 процента взломов связаны с человеческим фактором: «Будь то использование украденных учетных данных, фишинг, неправомерное использование или просто ошибка, — пишут исследователи, — люди продолжают играть очень большую роль в инцидентах и нарушениях, бреши одинаковые». Постоянно напоминают о важности осведомленности о кибербезопасности для предотвращения крупных атак на цепочки поставок. Рассмотрим эти примеры:

NotPetya проник в системы морского гиганта Maersk через единственный зараженный компьютер. Как поясняется в статье Wired об атаке, «финансовый директор подразделения Maersk в Украине попросил ИТ-администраторов установить бухгалтерское программное обеспечение MEDoc [средство для вредоносных программ NotPetya] на одном компьютере. Это дало NotPetya единственную точку опоры, в которой он нуждался».

Хакеры взломали Colonial Pipeline с помощью одного скомпрометированного пароля. По данным DBIR, использование украденных учетных данных и программ-вымогателей были двумя основными «разновидностями действий в сторонних инцидентах».

SolarWinds обвинила «компрометацию учетных данных и/или доступ через стороннее приложение» в крупной кибератаке, от которой она пострадала в конце 2020 года.

Во всех этих случаях, которые представляют собой несколько крупнейших кибератак в истории, поведение человека оказывало прямое влияние на способность киберпреступников проникать в защищенные системы. Хотя это напоминание о том, что небрежность и ошибки сотрудников являются одними из самых серьезных обязательств в области кибербезопасности для компаний в секторе цепочки поставок, оно также демонстрирует, что их наиболее эффективным активом в области кибербезопасности является осведомленность сотрудников. Помня об этом, подумайте, как компании могут предоставить сотрудникам возможность защищать цепочки поставок по всему миру.

Разработайте упреждающую программу повышения осведомленности о кибербезопасности. Когда так много кибератак является результатом человеческого поведения, становится ясно, что обучение сотрудников должно стоять на первом месте в списке приоритетов кибербезопасности любой компании. Компании часто осознают этот факт слишком поздно — 90%, например, говорят, что провели обучение сотрудников по вопросам кибербезопасности после атаки программ-вымогателей. Нет причин откладывать информирование сотрудников о киберугрозах, если вы уже пострадали от огромных финансовых и репутационных последствий кибератаки.

Убедитесь, что ваш информационный контент о кибербезопасности интересен и актуален. Самая большая ошибка компаний, когда они пытаются рассказать своим сотрудникам о киберугрозах, заключается в том, что они не понимают, как учатся занятые взрослые. Необходимо заинтересовать сотрудников убедительным, основанным на повествовании контентом о последних киберугрозах, использовать эффективные методы обучения, такие как геймификация, и давать им краткие (но последовательные) эпизоды и упражнения, которые не перегрузят учащихся ненужной информацией. Материалы, посвященные кибербезопасности, должны быть сосредоточены на конкретных угрозах, с которыми сталкиваются сотрудники, таких как риски третьих сторон в секторе цепочки поставок.

Предоставьте сотрудникам необходимые ресурсы и информацию. Вспомним три крупных кибератаки на цепочки поставок, упомянутые выше. NotPetya заразил всю систему Maersk, потому что один сотрудник загрузил вредоносное ПО на одно устройство. Это демонстрирует важность обучающего контента, который учит сотрудников распознавать различные формы вредоносного ПО. Атака также стала напоминанием о том, что безопасность физических устройств имеет решающее значение, особенно в эпоху удаленной работы, когда все больше сотрудников будут использовать кафе и терминалы аэропортов в качестве импровизированных офисов. Скомпрометированные учетные данные были замешаны в атаках Colonial Pipeline и SolarWinds, а DBIR 2022 года сообщает, что использование украденных учетных

данных является основным видом взлома. Компании могут ссылаться на эти факты, чтобы подчеркнуть важность использования таких инструментов, как менеджеры паролей и VPN.

Это лишь некоторые из способов, с помощью которых компании могут повысить осведомленность о кибербезопасности в своих цепочках поставок. Несмотря на то, что в ближайшие годы сектор цепочки поставок столкнется с еще более безжалостными и разрушительными кибератаками, бизнес-лидеры как никогда хорошо осведомлены об этой угрозе. Если вы являетесь лидером цепочки поставок, сейчас самое время сделать киберустойчивость одним из основных приоритетов на всех уровнях вашей организации. Когда сотрудники научатся выявлять и предотвращать кибератаки на цепочки поставок, они не только обеспечат безопасность компании, но и помогут всей экономике избежать катастрофических сбоев, с которыми мы столкнулись за последние несколько лет». ***(Shaun McAlmont. Why Cybersecurity Has Never Been More Important for the Supply Chain Sector // Keller International Publishing Corp (https://www.supplychainbrain.com/blogs/1-think-tank/post/35798-why-cybersecurity-has-never-been-more-important-for-the-supply-chain-sector). 21.10.2022).***

***

«Компания IBM Security (NYSE: IBM) объявила сегодня результаты глобального опроса, в ходе которого изучается решающая роль специалистов по реагированию на инциденты кибербезопасности в то время, когда физический и цифровой миры все больше сближаются. Исследование, опубликованное во время Национального месяца осведомленности о кибербезопасности, показало, что опрошенные специалисты по реагированию на инциденты — те, кто непосредственно реагирует на кибератаки — в первую очередь руководствуются сильным чувством долга по защите других; ответственность, которая все больше осложняется всплеском разрушительных атак, от распространения программ-вымогателей до недавнего роста вредоносного ПО Wiper.

Организации, играющие важную роль в мировой экономике, цепочках поставок и перемещении товаров, стали главными целями для подрывных атак. В 2021 году число кибератак на энергетические компании IBM Security X-Force увеличилось в четыре раза по сравнению с прошлым годом, в то время как производители столкнулись с атаками программ-вымогателей больше, чем в любой другой отрасли — от производителей продуктов питания до производителей медицинского оборудования, автомобилей и стали. Поскольку кибератаки угрожают основным услугам, необходимым для наших повседневных нужд, специалисты по реагированию на инциденты в этих отраслях сталкиваются с необходимостью защищать цифровую линию фронта. Фактически, 81% респондентов заявили, что распространение программ-вымогателей усугубило психологические требования, связанные с инцидентами кибербезопасности.

Глобальный опрос более 1100 специалистов по реагированию на инциденты кибербезопасности на 10 рынках, проведенный Morning Consult и спонсируемый IBM Security, выявил тенденции и проблемы, с которыми сталкиваются специалисты

по реагированию на инциденты в силу характера своей профессии. Некоторые основные моменты включают в себя:

Чувство служения. Более трети участников аварийно-спасательных служб были привлечены к работе на местах чувством долга по защите и возможностью помочь другим и бизнесу. Почти для 80% респондентов это стало одной из главных причин, по которым их привлекли в IR.

Борьба с несколькими фронтами — на фоне растущего числа кибератак в последние годы 68 % опрошенных специалистов по реагированию на инциденты заявили, что обычно им поручают реагировать на два или более пересекающихся инцидента одновременно.

Влияние на повседневную жизнь. Высокие требования к кибербезопасности также влияют на личную жизнь лиц, реагирующих на инциденты: 67% испытывают стресс или тревогу в повседневной жизни. Бессонница, эмоциональное выгорание и влияние на социальную жизнь или отношения, указанные респондентами. Несмотря на эти проблемы, подавляющее большинство признало, что у них есть сильная система поддержки.

«Реальные последствия кибератак в настоящее время вызывают обеспокоенность по поводу общественной безопасности и рост рисков, оказывающих давление на рынок», — сказал Лоранс Дайн, глобальный руководитель подразделения IBM Security X-Force Incident Response. «Ликвидаторы инцидентов — это защитники на переднем крае, стоящие между киберпреступниками, вызывающими сбои, целостность и непрерывность критически важных услуг. IBM приветствует все команды IR в сообществе кибербезопасности и важную роль, которую они играют в защите цифровой линии фронта».

Неравное поле битвы

В последние годы кибератаки не только стали более разрушительными, но и увеличился их объем. С 2020 по 2021 год X-Force зафиксировала почти 25-процентный рост числа инцидентов кибербезопасности, в которых участвовала ее команда по связям с инвесторами. Добавьте к этому исследование Check Point Software Technologies, которое указывает на 50-процентное увеличение общего числа сетевых атак в неделю в 2021 году по сравнению с 2020 годом. индустрия призвана реагировать на растущее число кибератак, существует лишь ограниченное число специалистов по безопасности, специально обученных и обладающих навыками реагирования на инциденты кибербезопасности.

В результате, в то время как многие IR-группы вынуждены сражаться на нескольких фронтах, предприятия могут остаться без необходимых ресурсов для смягчения последствий кибератак и восстановления после них. Исследование IBM показало, что 68% опрошенных специалистов по реагированию на инциденты считают обычным делом одновременно реагировать на два или более инцидента кибербезопасности, выделяя область, которая постоянно задействована. Среди респондентов из США 34% заявили, что средняя продолжительность взаимодействия с IR составляет 4–6 недель, а четверть назвали первую неделю наиболее напряженным или требовательным периодом взаимодействия. В этот период около трети респондентов работают в среднем более 12 часов в день.

Сильная система поддержки на месте

Поскольку службы реагирования на инциденты сталкиваются с давлением и высокими требованиями, связанными с киберреагированием, подавляющее большинство респондентов признали, что у них есть надежная система поддержки. В частности, большинство респондентов считают, что их руководство имеет четкое представление о деятельности, связанной с IR, а 95% говорят, что оно обеспечивает необходимую структуру поддержки для достижения успеха. Кроме того, 84% заявляют, что у них есть адекватный доступ к ресурсам поддержки психического здоровья, при этом многие респонденты (64%) обращаются за помощью в области психического здоровья из-за сложного характера реагирования на кибератаки.

Но компании могут дополнительно поддерживать службы реагирования на инциденты, будь то внутренние группы Blue Team или внешние группы по связям с инвесторами, которых они привлекают в случае киберкризиса, уделяя первоочередное внимание киберподготовке и создавая планы и сценарии, адаптированные к их среде и ресурсам. Это может помочь обеспечить более гибкое и быстрое реагирование в начале инцидента и уменьшить ненужный уровень нагрузки на бизнес.

Для этого важна ситуационная осведомленность об их инфраструктуре. Предприятия могут сосредоточиться на проверке своего состояния готовности с помощью имитационных упражнений не только для того, чтобы понять, как их команды будут реагировать на атаки, но и для того, чтобы дать возможность правильно интегрировать несколько команд, задействованных во время киберинцидента». ***(New IBM Study Finds Cybersecurity Incident Responders Have Strong Sense of Service as Threats Cross Over to Physical World // IBM (https://newsroom.ibm.com/2022-10-03-New-IBM-Study-Finds-Cybersecurity-Incident-Responders-Have-Strong-Sense-of-Service-as-Threats-Cross-Over-to-Physical-World). 03.10.2022).***

***

«Успешные кибератаки могут привести к значительным финансовым потерям и нанести ущерб бизнесу. Согласно недавним выводам команды Atlas VPN, 37% компаний теряют в среднем более 100 000 долларов за одну кибератаку. Помимо финансового ущерба, предприятия также портят свою репутацию, теряют корпоративную информацию и сталкиваются с перебоями в работе партнеров.

После успешной кибератаки 14% предприятий потеряли менее 5000 долларов. У 8% компаний было украдено от 5000 до 9999 долларов. Киберпреступникам сошло с рук до 49 999 долларов после кибератак на 16% предприятий. В целом 24 процента предприятий потеряли от 50 000 до 99 999 долларов.

Кроме того, 22 процента компаний понесли значительные убытки от 100 000 до 499 999 долларов США. Киберпреступники украли еще больше денег, от 500 000 до 999 999 долларов, у 11 процентов предприятий. Наконец, 4 процента компаний заявили, что потеряли более 1 миллиона долларов после успешной кибератаки. Всего 2 процента предприятий не знали о реальных потерях.

Писатель по кибербезопасности в Atlas VPN Вилюс Карделис делится своими мыслями о кибератаках на бизнес:

«Несмотря на то, что в последнее время многие компании вкладывают больше средств в кибербезопасность, самой важной проблемой является прозрачность. Компании боятся сообщать об инцидентах, опасаясь потерять доверие клиентов. Однако это делает кибератаки более опасными и распространенными, нанося значительный ущерб бизнесу».

Последствия кибератак

Помимо уже упомянутых финансовых потерь, предприятия часто несут дополнительные убытки после успешной кибератаки.

Почти треть (31 процент) предприятий столкнулись со сбоями в работе партнеров и клиентов и кражей финансовой информации. Более того, более четверти (28%) компаний пострадали от репутационного ущерба и кражи финансовой информации после успешной кибератаки.

Около четверти (24%) предприятий столкнулись с нарушением цепочки поставок. В то же время еще 23 процента компаний столкнулись с препятствиями в торговых или деловых операциях. Менее одной пятой (19 процентов) предприятий пострадали от потери бизнеса или контракта, в то время как кража денег имела место в 18 процентах компаний после успешной кибератаки». ***(Almost 40 Percent Of Businesses Lose More Than $100,000 Per Cyberattack // MITechNews.com (https://mitechnews.com/cyber-defense/almost-40-percent-of-businesses-lose-more-than-100000-per-cyberattack/). 09.10.2022).***

***

«…Игровая индустрия была одним из самых больших выгодопреобретателей от пандемии, увеличившись на 26 процентов в период с 2019 по 2021 год. Согласно недавнему отчету PricewaterhouseCoopers (PwC), к 2026 году рост мировой игровой индустрии составит 321 миллиард долларов.

К сожалению, по мере того, как количество игроков увеличивается, а потребители проводят больше времени в обширных виртуальных мирах, также наблюдается значительный рост киберпреступлений и киберпреступников, стремящихся украсть личную информацию людей и реальные деньги.

Компания Kaspersky, занимающаяся глобальной безопасностью и цифровой конфиденциальностью, опубликовала отчет («Выводы Касперского»), в котором отмечается, что в первой половине 2022 года возросла активность киберпреступников, злоупотребляющих геймерами. Эксперты по кибербезопасности предупреждают, что киберпреступность в играх увеличилась с начала пандемии, скрываясь в чит-кодах, микротранзакциях и сообщениях, которыми обмениваются онлайн другие игроки. Геймеры, пытающиеся загрузить новые игры из незащищенных или ненадежных источников, сталкивались с загрузкой вредоносного программного обеспечения, потерей своих игровых счетов и денег. Кроме того, выводы «Лаборатории Касперского» подтверждают, что в некоторых случаях были обнаружены нежелательные установки категории шпионских программ, способных «отслеживать любые данные, вводимые с клавиатуры, и делать снимки экрана». Согласно отчету Akamai, опубликованному в августе 2022 года, количество кибератак на веб-приложения с мая 2021 года по

апрель 2022 года увеличилось на 167% по сравнению с аналогичным периодом прошлого года.

Игровые компании становятся все более прибыльными целями для киберпреступников по мере расширения спектра кибератак. Кроме того, растущий объем данных, собираемых игровыми компаниями, делает их привлекательными целями. Эти компании более уязвимы к утечке данных, что приводит к потере данных клиентов и, кроме того, к тому, что их предложения продуктов (например, игры и платформы) временно отключаются от сети. В результате клиенты игровых компаний (то есть отдельные игроки) могут легко потерять игровой прогресс, деньги и конфиденциальные личные данные. Риски, связанные с кибербезопасностью, будут только усиливаться по мере того, как игровые компании будут все больше заниматься продажей, покупкой, обменом или хранением цифровых активов клиентов, таких как игровые жетоны и монеты, которые можно использовать для покупки цифровых продуктов в обширных виртуальных мирах. По данным «Лаборатории Касперского», из 28 игр, включенных в исследование, в первую тройку игр с наибольшим количеством вредоносных и нежелательных файлов вошли Minecraft, FIFA и Roblox.

Руководители игровых компаний должны помнить о своих юридических обязательствах по защите пользовательской информации и обеспечивать, чтобы их продукты (например, игры и платформы) были в безопасной среде. Канадский закон о конфиденциальности, регулирующий сбор личной информации в коммерческих целях, в общих чертах требует, чтобы предприятия применяли меры предосторожности для защиты личной информации. Например, федеральный закон, который также распространяется на большинство канадских провинций, требует мер безопасности для «защиты личной информации от потери или кражи, а также от несанкционированного доступа, раскрытия, копирования, использования или изменения». Обратите внимание, что этот закон ожидается. который вскоре будет заменен Законом о защите прав потребителей, который будет иметь аналогичные обязательства.

Управление киберрисками является фундаментальной проблемой для организаций любого размера, и небольшие игровые компании ни в коем случае не являются исключением. Согласно канадскому законодательству, директора корпораций несут ответственность за управление и надзор за управлением бизнесом и делами корпорации. Как правило, корпоративные директора обязаны действовать честно и добросовестно в интересах своей корпорации. Кроме того, они должны проявлять осторожность, умение и усердие, которые разумно предусмотрительный человек проявлял бы в сопоставимых обстоятельствах. Что касается управления киберрисками, то все чаще ожидается, что корпоративные директора будут играть активную роль в определении устойчивости корпорации к риску, обеспечивать, чтобы руководство предприняло разумные шаги для выявления и управления рисками с помощью соответствующей программы управления рисками, и, наконец, отслеживать любые значительные риски, которые могут повлиять на корпорацию. И хотя действующий федеральный закон не возлагает личную ответственность на директоров и должностных лиц за нарушения, новый законопроект Квебека № 64

налагает большие штрафы на лиц, которые не принимают надлежащих мер безопасности для защиты личной информации.

Для разработчиков игр, как и для любой компании, собирающей приватную информацию, лучшим лекарством от кибератак по-прежнему остается профилактика. Компании, разрабатывающие и эксплуатирующие игры и игровые платформы, должны придерживаться основополагающих принципов действующего и входящего законодательства Канады о защите данных, ограничивая сбор данными, которые им действительно нужны, запрашивая информированное согласие на сбор данных от игроков, использующих их продукты, размещаемые данные и продолжительность их хранения, а также обеспечение мер безопасности для защиты личной информации игроков». ***(Hyunju (Crystal) Park, Brent J. Arnold. THE HACKERS ARE COMING FOR THE GAMERS: LEGAL RISKS AND BEST PRACTICES FOR MINIMIZING LIABILITY // Gowling WLG International Limited (https://gowlingwlg.com/en/insights-resources/articles/2022/the-hackers-are-coming-for-the-gamers/). 31.10.2022).***

***

«Рост метавселенной подчеркивает необходимость решения проблем кибербезопасности, связанных с этой новой мультимедийной средой.

По оценкам инвестиционного банка Citi, на метавселенную будет приходиться 1% мировой экономики, которая к 2030 году может достичь от 8 до 13 триллионов долларов США. Из-за этого роста становится все более вероятным, что метавселенная будет подвергаться кибератакам, которые представляют реальный риск как для компаний, активных в метавселенной, так и для пользователей, которые получают к ней доступ.

Что такое метавселенная?

Метавселенная относится к цифровой вселенной, которая является результатом множества технологических элементов, включая виртуальную реальность и дополненную реальность. Идея состоит в том, что внутри метавселенной пользователи могут получить к ней доступ через средства трехмерного просмотра и получить «виртуальный» опыт. На самом деле можно создавать реалистичные аватары, например, с помощью NFT, знакомиться с другими пользователями или выполнять все те действия, которые мы выполняем «разрозненно» в Интернете, на одной платформе. Можно даже создать рынок недвижимости.

Знаменитый бренд Bored Ape Yacht Club, уже известный своей коллекцией NFT-игр скучающих обезьян, объявил о запуске оригинальной метавселенной. Названный Otherside, он ориентирован на геймификацию с децентрализованной структурой, эффективно формируя связь между метавселенной и рынком недвижимости. Это привело к продаже около 55 000 NFT, каждая из которых была продана за 305 монет Ape Coins, в результате чего каждый лот стоил в среднем 6 000 долларов США. Эта виртуальная продажа земли вызвала один из самых высоких скачков комиссий за транзакции в Ethereum.

Метавселенная требует одновременного использования множества технологий, в которых дополненная реальность, облачные технологии, Интернет

вещей и искусственный интеллект объединяются, чтобы быть функциональными, а также существует возможность создания уникальной экономики с помощью криптовалют и NFT.

Проблемы кибербезопасности и метавселенная

Учитывая задействованные технологии, риск стать жертвой кибератак в метавселенной очень высок. Одновременное использование различных технологий, сбор бесконечных объемов данных, как личных, так и неличных, а также использование блокчейна делают использование систем для мониторинга и предотвращения кибератак весьма сложным по сравнению с тем, что происходит в виртуальной или реальный мир. Например, в децентрализованном мире известны десятки случаев продажи контрафактных произведений или продуктов: контрафактный продукт остается в блокчейне навечно, и удалить его из блокчейна невозможно.

Хотя мы предполагаем, что фишинговая активность может резко увеличиться в метавселенной, также возможно увеличение:

Кража личных данных: злоумышленники с помощью информации, найденной в Интернете и в метавселенной, могут прибегнуть к краже личных данных пользователей, например, путем кражи аватара.

Кража криптовалюты: злоумышленники могут завладеть кошельками и ключами доступа пользователей в метавселенной, совершая необратимые действия.

Основная проблема кибербезопасности в метавселенной связана с личными данными (как и в реальном мире), которые станут основной целью атаки. Просто рассмотрите биометрические данные, публикуемые пользователями, чтобы воспользоваться преимуществами устройств, которые позволяют пользователям переключаться с виртуальной реальности (VR) на дополненную реальность (AR), которые используют биометрические данные пользователя для доступа в метавселенную.

Компании должны будут заранее подготовиться к предотвращению подобных атак. Им необходимо обеспечить безопасность и надежность своих систем безопасности и отсутствие уязвимостей, которые могут нанести серьезный ущерб не только экономике и репутации компаний, но и пользователям. Но по-прежнему не хватает регулирующих режимов, которые должны быть введены для обеспечения защиты метавселенной и ее пользователей». ***(Giulia Zappaterra, Enila Elezi. Metaverse and cybersecurity, what challenges for the future? // DLA Piper (https://www.dlapiper.com/en/us/insights/publications/2022/10/real-estate-gazette-new-technology/5-metaverse-and-cybersecurity-what-challenges-for-the-future/). 26.10.2022).***

***

«…Правительства вложили значительные средства в создание организаций, которые одновременно отслеживают угрозы и предоставляют практические советы компаниям и организациям, чтобы помочь им подготовиться к кибератакам, разработать надежные программы управления киберрисками и обеспечить устойчивость.

Такие организации, как Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) и Национальный центр кибербезопасности Великобритании (NCSC), регулярно публикуют обзоры общего состояния готовности предприятий к кибератакам в США и Великобритании. Их цель не в том, чтобы быть паникером, а в том, чтобы информировать бизнес-лидеров и команды о возникающих кибер-рисках, с которыми они сталкиваются, и о практических шагах, которые они могут предпринять для их смягчения. Как правило, это руководство перекликается с советами, предлагаемыми группами по информационной безопасности в организациях, и помогает проверить многие бизнес-обоснования для более значительных инвестиций в проекты кибербезопасности и инициативы по управлению киберрисками.

Обзор оценок киберрисков и уязвимостей CISA

Недавно CISA провела обзор своих оценок рисков и уязвимостей на 2021 финансовый год, в которых охвачены оценки рисков и уязвимостей (RVA) для 112 организаций федерального правительства США и частного сектора. В этом обзоре RVA были освещены некоторые модели, которые злоумышленники используют для атак и эксплуатации сетей, включая первоначальный вход, выполнение атаки, сохраняемость, повышение привилегий и эксфильтрацию. В нем также подчеркивается влияние на бизнес и приводятся практические шаги по каждому аспекту, которые компании могут предпринять для решения проблем.

В обзоре за 2021 финансовый год критические риски, отмеченные CISA, включали фишинговые атаки и широкое использование учетных данных безопасности по умолчанию. В анализе подчеркивается необходимость регулярного информирования о фишинговых атаках и использовании надежных паролей, которые регулярно меняются. В отчете также подчеркивается необходимость регулярного пересмотра методов вторжения, чтобы при возникновении инцидентов с использованием новых методов организации могли быстро реагировать. Другие проблемы подчеркивали необходимость смены паролей по умолчанию, регулярного обновления и исправления программного обеспечения, а также поиска и исправления открытых портов.

Отчет UK NCSC об угрозах кибербезопасности

Эти настроения были отражены в недавнем отчете NCSC Великобритании, в котором подчеркиваются особые риски, связанные с корпоративными подключенными устройствами (ECD). Устройства ECD включают ноутбуки, смартфоны и корпоративные устройства Интернета вещей (IoT), которые являются физическими устройствами — например, холодильники, детекторы дыма, камеры и датчики присутствия — которые содержат возможности подключения к сети, которые позволяют управлять ими удаленно. ECD популярны, поскольку они обеспечивают гибкость управления и экономию эффективности во многих рабочих средах.

Однако, несмотря на свою популярность, электронные компакт-диски могут представлять значительную угрозу безопасности, учитывая непонимание большинством сотрудников связанных с этим рисков безопасности, а также отсутствие видимости этих устройств в офисе. В отчете NCSC освещаются многие из угроз, которые несут в себе ECD. Хакеры используют их как отправную точку для

доступа к другим, более безопасным системам. Отсутствие видимости устройств IoT и использование настроек безопасности по умолчанию означает, что они подходят для боковых атак на другие системы, которые могут привести, например, к краже данных или атакам программ-вымогателей. Использование этих устройств в цепочке поставок компании также представляет собой угрозу, поскольку даже если компания придерживается жесткой политики РЗД и контролирует себя, может случиться так, что ее поставщики этого не сделают.

Эта ситуация подчеркивает проблему, с которой сталкиваются предприятия в отношении того, как лучше всего реагировать на киберриски, влияющие как на организацию, так и на третьих лиц, когда ресурсы и затраты остаются ограниченными.

Включение мощных возможностей управления киберрисками

Возможности новых технологий побуждают службы безопасности переосмысливать способы решения подобных задач. Теперь они могут предложить альтернативный способ управления кибер-рисками, передав внедрение и мониторинг политики безопасности бизнеса в руки конечных пользователей и их менеджеров, а не только небольшую и перегруженную группу безопасности.

Подход, основанный на SaaS, означает, что группы безопасности могут предоставить удобную для навигации библиотеку документов политики безопасности с мощными возможностями поиска и вопросов и ответов, которые позволяют сотрудникам понимать свои обязанности в темпе, который подходит им и их проектам. Возможности обучения и тестирования помогают улучшить навыки и осведомленность сотрудников о новых и возникающих угрозах безопасности. Возможности аттестации позволяют им документировать и предоставлять доказательства того, как они соблюдают стандарты безопасности. Возможности искусственного интеллекта позволяют командам по информационной безопасности знать, где стандарты не соблюдаются по мере изменения конкретных потребностей бизнеса.

Этот подход позволяет группам по информационной безопасности лучше направлять организацию и третьи стороны в отношении их политики кибербезопасности в темпе, которым они все могут управлять. Это также означает, что группа по информационной безопасности может оставаться окончательным арбитром программы управления киберрисками». ***(Javier Gutierrez. Emerging Cyber Risks in the US & UK // MITRATECH (https://mitratech.com/resource-hub/blog/emerging-cyber-risks-us-and-uk/). 12.10.2022).***

***

«Индустрия кибербезопасности за последние несколько лет получила широкое распространение, и по мере ее роста росла и ее ценность. Согласно исследованию, проведенному Statista, рынок кибербезопасности в настоящее время оценивается в 159,8 млрд долларов США и, как ожидается, вырастет до 345,4 млрд долларов США к 2026 году. Все формы и размеры взлетели до небес.

Предприятия по всему миру ощущают на себе последствия кибератак и преступлений. Согласно исследованию, проведенному Cybersecurity Ventures,

стоимость киберпреступлений достигла 6 трлн долларов в 2021 году, а ущерб, по оценкам, вырастет до 10 трлн долларов к 2025 году.

Поскольку киберпреступность становится все более прибыльной, число кибератак, вероятно, возрастет. Однако утечка данных не ограничивается только финансовыми потерями. Они могут повлиять на деловые операции, персонал, оценку, репутацию и финансы.

Будь то конфиденциальные или личные данные, компании ищут эффективные решения для обеспечения сетевой безопасности, конфиденциальности и безопасности своих данных и сохранения суверенитета. Но как?

Используйте инструменты отчетности о кибербезопасности.

Инструменты отчетности по кибербезопасности защищают предприятия от различного рода вредоносных атак и киберпреступлений. Кибервзломы — это не столько вопрос «если», сколько вопрос «когда». Стратегии управления рисками кибербезопасности должны быть сосредоточены на том, насколько хорошо они могут активно управлять угрозами и реагировать с помощью этих инструментов.

Прежде чем мы познакомим вас с инструментами отчетности, которые вам нужны, давайте разберемся, почему так важно отказаться от устаревших систем или электронных таблиц в пользу инструментов, использующих автоматизацию и созданных для нашей цифровой эпохи.

Почему электронные таблицы не работают?

Данные являются ценным активом для любого бизнеса — они являются частью различных ролей в бизнесе, включая исследования рынка, управление персоналом, внутренние продажи и многое другое. Однако многие компании по-прежнему используют устаревшие инструменты, такие как электронные таблицы, для передачи и визуализации этих данных. Согласно отчету Aberdeen Group, более 89% компаний ежедневно используют электронные таблицы.

Хотя электронные таблицы являются отличными инструментами, они не являются эффективными каналами для передачи данных, визуализации и мер безопасности.

Электронные таблицы неэффективны и могут подвергнуть ваш бизнес различным рискам безопасности. Они модульные, невероятно медленные, очень дорогие и неспособные обнаруживать уязвимости, которыми пользуются киберпреступники и хакеры.

Вот несколько причин, по которым многие компании по всему миру начали рассматривать электронные таблицы как плохой вариант:

Ручные рабочие процессы
Устаревшие оценки
Нет стандартизированной отчетности
Отсутствие единой системы соблюдения
Хранилища данных
Склонен к ошибкам
Кропотливый
Не предоставляет данные в режиме реального времени

Теперь, когда вы знаете, что электронные таблицы неэффективны, давайте узнаем о пяти лучших инструментах отчетности о кибербезопасности для выявления уязвимостей.

Пять инструментов киберотчетности, которые вы должны использовать

Ниже приведены пять лучших инструментов отчетности о кибербезопасности, которые сделают вашу жизнь проще.

Автоматизация

Автоматизация — это эффективный способ создания единой комплексной стратегии для управления различными рисками кибербезопасности. Этот инструмент отчетности позволяет упростить оценку рисков, обеспечивая при этом превосходное представление о состоянии безопасности и рисках.

Специалисты по управлению рисками и безопасности могут собирать данные посредством интеграции с помощью подходящих инструментов, которые позволяют создавать отчеты в режиме реального времени, автоматически оценивать и регистрировать риски. Это поможет вам быть в курсе актуальной информации, необходимой для понимания потенциальных и существующих рисков и защиты конфиденциальной информации.

Это позволяет вам составить интегрированный план реагирования на инциденты, управлять соблюдением требований в режиме реального времени, а не на определенный момент времени, и обеспечивать соблюдение компанией соответствующих стандартов или рамок.

Короче говоря, автоматизация помогает сэкономить ресурсы и время компании за счет сокращения усилий и времени, необходимых для запуска проектов, оценки рисков вручную или обновления требований соответствия.

Рабочий процесс оценки и отчетность

Этот инструмент отчетности помогает вам оценивать риски и ранжировать их по серьезности, чтобы определить приоритеты рисков, которые требуют немедленного внимания и исправления, а также тех, которые можно временно допустить, пока не будут решены все существенные проблемы.

Специалисты по безопасности могут легко отслеживать зрелость и производительность, используя отчеты по запросу, и отслеживать соответствие с любой настроенной или стандартной отраслевой структурой. Кроме того, это помогает отслеживать соответствие и контролировать позиции и пробелы.

Более того, этот инструмент обеспечивает большую уверенность в данных и помогает создавать прогнозную аналитику с помощью рутинного потока информации.

Кроме того, рабочий процесс оценки и отчетность помогают улучшить презентацию для заинтересованных сторон, способствуют общению и прозрачности, а также улучшают инвестиции в киберпространство.

Автоматизированный пешеходный переход

Независимо от ниши или отрасли, компании сталкиваются с различными нормативными изменениями и резким увеличением числа анкет для оценки безопасности поставщиков. Наряду с увеличением количества запросов на аудит безопасности и ожиданий в отношении отчетов, директорам по информационной

безопасности требуется представление в режиме реального времени их состояния безопасности и соответствия требованиям с помощью фреймворков.

Проект пешеходного перехода вручную сложен и требует огромных затрат времени и ресурсов. Кроме того, на картографирование могут уйти часы, и оно в основном основано на содержании элементов управления, а не на концепциях или намерениях. Независимо от того, выполняется ли она сторонней фирмой или внутренней командой, пешеходный переход является неотъемлемой частью любой программы соблюдения нормативных требований.

Хотите правильно перейти пешеходный переход? Выберите автоматизированный пешеходный переход.

Это помогает компаниям успешно предотвращать кибератаки, получая мгновенную информацию о различных положениях соответствия стандартам или структурам. Перейдите от традиционного (вручную) проекта сопоставления к автоматизированному, в котором стандарты, платформы и пользовательские элементы управления немедленно сопоставляются с любыми другими требованиями.

Автоматизированный пешеходный переход имеет следующие преимущества:

Почти мгновенные сопоставления

Неограниченное количество сопоставлений, доступных для выполнения

Точно основано на содержании и назначении элементов управления, а не только на словах

Реестр рисков

Реестр рисков — это популярный инструмент среди профессионалов и руководителей в области кибербезопасности, позволяющий специалистам-практикам измерять и отслеживать риски в централизованном месте. Он позволяет записывать выявленные риски, анализ их серьезности и основные управленческие действия.

Вы не сможете наблюдать за изменениями задокументированных рисков с течением времени, принимать обоснованные решения, группировать риски и сообщать о них, а также визуализировать и обсуждать их в своей компании, если у вас нет реестра рисков.

Проектные группы могут использовать реестры рисков для повышения своей кибербезопасности за счет эффективности, масштаба и соответствия требованиям.

Ниже перечислены некоторые преимущества реестров рисков:

Общекорпоративный взгляд на прошлые, настоящие и будущие сценарии кибер- и ИТ-рисков

Точно на основе данных в реальном времени

Смоделируйте решения для минимального снижения рисков и максимальной рентабельности инвестиций

Легко сворачивается и сообщается нетехническим заинтересованным сторонам

Отчеты и информационные панели в реальном времени

Важность KRI, визуализаций и метрик возрастает в геометрической прогрессии, особенно при оценке решений по управлению киберрисками.

Под повышенным вниманием со стороны Совета директоров и исполнительного руководства отчеты и информационные панели в режиме реального времени о кибербезопасности помогают отслеживать цели и удовлетворять потребности различных заинтересованных сторон, от Совета директоров до руководителей высшего звена.

Благодаря отчетам и информационным панелям в режиме реального времени специалисты по безопасности будут получать простые для понимания информативные аналитические данные, периодические обновления и отчеты, чтобы они могли легко сообщать заинтересованным сторонам о текущем состоянии безопасности, в том числе о киберрисках и состоянии соответствия.

Вывод

Современные организации сталкиваются с различными вызовами и проблемами, которые требуют тщательного мониторинга, отслеживания и оценки мер кибербезопасности для предотвращения случаев потери данных. Упомянутые выше инструменты создания отчетов о кибербезопасности помогают сократить объем ручного вмешательства и обеспечить ощутимую и реальную окупаемость инвестиций для вашей компании…» ***(Cybersecurity Reporting Tools That Will Make Your Life Easier // Techstrong Group (https://securityboulevard.com/2022/10/cybersecurity-reporting-tools-that-will-make-your-life-easier/amp/). 10.2022).***

***

«Согласно новым данным CyberSeek, потребность работодателей в специалистах по кибербезопасности продолжает ограничиваться доступностью талантов.

За 12-месячный период, закончившийся в сентябре 2022 года, работодатели перечислили 769 736 вакансий в области кибербезопасности или рабочих мест, требующих навыков кибербезопасности. Спрос со стороны работодателей на специалистов по кибербезопасности рос в 2,4 раза быстрее, чем в целом по экономике США. Девять из 10 лучших месяцев для размещения вакансий в области кибербезопасности за последние 10 лет пришлись на 2022 год.

Несмотря на небольшое снижение активности найма в последние месяцы по сравнению с рекордными объемами в начале этого года, общее количество вакансий в области кибербезопасности в третьем квартале 2022 года было на 30% выше, чем за тот же период 2021 года, и на 68% выше, чем в 2020 году. Соотношение спроса и предложения оставался стабильным на уровне 65, что означает примерно 65 специалистов по кибербезопасности на рынке труда — подавляющее большинство из них уже трудоустроены, на каждые 100 объявлений о вакансиях в области кибербезопасности.

Данные показывают, что требования к навыкам кибербезопасности для конкретных профессий резко возросли за последние 12 месяцев. Профессия кибербезопасности продолжает расширяться за счет специализированных областей, таких как тестер проникновения и аналитик угроз. Аналогичное расширение требований к навыкам кибербезопасности наблюдается для смежных должностей,

таких как аудитор (+336%), разработчик программного обеспечения (+87%), облачный архитектор (+83%) и инженер технической поддержки (+48%)…

«Спрос на таланты в области кибербезопасности растет уже много лет, и работодатели не собираются отказываться от газа, — сказал Уилл Маркоу, вице-президент по прикладным исследованиям в Lightcast. «Вот почему как никогда важно создать надежный канал кадров для обеспечения более безопасного цифрового мира. Мы не можем смириться с тем, что в нашей системе кибербезопасности остаются дыры только потому, что у нас недостаточно обученных работников, чтобы их закрыть». ***(Cybersecurity's importance and impact reaches all levels of the tech workforce // Help Net Security (https://www.helpnetsecurity.com/2022/10/27/cybersecurity-professionals-demand/). 27.10.2022).***

***

«Управление активами кибербезопасности является одним из столпов быстрой комплексной стратегии безопасности, поскольку оно позволяет группе безопасности поддерживать актуальную базу данных ИТ-активов и связанных с ними рисков безопасности.

Если один уязвимый ресурс используется в качестве отправной точки для значительно более крупной атаки, каждый узел ИТ-инфраструктуры будет подвержен угрозам или рискам. Управление киберактивами расширяет возможности группы по ИТ-безопасности благодаря прозрачности, необходимой для разработки комплексной стратегии безопасности, которая позволяет быстро и упреждающе устранять угрозы.

Необычная кибербезопасность

Большинство компаний сталкиваются с киберинцидентами, которые являются более мощными и опасными, чем когда-либо прежде, и одной из причин этого является переход к мультиоблачным распределенным ИТ-инфраструктурам для удаленной работы. Это привело к большему риску из-за плохого контроля доступа и неправильно настроенных систем. Эта проблема безопасности может быть решена путем использования надежных процессов управления киберактивами, которые будут развертывать новые ИТ-услуги или ресурсы, не позволяя безопасности отвлекать или мешать.

Ключевые результаты

Автоматизация необходима для обеспечения безопасности, поскольку обычно киберактивов в любой организации больше, чем сотрудников. Хосты, агенты и другие активы, связанные с устройствами, которые по-прежнему являются важными компонентами кибербезопасности, все еще находятся в стадии развития. Современные автоматизированные методы обеспечения безопасности необходимы для создания высоконадежных динамических сетевых инфраструктур. Группы ИТ-безопасности используют сетевые интерфейсы для перемещения трафика между узлами, размещая балансировщики нагрузки, прокси-серверы и службы трансляции сетевых адресов (NAT). Управление киберактивами оказывается полезным в отражении кибератак, поскольку большинство компаний очень подвержены атакам на цепочку поставок программного обеспечения.

Облачный прогноз

В большинстве организаций группы ИТ-безопасности, как правило, упускают из виду косвенные отношения между пользователями, устройствами, сетями и критическими данными, поэтому использование управления киберактивами становится все более важным для компаний. Важные данные и конфиденциальная информация создают проблемы конфиденциальности среди наиболее взаимосвязанных типов активов для пользователей, приложений, устройств и рабочих нагрузок. Ряд выводов о безопасности показывает, что многие журналы безопасности содержат результаты, которые идентифицируются как критические уязвимости или ожидания политики, а это означает, что средняя команда безопасности не знает о некоторых рисках безопасности.

Управление киберактивами помогает группам ИТ-безопасности обнаруживать угрозы до того, как они превратятся в серьезные проблемы. Если компании постоянно отслеживают ИТ-ресурсы на предмет новых развертываний и рисков, группам ИТ-безопасности не нужно ждать, пока они обнаружат активное привлечение, чтобы отреагировать.

Прозрачность безопасности

Когда предприятия подвергаются кибератаке, управление киберактивами гарантирует, что группы ИТ-безопасности имеют перечень активов и рисков. это гарантирует, что организации быстро получат представление о проблеме, ее причинах или последствиях. Благодаря управлению киберактивами группы ИТ-безопасности имеют обновленную запись, к которой они могут обратиться немедленно, вместо того, чтобы восстанавливать состояние развертывания и конфигурации ресурсов для исследования причин нарушения или уязвимости. Хорошая стратегия управления киберактивами помогает предприятиям обнаруживать наиболее вероятные недостатки, которые включают активы, в которых может отсутствовать конечное устройство, или активы, которые не сканируются и не контролируются должным образом…» ***(Nisha Sharma. Cyber Asset Management & IT Security Teams // ITSecurityWire (https://itsecuritywire.com/featured/cyber-asset-management-it-security-teams/amp/). 26.10.2022).***

***

«Отчет, опубликованный во вторник Aspen Digital Institute и некоммерческой группой Consumer Reports, предполагает, что большинство потребителей предпринимают соответствующие действия для повышения своей кибербезопасности и хотят, чтобы правительство и компании тоже внесли свой вклад.

В отчете не рассматривается, почему потребители делают больше для повышения своей кибербезопасности. Это происходит на фоне того, что правительство продолжает финансировать организацию под названием Национальный альянс кибербезопасности (в последние годы ежегодно выделяя более полумиллиона долларов) для повышения осведомленности о кибербезопасности в октябре. NCA, правление которого состоит из руководителей

крупных корпораций, подчеркивает роль отдельных лиц в защите общей цифровой экосистемы от киберугроз.

Consumer Reports провела опрос в июне, используя репрезентативную для страны выборку из 2103 взрослых американцев. В отчете сравнивались ответы с опросом 2019 года, в котором респондентов также спрашивали об их методах кибербезопасности.

Один вопрос показал, что 88% опрошенных в июне использовали надежные пароли для доступа к своим домашним сетям Wi-Fi по сравнению с 74% в 2019 году. Другой вопрос показал, что 72% потребителей устанавливают разрешения для приложений на вашем смартфоне, чтобы блокировать доступ к таким вещам, как ваша камера, местоположение или контакты, если они не нужны для работы приложения, по сравнению с 60% в 2019 году. Самое большое изменение за последние три года — рост с 50% в 2019 году до 77% в июне — произошло в количестве людей. которые сказали, что внедрили многофакторную аутентификацию.

«MFA — это самый важный шаг, который люди могут предпринять для защиты своих устройств и конфиденциальности, поэтому администрация сделала его приоритетным, в том числе потребовав его для федерального правительства в рамках исполнительного указа президента об улучшении национальной кибербезопасности», Об этом говорится в отчете советника по безопасности в области кибербезопасности и новых технологий Энн Нойбергер. «Я в восторге от этого прогресса и от того, что сегодня больше американцев находятся в безопасности, чем даже несколько лет назад».

Новый опрос показывает, что 75% респондентов хотя бы в некоторой степени обеспокоены конфиденциальностью личных данных, собранных в Интернете. Из тех, кто не проявлял особого беспокойства по поводу этой проблемы, 24% сказали, что это произошло потому, что «я все равно ничего не могу с этим поделать». Еще 18% этой группы заявили: «Я принимаю все возможные меры предосторожности в отношении конфиденциальности, поэтому я считаю, что безопасность и конфиденциальность моих личных данных не в моих руках».

Согласно отчету, на вопрос, «кто должен нести наибольшую ответственность за защиту конфиденциальности американцев в Интернете», 32% ответили, что компании, 33% — федеральное правительство, а 25% — сами потребители…» ***(Mariam Baksh. Senior administration officials and cybersecurity leaders marking Cybersecurity Awareness Month weighed in on a consumer survey examining how behaviors have changed over the last three years // Nextgov (https://www.nextgov.com/cybersecurity/2022/10/new-report-shows-significant-improvement-consumer-cyber-hygiene/378041/). 04.10.2022).***

***

«Брандмауэры следующего поколения хорошо работают, XDRing, IPS в режиме предотвращения, и мы на 100% выполнили наш еженедельный обучающий подкаст по вопросам безопасности. Да, у нас даже есть шифрование электронной почты всех исходящих сообщений с полной защитой от потери данных

с многофакторной аутентификацией! Подождите, разве мы только что не развернули CASB для DLP?

Как программы-вымогатели распространялись по нескольким виртуальным локальным сетям, защищенным микросегментацией и изоляцией?

Что-то не получилось! Или не сделал?

Неудача определяется как нечто, что должно было сработать, но не сработало. Должно быть, что-то пошло не так с одним из сотен адаптивных элементов управления, политик безопасности и одиннадцати MSSP, которых мы наняли для обслуживания двадцати облачных приложений, связанных с нашей централизованной системой нулевого доверия, работающей внутри облачного удаленного доступа SASE для людей, работающих над -помещение.

Что может пойти не так? Все или ничего.

Кибербезопасность стала процессом реагирования, чрезмерного реагирования и недостаточного реагирования, а не решением или стратегией. С более чем 1000 поставщиков, которые делают все возможное, чтобы показать свои лучшие качества по сравнению со своими конкурентами, потребляющие корпоративные директора по информационным технологиям и директорам по информационным технологиям продолжат взлом, кражу данных и программы-вымогатели.

С каждым новым уровнем адаптивного управления безопасностью должен быть слой новой и улучшенной защиты и новых поверхностей для атак. Почему вы подозреваете, что эти устройства выходят из строя, если организация включила решение CASB или радиоантенны 5G для повышения безопасности? Обеспечили ли они уникальную ценность для бизнеса за счет повышенного риска и затрат на кибербезопасность?

Почему кибербезопасность принадлежит совету директоров?

Кибербезопасность будет оставаться успешной до тех пор, пока организации не осознают, что без подлинного, полностью интегрированного, аполитичного, непредвзятого подхода к защите организации и ее сотрудников, активов и данных, прежде чем они рискнут погрузиться в апокалипсис цифровой трансформации, они будет продолжать терпеть неудачу.

Бизнес зависит от клиентов. Потребители ведут дела с людьми, которым они доверяют. Если потребитель потеряет веру в компанию, он будет меньше говорить о вашей организации и решит потратить свои деньги в другом месте.

Даже если вы только что потратили миллионы, основываясь на том, что ваши «доверенные консультанты» рекомендовали все эти «материалы» для соответствия требованиям SOC2, CMMC level3, HIPAA, NIST-800–53 и PCI.

Как жить с успешным провалом в киберпространстве?

Первая важная вещь, которую нужно помнить: как только кибербезопасность становится угрозой для организации, и вы решите внедрить технологию «флажок» от своих надежных поставщиков, вы уже проиграли. Во-вторых, самое важное, что нужно помнить, это не повторять то, что вы только что сделали; учиться на этом.

Продвижение вперед в области кибербезопасности начинается с осознания бизнесом того факта, что кибербезопасность интегрирована в культуру доверия компании. Каждое решение имеет защиту от кибербезопасности в ДНК. Приобретение компаний, наем подрядчиков, использование открытого исходного

кода для экономии денег (мы оставим это для другого блога) и, что мне больше всего нравится, всегда ведение бизнеса с одними и теми же VAR. «Доверенный советник» не должен иметь ничего общего с продуктами или услугами. Они только рассказывают вам, как защитить вашу организацию, повысив эффективность защиты от кибербезопасности за счет уменьшения возможных сбоев…» ***(John P. Gormally. Cybersecurity is a Successfully Failure // Medium (https://jpgormally.medium.com/cybersecurity-is-a-successfully-failure-9bcf92a1bc88). 10.10.2022).***

***

«Кибербезопасность существует уже несколько десятилетий, но многие предприятия не имеют инфраструктуры для защиты своих активов. На самом деле, некоторые считают, что это слишком дорого, и что их ресурсы лучше инвестировать в развитие бизнеса. Однако кибербезопасность необходима для предприятий любого размера и отрасли. Без этого компании могут потерять все.

Нарушения подвергают клиентов риску

Когда клиенты размещают заказ, они верят, что их личная информация в безопасности. Однако исторические нарушения поставили миллионы обычных людей под угрозу кражи личных данных; в худшем случае хакеры могут получить доступ к платежной информации и номерам социального страхования. Затем хакеры продают эту информацию в даркнете мошенникам, которые не стесняются портить репутацию своих жертв.

Хуже всего то, что без внутренней системы мониторинга угроз или управляемого обнаружения и реагирования (также называемого MDR) компании могут даже не знать, что они столкнулись с нарушением. Задержка ответов означает, что киберпреступники имеют больше доступа к информации, что означает больший ущерб. Когда информация о клиентах попадает в чужие руки, общественность ожидает, что компании сделают все правильно, заплатив за мониторинг кражи личных данных, расходы, которых можно было бы легко избежать с помощью надежной системы безопасности.

Хакеры могут взять бизнес в заложники

Программа- вымогатель представляет собой распространенную угрозу для бизнеса, поскольку она предлагает большие выплаты хакерам. В отличие от других взломов, программы-вымогатели не молчат — они объявляют о своем присутствии, блокируя доступ компаний к их системам. Затем хакеры связываются с компанией и угрожают уничтожить информацию, если компании не заплатят выкуп, отсюда и название.

Вы можете застраховать себя от таких атак, но их предотвращение обходится дешевле, если обеспечить надежную сетевую безопасность. Ведь разрекламированные кибератаки могут стоить более нескольких миллионов долларов.

Кибератаки отрицательно сказываются на имидже компании

Когда потребители узнают, что компания была взломана, они могут отказаться от сотрудничества с этим брендом в будущем. В конце концов, кто хочет рисковать своей информацией? Даже если компании обновят свою систему безопасности,

потребители могут почувствовать, что эти компании не ценят своих клиентов, и решат уйти в другое место. Устранение этого удара по репутации бренда требует значительных инвестиций, и предприятия могут легко избежать еще одних затрат.

Целями могут стать предприятия любого размера

Некоторым владельцам малого бизнеса может казаться, что их компании слишком малы, чтобы их можно было атаковать. К сожалению, хакеры не делают различий — они нападают на любого, кто не защищен должным образом. Атака может быть особенно разрушительной для стартапов и семейных магазинов, поскольку у них нет ресурсов для восстановления. Помимо компенсации клиентам и усиления защиты, предприятиям также может потребоваться защищать себя в суде, поскольку клиенты могут подать в суд, если нарушение произошло из-за халатности. Для небольших команд это может заставить их выйти из бизнеса.

Отсутствие кибербезопасности может увеличить страховые взносы

Как уже упоминалось, владельцы бизнеса теперь могут приобрести страховку от кибератак. Хотя это снижает непосредственные затраты на выкуп, обновления и судебные разбирательства, у этого есть своя цена. Как только ваша компания сталкивается с нарушением, ваша страховая премия может возрасти, поскольку страховая компания пытается возместить свои убытки. Вот почему крайне важно поддерживать отличную кибербезопасность, даже если у вас есть страховка.

Кибербезопасность может предотвратить большинство атак

По оценкам экспертов, профилактические меры могут остановить до 93% нарушений. На самом деле, большинство рекомендуемых действий достаточно просты. Например, специалисты по кибербезопасности советуют в качестве первой линии защиты внедрить двухфакторную аутентификацию, обучение сотрудников и регулярные обновления программного обеспечения. Поскольку киберпреступники создают новые способы обхода безопасности, компаниям следует адаптироваться в соответствии с рекомендациями экспертов.

Инвестирование в кибербезопасность может стоить немалых денег, но это не так дорого, как взлом. Все предприятия должны уделять приоритетное внимание защите системы, даже если риск атаки кажется небольшим. Это гарантирует их будущее и поддерживает их конкурентоспособность в технологическом веке». ***(Kevin Gardner. Why All Businesses Should Invest in Cybersecurity // TechSpective (https://techspective.net/2022/10/21/why-all-businesses-should-invest-in-cybersecurity/). 21.10.2022).***

***

«Киберпреступники всегда стремятся сделать свои атаки, мошенничества и кампании максимально эффективными. Это включает в себя использование всего, что доминирует в повестке дня новостей и находится на уме их жертв.

Экономическая неопределенность и риски кибербезопасности

Одним из примеров является текущая экономическая неопределенность и давление на стоимость жизни, с которыми сталкиваются многие потребители во всем мире. Стресс, страх и беспокойство, которые испытывает общественность, к сожалению, являются идеальным сценарием для киберпреступников.

Показательный пример: всего за двухнедельный период 1567 фишинговых кампаний по электронной почте, связанных с мошенничеством со скидками на энергию, были зарегистрированы через Службу сообщений о подозрительных электронных письмах (SERS) Action Fraud. Также: Мошенничество с друзьями и семьей — термин, используемый для кампаний, в которых мошенники выдают себя за членов семьи, чтобы обмануть родственников, чтобы отправить деньги для оплаты счетов — увеличился на 58% в последние месяцы, согласно данным TSB.

Риски внутри бизнеса

Хотя эти мошенничества могут быть нацелены в первую очередь на отдельных лиц, организации, в которых они работают, также могут подвергаться риску. Чрезвычайное давление (или принуждение) повышает вероятность того, что отдельные лица станут источником риска инсайдерской угрозы — кражи данных, средств или другой конфиденциальной информации у своих работодателей. Не говоря уже об угрозе со стороны мошенников, выдающих себя за руководителей или менеджеров с фиктивными запросами на перевод денег. Все может быть вектором потенциального инцидента — недовольные бывшие сотрудники, неиспользуемые учетные записи с полными правами администратора, неправильно настроенное облачное хранилище, оставляющее данные открытыми, и так далее.

Экономический спад и неопределенность заставят многие организации пересмотреть свои расходы и сократить их. Это естественная реакция.

Проблема с кибербезопасностью заключается в том, что по самой своей природе успешные программы кибербезопасности часто невидимы. Тихо работая в фоновом режиме, они предотвращают эскалацию угроз и инцидентов и не доводят их до уровня, когда они становятся заметными для остальной части организации. Если руководители не столкнулись с кризисом кибербезопасности на собственном опыте, у них может возникнуть соблазн уменьшить сумму, которую они инвестируют в имеющиеся у них инструменты и таланты. Но это тонкая грань — сокращение жизненно важных элементов управления и возможностей может повлиять на способность организации видеть, ощущать и реагировать на события до того, как они обострятся. Нарушение, как правило, разрушительно для компании, но одно в это время может быть еще более разрушительным.

Удаление наворотов, а не возможностей

В то же время на рынке кибербезопасности исторически доминировали специализированные точечные продукты. Компании могут накапливать всевозможные инструменты и решения для управления как своей ИТ-инфраструктурой, так и кибербезопасностью. Согласно исследованию Panaseer, переход к облачным технологиям и удаленной работе за последние два года привел к увеличению среднего количества инструментов безопасности, которыми должны управлять организации, с 64 до 76 на 19%. Это даже без учета более широкого набора имеющихся ИТ-активов, от облачных сервисов и программного обеспечения до рабочих станций, персональных мобильных устройств, пользователей и многого другого.

В зависимости от размера компании отдельные отделы могут использовать пересекающиеся инструменты для решения одной и той же проблемы. С таким количеством индивидуальных решений и программного обеспечения

неудивительно, что группы безопасности могут чувствовать себя перегруженными и неспособными отслеживать инциденты и реагировать на них.

Чрезмерное количество оповещений и предупреждений вызывает усталость и затрудняет отделение реальных угроз от ложных тревог, что усугубляет проблему. В среднем требуется 86 человеко-часов с использованием восьми различных инструментов, чтобы вручную составить опись всего, что может использовать организация. Результаты часто могут устареть к моменту завершения инвентаризации.

Эффективное обнаружение и реагирование на кибербезопасность возможно только в том случае, если ИТ-команды знают, с чем им приходится работать и как взаимодействуют пользователи и данные. Им нужна непрерывная, точная и актуальная информация для снижения угроз, управления рисками и нейтрализации инцидентов.

Хотя повышение эффективности и сокращение бюджетов является разумной реакцией в период роста затрат и снижения прибыли, киберпреступники никогда не отдыхают. Компании должны тщательно соблюдать грань между устранением раздувания и приятного и сокращением своих возможностей в области кибербезопасности, иначе лидеры могут оказаться в ситуации, когда им придется платить гораздо больше». ***(Chris Cochran. Economic uncertainty is increasing cybersecurity risks // Help Net Security (https://www.helpnetsecurity.com/2022/10/17/economic-uncertainty-increasing-cybersecurity-risks/). 17.10.2022).***

***

Сполучені Штати Америки та Канада

«7 октября 2022 года президент Байден подписал Исполнительный указ об усилении мер безопасности в отношении разведывательной деятельности США в области радиосвязи 1, который предназначен для выполнения обязательств США в рамках Трансатлантической системы конфиденциальности данных (DPF), о которой было объявлено в марте 2022 года. С новым исполнительным директором Для этого администрация Байдена стремится укрепить правовую основу для трансатлантических потоков данных после решения Шремса II от 2020 года в котором Суд Европейского союза (CJEU) отменил решение Европейской комиссии об адекватности, лежащее в основе схемы самосертификации рамочной схемы обмена конфиденциальной информацией между ЕС и США. Исполнительный указ создает дополнительные гарантии конфиденциальности и гражданских свобод для деятельности США по сбору разведывательных данных, а также новый «Механизм исправления разведывательных сигналов», который включает новый «Суд по рассмотрению защиты данных». Затем ожидается, что Европейская комиссия подготовит проект решения об адекватности, чтобы принять DPF в качестве действительного механизма передачи для передачи персональных данных из Европейского Союза в Соединенные Штаты.

В этом юридическом обновлении кратко излагаются основные изменения в соответствии с указом, дальнейшие действия ЕС и альтернативные базы для передачи данных между ЕС и США, в то время как ЕС оценивает DPF как реализованный посредством указа.

Ключевые события в рамках исполнительного указа

Основные положения указа:

Внедрить дополнительные меры безопасности и принципы ограничения деятельности США по сбору разведывательной информации. В дополнение к существующим ограничениям, налагаемым законом или актами исполнительной власти, исполнительный указ устанавливает новые ограничения на деятельность США по сбору разведывательной информации. Например:

Действия по сбору разведывательных сигналов должны проводиться для достижения «законных целей», изложенных в указе, включая, например, «защиту от угроз персоналу Соединенных Штатов или их союзников или партнеров». (В исполнительном указе также указаны «запрещенные цели» деятельности по сбору разведывательных данных, такие как «подавление или ограничение права на адвоката».)

В соответствии с распоряжением, любая деятельность по сбору разведывательных данных должна следовать определению, основанному на «разумной оценке всех соответствующих факторов», что конкретная деятельность «необходима для продвижения утвержденного приоритета разведки». Действия по сбору разведывательных сигналов «должны осуществляться только в объеме и таким образом, которые пропорциональны утвержденному приоритету разведывательных данных, для которого они были уполномочены».

Кроме того, директор национальной разведки должен получить оценку системы приоритетов национальной разведки от офицера по защите гражданских свобод США (CLPO) в Управлении директора национальной разведки (ODNI) «для того, чтобы гарантировать, что сигналы деятельность по сбору разведданных осуществляется для достижения законных целей». Директор должен представлять приоритеты сбора радиосигналов президенту через помощника президента по вопросам национальной безопасности на «регулярной основе».

В указе также неоднократно говорится, что деятельность по радиоразведке должна учитывать неприкосновенность частной жизни и гражданские свободы всех лиц, «независимо от их национальности или места проживания».

Ограничить массовый сбор личных данных. Распоряжение в соответствии с разделом 2(c) ограничивает массовый сбор радиоразведывательной информации теми видами деятельности, которые разрешены «на основании определения» соответствующих элементов IC, «что информация, необходимая для продвижения утвержденного приоритета разведывательной информации, не может разумно быть получены путем целенаправленного сбора». Получив разрешение, IC должен «применять разумные методы и технические меры, чтобы ограничить собираемые данные только тем, что необходимо для продвижения подтвержденного разведывательного приоритета, сводя к минимуму сбор не относящейся к делу информации». Любая разведывательная информация, собранная посредством

массового сбора, должна преследовать более ограниченный подмножество «целей», изложенных в указе.

Разработайте и применяйте политики и процедуры, направленные на минимизацию распространения и хранения личной информации, собранной с помощью радиоразведки. Исполнительный указ в соответствии с разделом 2(c) требует, чтобы каждый элемент IC, который обрабатывает личную информацию, собранную с помощью радиотехнической разведки, распространял эту личную информацию только в правительстве США, если «уполномоченное и должным образом обученное лицо имеет разумные основания полагать, что что личная информация будет надлежащим образом защищена и что получатель должен знать эту информацию». Исполнительный указ также ограничивает хранение личной информации лиц, не являющихся гражданами США, теми же стандартами и сроками хранения для сопоставимой информации, касающейся жителей США.

Требовать от разведывательного сообщества США обновления своих политик и процедур. Исполнительный указ в соответствии с разделом 2(c) предписывает каждому элементу IC обновить свои внутренние процессы, чтобы привести их в соответствие с гарантиями конфиденциальности и гражданских свобод, изложенными в исполнительном указе, в том числе путем выполнения следующих действий:

В течение одного года после распоряжения провести консультации с Генеральным прокурором, CLPO и Советом по надзору за соблюдением конфиденциальности и гражданских свобод (PCLOB), чтобы убедиться, что его политики и процедуры соответствуют расширенным гарантиям защиты конфиденциальности и гражданских свобод;

В течение одного года после распоряжения опубликовать эти политики и процедуры в максимально возможной степени, чтобы улучшить понимание общественностью его практики;

Назначить старших должностных лиц по юридическим вопросам, надзору и комплаенсу, которые осуществляют периодический надзор за деятельностью радиотехнической разведки, и предоставить этим должностным лицам доступ ко всей соответствующей информации;

Поддерживайте надлежащее обучение для всех сотрудников, имеющих доступ к средствам разведки, чтобы понять требования исполнительного распоряжения, а также политики и процедуры сообщения о несоблюдении и устранения несоблюдения.

Создайте «Механизм исправления разведывательных сигналов». Исполнительный указ в соответствии с разделом 3 установит механизм возмещения ущерба для рассмотрения жалоб, переданных соответствующим государственным органом в соответствующем штате, и оценки того, были ли нарушены какие-либо охватываемые законы США.

Во-первых, соответствующие штаты смогут подавать жалобы в CLPO. (Распоряжение устанавливает, что процесс подачи такого заявления будет установлен в течение 60 дней с момента издания распоряжения.) CLPO будет нести ответственность за первоначальное расследование жалоб и определение надлежащих средств правовой защиты.

Во-вторых, заявитель или элемент IC может обратиться в Суд по пересмотру защиты данных (DPRC) для пересмотра решения CLPO. Исполнительный приказ уполномочивает и предписывает Генеральному прокурору издавать постановления (которые были изданы в тот же день, что и указ) о создании КНДР. В консультации с министром торговли, директором национальной разведки и PCLOB генеральный прокурор назначит судей для работы в DPRC, которые имеют соответствующий опыт в области конфиденциальности данных и закона о национальной безопасности, принимая во внимание предыдущий судебный опыт, и которые не являлись на момент их первоначального назначения служащими правительства США. По каждому заявлению о пересмотре коллегия из трех судей DPRC созывается и выбирает «специального адвоката» с необходимым уровнем допуска для защиты интересов заявителя. В конечном счете, DPRC сможет провести обзор решений CLPO, и его решение будет обязательным для IC. PCLOB также будет иметь право ежегодно пересматривать этот процесс возмещения ущерба.

Следующие шаги от ЕС

Когда персональные данные передаются в страны за пределами Европейской экономической зоны (ЕЭЗ), передача должна осуществляться в соответствии с главой V GDPR. Глава V описывает несколько инструментов, на которые могут положиться предприятия при передаче данных в третьи страны. Одним из инструментов является решение об адекватности, утвержденное Европейской комиссией, которое подтверждает, что конкретные страны обеспечивают адекватный уровень защиты данных и средства правовой защиты для субъектов данных в соответствии со своим местным законодательством. Переводы в страны, не получившие решения об адекватности, включая Соединенные Штаты, должны предусматривать «надлежащие гарантии» для защиты персональных данных с помощью действующего механизма передачи данных, такого как Стандартные договорные положения (SCC), который в настоящее время является наиболее распространенным методом передачи персональных данных из ЕЭЗ в Соединенные Штаты.

Новая структура между ЕС и США для международной передачи персональных данных, реализованная посредством исполнительного указа, призвана действовать как «надлежащая защита» в соответствии с GDPR. Это будет означать, что в случае одобрения соответствующими регулирующими органами ЕС предприятия смогут передавать персональные данные в Соединенные Штаты без использования SCC, если получатель сертифицирован в соответствии с новым DPF.

Европейская комиссия теперь рассмотрит DPF и инициирует свой проект решения об адекватности и процедуру принятия. В рамках этого процесса Европейский совет по защите данных («EDPB») представит проект решения об адекватности на рассмотрение комитета, состоящего из представителей государств-членов ЕС. Кроме того, Европейский парламент может осуществлять свое право проверки решений об адекватности. После проверки Европейская комиссия может принять окончательное решение о достаточности для Соединенных Штатов в отношении предприятий, которые полагаются на DPF для передачи личных данных. Если Соединенные Штаты будут утверждены в качестве страны с адекватностью данных, передача данных из ЕС в США компаниями, сертифицированными в

соответствии с DPF, больше не потребует отдельных механизмов передачи данных для обеспечения дополнительных гарантий. Европейская комиссия объявила, что «американские компании смогут присоединиться к этой структуре, взяв на себя обязательство соблюдать подробный набор обязательств в отношении конфиденциальности».

Альтернативные механизмы передачи данных

Пока Европейская комиссия готовит обзор решения о достаточности данных, предприятия могут по-прежнему полагаться на другие действующие механизмы передачи персональных данных из ЕС в США, включая SCC и обязательные корпоративные правила. SCC, которые являются наиболее распространенным механизмом передачи данных между ЕС и США, могут быть включены в коммерческие контракты предприятий. С 27 сентября 2021 г. во всех новых контрактах должны использоваться новые SCC, выпущенные Европейской комиссией в июне 2021 г. (SCC 2021). По состоянию на 27 декабря 2022 года все новые и существующие контракты должны использовать SCC 2021 года. Европейская комиссия выпустила практическое руководство для предприятий, использующих SCC 2021 года для передачи данных». ***(Rajesh De, Marcus A. Christian, Veronica R. Glick, Arsen Kourinian, Stephen Lilley, Dominique Shelton Leipzig, David A. Simon, Howard W. Waltzman, Oliver Yaros, Ana Hadnes Bruder, Ellen Hepworth, Megan P. Von Borstel. President Biden Signs Executive Order on U.S. Intelligence Activities to Implement EU-U.S. Data Privacy Framework // Mayer Brown (https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/president-biden-signs-executive-order-on-us-intelligence-activities-to-implement-eu-us-data-privacy-framework). 10.10.2022).***

***

«В этом месяце федеральное правительство проводит обсуждения о том, как разработать метки кибербезопасности для маршрутизаторов, домашних камер и других потребительских устройств IoT. Цель состоит в том, чтобы помочь покупателям понять, насколько на самом деле безопасны продукты. Также в федеральной киберповестке октября: встреча с международными партнерами по борьбе с программами-вымогателями.

Белый дом объявил об этих и других инициативах в информационном бюллетене от 11 октября.

В документе рассматриваются многие цели, которые президент Джо Байден изложил в своем указе от мая 2021 года по национальной кибербезопасности. В нем был рассмотрен прогресс США в таких усилиях, как распространение передового опыта на федеральном уровне, рост рабочей силы в области кибербезопасности и продвижение исследований в области квантово-устойчивого шифрования.

В указе президента Байдена от мая 2021 года «Об улучшении национальной кибербезопасности» содержится призыв предоставить общественности больший контроль над своей подверженностью риску путем маркировки потребительских продуктов IoT этикетками, указывающими, насколько эти предложения кибербезопасны.

Белый дом теперь планирует в этом месяце собрать вместе частные компании, ассоциации и государственные органы, чтобы обсудить, как разработать такую маркировку. Конечная цель состоит в том, чтобы «общая этикетка для продуктов, которые соответствуют стандартам правительства США и тестируются проверенными и утвержденными организациями», говорится во вчерашнем информационном бюллетене.

БОРЬБА С ПРОГРАММОЙ-ВЫМОГАТЕЛЕМ НА МЕЖДУНАРОДНОМ УРОВНЕ

Наряду с указом Байдена май 2021 года также принес влиятельный отчет о программах-вымогателях. Целевая группа по программам-вымогателям, координируемая Институтом безопасности и технологий (IST), опубликовала отчет с подробным описанием глобального характера экосистемы программ-вымогателей и рекомендациями по борьбе с угрозой.

Примерно полтора года спустя информационный бюллетень Белого дома отслеживает прогресс. Среди основных моментов: Международная инициатива по борьбе с программами-вымогателями (CRI), которую федеральное правительство запустило в 2021 году для активизации международного сотрудничества и которая снова собирается с 31 октября по ноябрь.

Федеральные субъекты также стремились сделать кибервымогательство менее прибыльным и более болезненным, прервав поток выкупа и приняв более жесткие меры. В информационном бюллетене отмечается, что он наложил санкции на несколько микшеров криптовалюты, обычно используемых злоумышленниками-вымогателями, экстрадировал и заключил в тюрьму некоторых отдельных преступников, а также наложил санкции на кибер-деятелей, которые, как считается, были причастны к атаке SolarWinds.

США обращаются к международным партнерам и для решения других киберпроблем. Это включало усилия по установлению и обеспечению соблюдения кибернорм, что, по словам Белого дома, он поддерживает, критикуяи «наложение расходов» на Иран, когда правительство перешло черту, запустив кибератаки против правительства Албании. Белый дом также указал на «новый виртуальный механизм быстрого реагирования в НАТО, чтобы союзники могли эффективно и действенно предлагать друг другу поддержку в ответ на киберинциденты».

ГОСУДАРСТВЕННАЯ БЕЗОПАСНОСТЬ, КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА

Федеральное правительство также стремилось обеспечить безопасность своего собственного дома, потребовав многофакторной аутентификации во всех своих системах — что-то, обещанное майским исполнительным указом, — и разработав стратегию принятия нулевого доверия.

Более новые требования также ограничили федеральные агентства закупкой только программного обеспечения с функциями безопасности. Этот шаг призван защитить правительство, а также побудить поставщиков поднять все свои продукты до этого уровня, независимо от клиентской базы.

Ожидается, что финансирование, такое как Государственная и местная программа грантов в области кибербезопасности, поможет другим уровням правительства укрепить свои позиции в области кибербезопасности.

Белый дом также рекламировал усилия, направленные на то, чтобы выйти за рамки государственного сектора. Это включает в себя продвижение базовой кибергигиены и понимания угроз среди частных организаций, которые владеют и управляют большей частью критической национальной инфраструктуры. До сих пор это наблюдалось в банковском секторе, здравоохранении, транспорте и водном секторе.

СТРОИМ БУДУЩЕЕ: КАДРЫ И ИССЛЕДОВАНИЯ

Согласно отчету NASCIO, опубликованному на этой неделе, нехватка специалистов в области кибербезопасности остается насущной проблемой и серьезной проблемой для директоров по информационным технологиям штатов. Белый дом заявил, что стремится наращивать рабочую силу с целью создать больше возможностей для работы в киберпространстве и внести больше разнообразия в эту область. 120-дневный спринт по обучению кибербезопасности, запущенный в июле 2022 года, направлен на поддержку таких усилий.

Федеральное правительство также «более чем удвоило» инвестиции в квантовые исследования и разработки, стремясь сохранить конкурентоспособность в космосе и опередить угрозы. Это включает в себя усилия по разработке и развертыванию форм криптографии, предназначенных для защиты от взлома любых будущих квантовых компьютеров». ***(White House Reports on Federal Cybersecurity Progress // e.Republic (https://www.govtech.com/security/white-house-reports-on-federal-cybersecurity-progress). 12.10.2022).***

***

«Требования кибербезопасности для организаций, имеющих решающее значение для повседневного функционирования Соединенных Штатов, будут распространяться на новые сектора, заявил сегодня высокопоставленный чиновник администрации Байдена.

Администрация также намерена создать новую добровольную программу маркировки кибербезопасности для потребительских устройств на фоне общего признания того, что кибербезопасность превратилась из ниши в проблему качества жизни. Повсеместная связь означает, что хакеры могут заниматься чем угодно: от преследований и краж до атак на национальное государство.

Системы общественного водоснабжения скоро перейдут под действие нового мандата по кибербезопасности, выданного Агентством по охране окружающей среды, заявила Энн Нойбергер, заместитель советника Белого дома по национальной безопасности, во время мероприятия в Вашингтоне. По словам Нойбергера, существующие полномочия EPA по регулированию безопасности и защиты воды распространяются и на кибербезопасность.

По словам Нойбергера, Министерство здравоохранения и социальных служб изучает стандарты кибербезопасности для больниц. Федеральная комиссия по связи уже недавно инициировала процесс разработки правил, требующий от вещательных компаний и провайдеров сотовых сетей, которые передают оповещения о чрезвычайных ситуациях, наличия основных мер кибербезопасности, таких как план управления рисками.

По словам Нойбергера, Администрация транспортной безопасности, которая регулирует весь транспортный сектор, несмотря на то, что она наиболее известна обеспечением безопасности аэропортов, опубликует этой зимой обновленные директивы по кибербезопасности для общественного транспорта и пассажирских железных дорог. В июле агентство опубликовало вторую версию своей директивы по кибербезопасности для трубопроводной отрасли.

Позже в этом месяце Белый дом соберет производителей интернета вещей, чтобы обсудить программу добровольной маркировки продуктов, отвечающих минимальным стандартам безопасности. Программа начнется с маршрутизаторов и домашних камер, «наиболее распространенных и часто подвергающихся наибольшему риску технологий», говорится в сообщении Белого дома.

Проблемы кибербезопасности вырисовывались перед администрацией Байдена почти с самого начала, в том числе многодневная нехватка бензина у потребителей в мае 2021 года, вызванная атакой программы-вымогателя на Colonial Pipeline. Президент Джо Байден инициировал усилия по повышению кибербезопасности систем промышленного контроля в частном секторе посредством регулирования, где это возможно, и в других случаях с помощью добровольных мер. Примерно 85% систем США, необходимых для обычной жизни, таких как производство электроэнергии или оказание медицинских услуг, находятся в частной собственности.

В сентябре представитель Министерства внутренней безопасности признал, что администрация отстает от крайнего срока для развертывания целевых показателей производительности для всех 16 секторов, составляющих критически важную инфраструктуру.

По словам Нойбергера, администрация не намерена применять свои директивы ко всем организациям в секторе критической инфраструктуры. Вместо этого они предназначены для «крупных игроков», для которых сбой окажет большое влияние на американцев, сказала она». ***(David Perera. Biden Administration Ramps Up Cybersecurity Requirements // Information Security Media Group, Corp. (https://www.govinfosecurity.com/biden-administration-ramps-up-cybersecurity-requirements-a-20257). 13.10.2022).***

***

«Эксперты говорят, что малые предприятия должны серьезно относиться к кибербезопасности в более широкой среде, в которой последние статистические данные Национальной ассоциации уполномоченных по страхованию (NAIC) показывают, что средний коэффициент киберубытков для 20 ведущих страховых групп, предоставляющих страхование кибербезопасности в 2020 году, составляет 66,9%. 44,6% в 2019 году.

Стивен В. Тепплер, председатель практики кибербезопасности и конфиденциальности в юридической фирме Mandelbaum Barrett PC в Розленде, подчеркивает важность как кибербезопасности, так и предотвращения/реагирования на утечку данных. Он объясняет: «Вы хотите продолжать [управлять] своим бизнесом, и вы не хотите, чтобы вас загнали в землю [и вы несете] ответственность в четверть миллиона долларов, если у вас есть утечка данных [как] малый бизнес».

Он также советует: «Вложения в безопасность не окупаются, но, как и в страховании, оглядываясь назад, они выглядят очень и очень дешево».

Векторы угроз кибербезопасности

Что касается бесчисленных компаний, которые считают, что они уже должным образом справились с кибербезопасностью, статистика ФБР показывает, что проблемы явно остаются: например, в 2021 году было 19 954 инцидента компрометации деловой электронной почты (BEC), что практически не изменилось по сравнению с 19 369 в 2020 году. убытки достигли ошеломляющей общей суммы почти в 2,4 миллиарда долларов.

«[Актеры угроз] становятся все более изощренными [и] действуют как против малых, так и против крупных компаний, — объясняет Тепплер из Mandelbaum Barrett. «[Например, они] узнают, когда ваш сотрудник по кадрам или финансам уходит в отпуск, и если они смогут взломать электронную почту [этого человека], они затем подделают свою личность [и] вызовут банковский перевод. на мошеннический аккаунт. Это то, на что вы должны обращать внимание».

В отчете ФБР об интернет-преступлениях за 2021 год подробно говорится, что по крайней мере с начала пандемии COVID-19 преступники BEC, например, взламывают учетную запись электронной почты финансового директора, а затем запрашивают виртуальную встречу с сотрудником (сотрудниками) компании, на которой преступники вставляют неподвижное изображение генерального директора / финансового директора. После заявления о том, что звук не работает, или путем «глубокой подделки» звука генерального директора или финансового директора, преступники затем запрашивают мошеннический банковский перевод либо через саму виртуальную встречу, либо через скомпрометированную электронную почту финансового директора.

Каковы другие распространенные сценарии кибербезопасности? Майкл Джерати, главный специалист по информационной безопасности штата Нью-Джерси и директор Группы по интеграции кибербезопасности и связи Нью-Джерси (NJCCIC) (организация, входящая в состав Управления внутренней безопасности и готовности штата Нью-Джерси), сообщил журналу New Jersey Business Magazine, что «человеческий ошибки», в том числе отказ от смены паролей, отказ от использования многофакторной аутентификации (MFA), отказ от установки исправлений программного обеспечения/операционных систем и попадание под фишинговые электронные письма — ключевые области кибербезопасности, в которых преступники добиваются успеха.

В целом Джерати говорит: «То, как мы смотрим на кибербезопасность здесь [в NJCCIC] — особенно [с] злоумышленниками из любой точки мира, в любое время дня [и] с любым набором навыков (будь то начинающий злоумышленник или государственный деятель) – важно не то, насколько вы ценны, а то, насколько вы уязвимы».

И уязвимость может существовать в почти бесконечном множестве итераций. Например, Рашаад Баджва, основатель и генеральный директор базирующейся в Крэнбери Integris — национального поставщика премиальных услуг в области ИТ и кибербезопасности для малого и среднего бизнеса — предостерегает, что

предприятия не должны оставлять компьютерное оборудование без присмотра в офисах удаленной работы.

«В офисах стоит много компьютеров, коммутаторов и устройств Wi-Fi, которые не защищены, и сотрудники ими не пользуются», — объясняет он. «[Эти устройства] не исправляются и не контролируются, и ими можно воспользоваться». Однако он добавляет, что неблагоприятные инциденты (такие как дворники или другие лица, получающие доступ к компьютерам) еще не стали «мейнстримом среди плохих парней».

Подход к кибербезопасности

Имея на руках эти и другие угрозы кибербезопасности, малый бизнес может использовать по крайней мере два общих превентивных подхода: первый — связаться с адвокатом по кибербезопасности, который — на условиях адвокатской тайны — может порекомендовать компанию по киберстрахованию, экспертов по кибербезопасности и возможно, кризисная PR-фирма, последняя полезна в случае возникновения инцидента кибербезопасности. Адвокаты могут дополнительно оценивать как риски, так и политики кибербезопасности, выступать в качестве ответственных лиц во время разворачивающихся инцидентов кибербезопасности и при необходимости привлекать доверенных экспертов по киберкриминалистике.

Тепплер из Mandelbaum Barrett говорит о превентивной тактике в целом: «Под прикрытием конфиденциальности адвоката и клиента мы «проверяем машину» и убеждаемся, что она работает и что нет никаких утечек или неисправностей. Затем мы представляем [результаты] клиенту и говорим: «Послушайте, здесь у вас есть пробелы, а здесь их нет».

Другой метод решения проблемы кибербезопасности включает в себя простое обращение к поставщику управляемых ИТ-услуг, а затем при необходимости наем юриста для заключения контрактов и документации.

Однако не всегда достаточно адвоката. Баджва из Intergris объясняет: «Прежде чем [предприятия] найдут собственных адвокатов, компаниям следует поговорить со своими поставщиками киберстрахования, потому что у них часто есть адвокаты, с которыми они потребуют, чтобы вы работали».

Он добавляет: «То же самое относится и к таким компаниям, как наша. Мы помогаем с реагированием и возобновлением бизнеса после утечки [данных], но не каждая страховая компания работает с каждым ИТ-провайдером. У многих из них есть свои… тренеры по взлому, специалисты по кибербезопасности и криминалисты, с которыми они работают. Точно так же, как если бы вы попали в автомобильную аварию, [страховая компания] не обязательно работает с каждой ремонтной мастерской».

Превентивные меры

Какие конкретные шаги в области кибербезопасности могут предпринять малые предприятия? Опять же, они частично включают в себя использование многофакторной аутентификации (MFA), поддержание всего программного обеспечения в актуальном состоянии, а также обучение сотрудников осведомленности о кибербезопасности (например, обучение их не нажимать на неизвестные ссылки электронной почты, открывать неизвестные вложения или стать жертвой схем социальной инженерии). Готовность также означает правильную

настройку брандмауэров, закрытие портов (включая протокол удаленного рабочего стола (RDP)) и правильное использование облачных конфигураций. Эксперты также говорят, что хорошая защита конечных точек имеет ключевое значение, например, с расширенным обнаружением и реагированием (EDR) и управляемым обнаружением и реагированием (MDR), которые в основном связаны с обнаружением угроз и реагированием на них, в отличие от традиционного антивирусного программного обеспечения на основе шаблонов.

Но это еще не все: Тепплер из Mandelbaum Barrett объясняет, что компании должны не только учитывать все свои вычислительные устройства, но и понимать поток информации как внутри, так и в/из своей организации, кто имеет к ней доступ и в какой степени. Затем можно обнаружить пробелы в кибербезопасности.

Более широкие шаги

Более широкий подход компании может включать разработку политик кибербезопасности, резервного копирования, реагирования на инциденты, аварийного восстановления и обеспечения непрерывности бизнеса. Тепплер объясняет: «По сути, это то, что вы делаете, когда что-то происходит: кто что делает? Сделайте это понятным и проверяемым способом, и убедитесь, что вы практиковали… упражнение с фальшивым вторжением».

Вывод

Хотя ни один план кибербезопасности не является безопасным на 100%, Баджва из Integris говорит: «Мы подходим к моменту [во времени], когда существует несколько уровней защиты, чтобы уберечь людей от их собственных [кибер] ошибок… в отличие от прошлого, где один случайный щелчок, одна случайная ошибка [будет означать], что придется заплатить огромную цену».

Он добавляет: «Мы движемся в правильном направлении. … Я думаю, что технологии совершенствуются быстрее и лучше, чем способность плохих парней находить уязвимости».

Однако явные и реальные опасности остаются для всех компаний, особенно для тех, которые не используют надлежащие методы предотвращения.

Джерати из NJCCIC заключает: «Мы становимся [все более] зависимыми от подключенных систем во всем, что мы делаем, как в бизнесе, так и в нашей личной жизни. Очевидно, мы должны принять меры предосторожности, необходимые, чтобы не стать жертвами». ***(George N. Saliba. Hazards and Help with Cybersecurity // New Jersey Business Magazine (https://njbmagazine.com/monthly-articles/hazards-and-help-with-cybersecurity/). 06.10.2022).***

***

«В марте 2022 года президент Джозеф Байден подписал Закон об отчетности о кибер-инцидентах для критически важной инфраструктуры от 2022 года, который поручил Агентству кибербезопасности и безопасности инфраструктуры (CISA) разработать и внедрить правила, касающиеся отчетности о кибер-инцидентах и выплате выкупа. Согласно закону, CISA должна собирать информацию, которую она получает от подпадающих под действие организаций, и анализировать ее в той мере, в какой такая информация может быть

использована для определения способов предотвращения подобных инцидентов в будущем или сведения к минимуму вредных потенциальных последствий.

9 сентября 2022 года CISA объявила, что выпустит запрос на информацию (RFI) для сбора информации и комментариев по разработке правил отчетности, которые позволят CISA эффективно реагировать на киберинциденты и способствовать скоординированному подходу к предотвращению или смягчение подобных инцидентов в будущем. В тандеме с RFI CISA также будет проводить слушания по всей стране, чтобы предоставить широкой общественности форум для отзывов о правилах. Комментарии могут касаться тем, включая, помимо прочего, определения, содержание отчетности, процедуры отчетности и методы обмена информацией. Прежде чем опубликовать окончательное правило, CISA рассмотрит мнение общественности, полученное в ходе предстоящих слушаний, а затем опубликует уведомление о предлагаемом нормотворчестве.

Посредством закона CISA стремится предоставить целевым организациям возможность получать поддержку и помощь от государственных органов, а также предоставлять в CISA отчеты, «связанные с замаскированным кибер-инцидентом, для оценки эффективности средств контроля безопасности, выявления тактики, методов и процедур злоумышленников». использовать для преодоления этих средств контроля и других целей кибербезопасности, в том числе для оценки потенциального воздействия киберинцидентов на здоровье и безопасность населения, чтобы повысить ситуационную осведомленность о киберугрозах в критических секторах инфраструктуры». Закон также позволяет CISA отслеживать выплаты выкупа, связанные с киберинцидентами, и делиться собранной информацией с федеральными агентствами, чтобы оказывать помощь и реагировать соответствующим образом.

Сеансы прослушивания будут проводиться в течение всей осени, за ними последует Уведомление о предлагаемом нормотворчестве, которое будет содержать предлагаемые правила CISA в отношении отчетности о кибер-инцидентах и выплате выкупа». ***(KSENIA ANDREEVA, KELLI A. BOYLE. CISA Seeks Public Input on Cyber Incident and Ransom Payment Reporting // Morgan, Lewis & Bockius LLP. (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2022/10/cisa-seeks-public-input-on-cyber-incident-and-ransom-payment-reporting). 06.10.2022).***

***

«Согласно новому отчету, несмотря на обучение и наем сотен тысяч новых работников, нехватка рабочей силы в индустрии кибербезопасности только усугубляется, а не улучшается.

Международный консорциум по сертификации безопасности информационных систем, известный как ISC2, сообщает, что опрос 11 799 специалистов по кибербезопасности показывает, что общая глобальная численность персонала службы безопасности выросла за последний год до 4,6 миллиона человек, что на 11,1 процента больше.

Согласно отчету ISC2, некоммерческой организации, базирующейся в Александрии, штат Вирджиния, штат США по кибербезопасности вырос до 1,2 миллиона человек, что на 5,5 процента больше.

Увеличение рабочей силы является прямым результатом высокого спроса клиентов на инструменты и услуги безопасности на фоне всплеска кибератак по всему миру.

Но поскольку за последний год в индустрию кибербезопасности были наняты сотни тысяч людей, спрос на таланты продолжает превышать предложение, поскольку компании по всему миру изо всех сил пытаются укрепить свои системы безопасности.

В результате, согласно опросу ISC2, общее количество необходимых специалистов по кибербезопасности во всем мире выросло до 3,4 млн человек, что на 26,2% больше.

В США количество незаполненных рабочих мест выросло до 410 695, что на 9 процентов больше.

По данным ISC2, потребность в работниках наиболее остра в Азиатско-Тихоокеанском регионе, где за последний год количество необходимых работников выросло до 2,1 миллиона человек, что на 52,4 процента больше.

«Результаты показывают, что мы остро нуждаемся в специалистах по кибербезопасности, чтобы выйти на поле», — сказал Чар Россо, исполнительный директор ISC2, в интервью CRN по электронной почте. «Хотя только в этом году мы привлекли к работе 464 000 специалистов по кибербезопасности, дефицит рабочей силы продолжает расти, поскольку организации осознают стратегическую важность наращивания своих возможностей в области кибербезопасности».

Россо добавил, что «менеджеры по найму сказали нам, что им нужны члены команды начального и младшего звена с широкими базовыми навыками во многих областях».

Она добавила: «В частности, мы увидели, что навыки и опыт в области облачной безопасности пользуются большим спросом. Наша сертификация CCSP — одна из наших самых популярных сертификаций, и она предназначена для людей, желающих продвинуться в области облачной безопасности и архитектуры».

Россо также отметил, что организации сообщают о нехватке персонала по кибербезопасности среди всех ключевых категорий Национальной инициативы по образованию в области кибербезопасности (NICE). «Самая большая нехватка, с которой они сталкиваются, — это профессионалы в следственных функциях, таких как киберрасследование и цифровая криминалистика».

По словам Россо, один из способов сократить разрыв в найме для компаний, занимающихся кибербезопасностью, — расширить поле поиска новых работников.

«Чтобы добиться значительных успехов в сокращении нехватки кадров в области кибербезопасности, нам необходимо набирать людей из нетрадиционных слоев общества и устранять экономические и профессиональные барьеры, которые могут искусственно ограничивать рост или найм профессии», — сказал Россо.

«В частности, нам нужно привнести большее разнообразие в профессию, чтобы решать сложные задачи в нашей отрасли».

Кевин Макдональд, главный операционный директор и директор по информационным технологиям в Alvaka Networks, специалист по программам-вымогателям и MSP из Ирвина, штат Калифорния, согласен с тем, что сектор кибербезопасности должен иначе думать о том, как и кого он нанимает.

«Как отрасли мы должны наставлять людей и привлекать больше женщин», — сказал Макдональд, который также является сопредседателем Консультативного совета по кибербезопасности CompTIA.

Он сказал, что спрос на продукты и услуги в области безопасности продолжает расти.

«Компании, которые десятилетиями отрицали свои потребности в безопасности, теперь говорят: «О, мы должны что-то сделать», — сказал он. «К сожалению, в разработке не хватает рабочих».

В своем опросе ISC2 обнаружил, что 20 процентов респондентов заявили, что нехватка работников подвергает их организации «крайнему риску», а 54 процента заявили, что это подвергает организации «умеренному риску».

Согласно результатам опроса, нехватка рабочей силы особенно мешает таким категориям безопасности, как оценка и управление рисками; исправление критических систем; и обучение рабочих, среди других категорий.

Один результат опроса особенно озадачил Россо.

Она отметила, что в отчете четко показано, что «культура компании» во многом определяет опыт и удовлетворенность сотрудников фирмой.

«(Но) меня больше всего удивляет то, что многие организации не обязательно делают то, что наиболее эффективно, когда речь идет о поддержке своих групп безопасности и сотрудников», — сказала она CRN. «Только 28% специалистов по кибербезопасности сообщают, что их организации активно прислушиваются и ценят вклад всех сотрудников».

Хотя общая удовлетворенность сотрудников считается высокой в отрасли кибербезопасности, Россо сказал, что последнее, что нужно делать работодателям, — это отчуждать работников в условиях нехватки рабочей силы.

«Те, кто не удовлетворен культурными аспектами своей работы, говорят, что это влияет на их работу и реакцию на инциденты кибербезопасности, и они ищут новую работу», — сказал Россо. ***(Jay Fitzgerald. Cybersecurity Labor Shortage Grows Worse in U.S. And Worldwide: Report // The Channel Company (https://www.crn.com/news/security/report-cybersecurity-labor-shortage-grows-worse-in-u-s-and-worldwide). 24.10.2022).***

***

«Признание того, что у вас есть проблема, — это первый шаг к ее серьезному решению. Кажется, именно по этой причине Белый дом недавно объявил о своей инициативе «Укрепление кибербезопасности Америки».

Текст объявления содержит несколько утверждений, которые каждый, кто когда-либо читал о кибербезопасности, слышал много раз: повышение устойчивости, повышение осведомленности, противодействие атакам программ-вымогателей — этот список можно продолжить.

В тексте также есть некоторые новые аспекты, в том числе осознание того, что кибербезопасность не является, никогда не была и никогда не будет чем-то, что можно решить на уровне национального государства.

Белый дом также указал на предупредительные этикетки IoT в качестве решения и напомнил всем нам (и нам действительно нужно напоминание) о важности образования в области кибербезопасности. Давайте взглянем.

Международное сотрудничество имеет решающее значение

Ключевой момент, на который очень четко указывает заявление Белого дома, заключается в том, что кибератаки асимметричны в том смысле, что злоумышленники могут безнаказанно действовать через границы. Между тем, защитники часто будут ограничены правовыми требованиями, которые не допускают соразмерных ответов.

Злоумышленники чувствуют себя защищенными, потому что они пользуются более легкими регулятивными и правоприменительными мерами дома, в то время как они могут атаковать системы, работающие практически в любой точке планеты, независимо от того, насколько строго соблюдается закон в стране проживания цели.

Пока проблема не будет решаться на международном уровне, любые найденные решения будут не лучше пластыря. Инициатива Белого дома во многих случаях правильно заявляет, что международные партнеры и организации, такие как НАТО, будут играть решающую роль в пространстве кибербезопасности.

Это не идеальное решение. Да, совместная работа международных партнеров расширяет оборонный ландшафт до размеров, которые больше соответствуют масштабам проблемы. Однако это по-прежнему лоскутное решение с ограниченной эффективностью.

Нам нужно что-то вроде глобального договора, который фактически обеспечивает соблюдение закона о кибербезопасности. Просто подумайте, например, о влиянии международного морского права.

Тем не менее, обмен информацией о субъектах угроз, методологиях и новых методах, несомненно, отвечает интересам всех и, если он будет запущен надлежащим образом, позволит быстрее реагировать на новые угрозы.

Образование в области кибербезопасности по-прежнему имеет значение

Еще одним интересным аспектом инициативы «Усиление кибербезопасности Америки» является акцент на развитии образования в области кибербезопасности. Как нам постоянно и болезненно сообщают, кибербезопасность — это, прежде всего, проблема людей, а не проблема технологий.

Повышение грамотности в области кибербезопасности и обучение людей основам безопасного поведения в Интернете на всех этапах личной и деловой жизни будет иметь совокупный эффект как в снижении риска, так и в снижении воздействия любых инцидентов, которые неизбежно произойдут.

Возьмем, к примеру, Национальную инициативу по обучению кибербезопасности (NICE), поддерживаемую NIST. С формальной структурой, регулярными мероприятиями и обновлениями информационных бюллетеней это требует больших усилий. Конечно, ни одно решение не является надежным, но кумулятивный эффект каждой инициативы будет иметь значение.

Как насчет меток риска для устройств IoT?

Вокруг новой схемы маркировки рисков для устройств IoT ведутся горячие споры. Этикетки потребительской кибербезопасности предназначены для раскрытия

информации, аналогично тому, как на этикетках продуктов питания перечислены ингредиенты и показатели пищевой ценности.

Тем не менее, до сих пор не принято решение о том, насколько эффективным будет потребительский ярлык кибербезопасности. Новые уязвимости появляются постоянно, поэтому вопрос о том, насколько точным будет напечатанный полгода назад ярлык, когда устройство лежит на полке в Best Buy, является спорным.

Кроме того, без надлежащей международной поддержки инициатива по маркировке, вероятно, приведет к фрагментации, как это произошло с GDPR, поскольку некоторые веб-сайты теперь предпочитают просто блокировать всех посетителей из регионов, подпадающих под действие GDPR, вместо того, чтобы пытаться соблюдать требования GDPR.

Также есть опасения, что метка может быть просто меню «а ля карт» для злоумышленников. Если на этикетке четко указаны все меры кибербезопасности, предусмотренные для устройства, это просто облегчает задачу злоумышленнику, поскольку он может сэкономить время, пропуская стратегии атаки, которые явно не сработают.

Это пошаговый процесс

Маркировка потребительской кибербезопасности — это шаг в правильном направлении в условиях, когда добиться прогресса зачастую сложно. При правильном применении потребительские метки кибербезопасности могут привести к общему улучшению условий безопасности в Интернете и его различных сетях. То же самое касается растущего числа образовательных инициатив в области кибербезопасности.

Но, как говорится, дьявол кроется в деталях, а они еще не объявлены. Вывод заключается в том, что правительство США прилагает хоть какие-то усилия, чтобы помочь гражданам и предприятиям страны справиться с кризисом кибербезопасности…». ***(A Quick Look at the «Strengthening America's Cybersecurity» Initiative // The Hacker News (https://thehackernews.com/2022/10/a-quick-look-at-strengthening-americas.html). 21.10.2022).***

***

«Новое исследование, опубликованное на прошлой неделе KPMG, показывает, что, учитывая увеличение числа нарушений кибербезопасности, многие канадские бизнес-лидеры менее уверены в своей способности справиться с атакой.

Согласно опросу Global CEO Outlook Survey, проведенному KPMG International, число главных исполнительных директоров (CEO) крупных канадских компаний, которые заявили, что они «хорошо подготовлены» или «очень хорошо подготовлены» к кибератаке, сократилось на 17 процентных пунктов по сравнению с прошлым годом. Что касается тех, кто говорит, что они «не готовы», то их количество подскочило на три процентных пункта.

Руководители также ставят кибербезопасность на седьмое место после ряда других неотложных краткосрочных рисков, таких как экономика, потенциальная рецессия, вопросы регулирования и прорывные технологии.

Другой опрос, проведенный KPMG в Канаде, показал, что среди малых и средних предприятий (SMB) они чувствуют себя лучше подготовленными к кибератакам (рост на 9 процентных пунктов), но более двух третей из них признают, что их киберзащита может быть «намного сильнее», включая повышение осведомленности сотрудников о кибербезопасности. Они поставили кибербезопасность на второе место среди самых насущных проблем.

«Многие крупные компании годами вкладывали средства в технологии, инструменты и программы обучения сотрудников в области кибербезопасности, но киберугрозы становятся все более частыми и изощренными, — говорит Хартадж Ниджар, партнер и национальный руководитель индустрии кибербезопасности в KPMG в Канаде. «Поэтому, хотя сейчас компании могут быть зациклены на краткосрочных рисках, таких как рецессия, важно не упускать из виду, когда речь идет о кибербезопасности, потому что утечка данных может стоить организациям миллионы долларов, а это не то, что касается большинства компаний. может себе позволить в условиях экономического спада. Обеспечение безопасности данных компании — это инвестиция, которая всегда будет приносить дивиденды в будущем», — добавил он.

«Ситуация для малых и средних организаций отличается, потому что многие из них перешли от того, что до пандемии практически не имели цифровых платформ, к их сегодняшнему дню. В прошлом году, когда они создавали свои платформы, они, возможно, не уделяли кибербезопасности таких приоритетов, как сегодня», — говорит Роберт Мурман, партнер по кибербезопасности в KPMG в Канаде. «Теперь они лучше понимают риски и либо инвестируют, либо планируют инвестировать в соответствующие средства защиты для защиты своих организаций».

Основные моменты исследования KPMG International, проведенного в Канаде с точки зрения генерального директора:

56% руководителей крупных канадских компаний говорят, что они «хорошо подготовлены» или «очень хорошо подготовлены» к будущей кибератаке, по сравнению с 73% в 2021 году.

20% говорят, что они «недостаточно готовы» к кибератаке, по сравнению с 7% в прошлом году.

24% говорят, что у них нет плана по борьбе с потенциальной атакой программ-вымогателей, по сравнению с 5% в прошлом году.

Кибербезопасность сегодня является седьмой по актуальности проблемой. Экономические вопросы, проблемы регулирования и прорывные технологии были перечислены в качестве главных проблем.

62% заявили, что геополитическая неопределенность вызывает опасения по поводу кибератак в их организациях (ниже, чем в среднем по миру, составляющему 72%).

59% сказали, что создание сильной культуры кибербезопасности так же важно, как и создание технологических средств контроля, по сравнению с 83% в прошлом году (и ниже, чем в среднем по миру, составляющему 73%).

37% считают, что расстановка приоритетов и создание сильной киберкультуры не так важны, как технологический контроль, по сравнению с 3% в прошлом году.

Основные моменты опроса КПМГ в Канаде для малого и среднего бизнеса:

73% хорошо подготовлены к кибератаке, по сравнению с 64% в прошлом году.

56% малых и средних предприятий заявили, что в прошлом году они подвергались атакам киберпреступников (примеры включают атаки на электронную инфраструктуру и/или получение несанкционированного доступа к данным компании, фишинг, вредоносные программы, программы-вымогатели, отказ в обслуживании или внедрение вредоносного кода).

Половина из них заявили, что в прошлом году им приходилось сталкиваться с атакой программ-вымогателей.

59% заявили, что их страховые компании покрыли убытки, связанные с кибератаками.

68% сказали, что у них есть план борьбы с атакой программы-вымогателя, если она столкнется с ней.

68% заявили, что геополитическая неопределенность вызывает опасения по поводу кибератак на их организации.

73% заявили, что рассматривают информационную безопасность как стратегическую функцию и потенциальный источник конкурентного преимущества.

78% согласились с тем, что создание культуры кибербезопасности так же важно, как и создание технологических средств контроля». ***(Renaud Larue Langlois. Canadian companies risk neglecting cybersecurity as recession looms // ITBusiness.ca (https://www.itbusiness.ca/news/canadian-companies-risk-neglecting-cybersecurity-as-recession-looms/123107). 12.10.2022).***

***

«На прошлой неделе Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) опубликовало добровольные межсекторальные Цели эффективности кибербезопасности (CPG). CISA было необходимо подготовить CPG в соответствии с меморандумом по национальной безопасности об улучшении кибербезопасности для систем управления критически важной инфраструктурой, выпущенным президентом Байденом в июле 2021 года. Работая в координации с Национальным институтом стандартов и технологий (NIST) и межведомственным сообществом, CISA разработала «базовые цели производительности кибербезопасности, которые согласуются во всех критических секторах инфраструктуры».

CISA заявляет, что эти цели являются «приоритетным подмножеством методов кибербезопасности в области ИТ и операционных технологий (OT), которые владельцы и операторы критически важной инфраструктуры могут реализовать, чтобы значительно снизить вероятность и влияние известных рисков и методов злоумышленников». Подчеркнув, что цели являются добровольными и не всеобъемлющими, CISA смоделировала CPG на основе реальных угроз и тактик, методов и процедур (TTP) противника, наблюдаемых CISA и ее правительственными и отраслевыми партнерами, но в основном опиралась на NIST's Cybersecurity Framework (CSF).

Несмотря на широкую похвалу CSF, CISA сочла необходимым предложить более простую, компактную и сокращенную версию структуры NIST. «Стало ясно, что даже с исчерпывающими рекомендациями из таких источников, как NIST

Cybersecurity Framework, многие организации выиграют от помощи в определении и расстановке приоритетов наиболее важных методов кибербезопасности, а также поддержки в предоставлении убедительных аргументов для обеспечения адекватных ресурсов для снижения риска», — CISA. Говорит режиссер Джен Истерли во введении к CPG.

Однако CISA ясно дала понять, что NIST Framework по-прежнему актуальна. «Хотя CPG сопоставлены с соответствующими подкатегориями в NIST CSF, CISA по-прежнему рекомендует организациям использовать NIST CSF для разработки и усовершенствования комплексной программы кибербезопасности», — говорится в сообщении CISA.

Каждая цель включает в себя желаемый результат, TTP/устраненный риск, методику обеспечения безопасности, объем, рекомендуемые действия и ссылку на CSF (подкатегория наиболее тесно связана с практикой обеспечения безопасности). 28-страничный документ. Они сгруппированы вокруг восьми кратко подробных тем, в том числе:

Безопасность аккаунта
Безопасность устройства
Безопасность данных
Управление и обучение
Управление уязвимостями
Цепочка поставок/третья сторона
Ответ и восстановление
Другой
Цели CISA — это «хороший первый шаг»

Реакция на релиз CISA в целом была положительной. Представители Бенни Г. Томпсон (D-MS), председатель Комитета по внутренней безопасности, и Иветт Д. Кларк (D-NY), председатель Подкомитета по кибербезопасности, защите инфраструктуры и инновациям, выступили с заявлением, в котором говорится, что «Кибербезопасность Цели производительности для критической инфраструктуры (CPG) помогут владельцам и операторам упростить принятие решений о безопасности и установить четкие ожидания в отношении базовых средств контроля безопасности, которые должны быть предусмотрены для основных услуг и функций».

Патрик Миллер, президент и главный исполнительный директор Ampere Industrial Security и один из лидеров отрасли, который консультировал CISA при разработке CPG, сказал CSO, что считает документ CISA «действительно хорошим первым шагом». CPG «очевидно, что нужно будет измениться, и не только потому, что они будут совершенствоваться с течением времени», но CISA «получит больше отзывов от отрасли, когда люди действительно пройдут через это».

Том Боссерт, президент Trinity Cyber и бывший советник по национальной безопасности двух последних президентов-республиканцев, просмотрел копии документа CPG перед его публикацией, сообщил он CSO. «Я бы хотел, чтобы все списки соответствия были такими простыми и хорошо продуманными. Чтобы повысить вероятность того, что целевая аудитория примет эти рекомендации, убедитесь, что они ясны и понятны. И это именно то, что они есть. Они гораздо более

доступны, чем NIST Framework, которые могут быть пугающими и сложными, а иногда эквивалентными тому, чтобы дать студенту «Войну и мир».

Марк Монтгомери, старший директор Центра инноваций в области кибербезопасности и технологий и исполнительный директор Cybersolarium.org, сообщил CSO, что CPG «действительно важны для малого и среднего бизнеса». По словам Монтгомери, крупные компании, «то, что я бы назвал системно важной структурой критической инфраструктуры, или то, что Джен Истерли назвала бы приоритетными системно важными структурами», вряд ли будут нуждаться в легко усваиваемых советах, содержащихся в CPG, потому что они уже изучили NIST Framework и реализуют более амбициозные программы. «Речь идет о большой середине, и по этой причине я думаю, что в этом есть ценность», — говорит он.

Возможности для улучшения целей кибербезопасности

CISA планирует работать с критически важными секторами инфраструктуры для улучшения целей, поскольку она начинает разработку целей для конкретных секторов и выявляет любые дополнительные методы кибербезопасности, которые еще не включены в его общий базовый план. Боссерт сказал, что, судя по его обзору, не упоминаются какие-либо элементы управления сетевой безопасностью. «Это место, где я собираюсь работать с ними, чтобы посмотреть, сможем ли мы избавиться от внедрения новых возможностей».

«Я бы сказал, что они упустили и другие вещи, — говорит Монтгомери, — например, элементы управления, перечисленные в серии публикаций по безопасности CISA 800, или набор инструментов и документов по безопасности ISA Secure. «Возможно, это было преимуществом [для CISA] в более легком признании других доступных инструментов».

Хотя в целях упоминается цепочка поставок, «я думаю, что со временем они вернутся к ней, — говорит Монтгомери, — я подозреваю, что в следующий раз, когда мы увидим это обновление, мы увидим более крупный раздел, посвященный цепочке поставок.»

Как долго цели кибербезопасности будут оставаться добровольными?

Хотя CISA подчеркивает, что CPG являются строго добровольными, некоторые говорят, что тот факт, что CSF NIST теперь включен в рекомендации CISA в соответствии с меморандумом Белого дома о национальной безопасности, приближает желаемые результаты кибербезопасности к тому, чтобы стать нормативными требованиями. «Каждый раз, когда федеральное правительство выпускает что-то подобное, это будет «добровольно» цитироваться в эфире до тех пор, пока вам не сообщат добровольно, а затем вам просто скажут», — говорит Миллер.

По словам Миллера, организациям следует использовать CPG, чтобы улучшить свои позиции в области кибербезопасности и, возможно, предотвратить регулирование. «Я большой поклонник DHS, но если вы не ответите осмысленно, скорее всего, последует регулирование. «Основываясь на меморандуме, мы знаем, что, если мы не будем участвовать, мы вполне реально можем столкнуться с дополнительными правилами, которые, вероятно, будут очень похожи на эти в будущем. Так что мы могли бы, по крайней мере, начать идти по этому пути и начать демонстрировать некоторый прогресс».

«Я не думаю, что кто-то был бы удивлен, узнав, что эта администрация сигнализирует о намерении регулировать отрасль кибербезопасности, возможно, существенным образом», — говорит Боссерт. «Люди пытаются читать чайные листья, и те, кто пытается читать чайные листья, будут читать [CPG], поскольку, возможно, это первый шаг. И, возможно, вторым шагом будет превращение их в обязательные нормативные требования. Пока я так не читаю».

Цели CISA могут привести к внедрению лучших отраслевых практик кибербезопасности

В любом случае, CPG устанавливают контрольные показатели, которые регулирующие органы, страховщики и руководители могут использовать в качестве руководства для оценки эффективности кибербезопасности в соответствии с более формальной рубрикой. «Публикация этого документа Министерством внутренней безопасности придает ему дополнительный уровень внимания, который может привлечь внимание советов директоров и высшего руководства», — говорит Монтгомери.

CPG «может иметь большое значение, если вы изо всех сил пытаетесь получить бюджет или ресурсы», — говорит Миллер. «Если DHS спрашивает, это дает вам небольшой дополнительный толчок», чтобы получить финансирование от высшего руководства для кибербезопасности или заставить их помочь каким-либо другим образом.

«Поскольку DHS выпустило их, теперь в практическом смысле более вероятно, что компании в секторе критической инфраструктуры собираются принять их в качестве передового опыта или отраслевых стандартов», — говорит Боссерт. «Я думаю, что сейчас дело не в том, что правительство говорит им, что они должны это делать, а в том, что если все компании в их секторе, находящиеся в аналогичном положении, примут их, это станет базовым стандартом небрежности. Как только общие стандарты материализуются в любой отрасли или отраслевом сегменте, они, как правило, формируют основу передовой практики и поведения, которой другие соответствуют и, как мы надеемся, соответствуют или превосходят». ***(Cynthia Brumfield. CISA releases cybersecurity performance goals to reduce risk and impact of adversarial threats // IDG Communications, Inc. (https://www.csoonline.com/article/3678191/cisa-releases-cybersecurity-performance-goals-to-reduce-risk-and-impact-of-adversarial-threats.html). 31.10.2022).***

***

«Происходят кардинальные изменения в том, как федеральное правительство, особенно министерство обороны, собирается подходить к кибербезопасности. Это создаст более изменчивую и сложную среду, в которой фирмы и технологии, занимающиеся кибербезопасностью, должны быть готовы к работе, — среду, в которой нельзя жертвовать скоростью ради точности или наоборот.

Вот почему в мае 2021 года президент Байден издал указ, обязывающий все федеральные агентства внедрить систему безопасности с нулевым доверием, т. е. требующую, чтобы все пользователи — независимо от того, находятся они в сети организации или за ее пределами — проходили аутентификацию, авторизацию и

постоянную проверку на предмет из соображений безопасности, прежде чем получить доступ к приложениям или данным. Белый дом также предложил полагаться на системы непрерывного мониторинга, чтобы обеспечивать ситуационную осведомленность в режиме реального времени для более крупных сетей, эксплуатируемых армией и другими федеральными агентствами.

Что, если вместо того, чтобы ждать попытки взлома, вы могли бы предвидеть взлом до того, как он произойдет? Подсказка - кибераномалии. Обнаружение аномалий в кибербезопасности заключается в выявлении странных явлений или событий в системе, которые могут указывать на ошибки безопасности, структурные недостатки или откровенное мошенничество при обработке данных — события, которые открывают дверь потенциальному хакеру. Проблема заключается в том, что системы, использующие машинное обучение для отслеживания аномалий, отмечают так много аналитиков, что аналитики могут отвлекаться на бесконечно растущий набор ложноположительных предупреждений, начиная от внезапных всплесков трафика и заканчивая чрезмерным входом в систему из удаленных мест — «аномалией», которая стало новой нормой, когда люди работали из дома во время COVID.

Учитывая проблемы, связанные с растущим числом удаленных пользователей во время вспышки COVID, а также растущую киберугрозу, армия США обратилась за ответами к частному сектору.

Под руководством канцелярии министра армии Армейская аналитическая группа (AAG) начала искать способы устранить узкое место в мониторинге кибераномалий. В июне 2021 года директор AAG принял предложение от Entanglement, Inc., компании, занимающейся квантовыми вычислениями и искусственным интеллектом нового поколения, основанной в 2017 году, и Groq, Inc, американской компании по производству полупроводников, чтобы позволить армии опробовать их фирменная технология.

Что удалось сделать Entanglement, так это использовать оборудование Groq и основанное на квантовых вычислениях программное обеспечение для обнаружения аномалий в три раза больше, чем в предыдущих методах. Это согласно отчету армии, опубликованному 25 октября: в то время как более ранние усилия AAG могли обнаруживать 120 000 выводов в секунду, слияние Entanglement и Groq квантового моделирования и ИИ достигло скорости обнаружения аномалий 72 миллиона выводов в секунду при одновременном сопоставлении данных. чтобы получить более точную картину того, где находится угроза.

С тех пор Entanglement должен был достигать 100 миллионов выводов в секунду для ключевой рабочей нагрузки — подход, который приближает обнаружение киберугроз к порогу «полной наблюдаемой картины».

Это был не первый случай, когда Министерство обороны столкнулось с Entanglement, Inc. Во время пандемии COVID Пентагон проверил платформу Entanglement, которая использовала квантовый симулятор для оптимизации распространения средств индивидуальной защиты (СИЗ) по США. Платформа Entanglement продемонстрировала 90 процентное улучшение производительности по сравнению с алгоритмом, который считался современным. Затем Entanglement применила ту же методологию для разработки модели распределения и введения

вакцины, которая могла бы решить самую большую проблему операции Warp Speed, а именно, как справедливо и эффективно распределять готовую вакцину, но была принята слишком поздно.

Что все это значит? Entanglement Inc. — это еще одно указание на большую истину, то есть на то, что искусственный интеллект и машинное обучение; блокчейн и квант; все это является частью растущего сближения способов обработки и защиты данных, а также развития и защиты сетей в будущем. Существует и никогда не будет единого технологического решения наших проблем с кибербезопасностью. Вместо этого ответом будет ряд гибридных решений, в которых используются лучшие черты каждой технологии.

Клиенты кибербезопасности, такие как Пентагон и федеральное правительство, осознают тот факт, что до сих пор мы были похожи на фермера, который изобретает все более сложные замки для двери своего сарая после того, как украли лошадей, в то время как вор изобретает все более сложные замки. сложные отмычки. Решения в области кибербезопасности в ближайшее десятилетие будут сильно отличаться от своих предшественников. Entanglement, Inc — одна из компаний, которая показывает нам, где находится это будущее». ***(Arthur Herman. Cybersecurity Is Entering The High-Tech Era // Forbes (https://www.forbes.com/sites/arthurherman/2022/10/31/cybersecurity-is-entering-the-high-tech-era/?sh=65361fa7b110). 31.10.2022).***

***

«В четверг Google присоединился к другим отраслевым силам в поддержку законодательства о защите программного обеспечения с открытым исходным кодом.

Закон о защите программного обеспечения с открытым исходным кодом был представлен в сентябре лидером Сенатского комитета по внутренней безопасности Гэри Питерсом (штат Мичиган) и высокопоставленным членом Робом Портманом (республиканец, штат Огайо) и был быстро одобрен голосованием.

В случае принятия закона двухпартийное законодательство потребует от Агентства кибербезопасности и безопасности инфраструктуры (CISA) разработать в течение следующего года структуру рисков, в которой подробно описывается, как федеральное правительство полагается на открытый исходный код.

Законодательство включает в себя ряд других мер, направленных на безопасность открытого исходного кода, в том числе мандат на то, чтобы Административно-бюджетное управление издавало руководство по этой теме, а также приказы CISA нанимать больше экспертов по безопасности с открытым исходным кодом.

В Google заявили, что законопроект поможет «направить федеральное правительство в использовании программного обеспечения с открытым исходным кодом» и «отражает полезное внимание к безопасности и снижению киберрисков в ответ на недавний всплеск злонамеренной киберактивности против цепочки поставок программного обеспечения».

«Мы рады видеть постоянный акцент на важности безопасности программного обеспечения с открытым исходным кодом со стороны правительства США, и мы

надеемся, что как государственные, так и частные организации последуют их примеру, чтобы способствовать повышению кибербезопасности для экосистемы в целом», — говорится в сообщении компании. Четверг.

Фонд безопасности с открытым исходным кодом, в состав которого входят GitHub, Microsoft, Google, Canonical, Cisco, Facebook, Intel, HP, Tencent, IBM, Red Hat, Samsung и многие другие, также выступил в поддержку закона в прошлом месяце.

Воздействие Log4j

Первоначально законопроект был внесен в ответ на разногласия вокруг Log4j — широко распространенной уязвимости, скрытой в тысячах популярных инструментов.

Google принимал активное участие в расследовании этой уязвимости, а вице-президент Google по технике безопасности Хизер Адкинс вместе с руководителями Министерства внутренней безопасности возглавляла правительственную проверку инцидента.

В августе правление заявило, что организации «будут иметь дело с продолжающимся воздействием Log4j на долгие годы, может быть, десятилетие или дольше». Атаки, использующие эту ошибку, продолжают обнаруживаться более чем через 10 месяцев после обнаружения проблемы.

После Log4j стало известно о нескольких других уязвимостях с открытым исходным кодом, что побудило правительство США и Google активизировать усилия по устранению этой тенденции.

Сенатор Питерс сказал The Record, что уязвимость в Log4J «продемонстрировала, насколько мы полагаемся на открытый исходный код».

«Вот почему я возглавляю этот двухпартийный законопроект — помочь предотвратить использование киберпреступниками потенциальных уязвимостей, обнаруженных в широко используемом программном обеспечении с открытым исходным кодом, для нарушения жизни и средств к существованию», — сказал он.

«Я горжусь тем, что имею широкую двухпартийную поддержку этого закона, и буду продолжать работать над тем, чтобы он был подписан как можно скорее».

В Google заявили, что законопроект затрагивает несколько распространенных вопросов, которые теперь приходится задавать экспертам по безопасности при расследовании уязвимостей в программном обеспечении с открытым исходным кодом. Это заставит правительственные учреждения знать, содержит ли проект известные уязвимости и следовали ли сопровождающие проекта передовым методам обеспечения безопасности во время его разработки.

Вопросы о том, какие зависимости с открытым исходным кодом есть у части программного обеспечения и насколько безопасна цепочка поставок, теперь актуальны для государственных учреждений, закупающих инструменты.

«Мы надеемся, что структура, которая появится благодаря усилиям правительства США, будет стимулировать дальнейшие инвестиции в сообщества открытого исходного кода как со стороны государственного, так и частного секторов», — заявили в Google.

Google также вложила значительные средства в безопасность открытого исходного кода, пообещав выделить 100 миллионов долларов некоммерческим

организациям и фондам программного обеспечения, таким как Open Source Security Foundation, для поддержки создателей открытого исходного кода.

Технический гигант также объявил о нескольких инициативах, направленных на обеспечение безопасности с открытым исходным кодом, в том числе о новой спецификации программного обеспечения на прошлой неделе.

Сейчас закон ожидает голосования в Сенате США в полном составе, но в конечном итоге он может быть присоединен к другим законам, таким как ежегодный законопроект об оборонной политике». ***(Jonathan Greig. Google backs senate bill on securing open source software // The Record by Recorded Future (https://therecord.media/google-backs-senate-bill-on-securing-open-source-software/). 27.10.2022).***

***

«В июне 2022 года федеральное правительство представило свой первый в истории федеральный закон общего применения о кибербезопасности, направленный на защиту критической инфраструктуры. Реакция сначала была сдержанной, но положительной. Законопроект не прошел дальше первого чтения…

Законопроект C-26, формально озаглавленный «Закон о кибербезопасности», вносящий поправки в Закон о телекоммуникациях и вносящий соответствующие поправки в другие законы, налагает на операторов критической инфраструктуры позитивные обязательства по кибербезопасности (в отличие от конфиденциальности). В счете две части:

Поправки к Закону о телекоммуникациях: C-26 вносит поправки в федеральный Закон о телекоммуникациях, позволяющие федеральному правительству налагать обязательства на поставщиков телекоммуникационных услуг по «защите канадской телекоммуникационной системы»; а также

Закон о защите критически важных киберсистем («CCSPA»): законопроект также вводит совершенно новый закон, уполномочивающий правительство определять службы или системы как «жизненно важные» и налагать обязательства по защите данных на их операторов, требовать обязательной отчетности об инцидентах кибербезопасности и облегчить обмен информацией об угрозах «между соответствующими сторонами».

Приложение 1 к CCSPA определяет следующие службы и системы (все области существующей федеральной юрисдикции в соответствии с конституционным разделением полномочий) как жизненно важные:

Телекоммуникационные услуги

Межпровинциальные или международные системы трубопроводов и линий электропередач

Ядерные энергетические системы

Транспортные системы, находящиеся в законодательной компетенции парламента

Банковские системы

Клиринговые и расчетные системы

Правоприменительные механизмы в соответствии с CCSPA включают:

Право издавать приказы о соответствии;

Полномочия приказать оператору провести внутренний аудит, чтобы помочь регулирующему органу определить степень соблюдения оператором CCSPA и правил;

Полномочия проводить обыски помещений (очевидно, без ордера, за исключением случаев, когда обыск должен проводиться в «жилом доме», то есть в частном доме) для проверки соблюдения или предотвращения несоблюдения CCSPA и правил, и в процессе такого поиска, для доступа к любой обнаруженной «киберсистеме» и доступа к содержащейся в ней информации, для копирования и/или удаления обнаруженных документов или записей;

Возможность получения в одностороннем порядке ордеров на проведение обысков жилых домов;

При наличии ордера право применять силу для проведения обысков жилых домов;

Возможность наложения административных денежных взысканий в размере до: 1 миллион долларов США на человека (т. е. должностное лицо или директор, который «руководил, санкционировал, соглашался, соглашался или участвовал в совершении нарушения»), или 15 миллионов долларов на организацию.

CCSPA также устанавливает дисциплинарные уголовные преступления и уголовные преступления за нарушение положений CCSPA (включая, например, неспособность разработать, внедрить и поддерживать программу кибербезопасности, которая может быть уголовным преступлением).

Закон предусматривает освобождение от ответственности должностных лиц и директоров, если они добросовестно выполняли свои обязанности в соответствии с CCSPA, несмотря на нарушение. Защита должной осмотрительности доступна для нарушений CCSPA.

В конце сентября 2022 года Канадская ассоциация гражданских свобод вместе с коллективом, включающим Международную группу по мониторингу гражданских свобод, Канадский совет по конфиденциальности и доступу, а также несколько других групп и ученых, опубликовали свое «Совместное письмо с обеспокоенностью в отношении законопроекта C-26.» Заявляя о коллективном соглашении с целью повышения кибербезопасности, в Совместном письме далее говорится, что законопроект «является глубоко проблематичным и нуждается в исправлении», поскольку он «рискует подорвать наши права на неприкосновенность частной жизни и принципы подотчетное управление и надлежащее судебное разбирательство».

В совместном письме изложены несколько проблемных областей, в том числе следующие:

Усиленное наблюдение: законопроект позволяет федеральному правительству «тайно приказывать поставщикам телекоммуникационных услуг» «делать что-либо или воздерживаться от чего-либо… необходимого для защиты канадской телекоммуникационной системы, в том числе от угроз вмешательства, манипуляций или сбоев». Хотя в этой части законопроекта (раздел 15.2(2)) далее приводится несколько примеров того, что может повлечь за собой «что-либо делать», включая, например, запрет поставщикам телекоммуникационных услуг на использование определенных продуктов или услуг от определенных поставщиков или требование

обслуживания поставщиков для разработки планов безопасности - коллектив выражает обеспокоенность тем, что право приказывать телекоммуникационным компаниям «делать что-либо» «открывает дверь для наложения обязательств по слежке на частные компании и других рисков, таких как ослабление стандартов шифрования».

Прекращение основных услуг: C-26 позволяет правительству «запретить лицу или компании получать определенные услуги, а также запретить любой компании предлагать эти услуги другим лицам секретным распоряжением правительства», что повышает риск «компаний или людей отключают от основных услуг без объяснения причин».

Подрыв конфиденциальности: Законопроект предусматривает сбор данных от назначенных операторов, что потенциально может позволить правительству «получать идентифицируемую и обезличенную личную информацию и впоследствии распространять ее среди местных и, возможно, иностранных организаций».

Отсутствие «барьеров для сдерживания злоупотреблений»: законопроект позволит правительству действовать без предварительного требования о проведении оценок пропорциональности, конфиденциальности или справедливости для защиты от злоупотреблений, что касается коллектива, учитывая суровость наказаний, предусмотренных законом.

Секретность, препятствующая подотчетности, надлежащей правовой процедуре и государственному регулированию: многие опасения коллектива связаны с тем фактом, что правительственные распоряжения, издаваемые в соответствии с законопроектом, могут быть сделаны тайно, без требований к публичной отчетности, что делает невозможным мониторинг и оспаривание правозащитными группами и общественностью. как осуществляется власть по законопроекту. Секретность, связанная с такими приказами, может ограничить возможность операторов, которым выданы приказы, обжаловать их в суде, поскольку ключевые доказательства секретных приказов (которые потребуются для оспаривания в суде) также могут храниться в секрете от операторов.

Возможность злоупотреблений со стороны CSE: CCSPA предоставит Управлению безопасности связи (федеральному агентству, отвечающему за кибербезопасность, но, что более важно, за разведку сигналов) доступ к большим объемам конфиденциальных данных, но не будет ограничивать использование таких данных его кибербезопасностью. мандат безопасности…

Деловой совет Канады опубликовал собственное письмо министру общественной безопасности, в котором выразил озабоченность деловых кругов по поводу законопроекта C-26. Сосредоточив внимание на предлагаемом CCSPA, Совет обеспокоен следующим:

Отсутствие подхода, основанного на оценке риска: CCSPA требует одинаковых действий от всех операторов, подпадающих под юрисдикцию закона, «независимо от уровня их кибербезопасности». соблюдать CCSPA «без какой-либо связанной с этим выгоды» для них.

Обмен информацией является односторонним: операторы обязаны предоставлять информацию правительству, но ничего не получают взамен от

правительства или других операторов, то есть законопроект упускает возможность реализовать режим обмена информацией, который мог бы принести пользу всем операторам, подпадающим под действие закона;

Правовой порог для выдачи указаний слишком низок: в соответствии с проектом правительство может издавать секретные приказы операторам «с целью защиты критически важной киберсистемы» (статья 20 (1)). Совет обеспокоен тем, что этот порог достаточно расплывчатый, чтобы позволить отдавать приказы даже в тех случаях, когда угроза критической системе «незначительна и, следовательно, не представляет реальной угрозы для национальной безопасности Канады».

Штрафы: Совет считает, что предлагаемые денежные штрафы и тюремные сроки являются «необоснованно высокими и ненужными для поощрения» операторов к принятию мер, требуемых CCSPA для улучшения их состояния кибербезопасности.

Утечка мозгов: Перспектива личной ответственности за определенные нарушения CCSPA может отговорить специалистов по кибербезопасности от трудоустройства в Канаде (Совет отмечает, что в Канаде уже существует более 25 000 незаполненных вакансий)…

В то время как другие группы, вероятно, прокомментируют законопроект в ближайшие недели, формирующийся консенсус заинтересованных сторон, по-видимому, заключается в том, что законопроект C-26 содержит множество недостатков, начиная от технических и заканчивая концептуальными и фундаментальными. Будет интересно посмотреть, выйдет ли законопроект из стадии рассмотрения комитетом и каким образом». ***(Brent J. Arnold. BILL C-26: RIGHTS GROUPS OPPOSE CANADA'S NEW CRITICAL INFRASTRUCTURE PROTECTION LAW // Gowling WLG International Limited (https://gowlingwlg.com/en/insights-resources/articles/2022/bill-c-26-rights-groups-oppose-infrastructure-law/). 31.10.2022).***

***

«11 октября 2022 года Белый дом выпустил пресс-релиз, в котором излагаются несколько инициатив, которые должны быть приняты правительством США для защиты своей киберинфраструктуры. Среди этих инициатив — разработка новой программы добровольной сертификации и маркировки устройств Интернета вещей (IoT).

В рамках этой программы продукты, соответствующие стандартам кибербезопасности, которые еще предстоит определить, будут сертифицированы и получат право использовать маркировку, подтверждающую их сертификацию. Первоначально в рамках программы основное внимание уделялось маршрутизаторам и домашним камерам. Программа будет сертифицировать продукты после обширного процесса тестирования и проверки, проводимого аккредитованными государством организациями.

Проект остается на ранних стадиях, и в октябре 2022 года будет проведен процесс консультаций с заинтересованными сторонами отрасли для обсуждения разработки и развертывания программы.

Объявление было сделано после пилотной программы, инициированной указом, подписанным президентом Байденом в мае 2021 года. Указ предписывал Национальному институту стандартов и технологий (NIST) инициировать две пилотные программы маркировки кибербезопасности: одну для устройств IoT. а другой для потребительского программного обеспечения. После завершения пилотной программы 4 февраля 2022 г. NIST опубликовал рекомендуемые критерии программы маркировки, а 10 мая 2022 г. был опубликован отчет о пилотной программе.

В этих документах рекомендуется использовать единую этикетку, указывающую, что продукт соответствует базовому стандарту, в сочетании с URL-адресом или QR-кодом, где потребитель может получить доступ к дополнительным сведениям о значении этикетки, критериям продукта и другой информации, связанной с кибербезопасностью. и программа сертификации.

Хотя конкретные стандарты кибербезопасности еще предстоит разработать, отчет NIST рекомендует, насколько это возможно, использовать существующие стандарты и гармонизировать схемы в Соединенных Штатах и во всем мире. Гармонизация, вероятно, поможет ускорить разработку программ, облегчит соблюдение производителями устройств IoT и поможет повысить признание потребителей на международном рынке.

Эта программа вряд ли первая в своем роде. Действительно, несколько программ маркировки были реализованы или аналогичным образом разрабатываются в разных юрисдикциях. Например, Германия, Финляндия и Сингапур уже внедрили свои собственные поддерживаемые государством программы маркировки кибербезопасности для подключенных устройств. Великобритания также объявила об аналогичной инициативе в 2020 году и поддержала отраслевые пилотные проекты.

Эти режимы в значительной степени основаны на уже разработанных стандартах, прежде всего EN 303 645, разработанном Европейским институтом телекоммуникационных стандартов (ETSI). В дополнение к этой общей основе, между правительствами также осуществлялось сотрудничество для дальнейшего согласования этих инициатив. Например, Финляндия и Сингапур подписали Меморандум о взаимопонимании, в соответствии с которым продукт может пройти сертификацию в рамках обеих программ маркировки с помощью одной заявки. Сообщалось, что США сотрудничают с ЕС в разработке их программы маркировки с намерением, чтобы американские продукты с маркировкой кибербезопасности продавались по всему миру.

По мере распространения этих программ во всем мире в будущем может стать возможным внедрение аналогичного знака в Канаде — либо в рамках сотрудничества с США, либо в рамках инициативы «Сделано в Канаде».

Канадские организации и потребители, вероятно, знакомы с аналогичной схемой добровольных сертификационных знаков, установленной правительством США в отношении энергоэффективности. ENERGY STAR, по образцу которого, как указал Белый дом, должен быть создан проект кибербезопасности, является сертификационным знаком Агентства по охране окружающей среды США (EPA). Он также находится в ведении Министерства природных ресурсов Канады в Канаде.

Он лицензирован для использования организациями, продукция которых соответствует установленным государством критериям энергоэффективности, и с тех пор стал широко узнаваемым потребительским символом. Таким образом, существует прецедент сотрудничества между Канадой и США по аналогичным схемам сертификации.

Процесс консультаций с участием многих заинтересованных сторон по аналогичной инициативе по маркировке кибербезопасности IoT уже состоялся в Канаде. В партнерстве с Министерством инноваций, науки и экономического развития Канады (ISED) несколько канадских учреждений участвовали в проекте под названием «Канадский многосторонний процесс: повышение безопасности Интернета вещей», окончательный отчет которого был опубликован в 2019 году. Среди его усилий было создание рабочей группы. поручено дать рекомендации для аналогичного режима маркировки кибербезопасности IoT. Многие из этих рекомендаций основаны на существующих схемах в других странах мира и ссылаются на региональные инициативы по разработке стандартов, реализуемые в Великобритании, ЕС, Австралии, США и Канаде.

Подобная программа сертификационных знаков кибербезопасности также имела бы прецедент в Канаде. В 2019 году ISED в сотрудничестве с Канадским центром кибербезопасности реализовал аналогичную инициативу по добровольной сертификации в отношении корпоративной кибербезопасности. Программа сертификации CyberSecure Canada, администрируемая независимыми органами по оценке, аккредитованными Советом по стандартам Канады, позволяет малым и средним организациям, демонстрирующим соответствие базовому набору методов обеспечения безопасности, использовать сертификационный знак CyberSecure Canada. Программа будет обновлять свои требования, чтобы привести их в соответствие с национальным стандартом, разработанным 1 января 2023 года.

В настоящее время разработка программы маркировки в США находится на ранней стадии, и в Канаде аналогичная программа не находится в активной разработке. Кроме того, добровольный характер этих инициатив означает, что канадские организации, которые экспортируют устройства IoT в юрисдикции с действующими программами, не обязаны соблюдать определенные наборы стандартов кибербезопасности, помимо тех, которые предусмотрены законодательством.

Влияние этих программ на покупательское поведение еще предстоит выяснить. Тем не менее, учитывая очевидную популярность режимов маркировки кибербезопасности среди заинтересованных сторон в отрасли и растущее признание со стороны правительств, канадские организации, экспортирующие устройства для подключения, могут захотеть изучить такие программы как средство укрепления доброжелательности среди своих потребителей и доверия к качеству своей продукции». ***(Caitlin Schropp. IOT CYBER SECURITY CERTIFICATION PROGRAMS ARE BECOMING MORE PREVALENT. WHAT DOES IT MEAN FOR CANADIAN ORGANIZATIONS? // Gowling WLG International Limited (https://gowlingwlg.com/en/insights-resources/articles/2022/iot-cyber-security-certification-programs/). 31.10.2022).***

***

«Два судебных дела в США за последний месяц свидетельствуют о том, что регулирующие органы и прокуроры все более полны решимости принимать личные меры против директоров и руководителей высшего звена, которые не в состоянии адекватно бороться с нарушениями кибербезопасности.

В начале октября бывший начальник службы безопасности Uber был признан виновным в совершении уголовного преступления за то, что не сообщил властям о кибер-взломе. Считается, что это первый случай, когда руководитель американской компании подвергается уголовному преследованию за кибер-взлом, и теперь ему грозит тюремный срок до восьми лет. Ранее на этой неделе Федеральная торговая комиссия (FTC) объявила, что приняла меры против генерального директора Drizly (онлайн-бизнес по доставке напитков) из-за сбоев в системе безопасности компании, которые привели к кибер-взлому, в результате которого была раскрыта личная информация 2,5 миллиона клиентов.

Учитывая глобальный характер тенденций в области регулирования и тот факт, что кибер-взломы все чаще становятся фактом деловой жизни, британские директора будут обоснованно обеспокоены перспективой потенциального увеличения риска личной ответственности, возникающего в результате кибер-взломов. Однако более пристальный взгляд на факты каждого из этих дел позволяет предположить, что отягчающие обстоятельства побудили власти принять меры в отношении соответствующих лиц.

В первом случае уголовные обвинения против бывшего начальника службы безопасности Uber (Джеймса Салливана) были связаны с тем фактом, что, когда в 2016 году произошло соответствующее кибер-взлом, Uber уже находился под следствием FTC за более раннее кибер-взлом в 2014 году. В 2016 году хакер получил доступ к записям клиентов и потребовал платеж в размере 100 000 долларов США, который в конечном итоге был выплачен командой г-на Салливана. Г-н Салливан не сообщил FTC об инциденте, несмотря на продолжающееся расследование, и прокуратура утверждала, что он также предпринял шаги, чтобы скрыть инцидент внутри компании. Действия г-на Салливана привели к тому, что он был уволен из Uber.

Во втором случае решение FTC принять меры против генерального директора, а также против самой компании было обусловлено тем фактом, что обе компании были предупреждены о проблемах с процедурами безопасности компании после кибератаки двумя годами ранее. Несмотря на это, компания не смогла реализовать основные меры кибербезопасности, публично заявив, что у нее есть соответствующие средства защиты. Предлагаемый заказ FTC требует, чтобы компания и генеральный директор реализовали программу информационной безопасности для защиты данных клиентов. FTC заявила, что это «гарантирует, что генеральный директор столкнется с последствиями небрежности компании».

Таким образом, оба этих случая связаны с отягчающими обстоятельствами, которые могут поставить их за рамки «типичного» сценария, когда директора сталкиваются с кибер-взломом и делают все возможное, чтобы справиться с ним честно и разумно.

Что касается Великобритании, то, несмотря на то, что директора могут столкнуться с личной ответственностью и осуждением со стороны регулирующих органов в результате того, что их компания пострадала от кибератаки или неправомерно справилась с ней, мы видели очень мало попыток привлечь директоров или старших менеджеров к личной ответственности в таких обстоятельствах. На сегодняшний день судебные иски и действия регулирующих органов в основном были направлены против компании, пострадавшей от нарушения. Однако останавливаться на достигнутом директору не стоит. Британские регулирующие органы уже давно четко заявляют, что кибербезопасность — это вопрос на уровне совета директоров, который требует серьезного и значимого участия высшего руководства. Поэтому директора должны исходить из того, что, как и Федеральная торговая комиссия, регулирующие органы Великобритании будут очень внимательно следить за поведением отдельных директоров в связи с любым нарушением кибербезопасности, от которого пострадала их компания, и что при наличии подобных отягчающих факторов,

Кроме того, в английских судах все чаще встречаются попытки привлечь директоров к личной ответственности за халатность и нарушение служебных обязанностей, например, в отношении вопросов, связанных с ESG. Тот факт, что кибербезопасность в настоящее время прочно зарекомендовала себя как ключевой бизнес-риск, означает, что директора могут все чаще ожидать, что кибер-взлом, от которого пострадала их компания, приведет к большему давлению, чтобы продемонстрировать, что они предприняли разумные шаги как для предотвращения нарушения, так и для подготовки к устранению. любое произошедшее нарушение.

На этом фоне британским советам директоров следовало бы прислушаться к предупреждению FTC: «Генеральные директора, которые экономят на безопасности, должны принять это к сведению». ***(Lawson Caisley. Director liability for cyber breaches: transatlantic warning signs? // White & Case LLP (https://www.whitecase.com/insight-alert/director-liability-cyber-breaches-transatlantic-warning-signs). 27.10.2022).***

***

Країни ЄС та Великобританія

«Европейский совет и Европейский парламент недавно достигли предварительного соглашения по тексту предложенной ЕС Директивы о минимальных стандартах кибербезопасности, которая должна быть реализована на всей территории ЕС (NIS2). Ожидается, что текст будет официально принят в ближайшие месяцы. NIS2 стремится заменить и укрепить действующую Директиву ЕС о сетях и информационном обществе (Директива NIS) и применяется к определенным важным и важным организациям, работающим в определенном списке секторов, включая обычно считающиеся критически важными объектами инфраструктуры.

Ключевые разработки, вытекающие из NIS2, включают:

Более широкий охват: NIS2 применяется к более широкому кругу секторов и организаций, чем те, на которые распространяется действующая Директива NIS.

Надзор и подотчетность «органов управления»: NIS2 налагает прямые обязательства на «органы управления» в отношении реализации и надзора за соблюдением их организацией законодательства, что может привести к штрафам и временному запрету на выполнение управленческих функций, в том числе на уровне высшего руководства C-Suite.

Меры по управлению кибер-рисками, в том числе проверка цепочки поставок: NIS2 требует, чтобы организации реализовывали меры по управлению кибер-рисками, которые включают требования по снижению рисков безопасности и комплексную проверку сторонних поставщиков/услуг.

Измененные требования к отчетности об инцидентах: NIS2 налагает обязательства по уведомлению поэтапно, включая первоначальное уведомление в течение 24 часов после того, как стало известно об определенных инцидентах или киберугрозах (вместо простого «без неоправданной задержки», как в Директиве NIS), «промежуточное» и «окончательное». обязательства по отчетности.

Штрафы и санкции: Государства- члены могут по своему усмотрению устанавливать эффективные, пропорциональные и сдерживающие санкции за нарушения NIS2, а также административные штрафы за определенные нарушения в размере до 10 миллионов евро или 2% от общего мирового оборота (в зависимости от того, что больше).

В этой статье мы описываем некоторые изменения, связанные с предлагаемой NIS2, и объясняем, почему законодательство, вероятно, окажет влияние не только на те организации, которые непосредственно подпадают под действие законодательства, но также на их поставщиков и поставщиков услуг.

Расширенная область применения NIS2

Директива NIS - текущая сфера применения

Текущая Директива NIS была принята в 2016 году как первое законодательство о кибербезопасности в ЕС. Его цель состояла в том, чтобы достичь высокого общего уровня кибербезопасности в ЕС, и законодательство направлено на реализацию определенных обязательств по управлению рисками и отчетности для операторов основных услуг (OES) (например, организаций, обслуживающих критически важную энергетическую, медицинскую или транспортную инфраструктуру). и поставщики цифровых услуг (DSP) (некоторые поставщики онлайн-рынков, онлайн-поисковых систем и услуг облачных вычислений).

NIS2 - переход к «основным» и «важным объектам» и расширение сектора

Организации должны принять к сведению, что NIS2 будет применяться к более широкому кругу организаций, чем в настоящее время подпадает под действие Директивы NIS. В рамках NIS2 пул объектов, входящих в область действия, будет расширен, чтобы охватить определенные «основные» объекты (указанные в Приложении I NIS2) и «важные» объекты (указанные в Приложении II NIS2). Следовательно, различие, существующее в настоящее время в соответствии с Директивой NIS в отношении OES и DSP, будет заменено. Аналогичным образом, в то время как дальнейшая ясность в отношении области действия NIS2 в конечном итоге будет раскрыта после внедрения в различных государствах-членах, NIS2

расширит количество секторов, которые в настоящее время охватываются Директивой NIS. Например, в дополнение к секторам, подпадающим под действие Директивы NIS, NIS2 также распространяется на организации, работающие в следующих секторах:

Цифровая инфраструктура и цифровые провайдеры, включая провайдеров общедоступных сетей или услуг электронных коммуникаций, платформ социальных сетей и услуг центров обработки данных.

Сточные воды и управление отходами

Производство некоторых критически важных продуктов (таких как фармацевтические препараты, медицинские устройства или химикаты)

Еда

Пространство

Почтовые и курьерские услуги

Государственное управление

Помимо охвата более широкого круга секторов, NIS2 также предоставляет более подробную информацию о том, какие организации в этих соответствующих секторах подпадают под действие предлагаемого законодательства. В то время как в настоящее время в соответствии с Директивой NIS государства-члены несут ответственность за составление списков OES и DSP, Директива NIS2:

вводит предельный размер, чтобы все средние и крупные предприятия, работающие в секторах, охватываемых новым текстом, должны были соблюдать требования, содержащиеся в NIS2; а также

применяется к определенным «важным» и «необходимым» объектам (независимо от их размера) в определенных обстоятельствах, таких как:

организации, предоставляющие определенные общедоступные сети электронной связи или общедоступные услуги электронной связи

реестры доменных имен верхнего уровня и поставщики услуг системы доменных имен

юридические лица, предлагающие услуги, при этом потенциальное нарушение этих услуг может повлиять на общественную безопасность, общественную безопасность или здоровье населения.

юридические лица, предлагающие услуги, при этом потенциальное нарушение работы сервиса может вызвать системные риски, особенно в секторах, где нарушение может иметь трансграничное воздействие

Ответственность руководства за управление рисками кибербезопасности

НИС2 повышает уровень ответственности, которую должны нести «органы управления» (в формулировке НИС2) существенных и ответственных субъектов в обеспечении соблюдения элементов НИС2. Он предусматривает обязательство государств-членов при внедрении НИС2 обеспечивать, чтобы органы управления:

- утвердить меры по управлению рисками кибербезопасности, принимаемые организацией, например, меры по управлению рисками, связанные с обеспечением безопасности цепочки поставок;
- контролировать выполнение мероприятий по управлению рисками;

- пройти специальное регулярное обучение, чтобы получить необходимые знания и навыки для выявления и оценки рисков кибербезопасности для их основной или важной организации; а также
- несут ответственность за несоблюдение юридическими лицами.

Практическим следствием этого требования является то, что органы управления организаций, подпадающих под действие NIS2, могут быть признаны ответственными, если эти организации нарушают свои обязательства в соответствии с NIS2. В конечном счете, возложение ответственности за управление рисками кибербезопасности на уровень управления основных и важных субъектов демонстрирует склонность к тому, чтобы управление рисками кибербезопасности возлагалось на высшее руководство. Органы управления несут окончательную ответственность, и любое незнание может привести к серьезным последствиям, включая ответственность руководства и административные штрафы, как это предусмотрено в национальном законодательстве.

Текущий текст NIS2 не определяет, что представляет собой «орган управления», что является аспектом, который в конечном итоге будет определяться применением национального законодательства в государствах-членах. Однако НИС2 предполагает, что лица, выполняющие управленческие функции, могут считаться «руководящим органом». NIS2 предусматривает, что эти лица могут быть подвергнуты принудительным мерам за несоблюдение организацией требований NIS2. Например, в контексте основных юридических лиц, NIS2 позволяет государствам-членам предусмотреть в своем национальном транспонирующем законодательстве, что соответствующие органы или суды временно запрещают отдельным лицам выполнять управленческие обязанности на уровне высшего руководства высшего звена до тех пор, пока не будут предприняты необходимые действия для устранения недостатков и/или выполнения запрошенных требований. компетентными органами.

В дополнение к временным запретам, с точки зрения общественной репутации, NIS2 позволяет государствам-членам требовать, чтобы лица, нарушающие права, сделали публичное заявление не только о том, что нарушение NIS2 произошло, но и с указанием лиц, ответственных за нарушение. Более того, в соответствии с NIS2 государства-члены могут свободно устанавливать правила о штрафах в своем внутреннем имплементирующем законодательстве. Наказания должны быть эффективными, пропорциональными и оказывающими сдерживающее воздействие, и в преамбуле к действующему тексту NIS2 четко указано, что они могут включать уголовные наказания за нарушение законодательства. Следовательно, важно, чтобы организации, работающие в сфере NIS2, обращали внимание на национальные правила государств-членов, трансформирующие NIS2, и связанный с ними режим наказания (как уголовный, так и гражданский), содержащийся в этих национальных правилах.

Меры по управлению рисками кибербезопасности

NIS2 нацелен на более согласованный подход к управлению кибербезопасностью, чтобы смягчить несоответствия в устойчивости к кибербезопасности в рассматриваемых секторах. С этой целью в NIS2 изложены семь ключевых мер, которые должны принимать все основные и важные

организации для управления рисками, связанными с безопасностью сетей и информационных систем этих организаций при предоставлении своих услуг. Эти меры таковы:

Анализ рисков и политики безопасности информационных систем

Обработка инцидентов (предотвращение, обнаружение и реагирование на инциденты)

Непрерывность бизнеса и антикризисное управление

Безопасность цепочки поставок — включая связанные с безопасностью аспекты отношений между каждым субъектом и (i) его поставщиками или (ii) поставщиками услуг (такими как поставщики услуг хранения данных и услуг по обработке или поставщики управляемых услуг безопасности)

Безопасность при приобретении, разработке и обслуживании сетевых и информационных систем, включая обработку уязвимостей и раскрытие информации

Политики и процедуры для оценки эффективности мер по управлению рисками кибербезопасности

Использование криптографии и шифрования

Надлежащая проверка цепочки поставок — поставщики услуг, связанных с ИТ, на которые следует обратить внимание

Новые меры кибербезопасности требуют от организаций, подпадающих под действие NIS2, снижать риски безопасности в цепочке поставок своих поставщиков / поставщиков услуг, включая оценку и учет общего качества продуктов и методов кибербезопасности своих поставщиков и поставщиков услуг.

В проекте текста NIS2 отмечается, что организации стали жертвами кибератак, в ходе которых злоумышленники поставили под угрозу безопасность сети и информационных систем организации, используя уязвимости, влияющие на сторонние продукты и услуги. Следовательно, организации, не входящие в непосредственную сферу действия NIS2, предлагающие такие продукты и услуги, могут в конечном итоге попасть под действие нового законодательства, например, если организация будет предоставлять определенные услуги, связанные с ИТ, клиентам, подпадающим под сферу действия NIS2 и, следовательно, обязанным осуществлять цепочку поставок. внимательность к организации-поставщику. В настоящее время в черновом тексте NIS2 указывается, что поставщики управляемых услуг безопасности, таких как реагирование на инциденты, тестирование на проникновение, аудит безопасности и консультационные услуги, потребуют повышенного внимания от организаций, входящих в NIS2.

Чистый эффект обязательств по обеспечению безопасности цепочки поставок заключается в том, что организации, предоставляющие услуги безопасности сетей и / или информационных систем клиентам в расширенных секторах, охватываемых NIS, должны быть готовы к более частым вопросам со стороны клиентов NIS2 относительно их методов кибербезопасности и информационной безопасности. политики. Такие вопросы могут относиться как к отдельным решениям, так и к общим практикам управления рисками в области кибербезопасности и информационной безопасности, применяемыми этими поставщиками.

Требования к отчетности об инцидентах и киберугрозах

NIS2 вносит поправки в требования к отчетности об инцидентах в соответствии с действующей Директивой NIS, требуя, чтобы важные и важные организации должны без неоправданной задержки уведомлять соответствующие компетентные органы 1 или одну из групп реагирования на инциденты компьютерной безопасности (CSIRT) одного из государств-членов:

любой инцидент, оказывающий существенное влияние на предоставление их услуг, включая инцидент, который вызвал или может привести к существенному сбою в работе или финансовым потерям организации. Требования к сообщениям об инцидентах включают первоначальное уведомление в течение 24 часов после того, как стало известно об инциденте (вместо простого «без неоправданной задержки», как в Директиве NIS), и включают промежуточные и окончательные обязательства по отчетности; а также любая выявленная серьезная киберугроза, которая потенциально могла привести к серьезному инциденту.

Штрафы и пени

NIS2 позволяет государствам-членам ЕС налагать административные штрафы в размере не менее 10 миллионов евро или до 2% от общего мирового оборота организации за предыдущий финансовый год (в зависимости от того, что больше) для организаций, подпадающих под действие NIS2, которые нарушают меры по управлению рисками кибербезопасности. и/или обязательства по отчетности об инцидентах кибербезопасности. Это в дополнение к широкому усмотрению, которое NIS2 предоставляет государствам-членам для реализации своих собственных национальных правил о штрафах за нарушение предлагаемого законодательства, как указано ранее в этой статье.

Сроки принятия и шаги, которые необходимо предпринять в это время

На этом этапе организациям следует рассмотреть область применения NIS2 и определить, попадает ли в нее их бизнес. Если организация приходит к выводу, что она, вероятно, подпадает под действие нового законодательства, ей следует рассмотреть организационные, финансовые и технические шаги, которые потребуются для подготовки к выполнению требований NIS2. Например, с точки зрения расходов на ИКТ, Европейская комиссия ожидает, что организации столкнутся с максимальным увеличением расходов на безопасность ИКТ на 22% в первые несколько лет после внедрения NIS2 (максимальное увеличение на 12% оценивается для организаций, которые уже находятся под сфера применения действующей Директивы NIS). Кроме того, организации, входящие в сферу охвата, должны следить за тем, как NIS2 реализуется в ключевых юрисдикциях ЕС, где они работают.

Кроме того, организации, предлагающие продукты/услуги для информационной и сетевой безопасности, также должны быть готовы к комплексной проверке со стороны организаций NIS2. Таким образом, эти организации, не входящие в сферу компетенции, должны обеспечить наличие эффективных документированных процессов для управления рисками безопасности, связанными с их предложением продуктов / услуг, в ожидании любой такой комплексной проверки.

Что касается сроков реализации, то текст NIS2 был предварительно согласован Европейским парламентом и Европейским советом, и теперь оба эти учреждения

должны официально принять текст. Ожидается, что NIS2 будет принят в 2022 году, и после его принятия у государств-членов будет 21 месяц, чтобы включить NIS2 в национальное законодательство. Маловероятно, что он будет принят и официально перенесен во все национальные законы государств-членов ЕС как минимум до конца 2024 года». ***(Ana Hadnes, Bruder David A., Simon Reece Randall. NIS2 Directive New Cybersecurity Rules Expected in the EU // Mayer Brown (https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/nis2-directive-new-cybersecurity-rules-expected-in-the-eu). 06.10.2022).***

***

«Каждые 11 секунд в мире организация становится жертвой программы-вымогателя, и, по оценкам, в 2021 году годовой ущерб от киберпреступлений в планетарном масштабе составил 5 500 миллиардов евро.

Эти тревожные цифры заставили Европейскую комиссию серьезно заняться проблемой и включить кибербезопасность в список своих приоритетных действий. Параллельно с пересмотром директивы «Сетевая и информационная безопасность» (NIS) президент Европейской комиссии объявил в сентябре 2021 года о подготовке нового законодательного акта о киберустойчивости, «Закона о киберустойчивости» (КРА).

Определение Закона о киберустойчивости (CRA)

Основываясь на Стратегии кибербезопасности ЕС до 2020 года, CRA вводит общие правила кибербезопасности для производителей и разработчиков продуктов с цифровыми элементами, охватывающих как аппаратное, так и программное обеспечение. Целью этого документа является защита потребителей и компаний от рисков кибербезопасности при использовании ими проводного и подключенного оборудования, а также программного обеспечения.

15 сентября 2022 года Комиссия представила первый проект, который будет представлен на рассмотрение Европейского парламента и Совета.

Эта первая версия дает возможность взглянуть на будущие обязательства, которые будут регулировать продажу продуктов с цифровыми элементами в соответствии с проектом Комиссии.

На какие продукты распространяется Закон о киберустойчивости?

Закон о киберустойчивости носит широкий характер, предложение Комиссии установить общие правила для всех «продуктов, содержащих цифровые элементы», понятие, определенное в статье 3 проекта как «любой программный или аппаратный продукт и его решения для удаленной обработки данных, включая программное обеспечение». или аппаратные компоненты, которые будут размещаться на рынке отдельно». Это определение будет включать все подключенное оборудование (компьютеры, телефоны, бытовую технику, автомобили, игрушки, устройства виртуальной помощи и т. д.), а также системы такие как VPN, антивирусы, менеджеры паролей, необходимое программное обеспечение для управления облачными сервисами или операционные системы упомянутого выше оборудования. Для ясности проект CRA содержит список соответствующих продуктов и программного обеспечения.

Следует отметить, что европейский законодатель намерен провести различие между общей категорией продуктов, содержащих цифровые элементы, и теми, которые считаются «критическими», причем эта вторая категория представляет 10% объектов, на которые распространяется регулирование. Сама эта вторая категория будет подразделяться на два класса в соответствии с уровнем критичности рисков. В зависимости от класса, к которому оно относится, программное или аппаратное обеспечение будет подлежать более или менее строгому контролю и обязательствам.

Каковы новые обязательства производителей и дистрибьюторов?

Комиссия объявляет о ряде мер, которые вращаются вокруг двух осей: повышение уровня кибербезопасности продуктов и повышение уровня информации для потребителей и предприятий.

Меры, предлагаемые в рамках проекта CRA, будут определять:

Правила, которые необходимо соблюдать при размещении на рынке продуктов, подпадающих под действие правил кибербезопасности;

Обязанности производителей при проектировании, разработке и производстве данной продукции;

Основные требования, предъявляемые к производителям на протяжении всего жизненного цикла продукции. Производители будут распространять исправления безопасности и внедрять процедуры управления уязвимостями.

Информация о безопасности продукции должна быть включена во всю документацию, сопровождающую продукцию. Эта информация будет касаться безопасности, технической поддержки, предлагаемой поставщиком, или установки обновлений безопасности.

Каковы исключения из режима Закона о киберустойчивости?

Хотя сфера действия предлагаемого Закона о киберустойчивости относительно широка, следует ожидать определенных исключений.

Прежде всего, Комиссия указывает, что программное обеспечение, предоставляемое как услуги (такие как обмен мгновенными сообщениями), а не как продукты, не будет подпадать под действие предлагаемого закона. Последнее распространяется только на продукты, содержащие цифровые элементы, продаваемые на европейском рынке. Однако это программное обеспечение, предоставляемое как услуга, будет регулироваться директивой NIS 2, а также другим отраслевым законодательством. Однако эти правила содержат технические требования и предлагают уровень защиты кибербезопасности, эквивалентный уровню, обеспечиваемому CRA.

По той же причине проект CRA также не будет охватывать разработанное внутри компании программное обеспечение, такое как системы электронных медицинских карт.

Наконец, предусмотрены исключения для определенных категорий продуктов, для которых уже существует европейское законодательство, устанавливающее требования кибербезопасности. Это особенно касается медицинских устройств или устройств для авиационной и автомобильной промышленности.

Какие обязательства подлежат мониторингу и санкциям?

Разумеется, законодатель намерен контролировать применение этих новых обязательств. Таким образом, предусмотрено, что государства-члены назначат

органы по надзору за рынком, ответственные за выполнение обязательств, предусмотренных CRA.

Эти органы могут принять несколько мер. В частности, они могут потребовать от операторов прекратить несоблюдение требований, ограничить доступность продукта, устранить риск. Они также могут потребовать отзыва товара или его изъятия из продажи.

Эти прерогативы будут сопровождаться санкциями в виде штрафов, которые могут достигать 2,5% от оборота или даже 15 миллионов евро». ***(Gérard Haas, Romain Delangle. Cyber Resilience Act (CRA): définition, obligations et sanctions // HAAS AVOCATS (https://info.haas-avocats.com/droit-digital/cyber-resilience-act-cra-definition-obligations-sanctions). 03.10.2022).***

***

«Поскольку Европа стремится расширить свое покрытие 5G и сократить разрыв с другими регионами, кибербезопасность должна учитываться на всех этапах этого процесса, заявила депутат Европарламента Цветелина Пенькова, выступая на мероприятии, посвященном будущему 5G, организованном GSMA на этой неделе.

Это особенно важно, добавила она, по мере увеличения обмена и использования данных, а также в контексте текущей геополитической ситуации в отношении вторжения России в Украину, «которое мы не должны игнорировать и которое также повлияет на безопасность сети» и безопасность данных в Европе».

Регуляторное внимание к кибербезопасности в последние годы возросло, и с момента начала войны в Украине в феврале вновь обратился к повышению устойчивости к угрозам.

В прошлом месяце Комиссия выдвинула свой предложенный Закон о киберустойчивости, целью которого является внедрение подхода «безопасность по дизайну» для повышения безопасности подключенных устройств в Интернете вещей.

Что касается развития инфраструктуры 5G в Европе, заинтересованные стороны заявили, что необходимо всесторонне учитывать соображения кибербезопасности.

Однако, в то время как ЕС отстает от многих других регионов, когда речь идет о развертывании 5G, ситуация обратная, когда речь идет о приоритизации кибербезопасности, сказала Пенькова, отметив, что многие глобальные партнеры, находящиеся на более позднем этапе развертывания своих сетей, не имеют нормативно-правовой базы кибербезопасности, которая ЕС продвигался вперед.

«Тот факт, что мы создаем безопасную и отказоустойчивую сеть и уделяем большое внимание кибербезопасности, не означает, что все наши партнеры также уделяют этому столько внимания», — сказала она.

«Нам нужно лучше поощрять их к принятию необходимых мер, чтобы гарантировать, что когда мы говорим о передаче и использовании данных, мы не можем ограничить это только ЕС».

Депутат добавил, что отказоустойчивая и безопасная инфраструктура 5G принесет пользу как предприятиям, так и потребителям, а развитие менее

фрагментированного рынка телекоммуникаций в ЕС станет необходимым элементом, помогающим Европе догнать остальной мир с точки зрения подключения 5G.

Эту точку зрения поддержали несколько выступавших на мероприятии GSMA, многие из которых подчеркивали необходимость консолидации рынка для адекватного решения проблемы.

Сложность этого, отметил Матиас Бауэр, директор Европейского центра международной политической экономии, частично связана с характером самого ЕС и его объемом различий в регулировании и физическом ландшафте, характерных для конкретных стран.

«ЕС — это не одна страна; в будущем это не будет единой страной. У нас даже нет большого единого рынка, который можно было бы сравнить с США, Китаем, Бразилией или Индией», — сказал он, добавив, что у властей также существуют очень разные степени срочности, когда речь идет о необходимости установки сетей 5G.

«Я считаю, — сказал он, — что нет реального чувства безотлагательности, не говоря уже о стремлении к глобальному лидерству».

Хотя на бумаге среди регулирующих органов и институтов ЕС существует аппетит к инновациям, он отметил, что «часто политика реализуется на уровне ЕС — в меньшей степени на национальном уровне — что на самом деле подрывает международную торговлю, международные инновации и инновации в интернет-приложениях».

Таким образом, консолидация и ускорение развития сети, по словам Якоба Грайнера, вице-президента по европейским делам Deutsche Telekom, станут необходимыми первыми шагами, если Европа хочет создать единый телекоммуникационный рынок.

Однако, добавил он, директивным органам также необходимо будет продумать такие вопросы, как высокая стоимость и несправедливое лицензирование радиочастотного спектра, а также парадокс стагнации доходов и роста затрат на передачу данных и развертывание, если проблемы в секторе будут решаться. Столкнуться». ***(Molly Killeen. Stakeholders urge cybersecurity focus in 5G deployment // EURACTIV MEDIA NETWORK BV. (https://www.euractiv.com/section/digital/news/stakeholders-urge-cybersecurity-focus-in-5g-deployment/). 07.10.2022).***

***

«Глава национального агентства кибербезопасности Германии находится под пристальным вниманием в связи с сообщениями о связях с российской разведкой, заявили официальные лица в понедельник.

Арне Шенбом, возглавляющий агентство BSI, десять лет назад стал соучредителем группы по кибербезопасности, объединяющей экспертов из государственных учреждений и частного сектора. Немецкие СМИ сообщили, что одним из ее участников является компания, основанная бывшим агентом российской разведки.

«Министерство внутренних дел серьезно относится к сообщениям, о которых стало известно в выходные, и проводит их всестороннее расследование», — говорится в заявлении министерства.

В Германии растет обеспокоенность тем, что критически важная инфраструктура страны может стать мишенью для России из-за поддержки Берлином Украины. В субботу очевидный акт саботажа вынудил немецкую железнодорожную компанию Deutsche Bahn остановить пассажирские и грузовые поезда на северо-западе страны почти на три часа.

После почти трехчасовой приостановки в Deutsche Bahn заявили, что проблема — «отказ цифровой системы радиопоезда» — была решена, но некоторые сбои все же можно ожидать. Позже он заявил, что отключение было вызвано саботажем.

Министр транспорта Фолькер Виссинг заявил, что кабели, которые «необходимы для безопасного движения по железной дороге», были намеренно перерезаны в двух разных местах. Он сказал, что федеральная полиция Германии расследует инцидент». ***(German cybersecurity chief investigated over Russia ties // ABC News Internet Ventures (https://abcnews.go.com/Business/wireStory/german-cybersecurity-chief-investigated-russia-ties-91274203). 10.10.2022).***

***

«Міністерка внутрішніх справ Німеччини Ненсі Фезер шукає заміну голові Федерального відомства з безпеки у сфері інформаційної техніки (BSI) Арне Шенбому.

Чиновник, імовірно, перебував у контакті з асоціацією Cyber-Sicherheitsrat Deutschland, яка, за даними журналістів, пов'язана з російськими спецслужбами, повідомляє Bild.

«Фезер має намір у найкоротші терміни усунути нинішнього главу відомства, завданням якого є захист німецького кіберпростору від хакерських атак. Через це вона відмовилася від участі в запланованій на 13 жовтня презентації звіту про діяльність BSI за 2022 рік і спільної з відомством пресконференції», – ідеться у повідомленні.

Активне невдоволення Шенбомом, як зазначають ЗМІ, виникло після виходу розслідування на телеканалі ZDF. Водночас Шенбома не можуть просто звільнити з посади через нюанси німецького законодавства. Його, найімовірніше, переведуть до іншого відомства.

Депутати Бундестагу раніше зазначали, що з початку російського вторгнення в Україну на Німеччину почастішали кібератаки. Ситуація з ІТ-безпекою у ФРН вважають «надто напруженою». ***(Очільника німецького відомства з кіберзахисту замінять за зв'язки з РФ // Gazeta.ua (https://gazeta.ua/articles/world-life/_ochilnika-nimeckogo-vidomstva-z-kiberzahistu-zaminyat-za-zvyazki-z-rf/1115091). 10.10.2022).***

***

«Більше половини польських компаній побоюються кібератак. Дослідження, проведені серед менеджерів і директорів компаній, показують, що через пандемію коронавірусу та напад Росії на Україну підприємства дедалі частіше звертають увагу на питання кібербезпеки.

За словами системного інженера Ґжеґожа Ноцоня, пандемія викликала зростання значення безпеки у інтернет-просторі — кібербезпека стала пріоритетом для понад 60 відсотків польських компаній.

«Компанії, які піддаються найбільшому ризику атак, це компанії, що займаються логістикою та транспортом, а також комерційні, комунікаційні та IT-компанії. Найбільше підприємців хвилює те, що кібернапади можуть призвести до проблеми зі здійсненням платежів, до поганого фінансового стану компанії, а також спричинити проблеми із виконанням послуг і замовлень», — говорить спеціаліст.

Більше половини опитаних компаній повідомили, що вони запровадили заходи безпеки для віддаленої роботи, а також найняли спеціалістів для відстежування можливих загроз.

Дослідження проводилося серед понад 300 польських компаній. Подібні дослідження були проведені також у Чехії та Угорщині». (***Польські компанії бояться кібератак // Polskie Radio S.A. (https://www.polskieradio.pl/398/7856/Artykul/3057878,%D0%9F%D0%BE%D0%BB%D1%8C%D1%81%D1%8C%D0%BA%D1%96-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%97-%D0%B1%D0%BE%D1%8F%D1%82%D1%8C%D1%81%D1%8F-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA). 22.10.2022).***

***

«В Європі є багато міст і регіонів, де фахівець з кібербезпеки може знайти роботу або переїхати, щоб розвивати кар'єру в цьому швидкозростаючому секторі. Потреба у кваліфікованих фахівцях також зростає в геометричній прогресії. Законодавство, таке як Європейський закон про кібербезпеку і GDPR, також підвищило попит на фахівців з безпеки. Залежно від того, де ви хочете працювати, зарплати можуть бути високими. Для визначення лідера континенту Глобальний індекс кібербезпеки Організації Об'єднаних Націй пропонує гострий погляд завдяки глибокому зануренню в сильні і слабкі сторони кожної країни. Країни оцінюються за їхніми правовими структурами, технічними можливостями, організаційними повноваженнями, розбудовою потенціалу та співпрацею. В Європі перше місце посідає Велика Британія, а Лондон є провідним містом у сфері кібербезпеки.

Існує багато причин, чому Лондон є таким центром кібербезпеки. Існує потужна політична підтримка фінтех-індустрії з точки зору проведеного у 2021 році на замовлення уряду Огляду Каліфи, який визначив кілька центрів діяльності по всій Великобританії, а також надав низку рекомендацій для підтримки сектору.

На національному рівні Велика Британія також знаходиться на висхідній траєкторії від своєї новаторської Національної стратегії кібербезпеки 2016 року зі створенням Національних кібервійськ у 2021 році і переробленим планом на 2022 рік для забезпечення можливості продовжувати адаптацію, інновації та інвестиції. Крім того, в країні розташована низка оборонних компаній, таких як BAE Systems, Thales, Lockheed Martin Corporation і Northrop Grumman, а також власні кібер-компанії, такі як Darktrace і Becrypt. Всі ці компанії мають провідні вимоги до фахівців з кібербезпеки.

Відкриті вакансії – це одне, але вони мають бути підкріплені кадровим резервом. Це забезпечується і тут завдяки великій кількості вищих навчальних закладів Великої Британії, які пропонують бакалаврські і магістерські програми.

Для тих, хто вже працює в цій галузі, існує безліч можливостей для налагодження контактів. Лондон є глобальним центром призначення і транспортним вузлом, що робить його чудовим місцем для життя і роботи.

Якщо ви хотіли б розпочати кар'єру в галузі кібербезпеки в одному з найдинамічніших міст Європи, ми пропонуємо вам ознайомитися з трьома відкритими вакансіями, наведеними нижче. На сайті вакансій The House of Talent ви знайдете ще багато цікавих пропозицій.

Наприклад, Інженер з виявлення кібербезпеки, Avertium, (віддалена робота). Команда Avertium з розвідки кіберзагроз шукає інженера з виявлення кіберзагроз для створення користувацьких наборів правил виявлення та іншого контенту для різних платформ безпеки, включаючи SIEM, EDR, SOAR тощо. Ви повинні добре розуміти мови пошукових запитів та стратегії розбору логів, а також мати досвід створення кастомного контенту щонайменше для однієї платформи безпеки.

Чи от – Старший спеціаліст з внутрішнього контролю, Exclusive Networks Limited, Лондон. Як старший спеціаліст з внутрішнього контролю, ви діятиме на випередження та працюватиме над ініціативами в масштабах всієї компанії, здійснюватиме постійний моніторинг та адаптацію системи внутрішнього контролю, братимете участь в оновленні групових політик та процедур, а також блок-схем процесів та матриць моніторингу ризиків.

І нарешті, Консультант з питань стійкості та безперервності бізнесу, BCT Resourcing, Лондон. Ви приєднаєтесь до команди з питань репутації, кризових ситуацій та стійкості в якості консультанта з питань стійкості та безперервності бізнесу, щоб допомогти у забезпеченні потреб клієнтів у плануванні, розбудові стійкості, підготовці до подій та інцидентів». ***(Julia Alexandrova. Лондон визнано найкращим містом Європи для фахівців з кібербезпеки // Root Nation (https://root-nation.com/ua/news-ua/it-news-ua/ua-london-viznano-naykraschim-mistom-evropi-dlya-fahivtsiv-z-kiberbezpeki/). 24.10.2022).***

***

«Восточно-европейский оператор связи A1 Telekom Austria подводит итоги октября, который был международным месяцем кибербезопасности, признав, что только в августе во многих странах группы было совершено 28 миллионов атак.

Компания, работающая в Австрии, Болгарии, Беларуси, Хорватии, Северной Македонии, Сербии и Словении, предупреждает, что конечные пользователи «подвергаются различным киберугрозам в своей частной онлайн-активности, включая поддельные новостные сайты, поддельные приложения для знакомств, игровые платформы., и многое другое».

Компания сообщает, что Whalebone, стартап, базирующийся в кампусе A1 Start Up Campus в Вене с 2017 года, активизирует свое партнерство с A1 в рамках A1 Net Protect.

Ричард Малович (на фото), генеральный директор Whalebone, сказал: «A1 Net Protect — это революционное решение с новаторскими результатами. Это позволяет обычным интернет-пользователям оставаться в безопасности независимо от того, какие устройства и приложения они используют».

Он сказал: «Рекордно большое количество обнаруженных угроз для конечных пользователей нескольких компаний A1 в регионе Центральной и Восточной Европы [Центральная и Восточная Европа] в августе прошлого года (28 338 483) отражает растущую популярность сервиса и жизненно важную роль, которую он играет в защите конечных пользователей.».

Алехандро Платер, главный операционный директор A1 Telekom Austria Group, сказал: «Кибербезопасность является основой успешной цифровой трансформации и имеет соответствующий статус во всей A1 Group».

Whalebone говорит, что в первую очередь фокусируется на разрешении DNS на сетевом уровне и защите от кражи личных данных и направлен на защиту домашних гаджетов, таких как интеллектуальные термостаты или камеры.

Плейтер сказал: «Чтобы предоставить нашим клиентам максимально возможную защиту от кибератак и других виртуальных угроз, мы предлагаем бесчисленное количество продуктов и услуг и регулярно обращаем внимание на опасности. Как ведущий поставщик в регионе Центральной и Восточной Европы, у нас, естественно, есть преимущество, заключающееся в том, что мы можем поддерживать процессы защиты с помощью соответствующих сложных технологий». ***(Alan Burkitt-Gray. A1 Telekom Austria steps up activity on cybersecurity // Capacity Media (https://www.capacitymedia.com/article/2atpxg7kakt339mwxbeo0/news/a1-telekom-austria-steps-up-activity-on-cybersecurity). 31.10.2022).***

***

«…Правительство в рамках своей Национальной киберстратегии на период до 2022 года, опубликованной Кабинетом министров в начале этого года, подчеркнуло решающую роль цифровой экономики в более широкой повестке дня — не в последнюю очередь в развитии образования и навыков, но и в долгосрочной перспективе в плане цифровой трансформации экономики для содействия ее росту.

Частично это допускает наличие онлайновых и цифровых уязвимостей, и поэтому, хотя стратегия цифрового «роста» по праву занимает центральное место, повышение устойчивости и борьба с преступностью в этой области имеют решающее значение; без них доверие к стратегии будет серьезно подорвано.

Где мы сейчас?

Во-первых, хорошие новости. Согласно исследованию PWC Global Economic Crime Survey 20221, за последние два года с 2020 года число трех из пяти основных видов мошенничества, о которых сообщают британские респонденты, — киберпреступность, мошенничество с клиентами и мошенничество с платежными ведомостями — сократилось. Многообещающее начало… но:

64% всех респондентов из Великобритании сталкивались с мошенничеством, коррупцией или другими экономическими преступлениями;

51% этих мошеннических действий были совершены за пределами организации — клиентами, хакерами или поставщиками поставщиков; а также

хотя технологии помогли, наиболее эффективным методом обнаружения наиболее серьезных случаев было существующее внутреннее управление рисками мошенничества, включая мониторинг активности, внутренний мониторинг и безопасность.

Противоречие между расширением прав и возможностей людей или внедрением технологий в борьбе с киберпреступностью уже давно находится в центре споров о передовом опыте.

Люди рискуют

Вызывает тревогу тот факт, что информирование посредством разоблачений, предупреждений или внутренних кадровых перестановок оказалось наименее эффективным для выявления преступной деятельности. Одно из объяснений, возможно, заключается в том, что организации больше доверяют процессам и технологиям, чем обучению своих сотрудников выявлению и обнаружению мошенничества как внутри, так и вне бизнеса. Для всех организаций это тщательный баланс ресурсов, особенно там, где сотрудники и их время в большом почете. Итак, один вывод из опроса заключается в том, что обучение и повышение осведомленности сотрудников приносят дивиденды.

Еще одна тревожная тенденция, выявленная PWC, связана с увеличением объема внешнего мошенничества, нацеленного на организации. Отчасти это свидетельствует о повышении риска в цепочках поставок, а также в виртуальной клиентской базе.

Закупка услуг и доверие к поставщикам, таким образом, является особой слабой стороной. Понятно, что решения на основе искусственного интеллекта для адаптации и управления клиентами сами по себе пока не кажутся надежным решением. Спрос на определенные материалы в текущем экономическом цикле, когда санкции сказываются на предложении, и поиск более дешевых и более доступных альтернатив вынуждают предприятия и организации брать на себя больший риск при кредитовании, а также часто приводят к удлинению их цепочек поставок. Там, где эти риски не контролируются, а процессы проверки личности и безопасность поставщиков могут быть менее строгими, организации могут подвергаться большему риску мошенничества, кражи данных и экономических преступлений.

С этой целью, хотя предприятия в целом понимают необходимость большей прозрачности в отношениях с поставщиками, необходимой для процессов KYC и AML или по причинам ESG, возросшая нагрузка на управление отношениями становится решающим фактором в борьбе с киберпреступностью. В экономически трудные времена должное усердие приобретает еще большее значение, но неизбежно иногда упускается из виду, преднамеренно или нет, и такие упрощения могут привести к большей уязвимости и потенциальному ущербу.

Одним из положительных моментов на горизонте является запланированный законопроект об экономических преступлениях и корпоративной прозрачности, который предусматривает более тщательную проверку личности директоров и лиц, имеющих значительный контроль. Если законопроект будет утвержден в качестве

закона, есть надежда, что соответствующий закон остановит злоупотребление процессом регистрации в Регистрационной палате, в котором было много случаев фиктивных директоров или компаний-фениксов, созданных для преступных целей. В качестве общедоступного онлайн-хранилища данных, доступного для всех, это было бы хорошей отправной точкой.

Технологические риски

Поскольку 90 % предприятий и 80 % благотворительных организаций (включая школы и университеты) имеют цифровой след (например, возможность платить в Интернете, использовать сетевые устройства или хранить информацию в электронном виде), потенциал роста кибер-виктимизации сейчас, по понятным причинам, выше, чем когда-либо прежде.

Однако стоит отметить, что переход на онлайн или удаленную работу во время пандемии не привел к быстрому всплеску киберпреступности, хотя он, безусловно, вырос. Удивительно, но объем не имеет значения, а общее количество преступлений падает. В технической изощренности киберпреступников произошла эволюция, что является отличительной чертой кибермошенничества за последние 12 месяцев.

Обзор нарушений кибербезопасности 2022 года определяет попытки фишинга как наиболее распространенную угрозу: в результате 83% британских организаций (включая благотворительные и образовательные учреждения), подвергшихся атакам, пострадали. Обман сотрудников мошенническими поддельными электронными письмами со ссылками на зараженные вредоносным ПО документы или поддельные веб-сайты остается серьезной проблемой для большинства организаций. Каждая пятая жертва также идентифицировала вредоносное ПО, DDoS-атаки (отказ в обслуживании) и программы-вымогатели, демонстрируя гораздо более высокий уровень изобретательности и изменение вектора атаки со стороны так называемых злоумышленников.

Более крупные организации (с доходом >5 миллионов фунтов стерлингов), с их большими возможностями и более комплексной кибербезопасностью, подверглись более чем одному из этих типов атак в прошлом году, что означает разнообразие используемых методов и частоту этих атак. увеличение.

В ответ устойчивость организаций к защите от киберпреступлений зависит от их ИТ-ресурсов и безопасности, а также от принятых мер и способности реагировать. Опрос подтверждает, что хотя эти многогранные атаки встречаются реже, чем фишинг, они оказывают гораздо более существенное влияние на организацию-жертву. Масштабы и серьезность воздействия таких многогранных атак приводят к увеличению времени восстановления, более высоким потенциальным затратам (и потерям) и большему ущербу для репутации и морального духа персонала.

Хотя большинство организаций осознают необходимость политики бдительности и предотвращения, тем не менее, они реагируют и полагаются на ту или иную форму нечетко сформулированного плана реагирования. Важно отметить, что у меньшего числа есть упреждающие меры и письменные инструкции. Последнее должно стать частью целостного подхода к устранению инцидентов, предусматривающего четкие линии отчетности, раннее взаимодействие со страховщиками или киберспециалистами, уведомление регулирующих органов и связь с заинтересованными сторонами и общественностью, где это необходимо.

Технологии против людей

Перед лицом возросших технологических проблем неудивительно, что отчет DCMS о нарушениях кибербезопасности, в котором были опрошены 10 организаций, подвергшихся кибервзлому, подтвердил, что они больше полагаются на технологии, а не на людей. Хотя их опыт этих взломов был неприятным и разрушительным, лишь немногие по-настоящему понимали или фактически измеряли финансовые последствия для своего бизнеса, такие как время управления и затраты на расследование и устранение последствий. Обзор тем этого исследования помогает объяснить проблемы, стоящие перед многими организациями.

Многие организации, по-видимому, сосредоточились на мерах по исправлению положения, таких как информирование попечителей/директоров, оценка масштаба и выявление источника нарушения, в том числе (если позволял бюджет) и опора на кибербезопасность. Малый и средний бизнес особенно пострадал, когда аутсорсинговые поставщики управляемых услуг (для электронной почты и хранения данных), на которых полагалась организация, были на расстоянии вытянутой руки, и организация не могла должным образом оценить их производительность, что привело к неоднозначным (часто негативным) ответам. перед лицом происшествия. Хотя технологические средства защиты и минимизация сбоев являются частью любого ответа, лишь немногие по-настоящему понимали масштаб проблемы, с которой приходилось сталкиваться их организациям.

Во многих отношениях серьезность, с которой организация относится к этим проблемам, имеет основополагающее значение для их способности прийти в норму. Некоторые респонденты рассматривали кибербезопасность как проблему Совета директоров, но, по иронии судьбы, «настоящее» лидерство проявлялось только после нарушения. Даже тогда немногие организации потратили время на то, чтобы должным образом проанализировать истинное финансовое влияние и понять, рассмотреть и принять результаты обучения, чтобы улучшить свою безопасность в будущем.

Очевидно, что несоответствия в подходах приводят к неоднозначной реакции в целом. Разработка и реализация согласованной стратегии кибербезопасности является обязанностью высшего руководства. Учитывая постоянно растущие риски и важность, которую стратегия играет в защите организации от них, она должна стать постоянной темой для обсуждения на заседаниях совета директоров с принятием мер по устранению любых проблем или пробелов в политике, которые могут возникнуть.

Готовься и учись

И в этом заключается вызов. Организации, опрошенные DCMS, указали, что люди и культура были большей проблемой и слабыми местами в их реакции на киберриски, чем технологии, при этом признав, что уязвимость возросла на всех уровнях.

К счастью, хотя это и не панацея, но если ваша организация изучает эту проблему, существует исходное решение, объединяющее две явно отличающиеся друг от друга области уязвимости.

Правительственная национальная стратегия кибербезопасности содержит некоторые практические рекомендации в «10 шагах к кибербезопасности». Это

простой набор правил, который не только предоставляет организациям общие принципы для построения надлежащего управления и корпоративной политики, но и для выявления мошенничества, а также для повышения устойчивости. Взаимодействие с советом директоров, более эффективное управление, управление рисками поставщиков, управление рисками и активами, а также инвестиции в навыки, осведомленность и культуру в области кибербезопасности, включая письменный план реагирования на чрезвычайные ситуации, должны быть в центре любой политики.

Из этих 10 шагов вовлечение и обучение персонала выделяются как самая быстрая и легкая победа. Инвестиции в своих людей, проверка их и их полномочий при назначении и продвижении по службе, а затем внедрение культуры борьбы с мошенничеством в сотрудников, осведомленных о киберпреступности, несомненно, сэкономит деньги вашей организации». ***(Paul Wainwright. Economic crime and cybercrime — it's time to pay more attention // Browne Jacobson LLP (https://www.brownejacobson.com/training-and-resources/resources/legal-updates/2022/10/public-sector-cybercrime). 18.10.2022).***

***

«Предприятия должны относиться к киберпреступлениям как к серьезной стратегической угрозе и более тесно сотрудничать с правительством, чтобы защитить себя и свои данные, предупредил канцлер герцогства Ланкастер Надхим Захави.

Его замечания прозвучали после того, как новые данные показали, что 1,6 миллиона человек стали жертвами киберпреступников в Великобритании в прошлом году, а десятки тысяч компаний также подверглись хакерским атакам, мошенничеству и попыткам шантажа в этот период.

Это в дополнение к отраслевым данным, показывающим, что Великобритания является третьей страной, на которую больше всего нацеливаются киберсубъекты национального государства, после США и Украины, причем правительство является наиболее целевым сектором.

В качестве ведущего министра кибербезопасности г-н Захави возглавляет движение бизнеса по ужесточению безопасности и объединяет лидеров отрасли для формирования Национального консультативного совета по кибербезопасности, который будет регулярно встречаться для обсуждения реальных угроз и способов противодействия им.

Г-н Захави возглавит совет вместе с Шэрон Барбер, директором по безопасности Lloyds Banking Group.

Укрепление кибербезопасности также поможет реализовать планы правительства по развитию экономики и обеспечить успешные инвестиции в инфраструктуру, навыки и инновации.

Г-н Захави говорит, что компании должны рассматривать киберпреступность как проблему на уровне правления, которая требует стратегического подхода, если мы хотим успешно справиться с ней. Чтобы проиллюстрировать этот момент, правительственные исследования показывают, что только 23% фирм имеют план кибербезопасности.

Правительство разработало Национальную киберстратегию, которая подкреплена финансированием в размере 2,6 млрд фунтов стерлингов до 2030 года.

Канцлер герцогства Ланкастер Надхим Захави сказал:

«Британский бизнес лежит в основе нашей экономики и станет ключевой частью наших амбициозных планов экономического роста, которые обеспечат более высокую заработную плату и больше возможностей для людей по всему Соединенному Королевству. Одним из составных элементов нашего плана является онлайн-безопасность государственных услуг и частного сектора. Потому что невозможно добиться экономического роста без экономической безопасности в цифровом мире.

«Нам нужно, чтобы организации делали больше для усиления своей киберзащиты. Судя по количеству предприятий, которые пострадали от кибератак, это область уязвимости. Компании должны понимать, что киберугроза, с которой мы сталкиваемся, больше не является проблемой только для ИТ-отделов компании — это проблема на уровне совета директоров, которую необходимо решать с помощью вмешательства на уровне совета директоров.

«Итак, мое послание бизнесу ясно; более тесно сотрудничайте с нами в развитии навыков, обучении и онлайн-защите, что окажет положительное влияние на успех ваших компаний и, в свою очередь, поможет нам реализовать наш амбициозный план по повышению экономического процветания и положить больше денег в карманы людей».

В своем выступлении в рамках Сингапурской международной кибернедели министр кабинета министров баронесса Невилл-Рольфе сегодня расскажет о необходимости совместной работы бизнеса, правительства и партнеров для борьбы с киберпреступностью. Она подчеркнет важность сотрудничества с партнерами по всему международному сообществу в свете существующих глобальных угроз.

Эти угрозы были отмечены сэром Джереми Флемингом, директором GCHQ, во время выступления в Лондоне на прошлой неделе.

Государственный министр баронесса Невилл-Рольф сказала:

«Каждый год киберпреступники теряют миллиарды фунтов стерлингов, нарушая работу ключевых государственных служб или жизненно важных секторов национальной экономики, и важно, чтобы мы как общество серьезно относились к этой угрозе.

«Только если мы повысим нашу киберустойчивость по всей стране, укрепим наши наступательные и оборонительные возможности и бизнес-системы и обеспечим, чтобы каждый играл свою роль в кибербудущем Великобритании, мы сможем процветать благодаря возможностям, которые дает онлайн-мир.

«Как ведущая ответственная кибердержава, мы также будем продолжать создавать альянсы с демократическими партнерами по всему миру для защиты свободного, открытого и мирного киберпространства».

Правительство хочет, чтобы предприятия поднимали вопрос кибербезопасности и обеспечивали, чтобы советы компаний регулярно получали брифинги об угрозах, имели стратегию кибербезопасности и план реагирования на киберинциденты, управляли рисками кибербезопасности в цепочке поставок, обучали персонал и следили за тем, чтобы компания устройства защищены.

Также был опубликован Инструментарий Business Board, чтобы дать фирмам четкое руководство о том, что они могут сделать для снижения рисков, наряду с 10 шагами к кибербезопасности, чтобы помочь предприятиям управлять рисками и определить меры, которые можно предпринять для повышения безопасности». ***(Zoe Deighton Smythe. Government drive to boost UK business cybersecurity // Security Industry Group (https://securityonscreen.com/government-drive-to-boost-uk-business-cybersecurity/). 27.10.2022).***

***

Індія

«Министерство электроники и информационных технологий (MeitY) недавно обновило свои рекомендации по кибербезопасности для государственных служащих, которые впервые были опубликованы в июне этого года. Новые руководящие принципы включают в себя, среди прочего, положения по обеспечению безопасности локальных вычислительных сетей (ЛВС) министерств и ведомств, а также требования к ведению журналов.

В последней версии рекомендаций, с которой ознакомился Moneycontrol, разъясняется, что должны делать руководители по информационной безопасности (CISO) государственных министерств и ведомств, чтобы локальные сети офисных сетей не были уязвимы для кибератак.

Национальный центр информатики (NIC), подразделение MeitY, выпустил последнюю версию 5 сентября. NIC удовлетворяет все виды потребностей в информационных и коммуникационных технологиях (ИКТ) на всех уровнях правительства, проектирует и разрабатывает и т.п.

В руководящих принципах правительство сначала заявило, что все правительственные приложения, веб-сайты и службы должны размещаться в центрах обработки данных или у поставщиков облачных услуг, одобренных MeitY.

В нем указано, что такие приложения не должны размещаться в LAN-сегменте министерств или ведомств.

«Все ИКТ-устройства должны быть подключены через интернет-шлюз сети NIC (т.е. NICNET), а любое другое прямое интернет-соединение, т.е. широкополосное, 3G/4G/5G, должно быть немедленно прекращено», — говорится в директиве.

NICNET — это спутниковая общенациональная компьютерная сеть, разработанная NIC.

В руководстве также содержится просьба к директорам по информационной безопасности обеспечить наличие у всех министерств и ведомств плана управления киберкризисом (CCMP), который подготовлен и реализован.

Ранее в июле Moneycontrol сообщил, что только около половины департаментов и министерств индийского правительства имеют CCMP.

В 2019 году был запущен «КККП по противодействию кибератакам и кибертерроризму», чтобы создать основу для министерств/ведомств/органов по борьбе с кибератаками.

Кроме того, правительство ввело строгие меры контроля доступа ко всем подключенным системам и ИТ-устройствам в ведомствах и министерствах.

«Настройте брандмауэр узла на всех системах, чтобы ограничить боковое перемещение в пределах одной сети, — говорится в одном из руководств.

Правительство также включило требования к ведению журнала в последнюю версию руководящих принципов.

«Убедитесь, что ведение журнала включено во всех системах ИКТ, включая, помимо прочего, веб-сайты/приложения, базы данных, операционные системы, устройства ИКТ», — говорится в руководстве, добавляя, что журналы должны храниться не менее одного года.

Важно отметить, что правительство через Индийскую группу реагирования на компьютерные чрезвычайные ситуации внедрило указания по кибербезопасности, которые включают аналогичные требования к ведению журналов для всех типов юридических лиц.

Хотя большинство новых обновлений предназначалось для директоров по информационной безопасности, правительство также внесло некоторые изменения в свои инструкции для сотрудников.

Например, в нем говорилось, что если кто-то участвует в деликатном обсуждении, ему следует «выключить мобильный телефон или оставить его в безопасном месте за пределами комнаты для переговоров».

Он также посоветовал сотрудникам обратить внимание на несоответствие между разрешениями, которые может запрашивать приложение, и его функциями.

Что касается использования социальных сетей, правительство попросило сотрудников «ограничивать и контролировать использование / раскрытие личной информации при доступе к социальным сетям и сетевым сайтам», согласно руководящим принципам.

Moneycontrol обратился к MeitY и NIC с запросами по этому поводу, и сообщение будет обновлено, когда будет получен ответ». ***(Aihik Sur. Govt updates cybersecurity guidelines to boost dept LAN security // e-Eighteen.com Ltd. (https://www.moneycontrol.com/news/business/govt-updates-cybersecurity-guidelines-to-boost-dept-lan-security-9326281.html). 14.10.2022).***

***

«В 2021 году в Индии было зарегистрировано более 3000 жертв кибератак, что является четвертым по величине показателем в мире после США, Великобритании и Канады, а количество атак программ-вымогателей увеличилось на 120%. Это также был год, когда стоимость восстановления после атак программ-вымогателей выросла до 3,38 млн долларов с 1,1 млн долларов в 2021 году. Ранее, в 2020 году, в Juspay произошла утечка данных, которая затронула 35 миллионов записей клиентов, включая информацию о кредитных картах и сканирование отпечатков пальцев. А ранее в этом году, в феврале, Air India сообщила о крупной атаке, в результате которой были скомпрометированы записи более 4,5 миллионов клиентов.

В целом данные из недавнего отчета Университета Суррея показывают, что кибератаки на индийские предприятия и другие отрасли удвоились за последние три

года. Возможно, очевидно, что главным фактором, способствующим этим атакам, является распространение удаленной работы и революция IoT. Работа на дому увеличивает количество конечных точек в разных регионах, многие из которых не защищены, поскольку люди используют личные сети или общедоступные системы Wi-Fi для входа в систему. Меры по исправлению положения, такие как двухфакторная аутентификация, обеспечивают некоторую защиту, но этого недостаточно — современные киберпреступники очень изощренны в своих атаках. Например, с помощью фишинга они могут убедить сотрудников расстаться с важной информацией о компании, выдавая себя за менеджера или представителя компании. Что касается Интернета вещей, взаимосвязанность систем и сетей значительно повышает гибкость — обратная сторона, однако кибер-взлом в одной точке может быстро распространиться на остальную часть цепочки. Распределенные DoS-атаки, например, используют стандартные коммуникационные протоколы системы, чтобы перегрузить систему и получить контроль.

Очевидно, что когда речь идет о корпоративной кибербезопасности, простого применения брандмауэров уже недостаточно. Очень важно глубоко изучить природу и расположение уязвимостей, чтобы компании могли создать подходящую защиту.

Что такое уязвимость в кибербезопасности?

По сути, уязвимость — это слабое место в мерах безопасности компании, которым потенциально может воспользоваться киберпреступник. Это может быть связано со слабостью брандмауэров, защищающих внутренние сети, или просто с конечными точками пользователей без надлежащей защиты. Уязвимости могут возникать из-за плохо защищенного оборудования или программного обеспечения, ошибок в конкретной операционной системе, бэкдор-программ, неадекватной защиты паролем или человеческой ошибки из-за плохой осведомленности о безопасности.

Почему исследование уязвимостей имеет значение

Средняя стоимость утечек данных в 2021 году составила 4,24 миллиарда долларов, что на 10% больше, чем в 2020 году. И по мере того, как все больше и больше компаний выбирают удаленную работу и переходят в облако, эта сумма будет только расти. Утечки данных и другие кибератаки имеют далеко идущие последствия для любой компании, включая кражу интеллектуальной собственности, взлом сетей и вторжение в конфиденциальность данных потребителей (особенно личной информации). Их очистка потребует не только денег, но и усилий, что означает отклонение от основной деятельности и часто длительные перерывы. Кроме того, уязвимости системы кибербезопасности могут значительно повлиять на репутацию компании — даже возможность утечки данных может подорвать доверие. Это наносит ущерб прибыли компании и вызывает общественное сопротивление преимуществам взаимосвязанной цифровой экосистемы.

Поэтому понятно, что компании стремятся увеличить свой бюджет на кибербезопасность для дополнительных исследований и защитных мер. И несколько брендов предлагают решения для управления безопасностью для выявления и сортировки уязвимостей, особенно в устаревших инфраструктурах данных, которые менее защищены от современных атак. Для этого есть несколько шагов. Во-первых, тестер кибербезопасности проводит глубокое исследование текущих и

потенциальных уязвимостей системы. Они также анализируют существующие меры безопасности на предмет сильных и слабых сторон. Меры реагирования обычно включают упреждающую защиту конечных точек во всех приложениях и инфраструктурах, а также настройку системы контроля повреждений, которая срабатывает в случае атаки. Здесь также важно отметить, что не все уязвимости требуют немедленных действий — по-прежнему важно знать, где они находятся, и классифицировать их как с низким или высоким риском. При выборе поставщика для тестирования уязвимостей следует позаботиться о подтверждении его опыта в области безопасности приложений, мобильных устройств, инфраструктуры и IoT, что включает в себя обеспечение того, чтобы они использовали наиболее подходящие инструменты для каждого варианта использования.

Путь вперед для индийской кибербезопасности

Будучи развивающейся цифровой экономикой, Индия осознает риски кибербезопасности и предпринимает шаги в правильном направлении. В 2019 году Департамент науки и технологий правительства Индии объявил об исследовательской инициативе в области кибербезопасности для разработки перспективных технологий, которые могут защитить информационные системы от киберпреступности. Персонал в области кибербезопасности вырос со 110 000 в 2019 году до 218 000 в 2021 году, а услуги в области кибербезопасности за то же время выросли с 4,3 млрд долларов до 8,48 млрд долларов. А на 2023 финансовый год правительство Индии выделило 515 крор индийских рупий на кибербезопасность и заявило, что индийская группа реагирования на компьютерные чрезвычайные ситуации будет внимательно следить за всеми киберугрозами и атаками. В таком динамичном и ориентированном на цифровые технологии мире, как наш, постоянные исследования обеспечивают постоянную безопасность». ***(Swapnil Naik. Fortifying fault lines: Investing in vulnerability research to strengthen cybersecurity // Bennett, Coleman & Co. Ltd. (https://timesofindia.indiatimes.com/readersblog/afour-tech/fortifying-fault-lines-investing-in-vulnerability-research-to-strengthen-cybersecurity-45698/). 13.10.2022).***

***

Австралія

«ISACA опубликовала результаты своего первого исследования потребительской кибербезопасности, которое показывает, что у каждого третьего домохозяйства потребителей в Австралии киберпреступники украли личную информацию, что приводит к растущему чувству безнадежности у потребителей, которые думают, что ничего нельзя сделать для их защиты от киберпреступности.

Отчет, который совпадает с последствиями недавнего взлома Optus в Австралии, имеет решающее значение для демонстрации отношения потребителей к цифровому доверию и является для компаний надежной проверкой взглядов и действий, предпринимаемых потребителями.

Отчет показывает, что ожидания стать жертвой киберпреступности высоки: почти каждый второй потребитель в Австралии признает, что может столкнуться с кражей личных данных, мошенничеством или мошенничеством.

К сожалению, для австралийских компаний, которые столкнулись с нарушением безопасности персональных данных своих клиентов (PII), каждый четвертый потребитель разорвал отношения с компанией.

Джо Стюарт-Раттрей, Консультативная группа по информационной безопасности ISACA, заявила, что понимание и прислушивание к мнению потребителей о цифровом доверии должны стать приоритетом и считаться частью «обычного бизнеса» для компаний сегодня.

«Мы знаем, что доверие к цифровым технологиям среди профессионалов и потребителей быстро снижается с 2019 года, поэтому недавняя атака на Optus будет иметь последствия, которые нам еще предстоит осознать в ближайшие годы», — сказал Стюарт-Рэттрей.

«Это также вызывает озабоченность в связи с эффектом домино, который это нарушение оказывает на более широкое деловое сообщество и правительство, учитывая огромные ресурсы и затраты, связанные с ликвидацией последствий такой серьезной кибератаки.

«Остается также вопрос о том, подорвет ли взлом Optus доверительные отношения в секторе телекоммуникаций и коммунальных услуг в целом или он будет сосредоточен на самой компании».

Независимо от обязательной отчетности о нарушении данных, подлежащей уведомлению, требуемой в соответствии с Законом Австралии о конфиденциальности, отчет показывает, что 32% опрошенных австралийских потребителей считают, что компании занижают информацию о нарушении, даже если это требуется, а 30% не уверены, что бизнес может безопасно защитить их PII.

Респонденты в Австралии в некоторых случаях продемонстрировали разные взгляды на своих глобальных коллег, в том числе:

54% респондентов указали, что компания, с которой они ведут бизнес, вероятно, подвергнется кибератаке в 2022 году (58% по всему миру).

34% потребителей сообщили о значительном росте киберпреступности за последние двенадцать месяцев (31% в мире).

30 % не уверены, что компания может безопасно защитить свою PII (23 % по всему миру).

45% считают, что они, вероятно, станут жертвой киберпреступности (39% в мире).

Исследование показывает, что с падением доверия потребителей значительное число австралийских потребителей (58%) будут более уверенно вести дела с компаниями, которые нанимают сертифицированных специалистов по кибербезопасности.

Кроме того, 61 % опрошенных потребителей считают, что компании должны получать независимую оценку по методам обеспечения безопасности данных, а оценки должны быть доведены до сведения общественности.

«Потенциальная потеря бизнеса и необходимость восстановления и поддержания доверия потребителей подчеркивают важность инвестиций в

надежные меры предосторожности в области кибербезопасности», — добавил Стюарт-Рэттрей. «Профессионалы в области безопасности играют решающую роль в защите личной информации клиентов, поэтому важна прозрачность, а также соблюдение необходимых законов и правил о конфиденциальности».

Глобальное исследование проводилось с участием более 3000 потребителей в Австралии, США, Великобритании и Индии…» ***(Australian companies with compromised cybersecurity at risk of losing one in four customers according to a new ISACA study // iTWire (https://itwire.com/guest-articles/guest-research/australian-companies-with-compromised-cybersecurity-at-risk-of-losing-one-in-four-customers-according-to-a-new-isaca-study.html). 14.10.2022).***

***

«Масса взломов некоторых крупнейших компаний Австралии сделала страну мишенью для подражательных атак, а нехватка навыков оставляет недоукомплектованные, перегруженные кадры специалистов по кибербезопасности неспособными остановить это, говорят эксперты по технологиям.

Когда в понедельник было раскрыто еще одно потенциальное нарушение конфиденциальных данных — атака программы-вымогателя на коммуникационную платформу для военнослужащих — эксперты по кибербезопасности связали волну громких нарушений с общим фактором: человеческим фактором.

Между австралийской телекоммуникационной компанией № 2 Optus, которая принадлежит Singapore Telecommunications Ltd (STEL.SI) и крупнейшей медицинской страховой компанией страны Medibank Private Ltd (MPL.AX), около 14 миллионов учетных записей клиентов подверглись взлому данных, что эквивалентно 56% населения - только с 22 сентября.

Утверждение о слабости рабочей силы указывает на проблему, для которой нет быстрого решения.

После закрытия границ из-за COVID-19, которое закончилось в конце 2021 года, австралийские иммиграционные чиновники говорят, что они все еще обрабатывают один миллион заявлений на получение визы от людей, желающих работать в стране, многие из которых работают в сфере технологий и кибербезопасности для работодателей, желающих заполнить вакансии за границей.

«У них недостаточно обученных людей, чтобы относиться к этому серьезно и делать то, что необходимо», — сказал Санджай Джа, главный научный сотрудник Института кибербезопасности Университета Нового Южного Уэльса.

«Иногда вы ставите галочку в электронной таблице Excel и не понимаете, что делаете, и тогда результат не будет хорошим. Вам нужны люди, которые действительно квалифицированы и должным образом обучены».

Согласно исследованию отрасли кибербезопасности, благодаря тому, что программное обеспечение для взлома стало легче приобретать в Интернете, а переход на работу из дома оставляет больше слабых мест в корпоративных сетях, количество утечек данных во всем мире утроилось за два года. На этой неделе 37 стран, в том числе Австралия, встретятся в Белом доме с целью борьбы с программами-вымогателями и другими киберпреступлениями.

Всплеск вызвал шок в корпоративной Австралии, в частности, из-за высокой видимости целей и конфиденциальности их данных, включая миллионы медицинских карт.

Эксперты говорят, что постоянный поток уведомлений о небольших нарушениях может быть результатом того, что хакеры стремятся повторить успех других…» ***(Byron Kaye, Lewis Jackson. Analysis: In Australia, a hacking frenzy spurred by an undersized cybersecurity workforce // Reuters (https://www.reuters.com/technology/australia-hacking-frenzy-spurred-by-an-undersized-cybersecurity-workforce-2022-10-31/). 31.10.2022).***

***

Інші країни

«…Эта статья направлена на изучение концепции киберпреступности, кибербезопасности, положения закона, а также законодательных усилий по осуществлению и обеспечению соблюдения киберпреступлений в Нигерии.

КАТЕГОРИИ КИБЕРПРЕСТУПЛЕНИЙ

Для надлежащего изучения этого дискурса необходимо указать на различные категории киберпреступлений, которые включают:

Киберпреступления против физических лиц; Эта категория преступлений непосредственно затрагивает лиц/физических лиц. Киберпреступления, совершенные против людей, включают в себя различные преступления, такие как преследование кого-либо с использованием компьютера, например, фишинг по электронной почте, социальная инженерия, киберпреследование и другие. Это преступление также распространяется на незаконный оборот, распространение, размещение и распространение непристойных материалов, включая порнографию и непристойное разоблачение.

Киберпреступления против собственности. Некоторые онлайн-преступления совершаются против собственности, такой как компьютер или сервер. Эти преступления включают DDIS, взлом, передачу вирусов, киберсквоттинг, компьютерный вандализм, нарушение авторских прав и нарушение прав интеллектуальной собственности.

Киберпреступления против правительства. Третья категория киберпреступлений — это преступления против правительства. Кибертерроризм является одним из видов преступлений в этой категории. Рост Интернета показал, что среда киберпространства используется отдельными лицами и группами для угроз правительству и гражданам страны.

Законы, регулирующие кибербезопасность, сильно различаются от юрисдикции к юрисдикции и от одной страны к другой. Таким образом, уместно, чтобы граждане были осведомлены о законах о кибербезопасности в своих конкретных странах, чтобы обеспечить полное информирование о преступлениях, связанных с кибербезопасностью. В зависимости от преступления, может быть штраф или, возможно, тюремное заключение в качестве наказания.

В Нигерии основным законодательным актом, касающимся предотвращения киберпреступлений, является Закон о киберпреступности (запрещение и предотвращение) 2015 года. Закон обеспечивает эффективную и всеобъемлющую правовую, нормативную и институциональную основу для запрета, предотвращения, обнаружения, судебного преследования и наказания за киберпреступления в Нигерия. Кроме того, в нем содержатся положения, обеспечивающие защиту критической национальной информационной инфраструктуры и способствующие кибербезопасности.

В последующих параграфах будут проанализированы конкретные положения Закона о киберпреступности (запрещение и предотвращение), которые касаются различных категорий киберпреступлений.

ПОЛОЖЕНИЕ ЗАКОНА О КИБЕРПРЕСТУПЛЕНИЯХ В ОТНОШЕНИИ КИБЕРБУЛЛИНГА И КИБЕРСТАЛКИНГА

Киберзапугивание и киберпреследование являются наиболее распространенными формами киберпреступлений против физических лиц. Закон о киберпреступности (запрещение и предотвращение) определяет киберпреследование как преднамеренное действие, при котором преступник передает или вызывает передачу сообщений, которые являются крайне оскорбительными или непристойными (включая порнографическое содержание) через компьютерную систему с намерением запугать получателя и вызвать запугивание, враждебность, ненависть или ненужное беспокойство по отношению к получателю.

В Законе, в частности, говорится, что правонарушитель совершает преступление в соответствии с Законом и подлежит наказанию в виде штрафа в размере не более 7 000 000,00 новозеландских долларов или лишения свободы на срок не более 3 лет, либо и того, и другого.

В соответствии с положениями настоящего Закона любое лицо, которое запугивает, угрожает или преследует другое лицо путем преднамеренной передачи через компьютерную систему любой информации, содержащей любую угрозу похищения человека или любое обращение с причинением вреда человеку, или любое требование или просьбу о выкупе за освобождение любого похищенного лица, вымогать деньги у лица, фирмы, ассоциации или корпорации, и такое общение вызывает у такого другого лица страх перед смертью, насилием или телесными повреждениями виновен в правонарушении и подлежит наказанию в виде 10-летнего срока. лет и/или минимум 25 000 000 N.

ПОЛОЖЕНИЕ ЗАКОНА О КИБЕРПРЕСТУПЛЕНИЯХ 2015 ГОДА В ОТНОШЕНИИ КИБЕРСКВОТИНГА

Проще говоря, киберсквоттинг — это несанкционированная регистрация и использование доменных имен в Интернете, которые идентичны или похожи на существующие товарные знаки, знаки обслуживания, названия компаний или личные имена. Из-за дешевизны доменных имен киберскваттеры обычно покупают несколько доменных имен с намерением продать их владельцам бизнеса, тем самым получая от этого огромную прибыль.

При решении проблемы киберсквоттинга Закон о киберпреступности (запрещение и предотвращение) предусматривает, что любой, кто умышленно

использует или использует имя, фирменное наименование, товарный знак, доменное имя или другое слово или фразу, зарегистрированную, принадлежащую или используемую любым лицом, юридическое лицо или принадлежащее федеральному правительству, правительству штата или местному правительству в Нигерии, в Интернете или любой другой компьютерной сети, без полномочий или права и с целью вмешательства в их использование владельцем, владельцем регистрации или законным предыдущим пользователем, совершает правонарушения и подлежит наказанию в случае осуждения в виде лишения свободы на срок не более 2 лет или штрафа в размере не более 5 000 000,00 новозеландских долларов, либо штрафа и тюремного заключения.

ПОЛОЖЕНИЕ ЗАКОНА О КИБЕРПРЕСТУПЛЕНИЯХ 2015 ГОДА В ОТНОШЕНИИ КИБЕРТЕРРОРИЗМА

Киберпреступность проявляется в терроризме, когда отдельное лицо или группа лиц незаконно нападают и/или угрожают нападением на правительство посредством использования компьютеров, сетей и хранящейся в них информации с намерением запугать или принудить правительство или его народ в продвижении политических интересов. или социальные цели, или облегчение взлома правительственного или военного веб-сайта. Например, до взрыва 1 октября 2010 года в Абудже MEND использовала Интернет, чтобы сообщить о своей уловке службам безопасности. Лицо, утверждающее, что оно симпатизирует группе «Боко Харам», получило доступ и разместило в Интернете профили более пятидесяти бывших и действующих сотрудников Службы государственной безопасности (СГБ), включая кодовый номер, дату назначения, страну происхождения, банковский счет. среди других.

Хотя аналогичные положения содержатся в Законе о терроризме (предупреждении), Закон о киберпреступности (запрещение и предотвращение) в равной степени предусматривает, что любое лицо, которое получает доступ или обеспечивает доступ к любой компьютерной системе или сети в целях терроризма, совершает преступление и несет ответственность. по приговору к пожизненному заключению.

ДРУГИЕ ЗАМЕЧАТЕЛЬНЫЕ ПОЛОЖЕНИЯ ЗАКОНА О КИБЕРПРЕСТУПЛЕНИЯХ (ЗАПРЕТ И ПРЕДОТВРАЩЕНИЕ) 2015 ГОДА

Следует отметить, что положения Закона не ограничиваются тем, что было рассмотрено выше. Закон, в частности, предусматривает следующее;

Преступления против критической национальной информационной инфраструктуры

Взлом компьютерных систем и изменение данных

Несанкционированный доступ к защищаемым системам

Незаконная регистрация Интернет-кафе или использование незарегистрированного Интернет-кафе

Системное вмешательство

Перехват электронных сообщений, электронной почты, электронных денежных переводов

Вмешательство в критическую инфраструктуру

Умышленное неправильное направление электронных сообщений

Незаконные перехваты

Компьютерная подделка

Мошенничество, связанное с компьютером

Кража электронных устройств

Несанкционированное изменение компьютерных систем, сетевых данных и вмешательства в систему

Публикация фальшивых цифровых подписей и сертификатов

Кибертерроризм

Исключения для публикации финансовыми учреждениями и разрешенные варианты

Мошенническая выдача электронных инструкций

Фальсификация исходных компьютерных документов

Кража личных данных и выдача себя за другое лицо

Детская порнография и связанные с ней правонарушения

Киберпреследование

Киберсквоттинг

Расистские и ксенофобские преступления

Покушение, заговор, пособничество и подстрекательство

Импорт и производство электронных инструментов

Нарушение конфиденциальности и неприкосновенности частной жизни

Манипуляции с банкоматами/POS-терминалами

Фишинг, спам, распространение компьютерных вирусов

Мошенничество с электронными картами

Использование мошеннического устройства или подключенных электронных писем и веб-сайтов

ВЫВОД

Киберпреступность в Нигерии растет в основном из-за неэффективности и несоблюдения законов, направленных на борьбу с ними. Хотя Закон о киберпреступлениях, Закон о терроризме, Уголовный кодекс, Уголовные законы штатов и т.д. содержат положения, направленные на борьбу с киберпреступлениями и кибербезопасность, отсутствие надлежащего и четкого правоприменительного механизма привело к всплеску преступной деятельности в киберпространстве. Однако считается, что при наличии надлежащего механизма реализации и обеспечения соблюдения пробелы в законах о киберпреступлениях и кибербезопасности будут устранены, по крайней мере, в разумной степени. Это привело к резкому сокращению киберпреступлений». ***(AN EXAMINATION OF CYBER CRIMES AND CYBERSECURITY UNDER THE NIGERIAN LAW // The Trusted Advisors (https://trustedadvisorslaw.com/an-examination-of-cyber-crimes-and-cybersecurity-under-the-nigerian-law/). 04.10.2022).***

***

«Правительство Малайзии объявило об увеличении ассигнований на кибербезопасность и связь в годовом бюджете. Правительство также объявило об инициативах по развитию ESG среди организаций в стране.

Хотя многие считали, что бюджет задаст темпы развития экономики Малайзии в 2023 году, все еще есть те, кто считает, что на развитие технологий можно было бы выделить больше средств. Что касается подключения, в общей сложности 700 миллионов ринггитов было выделено для расширения покрытия сети в 47 промышленных зонах и 3700 школах, а 1,3 миллиарда ринггитов будут инвестированы в продолжение развертывания 5G в стране в рамках программы JENDELA.

Венг Ю Вонг, основатель и управляющий директор Open DC, пояснил, что 1,3 миллиарда ринггитов, выделенные на инфраструктуру Digital Nasional Berhad, будут потрачены на расширение покрытия 5G, чтобы охватить 70% густонаселенных районов, что позволит телекоммуникационным компаниям предоставлять высокоскоростной беспроводной доступ в Интернет для массы.

«По мере расширения покрытия 5G будет охвачено больше промышленных зон, что позволит развернуть IR4.0 по каналам 5G с малой задержкой. При этом расширение покрытия 5G также поможет улучшить сектор автоматизации, выведя на совершенно новый уровень скорость передачи данных, надежность, количество подключенных устройств и, что, возможно, самое главное, более низкую задержку», — заявил Вонг.

Правительство также увеличит гарантию финансирования схемы финансирования зеленых технологий (GTFS) до 3 млрд ринггитов до 2025 года, особенно для секторов электромобилей с гарантированным лимитом до 60%. Учитывая глобальный интерес к развертыванию центров обработки данных, работающих на экологически чистой энергии, Вонг надеется, что будет также выделен бюджет для стимулирования центров обработки данных к переходу на экологически чистые возобновляемые источники энергии.

Увеличение бюджета на усиление кибербезопасности

Что касается кибербезопасности, правительство выделило более 73 миллионов ринггитов на повышение уровня кибербезопасности Малайзии, особенно в области мониторинга угроз, обнаружения и отчетности, а также на развитие национального потенциала киберкриминалистики. Правительство также создаст Национальный центр реагирования на мошенничество, который стратегически усилит неустанные усилия страны по борьбе с киберпреступностью.

Согласно заявлению IDC, необходимы постоянные инвестиции и наращивание потенциала в области кибербезопасности, чтобы преобразование было безопасным, устойчивым и надежным. Кроме того, развивая свои собственные возможности безопасности, Малайзия также решает проблемы цифрового суверенитета, позволяя ей лучше контролировать свою цифровую инфраструктуру, активы и данные.

Джеймс Сивалингам, старший программный менеджер IDC Malaysia, прокомментировал: «Малайзия находится на поворотном этапе своего перехода к цифровым технологиям, когда предприятия и учреждения государственного сектора в стране переходят от эпохи цифровой трансформации к организациям, ориентированным на цифровые технологии. Запланированная модернизация национальной коммуникационной инфраструктуры и инициативы по расширению возможностей предприятий по внедрению цифровых технологий и автоматизации подчеркивают намерение Малайзии еще больше ускорить инициативы по

цифровизации, чтобы стать экономикой, ориентированной на цифровые технологии».

Создание Национального центра реагирования на мошенничество будет осуществляться в сотрудничестве с Королевской полицией Малайзии (PDRM), Bank Negara Malaysia (BNM), Малайзийской комиссией по связи и мультимедиа (MCMC), Национальным центром по борьбе с финансовыми преступлениями (NFCC) и финансовые институты.

«Это имеет решающее значение, поскольку централизация различных ведущих национальных агентств в рамках единого подразделения стратегически усилит неустанные усилия нашей страны по борьбе с киберпреступностью. Создание центра, безусловно, хорошо сочетается с предлагаемым выделением 73 миллионов ринггитов компании CyberSecurity Malaysia (CSM) для повышения устойчивости страны к кибербезопасности за счет улучшения возможностей мониторинга, обнаружения и отчетности о киберпреступлениях», — отметил Го Чи Хо, управляющий директор Trend Micro. Малайзия и страны зарождения.

Сук Хуа Лим, региональный менеджер Palo Alto Networks, Малайзия, также поделилась своим мнением, заявив, что более важно уделять внимание основным принципам, включая увеличение инвестиций в инфраструктуру защиты от кибербезопасности и раннее обнаружение. Это ключ к успеху развёртывания 5G.

Развитие цифровой экономики

Между тем, PIKOM, Национальная технологическая ассоциация Малайзии, благодарит правительство за представление бюджета, в который включены усилия по развитию талантов, росту предпринимательства и укреплению цифрового пространства.

«Чтобы технологическая отрасль стремилась стать движущей силой цифрового роста, абсолютно необходимо обеспечить, чтобы рабочая сила была способна соответствовать отраслевым навыкам и меняющимся требованиям к работе. Выделение 750 миллионов ринггитов на повышение квалификации до 800 000 талантов, мы можем ожидать, что упор на учебные курсы, связанные с технологиями, поможет не только талантам в технологической отрасли, но и во всех отраслях быть готовыми к будущему», — сказал председатель ПИКОМ д-р Шон Сих.

Интересно, что ПИКОМ ожидал большего внимания к долгосрочным экономическим стратегиям, чтобы подготовить страну к цифровой трансформации для обеспечения устойчивого и справедливого экономического роста. Бюджетные ассигнования на электронную коммерцию и кибербезопасность могли бы быть более значительными, а финансирование цифровой трансформации стало бы доступным для более широкого сегмента бизнеса.

«Хотя мы чувствуем, что определенное внимание уделяется МСП и занятости, также необходимо дополнить их правильной инфраструктурой, чтобы предприятия могли работать как можно более комплексно, оснащены готовыми к будущему талантами и обеспечивали сквозные продажи и услуги на рынок. Мы чувствуем, что где-то между ними есть разрыв, и мы надеемся, что его удастся устранить, поскольку в следующем году мы столкнемся с новыми проблемами, связанными с деловым и экономическим климатом», — заключил д-р Сих. ***(Aaron Raj. Increased allocations***

for cybersecurity and connectivity in Malaysia's Budget 2023, but is it enough? // Tech Wire Asia (https://techwireasia.com/2022/10/increased-allocations-for-cybersecurity-and-connectivity-in-malaysias-budget-2023-but-is-it-enough/). 10.10.2022).

***

«Служба электронной безопасности Азербайджана работает над повышением кадрового потенциала в сфере кибербезопасности…

Служба регулярно анализирует общую ситуацию с кибербезопасностью в стране, проводит мониторинг информационных ресурсов и систем, расследует обращения граждан и частных организаций и оказывает им соответствующую поддержку.

Кроме того, служба информирует об актуальных киберугрозах и обучает граждан, частные и другие организации борьбе с ними.

«Достигнута договоренность с Ассоциацией индустрии информационно-коммуникационных технологий о совместном сотрудничестве в сфере кибербезопасности», — сообщает служба.

Примечательно, что Азербайджан постоянно принимает меры по предотвращению киберугроз и угроз, связанных с информационной безопасностью. В 2021 году Азербайджан занял 40-е место среди 194 стран в Глобальном индексе кибербезопасности.

Азербайджан разработал стратегию кибербезопасности, которая охватывает период с 2019 по 2022 год. Стратегия была разработана исходя из необходимости повышения уровня национальной кибербезопасности в Азербайджане и снижения угроз для информационных систем. Планируется принять новую стратегию развития сектора кибербезопасности Азербайджана с 2022 по 2027 год.

Сектор кибербезопасности включен в стратегию развития Азербайджана до 2030 года». ***(Ayya Lmahamad. Azerbaijan working to improve human resources capacity in cybersecurity sector // Azernews (https://www.azernews.az/business/200779.html). 14.10.2022).***

***

«В ответ на письмо президента Пакистана д-ра Арифа Алви премьер-министру канцелярия премьер-министра поручила Министерству информационных технологий и телекоммуникаций создать комитет экспертов высокого уровня для анализа «киберугроз и вызовов» государственным учреждениям.

Согласно пресс-релизу палаты представителей, комитет, который возглавит федеральный министр информационных технологий и телекоммуникаций, представит свои рекомендации в канцелярию премьер-министра для дальнейшего рассмотрения этого вопроса.

В своем письме президент отметил, что это сообщение было продолжением его постоянных обращений к лицам, формирующим общественное мнение, лицам, принимающим решения, политикам и стратегам в Пакистане, о том, что «кибермощь», представляющая собой эффективное развертывание

кибервозможностей государством для достижения его национальные цели», была важной областью, в которой Пакистану необходимо было усердно работать и стать важным игроком.

Президент подчеркнул, что для Пакистана важно обдумать, как развивать и использовать свою политику, приняв многофакторный целостный национальный подход к использованию кибермощи с целью уменьшения национальной поверхности атак.

Он сказал, что также важно достичь эффективных возможностей реагирования и защиты от любых возможных вторжений, способных парализовать все учреждения, коммунальные службы, оборону, бизнес, цифровую цепочку поставок, финансы, государственные услуги, а также контроль информации и связь.

Раскрывая тему, президент определил восемь стратегических областей, которые необходимо серьезно обсудить как национальную проблему для защиты страны от возможных киберугроз, в том числе: укрепление и совершенствование национальной киберзащиты; контроль и манипулирование информационной средой для распространения точки зрения страны в мире и удаление экстремистских материалов из социальных сетей; сбор внешней разведывательной информации по вопросам национальной безопасности; использование национальных кибер- и коммерческих технологий; уничтожение или вывод из строя инфраструктуры противника в случае атаки; определение международных и национальных кибернорм и технических стандартов; понимание движения богатства в кибермире, включая криптовалюты и утечки данных, а также наблюдение и мониторинг внутренних групп (преступных организаций,

Комитет представит свои рекомендации для дальнейшего рассмотрения этого вопроса в ближайшее время.

В дополнение к письму, адресованному премьер-министру, президент также направил отчет в соответствующие учреждения, чтобы обеспечить основу для целостной разработки убедительной стратегии кибермощи и развития необходимых человеческих ресурсов для обеспечения более светлого будущего страны». ***(On President's letter, PMO sets up committee to analyze cyber threats // Pakistan Today (https://www.pakistantoday.com.pk/2022/10/20/on-presidents-letter-pmo-sets-up-committee-to-analyze-cyber-threats/). 20.10.2022).***

***

«В октябре 2022 года на Филиппинах стартовал Месяц кибербезопасности на фоне национальной обеспокоенности по поводу роста числа кибератак, киберпреступлений и других проблем, связанных с утечкой данных клиентов. Осведомленность об этих кибератаках и защита от них доступны многим, но, несмотря на это, риски кибератак на Филиппинах по-прежнему высоки — с учетом этого клиентам необходимо проявлять особую бдительность при доступе к финансовым услугам в Интернете.

В ответ на эти новые тенденции и проблемы правительство Филиппин и, в частности, Департамент информационных и коммуникационных технологий обсудили планы по обеспечению более эффективных методов защиты данных, которые представили Национальный план кибербезопасности до 2022 года. Этот

план направлен на реализацию и обеспечение соблюдения механизмов для создания общества, образованного в области кибербезопасности и устойчивого к киберугрозам, безопасных инфраструктур и сетей и эффективной координации с правоохранительными органами в случае нарушения.

Недавно подписанный закон о регистрации SIM-карт направлен на требование регистрации модулей идентификации абонента (SIM-карт) для электронных устройств. При этом он будет способствовать привлечению к ответственности и предоставит правоохранительным органам механизмы для раскрытия преступлений, совершенных анонимно.

Эти меры становятся все более актуальными из-за широко распространенных проблем с кибербезопасностью на Филиппинах. Распространение текстовых спам-сообщений, содержащих мошенничество, например, было самой безудержной проблемой для миллионов филиппинцев в последние месяцы. Многие пользователи сообщают, что анонимные номера получают их имена и номера мобильных телефонов и получают сообщения с мошенническими ссылками с целью получения финансовой выгоды.

По словам Эрла Меливо, исполняющего обязанности директора WorldRemit в Азиатско-Тихоокеанском регионе, защита онлайн-аккаунтов и выбор безопасных и надежных брендов для взаимодействия — это только начало обеспечения вашей безопасности в Интернете.

В современном обществе сбор личной информации необходим для проведения финансовых транзакций, но клиенты должны осознавать, кому они предоставляют эти данные.

«Остановите, проверьте и отклоните каждое подозрительное сообщение. Поскольку мошенничество и мошенничество продолжают расти, все филиппинцы должны сохранять бдительность и усердие», — сказал Меливо.

В то время как цифровые денежные переводы считаются сектором с высоким риском финансовых преступлений, регулируемые организации, такие как WorldRemit, сохраняют высокую приверженность кибербезопасности, поскольку они часто работают рука об руку с регулирующими органами и банками-партнерами по всему миру. Это воплощено в конкретных процессах, в которых заложена культура соблюдения.

«У нас есть опытная команда по соблюдению требований, которая понимает и выявляет риски финансовых преступлений. Кроме того, наше давнее членство в FinTech Financial Crime Exchange также помогло платформе регулярно пересматривать свои меры безопасности и обеспечивать защиту пользовательских транзакций от любых внешних угроз», — сказал Меливо». ***(Steps towards stronger cybersecurity in the Philippines // Manila Bulletin The Nation's Leading Newspaper (https://mb.com.ph/2022/10/23/steps-towards-stronger-cybersecurity-in-the-philippines/). 23.10.2022).***

***

«Правительство Вьетнама издало долгожданный Указ № 53/2022/ND-CP (Указ 53), детализирующий несколько статей Закона о кибербезопасности 2018 года.

Постановление № 53 было издано 15 августа и вступило в силу с 1 октября 2022 года.

Какие данные должны храниться во Вьетнаме?

Вкратце, в соответствии с решением, изданным министром Министерства общественной безопасности (MoPS) в отношении иностранных предприятий, во Вьетнаме должны храниться следующие данные (регламентированные данные):

Данные о личной информации пользователей услуг во Вьетнаме (т.е. данные в виде символов, букв, цифр, изображений, звуков и т.п., которые могут использоваться для идентификации человека)

Данные, генерируемые пользователями услуг во Вьетнаме (т. е . данные в виде символов, букв, цифр, изображений, звуков и т. п., описывающие процесс участия, эксплуатации и использования киберпространства пользователями услуг, а также информация об используемом сетевом оборудовании и услугах). для подключения к киберпространству на территории Вьетнама), включая имя учетной записи, время использования услуги, информацию о кредитной карте, адрес электронной почты, сетевой (IP) адрес последнего входа и выхода, зарегистрированный номер телефона, связанный с учетной записью или данными и

Данные об отношениях пользователей услуг во Вьетнаме (т.е. данные в виде символов, букв, цифр, изображений, звуков и т.п., описывающие, идентифицирующие отношения пользователей услуг с другими в киберпространстве), включая списки друзей и списки групп с которыми пользователи службы подключаются или взаимодействуют.

Кто должен хранить данные во Вьетнаме?

Статья 26.3 Закона о кибербезопасности дает широкое толкование предприятий, на которые распространяется требование о хранении данных, что вызывает сомнения в его применимости.

В частности, отечественные и иностранные предприятия, предоставляющие услуги в (i) телекоммуникационных сетях; (ii) Интернет; и/или (iii) дополнительные услуги в киберпространстве во Вьетнаме, которые осуществляют деятельность по сбору, использованию, анализу и обработке данных «пользователей услуг во Вьетнаме» (определяемых как организации и лица, использующие киберпространство на территории Вьетнама), должны хранить Регулируемые данные во Вьетнаме.

Хотя дополнительных указаний относительно конкретных услуг, требующих хранения данных во Вьетнаме отечественными предприятиями, нет, Постановление 53 перечисляет следующие конкретные услуги во Вьетнаме (Применимые услуги), требующие хранения данных иностранными поставщиками услуг во Вьетнаме:

- Телекоммуникационные услуги
- Хранение и обмен данными в киберпространстве
- Предоставление национальных или международных доменных имен пользователям услуг во Вьетнаме
- Электронная коммерция
- Онлайн платеж
- Посреднические платежные услуги
- Услуги транспортного соединения через киберпространство

- Социальные сети и социальные сети
- Онлайн видеоигры и
- Услуги, которые предоставляют, управляют или управляют другой информацией в киберпространстве в форме сообщений, голосовых вызовов, видеозвонков, электронной почты, онлайн-чатов.

Однако не все иностранные предприятия, предоставляющие Применимые услуги, должны хранить свои Регулируемые данные во Вьетнаме. В связи с этим Указ 53 предусматривает дополнительные условия для инициирования требования о хранении данных во Вьетнаме (условия инициирования), в частности, следующие:

услуга, предоставляемая предприятием, используется для совершения нарушений Закона о кибербезопасности и

Департамент кибербезопасности и предотвращения и контроля преступлений в сфере высоких технологий MoPS (Департамент кибербезопасности) уведомил и запросил координацию, предотвращение, расследование и рассмотрение в письменной форме, но

заинтересованное предприятие не соблюдает, не соблюдает полностью или предотвращает, препятствует, отключает или отменяет меры по защите сетевой безопасности, осуществляемые силами, специализирующимися на защите сетевой безопасности.

Тем не менее, существует исключение из условий запуска. В частности, в случае возникновения форс-мажорных обстоятельств, когда иностранное предприятие не может выполнить требования по хранению данных, оно должно уведомить об этом Департамент кибербезопасности в течение трех рабочих дней для проверки. В течение 30 дней такое иностранное предприятие также должно решить проблему.

В какой форме должны храниться данные во Вьетнаме?

Указ 53 не содержит каких-либо конкретных требований, но позволяет соответствующим предприятиям, как отечественным, так и иностранным, выбирать форму хранения своих данных во Вьетнаме.

Как долго данные должны храниться во Вьетнаме?

Если в соответствии с Указом 53 применимые отечественные предприятия обязаны автоматически хранить Регулируемые данные во Вьетнаме, для применимых иностранных предприятий Регулируемые данные будут храниться в течение определенного периода, указанного в запросе на хранение данных от министра Минздрава, начиная с момента предприятие получает такой запрос. В любом случае минимальный срок хранения данных должен быть не менее 24 месяцев.

Отмечается, что во всех случаях хранение данных иностранными предприятиями во Вьетнаме должно быть завершено как можно скорее в течение 12 месяцев с даты выдачи министром постановления МПС об этом. Кроме того, в случае запроса Мининформации или Мининформсвязи о блокировании или удалении запрещенной информации системные журналы для расследования и устранения нарушений законодательства о сетевой безопасности должны храниться не менее 12 месяцев. Постановление 53 не указывает, когда начинается указанный

12-месячный период, но разумно предположить, что он начинается с даты получения предприятием запроса Департамента кибербезопасности.

Другие связанные требования к хранению данных, о которых должны знать предприятия

В дополнение к указанному требованию о хранении данных во Вьетнаме отечественные и иностранные предприятия должны знать следующие общие требования:

В случаях, когда предприятие не собирает, не использует, не анализирует и не обрабатывает все необходимые данные, оно должно согласовать свои действия с отделом кибербезопасности, чтобы подтвердить и приступить к хранению данных, которые в настоящее время собираются, используются, анализируются и обрабатываются.

В тех случаях, когда предприятие собирает, использует, анализирует и/или обрабатывает дополнительные необходимые данные, предприятие несет ответственность за координацию с отделом кибербезопасности для добавления в список данных, которые должны храниться во Вьетнаме.

Требования, которые должны знать иностранные предприятия при создании своих филиалов или представительств во Вьетнаме

Иностранное предприятие, предоставляющее Применимые услуги во Вьетнаме, также может получить от министра МПС просьбу об открытии филиала или представительства во Вьетнаме. Указ 53 ничего не говорит о цели этого требования. Однако представляется, что наличие филиала или представительства во Вьетнаме поможет иностранному предприятию лучше сотрудничать с местными органами власти во Вьетнаме и решать вопросы, связанные с его Регулируемыми данными, хранящимися во Вьетнаме.

Отмечается, что во всех случаях филиал или представительство иностранного предприятия во Вьетнаме должны быть созданы как можно скорее и в течение 12 месяцев с даты принятия решения Министром Минздрава с просьбой к предприятию создать свой филиал. или представительство во Вьетнаме.

Также отмечается, что иностранное предприятие обязано сохранить свой филиал или представительство во Вьетнаме в течение периода времени, начиная с даты получения запроса от министра МПС до прекращения деятельности этого предприятия или деятельности (т. е. прекращение предоставления Применимых услуг) во Вьетнаме.

Возможные санкции

Предприятия, которые не соблюдают положения Закона о кибербезопасности и Постановления № 53, в зависимости от характера и серьезности их нарушений могут столкнуться с рядом санкций…» ***(LUU Tien Ngoc, LE Tuan Anh. Vietnam: Cybersecurity regulations for data storage and setting up a branch office // DLA Piper (https://www.dlapiper.com/en/us/insights/publications/2022/10/vietnam-cybersecurity-regulations-data-storage/). 10.2022).***

***

«Загроза нових гібридних атак на Німеччину зросла після вибухів на «Північному потоці».

Водночас не йдеться про ворожу армію із солдатами й танками, яка атакує країну. Про це заявив очільник Територіального командування Бундесверу генерал-лейтенант Карстен Броєр, пише Bild.

«Є і операції впливу, з атаками на інфраструктуру й з кібератаками. Або, наприклад, польоти безпілотників-розвідників над казармами. Це як уколи, що мають посіяти невпевненість серед населення та похитнути довіру до нашої держави», – сказав Броєр.

Тим державним органам, які відповідають за безпеку ФРН, потрібно бути готовими до нових загроз, вважає генерал.

«Кожна трансформаторна станція, електростанція, трубопровід може бути атаковані або стати однією з можливих цілей», – наголосив Броєр.

Він також застеріг від недооцінки ядерних загроз з боку Росії, проте закликав «зберегти спокій і врівноваженість».

«Наш спосіб життя і цінності, все наше суспільство під загрозою», – вважає він.

Територіальне командування Бундесверу офіційно представили в Берліні 27 вересня 2022 року. У його завдання входить підготування та залучення військових для розв'язання різних завдань усередині Німеччини». ***(Німеччина може зіткнутися з гібридними атаками – генерал Бундесверу // Gazeta.ua (https://gazeta.ua/articles/world-life/_nimechchina-mozhe-zitknutisya-z-gibridnimi-atakami-general-bundesveru/1114953). 09.10.2022).***

***

«Некоторые из крупнейших аэропортов страны в понедельник подверглись кибератакам со стороны злоумышленника из Российской Федерации, подтвердил ABC News высокопоставленный чиновник, проинформировавший о ситуации.

Важно отметить, что целевые системы не занимаются управлением воздушным движением, внутренней связью авиакомпаний, координацией или транспортной безопасностью.

«Это неудобство», — сказал источник. Атаки привели к целенаправленному «отказу в публичном доступе» к общедоступным веб-доменам, которые сообщают о времени ожидания в аэропорту и перегруженности.

Атака типа «отказ в обслуживании» затронула более десятка веб-сайтов аэропортов, сообщил ABC News Джон Халтквист, глава отдела анализа разведывательных данных в компании по кибербезопасности Mandiant. Этот тип атаки существенно перегружает сайты, забивая их искусственными пользователями.

По словам Халтквиста, за атакой стоит пророссийская хакерская группа Killnet. Хотя было обнаружено, что подобные группы являются прикрытием для поддерживаемых государством субъектов, Халтквист сказал, что нет никаких

доказательств того, что российское правительство было причастно к организации этой атаки.

Впервые об атаках было сообщено около 3 часов утра по восточному времени, когда администрация порта уведомила Агентство кибербезопасности и безопасности инфраструктуры о том, что система аэропорта LaGuardia была атакована. LaGuardia была восстановлена, но впоследствии мишенью стали другие аэропорты по всей стране.

ФБР и Агентство по кибербезопасности и безопасности инфраструктуры, входящее в состав Министерства внутренней безопасности, заявили, что им известно об атаках.

Веб-сайты международного аэропорта Де-Мойна, международного аэропорта Лос-Анджелеса (LAX) и международного аэропорта Чикаго О'Хара оказались затронутыми в понедельник утром.

Позже в понедельник международный аэропорт Денвера, третий по загруженности аэропорт в стране, подвергся нападению и продолжает подвергаться нападениям, по словам представителя аэропорта.

«Как и многие другие аэропорты США, веб-сайт DEN стал мишенью», — сказал представитель ABC News. «Атаки начались сегодня около 11 часов утра и продолжаются. Злоумышленники пытаются заблокировать наш сайт, чтобы он стал недоступен для общественности».

«В настоящее время атаки не оказали существенного влияния, хотя мы внимательно следим за этими и любыми другими атаками. Мы также делимся информацией об этих атаках с TSA, CISA и другими аэропортами», — добавил представитель.

Международный аэропорт Хартсфилд-Джексон в Атланте сообщил около 10:30 утра по восточному времени, что его сайт снова запущен и работает и что «операции в аэропорту ни разу не пострадали».

«Сегодня рано утром работа сайта FlyLAX.com была частично нарушена», — говорится в заявлении LAX для ABC News. «Приостановка обслуживания была ограничена только частями общедоступного веб-сайта FlyLAX.com. Никакие внутренние системы аэропорта не были скомпрометированы, и не было никаких сбоев в работе».

LAX сообщил, что его веб-сайт снова заработал незадолго до 13:00. ET.

Группа «Killnet» активно действует с начала войны в Украине, преследуя украинских союзников и недавно присвоив себе заслуги в уничтожении правительственных веб-сайтов в США. По словам экспертов по кибербезопасности, они действуют на международном уровне и, как известно, проводят атаки по всей Европе.

Инженеры и программисты активно работают над тем, чтобы закрыть бэкдоры, позволившие провести атаки, и укрепить более важную компьютерную инфраструктуру.

Халтквист сказал, что атаки глушения, подобные той, что наблюдалась в понедельник утром, очень заметны, но в основном поверхностны и часто временны.

«Нам совершенно ясно, что ответственность взяла на себя российская кибергруппа», — заявил в понедельник сенатор от штата Нью-Йорк Чак Шумер,

продолжая связывать атаки с украинской бомбардировкой моста в Крыму в минувшие выходные. «Мы просим наши власти подтвердить, кто это сделал, а затем принять соответствующие решительные меры, чтобы русские знали, что им это не сойдет с рук. имеет право отомстить, потому что они защитили себя мостом, это возмутительно». ***(Josh Margolin, Sam Sweeney, Quinn Owen. Cyberattacks reported at US airports // ABC News Internet Ventures (https://abcnews.go.com/Technology/cyberattacks-reported-us-airports/story?id=91287965). 11.10.2022).***

***

«Через месяц после того, как Албания разорвала дипломатические отношения с Ираном после кибератаки, премьер-министр Албании прибыл в воскресенье в Израиль с трехдневным визитом, который включает встречу с представителями израильской киберзащиты.

В канцелярии премьер-министра Израиля Яира Лапида сообщили, что он и премьер-министр Албании Эди Рама обсудили общие проблемы, стоящие перед двумя странами, «с акцентом на иранскую угрозу».

Лапид сказал, что Израиль сделает все возможное, чтобы помочь в борьбе с Ираном, что он считает «национальным интересом и историческим обязательством».

Лапид опубликовал в Твиттере фотографию встречи израильской делегации с албанской стороной во главе с Рамой и сказал, что они договорились, что две страны «будут работать вместе для борьбы с киберугрозами, исходящими от Ирана».

Рама также должен был встретиться с президентом Израиля Исааком Херцогом и главой Национального киберуправления Израиля.

Албания разорвала дипломатические отношения после того, как обвинила Иран в июльской кибератаке на правительственные веб-сайты и службы Албании. Албания также обвинила Иран во второй кибератаке в сентябре на компьютерные системы полиции страны». ***(Albania, Israel Discuss Cybersecurity After Iran Attack // Voice of America (VOA) (https://www.voanews.com/a/albania-israel-discuss-cybersecurity-after-iran-attack/6802582.html). 24.10.2022).***

***

«Болгарські правоохоронці встановили особу людини, яка зранку 15 жовтня здійснила хакерську атаку на урядові сайти країни. Підозрюваний перебуває на території росії.

Про це повідомив заступник головного прокурора країни Борислав Сарафов Болгарському телеграфному агентству (БТА).

«Конкретна особа з конкретною адресою. І ця адреса — на території російської федерації», — сказав Сарафов. Він додав, що прокуратура розглядає позови про правову допомогу у зв'язку з розслідуванням.

За даними болгарських правоохоронців, державні сайти стали об'єктом хакерської атаки з російського міста Магнітогорськ.

Зараз справою займаються Державне агентство «Національна безпека», Головне управління «Боротьби з організованою злочинністю», а також спеціально створений відділ «Кіберзлочини» Національної слідчої служби…». ***(Маркіян***

Климковецький. Прокуратура Болгарії встановила особу хакера, який атакував урядові сайти. Він перебуває в росії // Громадське телебачення (https://hromadske.ua/posts/prokuratura-bolgariyi-vstanovila-osobu-hakera-yakij-atakuvav-uryadovi-sajti-vin-perebuvaye-v-rosiyi?tag=kiberataka). 16.10.2022).

***

«В Агентстві з кібербезпеки Латвії повідомляють, що протягом жовтня в країні щоденно фіксувалися спроби кібератак проти ресурсів державних установ.

Як повідомляє Delfi, про це розповіла представниця агентства Ліга Бесере…

За її словами, протягом жовтня спроби DDoS-атак на ресурси держустанов різної інтенсивності фіксуються кожен день. У більшості випадків атаки заблокували, але іноді зловмисникам вдалось сповільнити роботу ресурсів. Припускають, що за цим можуть стояти проросійські хакери.

Втім, у цілому ситуацію у кіберпросторі Латвії в агентстві вважають стабільною «з помірним рівнем загроз»…» ***(У Латвії повідомляють про щоденні спроби DDoS-атак проти держустанов // Європейська правда (https://www.eurointegration.com.ua/news/2022/10/20/7149023/). 20.10.2022).***

***

«Мы должны изменить наш подход к кибербезопасности, чтобы лучше конкурировать в сегодняшнем оспариваемом киберпространстве», — заявила контр-адмирал Трейси Хайнс, директор отдела корпоративных сетей и кибербезопасности ВМФ. «Кибербезопасность не может быть второстепенной. Наши противники постоянно используют киберсферу, чтобы подорвать преимущества нашей страны, и по этой причине кибернетика должна быть частью процесса приобретения с самого начала».

В августе 2022 года министр военно-морского флота Карлос Дель Торо опубликовал меморандум о стратегических намерениях, содержащий рекомендации по изменению подхода военно-морского ведомства к кибербезопасности. В этом меморандуме госсекретарь Дель Торо поручил отделу перейти от мышления, основанного на соблюдении требований, к более динамичной модели, основанной на философии готовности. И, следовательно, появилась «Cyber Ready».

Cyber Ready — это постоянное состояние осведомленности о кибербезопасности, при котором право на эксплуатацию (АТО) в сети ВМФ зарабатывается и управляется каждый день. Положение Cyber Ready обеспечивает безопасную доставку информации в нужные руки в нужное время и позволяет программам с сетевыми приложениями постоянно оценивать свою безопасность на наличие угроз и уязвимостей.

«Cyber Ready — прекрасный пример того, как мы становимся лучше и реальнее, — сказал контр-адмирал Хайнс. «Стандарт определения безопасности систем больше не будет полностью основываться на регулярном заполнении статических контрольных списков. Вместо этого это будет непрерывный процесс проверки и подтверждения кибербезопасности системы».

Все, что существует сегодня в сети Департамента военно-морского флота, должно пройти АТО, что представляет собой длительный процесс, который обычно переоценивается каждые три года. Это известно как подход, основанный на соблюдении требований. Однако, поскольку киберсреда постоянно меняется, готовность к кибербезопасности приравнивается к постоянному мониторингу сетей и систем, что возлагает на владельца системы ответственность за своевременное обновление и готовность к тому, чтобы кто-то или что-то проверил систему на наличие уязвимостей…» ***(See Yourself in Cyber: Adopting the Navy's Cyber Ready Initiative // U.S. Navy Office of Information (https://www.navy.mil/Press-Office/News-Stories/Article/3204693/see-yourself-in-cyber-adopting-the-navys-cyber-ready-initiative/). 31.10.2022).***

***

«В четверг парламенты Словакии и Польши подверглись кибератакам, что привело к нарушению системы голосования в законодательном органе Словакии, заявили парламентские власти.

«Атака была разнонаправленной, в том числе изнутри Российской Федерации», — говорится в заявлении Сената Польши.

Спикер Сената Польши Томаш Гродзки заявил, что это может быть связано с голосованием Сената в среду, объявившим российское правительство «террористическим режимом».

Вице-спикер парламента Словакии Габор Грендель заявил AFP: «Вся компьютерная сеть парламента парализована».

«Около 11:00 (09:00 по Гринвичу) мы собирались голосовать, когда глава нашего административного отдела сообщил нам о кибератаке на ИТ-систему парламента», — сказал он…

По словам депутата, все компьютеры и телефонные линии вышли из строя, что сделало невозможным голосование законодателей по нескольким законопроектам.

«Мы не определили источник этой проблемы, ее решают наши технические специалисты», — заявил спикер словацкого парламента Борис Коллар». ***(Slovak, Polish Parliaments Hit by Cyberattacks // Wired Business Media (https://www.securityweek.com/slovak-polish-parliaments-hit-cyberattacks). 28.10.2022).***

***

«Согласно отчету Booz Allen Hamilton, выпущенному в среду, кибератаки, спонсируемые китайским правительством, бросают вызов интересам национальной безопасности США внутри страны и за рубежом, но аналитики угроз и главные сотрудники по информационной безопасности могут лучше подготовиться к этим киберугрозам, поняв закономерности кибероперaций Пекина.

В отчете «Тот же плащ, больше кинжала: расшифровка того, как Китайская Народная Республика использует кибератаки» проанализировано более десятка кибератак, спонсируемых Китаем за последнее десятилетие, чтобы помочь определить, как, когда и почему Китайская Народная Республика или КНР —

использует свои кибервозможности. Booz Allen Hamilton обнаружил, что КНР в основном использует кибератаки для продвижения своих так называемых «основных интересов», которые в отчете определены как «безопасность, суверенитет и развитие».

«В конечном счете, продвижение этих интересов служит поддержанию легитимности и преемственности Коммунистической партии Китая», — говорится в докладе.

Используя различные организации КНР и связанных с государством субъектов для осуществления своей кибердеятельности, китайское правительство нацеливается на страны, организации и людей, включая «американские организации критической инфраструктуры и бесчисленное количество компаний с глобальными интересами», которые угрожают его выявленным основным интересам.

В отчете говорится, что вероятность того, что эти организации подвергнутся кибератаке, поддерживаемой КНР, увеличивается, когда учитываются такие факторы, как местоположение, сектор и действия. Страны, в которых у Китая нет явного преимущества во власти, политически значимые секторы и политические организации, такие как сектор полупроводников и антикоррупционные группы, а также организации, участвующие в борьбе с онлайн-цензурой и пропагандой КНР, подвергаются повышенному риску воздействия кибератак.

Как отмечается в отчете в обзоре кибератак, спонсируемых Китаем за последнее десятилетие, основная тактика КНР включает распределенные атаки типа «отказ в обслуживании»; порча веб-сайтов и «цифровых вывесок»; нарушение систем промышленного контроля, например, в энергетическом и энергетическом секторах; и более редкое использование программ-вымогателей. Эти нападения, в частности, были направлены против продемократического движения в Гонконге, помогли укрепить претензии Китая в Южно-Китайском море и нацелились на «сопротивляющихся политиков» на Тайване.

«Усиливающееся давление Пекина на Тайвань, в частности, значительно повышает вероятность кибератак, нарушающих критически важные цепочки поставок», — говорится в отчете, отмечая, что растущая обеспокоенность по поводу китайского вторжения в страну должна помочь в управлении рисками.

Один из авторов отчета, который попросил не называть его имени, учитывая деликатный характер темы, сказал Nextgov, что для директоров по информационной безопасности и аналитиков угроз, особенно в секторах и организациях с высоким уровнем риска, важно активно укреплять свою киберзащиту.

«Организации должны начать готовиться к этой растущей угрозе уже сейчас», — добавил автор. «Важно понять эти угрозы, прежде чем они выйдут на первый план».

В отчете рекомендуется, чтобы директора по информационной безопасности использовали уроки, извлеченные из изученных кибератак КНР за последнее десятилетие, для усиления своего подхода к управлению рисками. Некоторые из шагов, предлагаемых в отчете, включают проведение полномасштабной проверки устойчивости своих цепочек поставок директорами по информационной безопасности; проводить военные игры на руководящем уровне «на основе наблюдаемых и вероятных форм эскалации атакующих операций КНР»; укрепить

свои возможности обмена информацией с другими организациями и федеральными агентствами; и проверяйте или проверяйте свои средства безопасности на наличие угроз.

В отчете говорится, что эти шаги имеют решающее значение для директоров по информационной безопасности для предотвращения как кибератак, так и других нарушений или вторжений, которые могут быть использованы для продвижения интересов Китая или демонстрации его кибервозможностей.

Как отмечается в отчете, КНР «внедрилась в американских операторов газопроводов в ответ на стратегическую переориентацию США на Индо-Тихоокеанский регион» в 2011 и 2012 гг., но никогда не было никаких указаний на то, что эти нарушения использовались для нарушения работы газопровода. операции. Однако автор отметил, что это был сигнал КНР, что он может сделать это, если захочет, и это еще один признак того, что организациям следует быть более бдительными в своих усилиях по киберзащите.

«Если из этого и можно извлечь какой-то урок, так это то, что Китай показал, что киберпространство и кибербезопасность можно рассматривать в гораздо более широком смысле, как информационную безопасность», — сказал автор. «Да, на очень тактическом уровне важно защитить сети и убедиться, что сети не выходят из строя, но иногда это не размер сбоя, а сообщение, которое отправляется сбоем».

Доклад Буза Аллена Гамильтона вышел в тот же день, когда была опубликована стратегия национальной безопасности президента Джо Байдена, в которой частично подчеркивалась необходимость превзойти Китай и противостоять его кампаниям влияния по всему миру.

«Более боеспособные конкуренты и новые стратегии угрожающего поведения ниже и выше традиционного порога конфликта означают, что мы не можем позволить себе полагаться исключительно на обычные силы и ядерное сдерживание», — частично говорится в стратегии национальной безопасности администрации Байдена. «Наша оборонная стратегия должна поддерживать и укреплять сдерживание, а КНР — наша основная задача». ***(Edward Graham. A new report from Booz Allen Hamilton analyzed more than a dozen Chinese-sponsored cyberattacks over the past decade // Nextgov (https://www.nextgov.com/cybersecurity/2022/10/lessons-chinas-cyberattack-strategy-can-help-cisos-better-manage-threats-report-says/378365/). 13.10.2022).***

***

«Опрос, проведенный фирмой Venafi, занимающейся кибербезопасностью, показал, что российско-украинский конфликт оказывает существенное влияние на то, как компании рассматривают свою защиту и защищают себя от интернет-угроз. 64% респондентов считают, что их организации либо стали мишенью, либо пострадали от атак со стороны государства, и примерно столько же говорят, что вторжение в Украину и последующая деятельность напрямую заставили их изменить свою стратегию кибербезопасности.

Кроме того, 77% теперь считают, что в будущем будет постоянное состояние кибервойны, но большинство все еще не уверены, что они смогут обнаружить и

идентифицировать продвинутый национальный государственный шпионаж, если они станут мишенью.

Компании все больше осознают, что находятся под прицелом атак со стороны государства

Опрос Venafi был проведен в июле и в нем приняли участие 1100 лиц, принимающих решения в области безопасности (SDM) из компаний, расположенных в США, Австралии и ряде европейских стран.

Более половины респондентов не только считают, что они уже подвергались атакам со стороны государства, но и внесли изменения в свои методы кибербезопасности из-за российско-украинского конфликта. Хотя это произошло после того периода, когда был проведен опрос, в последнее время произошла эскалация атак на ключевых членов НАТО, которые оказывают помощь Украине, особенно в США, поскольку веб-сайты аэропортов по всей стране были недавно отключены распределенным кампания отказа в обслуживании (DDoS).

Как показывает этот пример, организациям теперь приходится беспокоиться не только о национальных хакерских командах, но и о самопровозглашенных «хактивистах», которые могут принять решение действовать в частном порядке от имени своей страны. 68% респондентов говорят, что у них были беседы с советом директоров и высшим руководством о каком-то аспекте российско-украинского конфликта и о том, как это может привести к нападениям на компанию.

Опрос также показал, что организации не считают, что это закончится, когда российско-украинский конфликт в конце концов будет разрешен. 82% говорят, что считают геополитику и кибербезопасность неразрывно связанными, а 77% считают, что им нужно готовиться к «вечной» кибервойне. Хотя они рассматривают атаки национальных государств как вездесущую угрозу, 63% говорят, что сомневаются, что смогут выявить или остановить эти атаки, если они станут мишенью.

Одно интересное замечание заключается в том, что, несмотря на эти результаты, 64% респондентов по-прежнему говорят, что они рассматривают физическую войну как большую проблему для своей конкретной страны, чем атаки национальных государств с помощью кибервойны, даже несмотря на то, что опрос был ограничен западными странами. которые в настоящее время не вовлечены в крупные конфликты.

Тейлор Эллис, аналитик клиентских угроз Horizon3.ai, считает, что многие организации до сих пор недостаточно точно оценивают уровень своего риска в этой области: «Поскольку вся эта дипломатия пошла не так, неудивительно, что войны ведутся… но они ведутся преимущественно в киберпространстве. Многие правы, полагая, что кибербезопасность и геополитика напрямую связаны».

«Несмотря на очевидную программу национального государства по нацеливанию на военные и правительственные цели, такие противники стали смелее и менее пренебрежительно атаковать частный бизнес, независимо от приверженности этой компании обслуживанию потребителей на международном уровне. Поэтому каждое частное учреждение должно привести свою политику в соответствие с принципом «безопасность прежде всего». Хотя в большинстве компаний есть ИТ-отделы, многим по-прежнему не хватает хорошо обученной и опытной команды по кибербезопасности в своей организации. Необходимо внести

такие изменения для более безопасной сети и структуры безопасности, а также набрать людей, которые могут эффективно выполнять работу (а не только команду из одного человека)», — отметил Эллис.

Конфликт между Россией и Украиной, возможно, навсегда изменил ландшафт кибербезопасности

Как отмечает Венафи, в последнее время Россия сосредоточила свое внимание на атаках целей в Украине с помощью вредоносных программ-«очистителей», уделяя особое внимание нанесению ущерба государственным учреждениям, а также, возможно, критически важной инфраструктуре в рамках подготовки к вероятному возобновлению военного наступления в зимние месяцы. Хотя до сих пор считается, что атаки на союзников по НАТО — дело рук российских преступных группировок и «хактивистов», существует множество предыдущих примеров того, как российское вредоносное ПО, предназначенное для Украины, убегало из зоны боевых действий и заражало другие компании по всему миру. Один из таких примеров произошел в первые недели российско-украинского конфликта, когда немецкая энергетическая компания столкнулась с вредоносным ПО, специально предназначенным для целей в Украине.

Венафи отмечает, что в то время как российско-украинский конфликт находится в центре внимания в настоящее время, китайские APT-группировки также активизировали свои шпионские кампании и имеют опыт нападения на иностранные компании с целью кражи конфиденциальной информации. А спонсируемые государством хакеры Северной Кореи используют свои передовые навыки для кражи денег из любых подходящих источников, о чем свидетельствует их неистовство в мире децентрализованных финансов в этом году.

Компании правы, сомневаясь в своей способности обнаруживать и отражать атаки национальных государств, поскольку правительства, которые наиболее активны в шпионаже, также являются основными в мире потребителями уязвимостей «нулевого дня», которые продаются на черном рынке.

Раджив Пимпласкар, генеральный директор Dispersive, отмечает, что они также обладают ресурсами, которых нет ни у одного частного субъекта в мире: «Субъекты национального государства имеют дополнительное преимущество в виде сложных наборов инструментов в сочетании с хорошо скоординированными человеческими и вычислительными ресурсами, которые могут сделать их особенно смертоносными. Депериметризация корпоративной сети за последнее десятилетие в сочетании с работой из дома во время пандемии COVID-19 создали идеальную угрозу потери контроля над инфраструктурой со стороны ИТ и расширили поверхность атаки, включив в нее Интернет. Типичные решения VPN или ZTNA останавливаются на сетевом уровне и не могут противостоять целенаправленным атакам со стороны субъектов национального государства, которые могут проникнуть в стек протоколов с помощью сложных атак.

Для организаций также важно не игнорировать потенциальную угрозу атак со стороны национальных государств просто из-за отсутствия информации, которая, по их мнению, могла бы заинтересовать эти страны. в качестве точки входа для атаки на цепочку поставок, которая должна в конечном итоге открыть дверь для более ценной цели.

Хлоя Мессдаги, руководитель отдела воздействия Cybrary, подробно рассказывается о том, как работает этот подход, и о том, на что хакеры готовы прыгать от системы к системе, чтобы добраться до точки интереса: «Группы безопасности должны помнить, что у них есть государственные заказчики или пользователи, у которых есть государственные заказчики., и поэтому они и их клиенты будут представлять интерес для злоумышленников. Злоумышленники работают, ища промежуточные лазейки, чтобы добраться до цели. Они будут двигаться от E к D, от C к B, чтобы добраться до A, их фактической цели — вдеть нить в иглу и пройти через более слабые точки входа. Например, через школы они передаются местному правительству, затем штату, а затем федеральному правительству, потому что в настоящее время мы все связаны между собой. Глобальные конфликты начинаются локально. Подумайте об этом так: «Чтобы взломать глобально, начните локально». ' Субъекты угрозы ищут самую легкую и наименьшую точку уязвимости. Северная Корея преследовала влиятельных лиц в хакерском пространстве, чтобы установить их потенциальные правительственные контакты, а затем перешла к более крупным целям». ***(Scott Ikeda. Russia-Ukraine Conflict Heightens Wariness of Nation-State Attacks as 64% Of Businesses Believe They Have Been Targeted // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/russia-ukraine-conflict-heightens-wariness-of-nation-state-attacks-as-64-of-businesses-believe-they-have-been-targeted/). 21.10.2022).***

***

«Междисциплинарная группа исследователей из Университета Карлоса III в Мадриде (UC3M) создала математическую модель, которая позволяет объяснить, в зависимости от различных социально-политических переменных, некоторые передовые кибератаки, которые обычно осуществляются странами. Это первый шаг к амбициозной цели прогнозирования возникновения этих кибератак.

Кибератаки, проанализированные этими исследователями, известны как продвинутые постоянные угрозы (известные как APT). «Их сложность указывает на то, что за ними стоят [страны]», — объясняет один из авторов исследования, Лорена Гонсалес Мансано, преподаватель Лаборатории компьютерной безопасности на факультете компьютерных наук UC3M. В этом исследовании они проанализировали, существует ли связь между кибератаками и определенными стратегическими, экономическими и военными событиями.

Несмотря на некоторую атрибуцию намерений этих APT, до сих пор не существовало математической связи, которая позволяла бы моделировать эти атаки. Однако эта работа под руководством лектора Гонсалеса, опубликованная в журнале Security and Communication Networks, указывает на возможность установления этой связи.

«Модель основана на информации, опубликованной в СМИ, и других экономических показателях, объясняющих возникновение APT», — говорит другой автор исследования, лектор Хосе Мария де Фуэнтес из той же исследовательской группы UC3M. Мотивы этих кибератак очень разнообразны. «Они гораздо более изощренные, чем те, которые могут повлиять на обычных пользователей. Обычно

они нацелены на кражу интеллектуальной собственности или шпионаж», — говорит Лорена Гонсалес Мансано.

Это исследование открывает двери для будущих направлений работы, таких как «предсказание кибератак путем наблюдения за другими переменными, которые не имеют ничего общего с кибермиром», по словам де Фуэнтеса. «Например, в некоторых случаях данные об уровне экспорта (например, мобильных телефонов) полезны для определения вероятности кибератаки в той или иной стране», — добавляет лектор Гонсалес Мансано.

Эта работа носит междисциплинарный характер и объединяет «геополитические факторы (для понимания отношений между странами) с данными о кибератаках и объединяет все это с математической точки зрения», — объясняют исследователи». ***(Study finds a mathematical link between sociopolitical events and advanced cyberattacks // Science X Network (https://techxplore.com/news/2022-10-mathematical-link-sociopolitical-events-advanced.html). 27.10.2022).***

***

«Вебсайти президента Болгарії та кілька інших урядових сайтів піддалися масштабній кібератаці. Про це з посиланням на генерального прокурора Івана Гешева повідомляє «Радіо Свобода». Також про це інформують Мінцифри Болгарії і телеканали країни.

За цими даними, окрім офісу президента, DDoS-атака паралізувала сайти Міноборони, МВС, Мін'юсту та Конституційного суду. Як завжди під час DDoS-атаки, на ці вебресурси надходила надмірна кількість запитів, що сповільнює роботу сторінок або виводить їх з ладу.

Як повідомив Гешев, атака була здійснена з російського міста Магнітогорськ.

Міністерство цифрових справ Болгарії інформує, що кіберфахівці змогли припинити хакерський напад, обійшлося без значних наслідків. Відповідальність на себе взяла російська хакерська група KillNet, повідомив телеканал Dnevnik. Про атаку угруповання повідомило на своєму Telegram-каналі. Учасники KillNet називають себе прокремлівськими патріотами. Мета їхніх атак – привернути увагу та поширити дезінформацію.

Як частина Євросоюзу Болгарія захищає європейські цінності, сказав Гешев, додавши, очікується, що це матиме наслідки…» ***(Хакери з російського Магнітогорська атакували сайт президента та уряду Болгарії // Інтернет-видання «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/30456/2022-10-16-khakery-z-rosiyskogo-magnitogorska-atakuvaly-sayt-prezydenta-ta-uryadu-bolgarii/). 16.10.2022).***

***

«Особистий телефон експрем'єра Великої Британії Ліз Трасс зламали хакери, імовірно пов'язані з російськими спецслужбами, - про це в суботу, 29 жовтня, повідомило видання The Mail on Sunday з посиланням на джерела в службах безпеки. За даними британських журналістів, злом було виявлено під час літньої передвиборчої кампанії консерваторів, коли Трасс ще очолювала міністерство закордонних справ Великої Британії.

Джерела газети вважають, що кіберзлочинці могли отримати доступ до «надсекретної інформації», зокрема до деталей переговорів із главами МЗС інших країн про війну РФ проти України, а також до докладних обговорень поставок зброї Києву - зловмисники завантажили листування Трасс за останній рік.

Хакери також отримали доступ до листування Трасс із її союзником і колишнім міністром фінансів Квазі Квартенгом, що містить критичні відгуки про тодішнього прем'єр-міністра Бориса Джонсона, стверджує видання.

У британському уряді відмовилися коментувати цю публікацію, зазначивши лише, що «існують надійні системи захисту від кіберзагроз». BBC і Sky News не змогли перевірити інформацію The Mail on Sunday.

Тим часом опозиційні політики закликають провести розслідування. Опубліковані відомості порушують «украй важливі питання національної безпеки», зокрема, чому і як стався витік інформації, заявила, зокрема, Іветт Купер із Лейбористської партії. «Важливо, щоб усі ці проблеми безпеки розслідували й вирішували на найвищому рівні», - підкреслила вона». ***(Ігор Бурдига. Daily Mail: Телефон Ліз Трасс зламали російські хакери // Deutsche Welle (https://www.dw.com/uk/daily-mail-telefon-liz-trass-zlamali-rosijski-hakeri/a-63596268). 30.10.2022).***

***

Кіберзахист критичної інфраструктури

«Железнодорожная отрасль всегда уделяла большое внимание безопасности, чтобы каждая поездка была максимально безопасной и не представляла опасности для пассажиров или сотрудников.

Но железнодорожные системы претерпели значительные изменения с момента их создания, особенно за последнее десятилетие, когда связность стала важнейшим компонентом железнодорожной инфраструктуры и подвижного состава. Эта эволюция, которая сделала поезда более эффективными, комфортными и безопасными, чем когда-либо прежде, не обходится без проблем. А именно, необходимость переориентировать внимание отрасли на безопасность, особенно на кибербезопасность, наряду со стандартными методами обеспечения безопасности.

Безопасность против безопасности

Безопасность и кибербезопасность преследуют одну цель: обеспечить безопасность пассажиров и сотрудников и обеспечить движение поездов по расписанию. Но смешивать их — значит обращаться к ним недостаточно. Для железных дорог безопасность обычно относится к защите пассажиров и систем от непреднамеренного вреда — ржавый механизм, сломанный сигнальный фонарь, ошибки в системе и т. д. Кибербезопасность — это защита людей и инфраструктуры от преднамеренного вреда — злоумышленников со злым умыслом.

В отличие от механической безопасности, основанной на проверенных временем принципах, кибербезопасность никогда не останавливается на достигнутом — она всегда должна быть на шаг впереди все более изощренных хакеров. Таким образом, чтобы оставаться в кибербезопасности, железнодорожная

отрасль должна постоянно улучшать и развивать свои решения в области кибербезопасности, чтобы противостоять следующей возникающей угрозе.

Одним из критических препятствий на пути к эффективной кибербезопасности железных дорог является сложность поиска баланса между проверенными и надежными протоколами безопасности и системами кибербезопасности, которые необходимо постоянно обновлять.

Состояние кибербезопасности в условиях эксплуатации железных дорог

Недавняя классификация железных дорог как «критической инфраструктуры» ускорила внедрение стандартизированных решений кибербезопасности, ориентированных на железные дороги. Новые протоколы и другие нормативные инициативы подталкивают отрасль к еще большей кибербезопасности — такие структуры, как CENELEC TS 50701 (в значительной степени основанный на IEC 62443) и последние директивы TSA в США.

Но такая стандартизация осложняется тем фактом, что железнодорожная отрасль состоит из разнообразных участников: операторов, интеграторов, поставщиков компонентов и сторонних поставщиков, предлагающих решения на разных этапах цепочки поставок. К счастью, участники железнодорожной отрасли стремятся решить растущие проблемы кибербезопасности с помощью инноваций и разработки новых продуктов и услуг.

Но даже с учетом того, что кибербезопасность является одним из приоритетов всей железнодорожной экосистемы, мы не можем недооценивать стоящие перед нами задачи — необходимые культурные изменения, длительный жизненный цикл железнодорожной продукции и растущую сложность железнодорожных систем, и это лишь некоторые из них.

Информация о кибербезопасности от InnoTrans Berlin 2022

Кибербезопасность была в центре внимания на недавней выставке InnoTrans в Берлине, крупнейшей в мире торговой выставке, посвященной отрасли железнодорожного транспорта.

Одной из выдающихся тенденций InnoTrans 2022 стал акцент на улучшении видимости в условиях эксплуатации железных дорог. Железнодорожные операторы знают, что они не могут защитить то, чего не видят, что создает серьезную проблему для этих систем в целом.

Еще одной ключевой тенденцией является спрос на интеграционные киберрешения, которые позволяют железнодорожным операторам делать больше с меньшими затратами. Сегодня операторы знают, что им необходимо защищать свои системы, и неустанно ищут решения, которые можно целостно интегрировать в сложные экосистемы.

Ожидания основных тем в ближайшие годы

В дальнейшем широкое развертывание решений кибербезопасности для железных дорог будет происходить не только в новых проектах (новые линии), но и в существующих железнодорожных средах (модернизация или расширение существующих линий). Учитывая, что большинство железнодорожных систем состоят из устаревших компонентов, крайне важно, чтобы отрасль работала над обеспечением безопасности уже существующих сред, даже если она стремится создавать новые, более безопасные по своей сути.

Сегодня решения в области кибербезопасности, необходимые в любой отрасли или на предприятии, особенно в критической инфраструктуре, должны быть глубоко внедрены в соответствующие бизнес-функции и иметь возможность преобразовывать предупреждения о киберугрозах в конкретные эффективные действия. Например, в такой отрасли, как железная дорога, где объекты и информация постоянно перемещаются через сверхсложную систему, никогда не бывает необходимого времени простоя для остановки операций и проверки активов, требующих исправления; вместо этого проблемы должны быть отмечены, а решения найдены на лету. Соответственно, железнодорожная отрасль продолжает разрабатывать решения в области кибербезопасности для железных дорог, поскольку общие решения просто не подходят для защиты таких уникальных и сложных систем, как наши железные дороги.

Возможно, наиболее важной среди новых тенденций является распространение обмена информацией. Исследования отраслевых аналитиков о состоянии кибербезопасности железных дорог и зрелости отрасли в целом показывают, что все больше и больше операторов начинают обмениваться данными, относящимися к кибербезопасности, и учиться друг у друга. Мы также можем ожидать лучшего сбора информации от организаций железнодорожной отрасли о типах кибератак, происходящих в отрасли, и о том, насколько эффективно они реагируют и устраняются — в конце концов, плохие парни работают вместе, чтобы распространять информацию. о слабостях и уязвимостях… почему бы и хорошим парням не объединиться, чтобы быть на шаг впереди?

Такая прозрачность имеет решающее значение для достижения баланса между структурой и постоянными изменениями, необходимыми для продвижения отрасли к более безопасному и эффективному будущему.

Все на борт Киберэкспресса

Несмотря на трудности, дела в железнодорожной отрасли выглядят оптимистично.

Операторы продолжают двигаться к культуре, в большей степени ориентированной на кибербезопасность, во всей отраслевой экосистеме, стремясь к прозрачности между множеством поставщиков, операторов, интеграторов, поставщиков компонентов и т. д.

Производители и операторы железных дорог должны не только продолжать обеспечивать высокий уровень кибербезопасности, но и использовать решения, которые являются специфичными для железных дорог и соответствуют стандартам безопасности как для новых, так и для устаревших систем — как на пути, так и вне его». ***(Amir Levintal, Eddy Thesee. All Aboard the Cybersecurity Express // Simmons-Boardman Publishing Inc. (https://www.railwayage.com/cs/all-aboard-the-cybersecurity-express/). 13.10.2022).***

***

«Агентство транспортной безопасности США заявило в среду, что планирует выпустить новые требования кибербезопасности для некоторых ключевых авиационных систем после того, как несколько веб-сайтов

аэропортов США в начале этой недели подверглись явно скоординированным атакам типа «отказ в обслуживании».

Управление транспортной безопасности (TSA) заявило, что кибератаки в понедельник, предположительно организованные пророссийскими хакерами, «не нарушили работу аэропорта или доступ к информации».

TSA отметила, что ранее «обновила свои программы авиационной безопасности, требуя, чтобы операторы аэропортов и авиакомпаний назначали координатора по кибербезопасности и сообщали об инцидентах кибербезопасности, проводили оценку кибербезопасности и разрабатывали меры по исправлению положения и планы реагирования на инциденты».

TSA добавила, что планирует «в ближайшее время выпустить дополнительные требования к кибербезопасности, основанные на характеристиках, для критически важных авиационных систем».

Федеральное авиационное управление (FAA) в качестве условия предоставления грантов на терминалы аэропортов заявило в прошлом месяце в уведомлении для аэропортов, что они должны продемонстрировать усилия «по рассмотрению и устранению рисков физической и кибербезопасности, связанных с видом транспорта, типом и масштабом проекта».

FAA добавило, что «проекты, которые должным образом не рассмотрели и не рассмотрели физическую и кибербезопасность и устойчивость… должны будут сделать это до получения средств на строительство».

Счетная палата правительства в отчете за 2020 год заявила, что FAA должно полностью внедрить ключевые методы для устранения рисков кибербезопасности.

GAO отметило, что «современные самолеты оснащены сетями и системами, которые обмениваются данными с пилотами, пассажирами, бригадами технического обслуживания, другими воздушными судами и авиадиспетчерами», и, если они не защищены должным образом, «могут подвергаться риску различных потенциальных кибератак».

GAO заявило, что в 2020 году не было сообщений об успешных кибератаках на системы авионики самолетов». ***(David Shepardson. TSA Plans New Cybersecurity Requirements After Pro-Russia Airport Hacks // Skift (https://skift.com/2022/10/12/tsa-plans-new-cybersecurity-requirements-after-pro-russia-airport-hacks/). 12.10.2022).***

***

«Администрация Байдена в среду предприняла попытку защитить химический сектор страны от кибератак, что стало последней попыткой защитить критически важную национальную инфраструктуру от цифровых атак.

«План химических действий» будет основываться на «извлеченных уроках и передовом опыте ранее запущенных планов действий для электроэнергетического, трубопроводного и водного секторов для удовлетворения потребностей этого сектора», — говорится в информационном бюллетене Белого дома.

Последний 100-дневный спринт, возглавляемый Агентством кибербезопасности и безопасности инфраструктуры (CISA), будет направлен на то,

чтобы побудить компании делиться информацией об угрозах с федеральным правительством, говорится в информационном бюллетене.

Представитель CISA сообщил Axios, что другие шаги будут включать создание координационного совета, состоящего из 15 групп химической промышленности, для сбора отзывов о том, как лучше всего улучшить цифровую защиту сектора, и мотивировать компании устанавливать датчики для мониторинга кибератак.

Ранее в октябре высокопоставленный чиновник Белого дома заявил, что в ближайшие месяцы администрация планирует сосредоточиться на секторах водоснабжения, связи и здравоохранения. На прошлой неделе директор CISA Джен Истерли заявила, что ее организация сосредоточит свое внимание на цифровой безопасности сектора водоснабжения, больниц и школ K-12.

Сегодняшнее объявление было сделано в связи с тем, что CISA и Национальный институт стандартов и технологий готовы обнародовать добровольные цели по обеспечению кибербезопасности для критически важной инфраструктуры, которые определят ожидания правительства в отношении организаций частного сектора…». ***(Martin Matishak. White House announces 100-day sprint on chemical sector cybersecurity // The Record by Recorded Future (https://therecord.media/white-house-announces-100-day-sprint-on-chemical-sector-cybersecurity/). 26.10.2022).***

***

«18 октября 2022 г. Управление транспортной безопасности («TSA») издало свою Директиву безопасности 1580/82-2022-01 о мерах по снижению кибербезопасности на железных дорогах и тестировании («Директива о железных дорогах»), регулирующую работу назначенных пассажирских и грузовых железнодорожных перевозчиков, вступившую в силу 24 октября 2022 г. Директива о железных дорогах основывается на усилиях TSA по защите критической инфраструктуры от кибератак и подготовке к ним.TSA разработало эту новую железнодорожную директиву в сотрудничестве с Агентством кибербезопасности и безопасности инфраструктуры («CISA»), Министерством обороны и Федеральным управлением железных дорог Министерства транспорта. Кроме того, TSA получило информацию от железнодорожной отрасли при разработке Директивы о железных дорогах.

Директива TSA по железным дорогам следует за рядом аналогичных директив по безопасности, направленных на трубопроводы, которые были изданы в ответ на кибер-инцидент Colonial Pipeline в 2021 году. Подобно тому, как трубопроводы подвергались атакам программ-вымогателей, железные дороги подвергались кибератакам, в том числе одной в 2012 году, которая замедлила поезда на Тихоокеанском Северо-Западе. Фактически, по мере того, как железные дороги внедряли новые технологии, такие как системы позитивного управления поездами для предотвращения железнодорожных аварий, также могли появиться новые киберуязвимости.

Эти и другие атаки на критическую инфраструктуру побудили TSA издать директивы, требующие от владельцев и операторов критической инфраструктуры принять определенные меры кибербезопасности. Эта новая директива о железных

дорогах во многом аналогична третьей директиве TSA о кибербезопасности трубопроводов, за исключением того, что TSA не требует от железнодорожных перевозчиков разработки плана реагирования на инциденты кибербезопасности в соответствии с этой директивой.

Директива о железных дорогах требует, чтобы железнодорожные перевозчики, на которые распространяется действие страховки, применяли определенные меры контроля доступа, такие как:

Политики сегментации сети и элементы управления, предназначенные для предотвращения нарушения работы системы операционных технологий, если система информационных технологий скомпрометирована или наоборот,

Политики сброса секретных аутентификаторов,

Многофакторная аутентификация или компенсирующие элементы управления для компонентов или активов операционных технологий,

Политики и процедуры для управления правами доступа на основе принципов наименьших привилегий и разделения обязанностей, а также

Стандарты, ограничивающие использование общих учетных записей.

TSA также требует политик и процедур постоянного мониторинга и обнаружения, включая возможности и процедуры для:

Защита от фишинговых атак по электронной почте;

Блокировать связь с известными или подозреваемыми вредоносными IP-адресами;

Блокировать и предотвращать выполнение несанкционированного кода, в том числе макроскриптов;

Мониторинг и/или блокировка подключений от известных или подозреваемых вредоносных систем управления и контроля;

Собирать и вести журналы для анализа данных о потенциальных вторжениях и аномальном поведении в критически важных киберсистемах и других операционных и информационных системах, которые напрямую связаны с критически важными киберсистемами;

Меры по смягчению последствий или ручное управление для обеспечения изоляции промышленных систем управления, когда инцидент кибербезопасности в системе информационных технологий создает риск для безопасности и надежности системы операционных технологий; а также

Стратегия управления исправлениями, которая отдает приоритет каталогу известных эксплуатируемых уязвимостей CISA.

Кроме того, Директива о железных дорогах обязывает железнодорожных перевозчиков принять план внедрения кибербезопасности, описывающий план организации по выполнению каждого из требований Директивы. После одобрения TSA этот план будет служить руководством для проверки соответствия TSA организаций, на которые распространяется действие страховки. Железнодорожные перевозчики также обязаны подавать ежегодные оценки соответствия в TSA. Нарушители новой Директивы о железных дорогах рискуют получить гражданско-правовой денежный штраф в размере до 11 904 долларов США за нарушение, согласно Политике TSA в отношении правоприменительных санкций на 2021 год. Директива о железных дорогах также требует от железнодорожных перевозчиков

разработать программу оценки кибербезопасности для оценки эффективности плана внедрения кибербезопасности, а также для выявления и устранения уязвимостей устройств, сетей и систем…

Новая директива о железных дорогах демонстрирует систематические усилия правительства по защите критически важной инфраструктуры от кибератак. Несмотря на то, что существует неопределенность в отношении обеспечения соблюдения директив TSA (поскольку общедоступная информация о соблюдении и соблюдении требований ограничена), нарушители рискуют получить штрафные санкции, начиная от письма-предупреждения или письма с исправлением и заканчивая гражданско-правовым денежным штрафом. Однако TSA решает обеспечить соблюдение Директивы о железных дорогах, владельцам и операторам критической инфраструктуры следует помнить, поскольку новые правила кибербезопасности также могут повысить ожидаемый уровень обслуживания». ***(Jeff Johnston, Briana Falcon, Warner Scott, and Winnie Johnson. More Regulations Coming Down the Tracks: TSA Issues New Security Directive for Enhanced Railroad Cybersecurity // Vinson & Elkins LLP (https://www.velaw.com/insights/more-regulations-coming-down-the-tracks-tsa-issues-new-security-directive-for-enhanced-railroad-cybersecurity/). 31.10.2022).***

***

Кіберзахист закладів охорони здоров'я

«Сектор здравоохранения в условиях полного перехода на цифровые технологии более чем когда-либо мобилизован для противостояния волнам компьютерных атак.

Это серьезная проблема для клиник, больниц, медицинских учреждений и других организаций, обрабатывающих конфиденциальные данные, которые являются основными целями для хакеров.

Отсутствие средств, гарантирующих эффективную кибербезопасность, постоянное увеличение объема данных, генерируемых деятельностью из-за цифровой трансформации услуг, стоимость данных о здоровье, которые обмениваются на твердые доллары в даркнете и т. д. нет недостатка в причинах, объясняющих уровень подверженности игроков сферы здравоохранения киберриску.

Больницы и другие медицинские учреждения — идеальные цели для хакеров

Каждый год, каждый месяц, каждую неделю новости напоминают нам об этой истине; медицинские учреждения чрезмерно подвержены киберрискам, что особенно тревожно для одного из самых чувствительных секторов нашего общества. Таким образом, кибератака программы-вымогателя, которой подвергся госпитальный центр Sud Francilien (CHSF) в Корбей-Эссонн 21 августа 2022 года, является еще одним примером длинного списка претензий.

При этом русскоязычная группировка Lockbit, которая с тех пор взяла на себя ответственность за атаку, потребовала выкуп в размере не менее 10 млн евро в обмен на возврат данных.

Для достижения своих целей злоумышленники CHSF использовали программы-вымогатели. Это вредоносное ПО, которое позволяет хакерам удерживать данные в заложниках, шифруя их, прежде чем требовать выкуп в обмен на ключ дешифрования.

К этому шантажу часто добавляется угроза раскрытия данных, восстановленных хакерами до их шифрования, раскрытие, последствия которого могут быть драматичными с точки зрения конфиденциальности заинтересованных лиц.

Примером этого является кибератака CHSF: не сумев получить запрошенный выкуп, хакеры распространили в Интернете тысячи конфиденциальных данных, таких как отчеты о медицинском осмотре, персонализированные карты пациентов и номера телефонов социального обеспечения. Менее чем через три дня после этого раскрытия данные уже просмотрели почти 3000 человек.

Инцидент, затрагивающий CHSF, далеко не единичный случай. С июня 2020 года Институт кибермира насчитал не менее 384 кибератак программ-вымогателей, направленных на сектор здравоохранения. Этот рисунок показывает, что хакеры предпочитают этот способ действий. Это срочно.

Французское правительство также недавно объявило, что выделит 25 миллионов евро на 2021 и 2022 годы для усиления кибербезопасности медицинских учреждений. Цель этого финансирования, в частности, состоит в том, чтобы увеличить количество больниц, прошедших курс безопасности, и предоставить им «технологическую и человеческую поддержку».

Помимо этого финансирования, необходимо решить всю киберпроблему; как на уровне предупреждения, так и на уровне реагирования.

Подготовка к кибератаке: повышение осведомленности, предотвращение и прогнозирование директивы NIS II

Организация и предусмотрительность необходимы для предотвращения кибератак.

Как предвидеть кибератаку в больнице?

Таким образом, повышение осведомленности сотрудников и пользователей имеет важное значение для снижения риска киберинцидентов.

Также важно знать методы работы хакеров и установить процедуры кризисного управления, чтобы обеспечить быстрое и эффективное реагирование в случае возникновения одного из выявленных сценариев. Написание Политики управления инцидентами — это не только хорошая практика, но и ключевой элемент соблюдения правил защиты данных.

Принятие киберстрахования, адаптированного к потребностям организации, также является хорошим рефлексом, если, конечно, компания соглашается позиционировать себя, что в наше время не самоочевидно.

Однако будьте осторожны, чтобы не мобилизовать только технические группы для реализации этих различных передовых практик: правовое управление также важно для предотвращения кибератак, а также для реагирования на инциденты.

Специалист по правовым вопросам окажет содействие как оперативному персоналу в реализации мер предосторожности и других действий, которые необходимо осуществить для соблюдения применимых правовых обязательств

(уведомление надзорных и надзорных органов, информирование лиц), так и лицам, принимающим решения в общее управление рисками, будь то на уровне договорного управления субподрядчиками, активации страховых полисов или даже кризисной коммуникации.

В этом смысле компаниям предлагается следовать последним рекомендациям ANSSI по кибербезопасности.

Каковы новые правила кибербезопасности с директивой NIS II

Здесь следует напомнить, что сектор здравоохранения уже подпадает под действие нескольких правил защиты данных: Общий регламент защиты данных (GDPR), правила, применимые к операторам основных услуг (OSE) и операторам важных жизненно важных функций (OIV), сертификация HDS, порядок от 12 мая 2021 года об электронной идентификации пользователей цифровых медицинских услуг…

Также речь пойдет об упреждении последствий предстоящего принятия редакции директивы «Сетевая и информационная безопасность» (NIS II).

Эта пересмотренная версия усиливает требования безопасности, предъявляемые к публичным игрокам, включая больницы, требуя от них принятия процедуры управления инцидентами, проведения аудитов для оценки эффективности мер или даже обеспечения безопасности цепочки поставок и повышения ответственности менеджеров.

Как эффективно реагировать в случае кибератаки на больницу?

Предотвращение киберрисков является важным аспектом защиты медицинских учреждений. На последних нападают каждый день, и вопрос не в том, будут ли эти атаки в конечном итоге успешны и прорвут оборону, а в том, когда?

Таким образом, каждое учреждение должно быть готово к реагированию, напоминая, что реакция на кибератаку требует соблюдения многих правил, которые выходят за рамки простого внедрения технических решений для защиты (например, карантин) и устойчивости (например, восстановление резервных данных)…

Таким образом, вмешательство юриста вместе с менеджерами и оперативными командами сразу после выявления инцидента позволит не только управлять кризисом (мониторинг внутренних процедур и соблюдения юридических обязательств, выявление и нейтрализация юридических рисков и т. но и предвидеть их последствия (споры с провайдерами, уголовная ответственность структуры, контроль компетентных органов, процедура административного взыскания, социальная напряженность, репутационные и финансовые риски и т.д.).

В дополнение к подаче жалобы, которая, безусловно, не является обязательной, но настоятельно рекомендуется, хотя бы для того, чтобы зафиксировать статус жертвы учреждения, мы должны, наконец, указать, что особое внимание должно быть уделено юридическим обязательствам, касающимся различных уведомлений, которые должны быть сделаны. в особо сжатые сроки.

Уведомление CNIL не позднее, чем в течение 72 часов после того, как стало известно об утечке данных (статья 33 GDPR);

Уведомление Агентства цифрового здравоохранения (ANS) и Регионального агентства здравоохранения, которые совместно анализируют, квалифицируют и

обрабатывают отчеты об инцидентах (статья L 1111-8-2 Кодекса общественного здравоохранения);

Заявление об инциденте безопасности Национальному агентству безопасности информационных систем (ANSSI), когда учреждение имеет качество OSE;

Уведомление лиц, затронутых нарушением (пациенты, сотрудники и т. д.), когда оно представляет высокий риск для этих лиц, что часто имеет место в отношении данных о здоровье (статья 34 GDPR);

Уведомление контроллера данных, когда больница выступает в качестве субподрядчика в своих отношениях с ним;

Наконец, как государственные служащие, директора больниц обязаны безотлагательно информировать прокурора в случае обнаружения преступления или проступка при исполнении своих функций (статья 40, пункт 2 Уголовно-процессуального кодекса)». ***(Stéphane Astier, Victoire Grosjean. Cybersécurité: les hôpitaux dans la tourmente des rançongiciels // HAAS AVOCATS (https://info.haas-avocats.com/droit-digital/cybersecurite-les-hopitaux-dans-la-tourmente-des-rancongiciels). 06.10.2022).***

***

«…Более двух третей поставщиков медицинских услуг являются жертвами киберпреступлений. На самом деле, согласно статистике Управления гражданских прав Министерства здравоохранения и социальных служб, каждый день происходит в среднем две утечки медицинских данных, что вдвое больше, чем четыре года назад. Каждое нарушение обходится организациям здравоохранения в среднем более чем в 10 миллионов долларов, согласно ежегодному отчету IBM о стоимости утечки данных. В 2021 году в результате атак были скомпрометированы данные 40 миллионов человек, а с 2009 года хакеры получили доступ к записям данных, представляющим 95% населения США.

Помимо украденных данных и потерянных денег, эти нарушения могут означать разницу между жизнью и смертью. Хотя мы надеемся увидеть больше действий правительства по защите данных здравоохранения, системам здравоохранения не следует ждать принятия этого закона. Сейчас им нужно укреплять собственную оборону. Особое внимание следует уделить защите медицинского оборудования.

Законодательное движение по кибербезопасности медицинских изделий

Федеральное правительство США рассматривает несколько предложений по регулированию соответствия требованиям кибербезопасности медицинских устройств для противодействия частым и клинически значимым кибератакам, с которыми сталкиваются системы здравоохранения по всей стране.

В апреле 2022 года FDA выпустило долгожданный проект руководства по безопасности медицинских устройств для общественного обсуждения. Документ предоставляет производителям устройств рекомендации по обеспечению кибербезопасности при проектировании устройств и связанных с ними предварительных представлениях. В соответствии с этой политикой производители оригинального оборудования (OEM) должны разработать процедуры для проверки и проверки конструкции подключенного устройства для разумной гарантии

безопасности и эффективности. FDA рекомендует OEM-производителям создать безопасную платформу разработки продуктов, чтобы уменьшить уязвимость продуктов и реализовать требования кибербезопасности медицинских устройств. Эта структура охватывает все аспекты жизненного цикла продукта, включая разработку, выпуск, поддержку и вывод из эксплуатации.

В настоящее время Сенат рассматривает Закон об усилении кибербезопасности для медицинских устройств. Предложение требует, чтобы FDA регулярно обновляло руководство по кибербезопасности, публиковало общедоступную информацию об улучшении кибербезопасности медицинских устройств и доступе к ресурсам, а также выпускало отчет, определяющий проблемы в кибербезопасности для медицинского оборудования, включая устаревшие устройства.

В соответствии с предложенным Сенатом Законом о защите и преобразовании киберздравоохранения (PATCH) OEM-производители должны будут предоставить информацию о безопасности подключенного медицинского устройства, прежде чем оно выйдет на рынок. Требования включают в себя раскрытие информации об уязвимостях и определенных процессах и процедурах, обеспечивающих доступность обновлений и исправлений для устройства на протяжении всего его жизненного цикла.

Палата представителей приняла Поправки к пищевым продуктам и лекарствам от 2022 года, дающие FDA полномочия требовать от производителей устройств включения определенной информации о кибербезопасности в их предварительные заявки в соответствии с недавним проектом руководства FDA. Закон о кибербезопасности здравоохранения также находится на рассмотрении в Палате представителей. Этот закон требует, чтобы Агентство кибербезопасности и безопасности инфраструктуры (CISA) и Министерство здравоохранения и социальных служб сотрудничали в улучшении мер кибербезопасности в больницах и других медицинских учреждениях и разрабатывали продукты, специально предназначенные для нужд медицинских учреждений. Организации также должны проводить обучение персонала здравоохранения по вопросам киберрисков и смягчению их последствий.

Эти предложения являются шагами в правильном направлении для лучшей защиты медицинских устройств от нарушений безопасности, но ни одно из них не близко к реализации. Нужны более быстрые действия.

Как принять упреждающие меры для обеспечения соответствия требованиям кибербезопасности медицинских устройств

Чтобы немедленно защитить здоровье и данные пациентов и подготовиться к будущему законодательству, системы здравоохранения должны оценивать и устранять текущие риски и создавать постоянную стратегию восстановления. Успешная программа кибербезопасности требует сотрудничества между клиническими инженерами и ИТ-командами, а также четко определенных рабочих процессов.

Начните со следования принципам кибербезопасности Национального института стандартов и технологий. Структура состоит из пяти принципов:

Определить: определите полный перечень устройств и программного обеспечения, политик кибербезопасности, юридических требований и уязвимостей.

Защита: включите соответствующие меры безопасности, включая контроль доступа и управление идентификацией, обучение персонала и политики защиты информации.

Обнаружение: определите соответствующие стратегии мониторинга для быстрого выявления событий кибербезопасности.

Ответ: Создайте план действий, чтобы отреагировать на нарушение.

Восстановление: разработайте стратегию восстановления любых возможностей или служб, затронутых инцидентом.

Внедрение решения для кибербезопасности медицинских устройств и организация мониторинга угроз в режиме реального времени помогает системам здравоохранения быть на шаг впереди хакеров (и соблюдать будущие требования). Системы здравоохранения могут начать определять приоритеты восстановления путем создания полного инвентарного списка медицинского оборудования с информацией об основных характеристиках оборудования, его местоположении и текущем использовании. Используя эти данные, группы управления устройствами оценивают киберуязвимость устройства, риск и влияние на безопасность пациентов, чтобы создать индикатор риска.

Каждая система здравоохранения будет иметь свой индивидуальный порог риска и приоритеты, поэтому подходы к восстановлению будут различаться. Вот почему каждой организации необходимо определить стратегию управления рисками. Включение технологии в план кибербезопасности медицинских устройств может улучшить мониторинг угроз за счет управления инвентаризацией оборудования и выявления уязвимостей, которые должны устранять группы медицинских устройств.

Кибератаки угрожают жизни пациентов и конфиденциальным данным и обходятся в значительные суммы денег. Хотя подготовка и предотвращение нападения непросты, они необходимы. Со временем помощь придет в виде правительственных постановлений, но тем временем системы здравоохранения должны разработать и внедрить собственную стратегию кибербезопасности для защиты своих пациентов». ***(Scott Trevino. Don't wait for medical device cybersecurity legislation: Act now to save patients' lives // Help Net Security (https://www.helpnetsecurity.com/2022/10/25/medical-device-cybersecurity-compliance/). 25.10.2022).***

***

Захист персональних даних

«У компанії Meta попередили, що мільйон користувачів Facebook завантажили або використали безневинні мобільні програми, які насправді можуть викрадати паролі доступу до соціальної мережі. Про це передає Le Monde. Pixels.

Згадані додатки були присутні у Google Play Store та Apple App Store під виглядом редакторів фото, ігор, VPN та інших сервісів. Після встановлення вони просили у користувачів ввести дані Facebook для користування певними функціями.

«Вони просто намагаються обманом змусити людей надати свою конфіденційну інформацію, щоб передати хакерам доступ до їхніх облікових записів», – сказав директор відділу кібербезпеки Meta Девід Агранович.

Представники Meta поділилися своєю інформацією з Apple та Google. У Google видалили більшість програм.

Агранович додав, що користувачі повинні бути обережні щодо того програмного забезпечення, яке запитує облікові дані без вагомих причин…». ***(Мільйон користувачів Facebook завантажили шкідливі програми - попередження Meta // ТОНЕТО (https://toneto.net/news/tehnologii/m--lyon-koristuvach--v-Facebook-zavantagili-shk--dliv---programi---poperedgennya-Meta). 11.10.2022).***

***

«Майже три чверті випадків шахрайства та витоку даних стосуються ринку e-commerce — здебільшого, це атаки з використанням соціальної інженерії, шкідливих програм та фішингових атак. Про це йдеться у дослідженні команди Visa з міжнародних ризиків, що зосереджене на періоді після пандемії.

Зокрема проти власників криптовалют використовується нове шкідливе програмне забезпечення, орієнтоване на віртуальні гаманці у вигляді розширення браузера та послуги криптомоста.

«У міру того, як роздрібна торгівля повертається до допандемічного рівня, шахраї знову використовують фізичні магазини як точки вразливості, продовжуючи водночас збагачуватися на електронній комерції, серед іншого, за допомогою шкідливих програм, програм-вимагачів та фішингових атак», – сказав Пол Фабара, директор з управління ризиками Visa.

Майже три чверті випадків шахрайства та витоку даних, розслідуваних командою Visa з міжнародних ризиків, стосувалися гравців ринку електронної комерції — здебільшого, це атаки з використанням соціальної інженерії та програм-вимагачів. Дуже поширені цифрові скімінгові атаки, націлені на платформи електронної комерції та інтеграцію стороннього коду.

Ці атаки проливають світло на необхідність суворих заходів безпеки на вебсайтах продавців та сторінках оплати, гарантуючи, що зовнішній код не буде включений до чутливих середовищ власників карток.

Фактично 42% респондентів в огляді Массачусетського технологічного інституту Moving money in a digital world | MIT Technology Review стверджують, що заходи безпеки важливі для їхніх клієнтів, а 59% визнають, що загрози кібербезпеці є найбільшою проблемою для розширення цифрових платежів. Багато хто надає пріоритет розширеним можливостям безпеки, таким як цифрові токени (32%), штучний інтелект та розширена авторизація (43%).

Крім атак на традиційну валюту, зловмисники використовують нові тактики для обману користувачів криптовалюти, зокрема нове шкідливе програмне забезпечення, орієнтоване на гаманці у вигляді розширення браузера для

користувачів цифрової валюти, а також інновації у схемах фішингу та соціальної інженерії.

Послуги криптомоста також є загрозою. З січня до лютого 2022 року в результаті трьох великих крадіжок з використанням вразливостей у різних мостових службах кіберзлодії отримали понад $400 мільйонів». ***(Близько 75% випадків світового шахрайства й витоків даних стосується електронної комерції // Інформаційне агентство ЛІГАБізнесІнформ (https://tech.liga.net/ua/ukraine/novosti/okolo-75-sluchaev-mirovogo-moshennichestva-i-utechek-dannyh-kasaetsya-elektronnoy-kommertsii). 14.10.2022).***

***

«Даже простая и распространенная ошибка, такая как опечатка в доменном имени, может привести к атакам кибербезопасности, последним из продолжающегося шквала вредоносных программ. Этот метод социальной инженерии, известный как перехват URL-адресов или «опечатка», основан на знании того, что легко нажать неверный ключ и в конечном итоге посетить не тот веб-сайт.

С минимальными усилиями хакер может копировать изображения, шрифты и текст для создания вредоносного веб-сайта, который выглядит как PayPal, Google Wallet, Microsoft Visual Studio, MetaMask и другие популярные веб-сайты. Эти поддельные веб-сайты также используются в фишинговых кампаниях всех видов, поскольку сходство доменного имени полезно для целого ряда укусов доверия.

Кампании по перехвату URL-адресов и фишинговым кампаниям не новы, но в последнее время их число увеличилось. Bleeping Computer с небольшой помощью охранной фирмы Cyble обнаружил более 200 доменов, которые выдавали себя за популярные веб-сайты для приложений Android и Windows, торговли криптовалютой и акциями, а также приложений для подписки». ***(Alan Truly. Typos can get you hacked in latest cybersecurity threat // Digital Trends Media Group, a Designtechnica Company (https://www.digitaltrends.com/computing/typos-can-get-you-hacked-latest-cybersecurity-threat/). 24.10.2022).***

***

«…В последнем ежегодном отчете Ponemon Institute и IBM о стоимости утечки данных говорится, что средняя глобальная стоимость утечки данных в этом году достигла рекордно высокого уровня в 4,35 миллиона долларов, что почти на 10% выше, чем в прошлом году.

Для организаций критической инфраструктуры стоимость взлома составила около 4,82 миллиона долларов. В результате около 60% взломанных организаций были вынуждены поднять цены на свои продукты и услуги.

Организации, которые более устойчивы к киберугрозам, справились лучше: у тех, у кого не было системы нулевого доверия, затраты на взлом в среднем на 1 миллион долларов выше, чем у тех, у кого она была.

Организации с группами реагирования на инциденты и регулярно тестируемыми планами реагирования на инциденты смогли сэкономить в среднем 2,66 миллиона долларов.

Во времена стремительного роста затрат и проблем с цепочками поставок немногие организации могут позволить себе убытки, простои и ущерб репутации, которые могут быть вызваны нарушением.

Киберустойчивость должна стоять на первом месте в повестке дня совета директоров, но во многих случаях она по-прежнему рассматривается как ИТ-императив — до тех пор, пока что-то не пойдет не так.

В отчете о киберустойчивых организациях Ponemon Institute за 2020 год отмечается, что наиболее устойчивые к киберугрозам организации превосходят другие более чем на 30% в своих возможностях предотвращать, обнаруживать, сдерживать кибератаки и реагировать на них.

В 2021 году Институт обнаружил, что киберриски и атаки программ-вымогателей усугубляются: 51% респондентов заявили, что сталкивались с утечкой данных за последние 12 месяцев, а 46% подверглись хотя бы одной атаке программ-вымогателей за последние два года.

61% тех, кто стал жертвой атаки программы-вымогателя, заплатили выкуп, и в большинстве этих случаев злоумышленники требовали выкуп в размере более 1 миллиона долларов.

Несмотря на растущие риски, только 23% оценили свою киберустойчивость на 9 или 10 баллов по шкале от 1 до 10.

В первом флагманском отчете WEF Global Cybersecurity Outlook, выпущенном ранее в этом году, говорится, что целых 87% руководителей планируют повысить киберустойчивость в своих организациях путем усиления политик, процессов и стандартов устойчивости в отношении того, как привлекать и управлять третьими сторонами.

Однако отчет показывает несоответствие между тем, что думали руководители, и тем, как специалисты по кибербезопасности и рискам оценивали усилия своих компаний по обеспечению устойчивости к киберугрозам.

В то время как 92 % опрошенных руководителей предприятий согласились с тем, что киберустойчивость была интегрирована в корпоративные стратегии управления рисками, а 41 % считали киберустойчивость приоритетом бизнеса, только 55 % опрошенных руководителей, занимающихся вопросами безопасности, согласились с тем, что она была интегрирована в корпоративное управление рисками, и лишь немногие поскольку 13% считают, что это установленный бизнес-приоритет.

Поскольку киберриски настолько распространены, советы директоров должны сделать киберустойчивость своим главным приоритетом и сосредоточиться на устойчивости, прежде чем приступать к другим инициативам по цифровой трансформации». ***(Cybersecurity the top risk business faces today // BusinessTech (https://businesstech.co.za/news/industry-news/637143/cybersecurity-the-top-risk-business-faces-today/). 24.10.2022).***

***

«ICO оштрафовала Interserve Group Ltd, аутсорсинговую и строительную компанию, на 4,4 миллиона фунтов стерлингов после того, как в 2020 году она

подверглась кибератаке, в результате которой были скомпрометированы личные данные 113 000 ее нынешних и бывших сотрудников.

Подробности кибератаки

Кибератака произошла, когда сотрудник Interserve, работавший дома, переслал фишинговое письмо другому сотруднику, который открыл его и скачал содержимое. Первоначальное фишинговое письмо не было помещено в карантин или заблокировано системой Interserve, а загрузка привела к установке вредоносного ПО на рабочую станцию сотрудника.

Антивирус Interserve поместил вредоносное ПО в карантин и отправил предупреждение, но Interserve не смогла провести достаточное расследование. В результате хакер получил доступ к 283 системам и 16 учетным записям и позволил им удалить антивирусное решение компании.

Личные данные до 113 000 сотрудников были зашифрованы и стали «недоступными». Данные, которые были скомпрометированы, охватывают 4 базы данных отдела кадров и включают в себя данные о номерах национальных страховых полисов и банковских счетах сотрудников, а также данные специальной категории, включая этническое происхождение, сведения о любой инвалидности и сексуальной ориентации.

Решение об ICO

ICO обнаружило, что Interserve:

не отреагировал на первоначальное предупреждение о подозрительной деятельности;

используются устаревшие программные системы и протоколы; а также

не хватало надлежащей подготовки персонала и недостаточных оценок рисков.

Сочетание этих факторов в конечном итоге создало уязвимость для кибератаки, как подчеркивалось в уведомлении о штрафе:

«Interserve должна была разумно осознавать риски, связанные с использованием устаревших систем поддержки, в частности, в обстоятельствах, когда риски использования устаревших систем поддержки были хорошо известны и задокументированы».

Отсутствие со стороны Interserve достаточных действий в отношении кибербезопасности равносильно нарушению закона о защите данных. В частности, не были приняты соответствующие технические и организационные меры для предотвращения несанкционированного доступа к информации людей, что является одним из ключевых принципов GDPR Великобритании.

Первоначально ICO направило Interserve «уведомление о намерениях» (как это было с TikTok) с предварительной суммой штрафа в размере 4,4 миллиона фунтов стерлингов. После рассмотрения представлений Interserve окончательная сумма штрафа не изменилась.

Джон Эдвардс, комиссар Великобритании по вопросам информации, сказал:

«Самый большой киберриск, с которым сталкиваются предприятия, связан не с хакерами за пределами их компании, а с самоуспокоенностью внутри компании. Если ваш бизнес не отслеживает регулярно подозрительную активность в своих системах и не реагирует на предупреждения, или не обновляет программное

обеспечение и не проводит обучение персонала, вы можете ожидать аналогичный штраф от моего офиса».

Основные выводы и последствия

В свете предупреждения ICO о том, что самый большой киберриск для бизнеса — это внутренняя самоуспокоенность, а не обязательно внешние субъекты угроз, бизнесу следует предпринять несколько практических шагов:

обновить обучение по кибербезопасности для сотрудников на всех уровнях их бизнеса;

применять активный подход к обучению и следить за тем, чтобы оно продолжалось, например, регулярно рассылать фишинговые электронные письма для проверки киберустойчивости; а также

обеспечить регулярную проверку и обновление ИТ-инфраструктуры и операционных систем

Поскольку Национальный месяц осведомленности о кибербезопасности подходит к концу, этот штраф подтверждает как позицию, которую ICO занимает в отношении несовершенных методов кибербезопасности, так и важность того, чтобы предприятия применяли упреждающий подход к обучению кибербезопасности и поддерживали свои системы и процедуры безопасности, чтобы гарантировать, что они готовы к кибератаке тогда, а не если она произойдет». ***(Isaac Bedi. ICO fines Interserve Group Ltd £4.4 million for failure to protect employee personal data // Burges Salmon (https://blog.burges-salmon.com/post/102i00u/ico-fines-interserve-group-ltd-4-4-million-for-failure-to-protect-employee-perso). 26.10.2022).***

***

«В ходе третьей крупной утечки данных за последний месяц хакеры пригрозили раскрыть личные данные клиентов Medibank, если их требования о выкупе не будут выполнены.

Спрос на вымогательство может подвергнуть до 3,9 миллионов австралийцев возможности мошенничества и кражи личных данных, и хакеры заявляют, что обнародуют данные 1000 «наиболее известных клиентов» поставщика медицинского страхования в качестве «предупредительного выстрела», если они не получают того, что хотят.

«[Мы] нашли людей с очень интересными диагнозами. И мы вышлем им их информацию по электронной почте», — заявили хакеры.

Medibank не обнародовал детали конкретных требований, но заявляет, что очень серьезно относится к угрозе.

Medibank, у которого почти 4 миллиона клиентов и который предоставляет ряд услуг, включая медицинское страхование, управление здравоохранением, а также телемедицинские услуги для государственных и корпоративных клиентов, впервые признал утечку данных на прошлой неделе, заявив первоначально, что не было никаких доказательств того, что конфиденциальные данные клиентов были украдены. был получен доступ.

Кибератака последовала за крупнейшей в истории Австралии, которая затронула клиентов Optus в конце сентября, и еще одной, которая затронула веб-сайт Woolworth My Deal в начале этого месяца.

Это реальность того, о чем давно предупреждали киберэксперты: Австралия является «легкой добычей» для киберпреступников. Это также показывает очень реальную опасность компаний, использующих «реактивные» политики и процедуры вместо того, чтобы делать больше и инвестировать больше в стратегии проактивной защиты.

Проблема привлекла внимание к безопасности данных, поскольку федеральное правительство обещает срочную реформу, которая может увеличить штрафы за нарушение конфиденциальности, но это слабое утешение для тех австралийцев, которые пострадали. Это все равно, что «закрыть ворота после того, как лошадь убежала».

Кроме того, государству выплачиваются штрафы. То, что многие клиенты могут предпочесть, — это некоторая форма личной компенсации за принуждение, вызванное такими инцидентами, а также время и усилия, которые они должны потратить, пытаясь смягчить ущерб и обеспечить собственную защиту.

Большинство из нас достаточно сообразительны, чтобы знать, что нам нужно регулярно менять наши пароли и данные для входа, опасаться необычных ссылок, быть осторожным с тем, что мы публикуем в Интернете на платформах социальных сетей, и внимательно следить за нашими банковскими балансами на предмет ненормальных транзакций.

Многие из нас берут на себя личную ответственность за нашу деятельность в Интернете и делают все возможное, чтобы защитить себя, и все же мы должны передавать данные компаниям и организациям и «надеемся», что они способны сделать то же самое.

Однако есть большое количество австралийцев, которые особенно уязвимы из-за значительного «цифрового разрыва» Австралии.

Австралийский индекс охвата цифровыми технологиями (ADII, 2021) показывает, что каждый четвертый житель Австралии по-прежнему лишен доступа к цифровым технологиям, то есть у них нет доступа к обычному стабильному Интернету. Как правило, это малообеспеченные люди, люди с низким уровнем образования и занятости, бездомные, проживающие в некоторых регионах, люди старше 65 лет и инвалиды.

Без доступа к Интернету или без навыков и уверенности в его использовании эти люди особенно подвержены риску, потому что они не могут самостоятельно предпринять шаги по исправлению положения.

Мошенничество с идентификацией может занять у человека годы, чтобы оправиться от него. Это также имеет ряд очень серьезных потенциальных последствий, особенно если кто-то использует украденную личность для совершения преступления, а это означает, что невиновный человек может быть обвинен в том, чего он не делал.

По мере быстрого развития цифровой эпохи данные стали исключительно ценными для компаний, поэтому, возможно, неудивительно, что хакеры пытаются вымогать большие суммы денег в обмен на данные. У них якобы есть 200 гигабайт информации, включая контактные данные клиентов, конфиденциальную информацию о здоровье и данные кредитных карт, но нет никакой гарантии, что даже если им заплатят, они вернут данные и просто исчезнут. Неизвестно также,

продавали ли они уже данные где-либо еще, прежде чем требовать требования от Medibank.

Тем не менее, угроза Medibank сделала еще один шаг вперед по сравнению с двумя предыдущими крупномасштабными взломами: хакеры заявили, что намерены найти в базе данных наиболее «высокопоставленных» людей, включая политиков, актеров, блоггеров, активистов, и отправить им электронное письмо. свою информацию, чтобы доказать, что у них есть данные, и оказать давление на переговоры. Они якобы заявили, что обнародуют информацию, если их требования не будут выполнены.

Для клиентов, которые, без сомнения, полностью утратили доверие к организации, особенно после ее первых заверений в том, что никакие конфиденциальные данные не были скомпрометированы или потеряны, предстоит напряженное ожидание, чтобы увидеть, что будет дальше и как люди смогут принять свои меры. собственные действия по решению проблемы.

В последние дни Австралийский центр кибербезопасности предупредил, что это может быть только началом, поскольку кибератаки становятся не только частыми, но и масштабными и изощренными». ***(Sonia Hickey. Australia Under Attack from Cyber Criminals // Sydney Criminal Lawyers® (https://www.sydneycriminallawyers.com.au/blog/australia-under-attack-from-cyber-criminals/). 20.10.2022).***

***

«18 октября 2022 г. Департамент финансовых услуг штата Нью-Йорк («NYDFS») объявил, что компания EyeMed Vision Care LLC («EyeMed») согласилась выплатить компенсацию в размере 4,5 млн долларов США за нарушения Регламента о кибербезопасности (23 NYCRR Part 500), которые способствовали к раскрытию сотен тысяч данных о здоровье потребителей в связи с событием кибербезопасности в 2020 году.

В ходе фишинговой атаки, которая длилась несколько дней в июне и июле 2020 года, злоумышленник получил доступ к папке электронной почты EyeMed, которая содержала конфиденциальные личные данные о здоровье за шесть лет, включая данные о несовершеннолетних. Приказ о согласии NYDFS отмечает, что несоблюдение EyeMed Регламента о кибербезопасности сделало EyeMed уязвимым для злоумышленников. В частности, регулирующий орган обнаружил, что EyeMed не внедрила многофакторную аутентификацию в своих системах электронной почты, не ограничила права доступа пользователей учетными записями, содержащими конфиденциальную информацию, и не внедрила достаточные протоколы хранения и удаления данных. Согласно постановлению о согласии, почтовый ящик, содержащий конфиденциальную информацию о потребителях, был защищен слабым паролем, которым поделились девять сотрудников. NYDFS также обнаружила, что EyeMed не смогла провести адекватную оценку рисков кибербезопасности, и в результате сертификаты кибербезопасности компании за календарные годы с 2017 по 2020 были «неправильными».

В рамках мирового соглашения EyeMed согласилась провести комплексную оценку рисков кибербезопасности и подготовить план действий по устранению

рисков, выявленных в ходе этой оценки». ***(NYDFS Fines EyeMed $4.5 Million for Cybersecurity Violations // Hunton Andrews Kurth LLP. (https://www.huntonprivacyblog.com/2022/10/24/nydfs-fines-eyemed-4-5-million-for-cybersecurity-violations/#page=1). 24.10.2022).***

***

«Кибербезопасность является одним из последних модных словечек, и это вполне заслуженно: до 9,7 миллиона клиентов Optus стали жертвами кибератаки 22 сентября 2022 года. Хотя полный масштаб нарушения еще предстоит определить, атака привела к несанкционированное раскрытие личной информации, включая имена, адреса, номера телефонов и номера документов, удостоверяющих личность, включая водительские права, Medicare и номера паспортов.

Вызывает тревогу тот факт, что в 2020-21 финансовом году было зарегистрировано более 67 500 случаев киберпреступлений, что почти на 13% больше, чем в предыдущем году.

В годовом отчете Австралийского центра кибербезопасности (ASCR) за 2020–2021 годы отмечается, что киберпреступления, связанные с мошенничеством, когда субъекты используют компьютеры или онлайн-сервисы для совершения мошенничества, представляют собой серьезную угрозу для потребителей, при этом наиболее распространенными источниками этих мошенничеств являются покупки. онлайн и онлайн-банкинг.

Совершенно очевидно, что кибербезопасность должна быть в центре внимания всех австралийцев и организаций.

11 октября 2022 года Управление Комиссара по информации Австралии (OAIC) начало расследование практики обращения с личными данными группы Optus в связи с утечкой данных. Если расследование OAIC выявит «серьезные и/или неоднократные» вмешательства в частную жизнь, OAIC имеет право потребовать штраф в размере до 2,2 миллиона долларов.

Что вы можете сделать, чтобы защитить себя?

Хотя, вероятно, будут наложены штрафы и предстоит законодательная реформа закона о конфиденциальности, тем временем вы можете предпринять некоторые шаги, чтобы сохранять бдительность в отношении кибератак. Это включает:

регулярная защита и мониторинг ваших устройств и учетных записей для выявления необычной активности;

обеспечение актуальности приложений с последними обновлениями безопасности; а также

включение многофакторной аутентификации для всех учетных записей.

Какие обязательства организации несут перед потребителями по защите от рисков кибербезопасности?

В соответствии с Законом о корпорациях 2001 г. (Cth) директора и лицензиаты AFS в равной степени обязаны проявлять должную осмотрительность, действовать честно и справедливо, а также обязаны иметь адекватные системы управления рисками для управления рисками кибербезопасности.

В случае с Optus расследования OAIC оценят, предприняла ли организация разумные шаги для защиты личной информации, которой она располагала, от несанкционированного использования и раскрытия, и была ли собранная и сохраненная информация необходимой для выполнения их деловых операций.

Аналогичный тест был принят судьей Рольфе в деле ASIC против австралийского лицензиата финансовых услуг RI Advice Group Pty Ltd в мае 2022 года. В этом случае судья Рольф ясно дал понять, что стандарт систем управления рисками кибербезопасности, необходимый для каждого лицензиата AFS, будет оцениваться разумная адекватность системы и соответствующий технический опыт квалифицированного специалиста, которому поручено оценивать риски, с которыми сталкивается бизнес в отношении его операций и ИТ-среды.

Какие шаги могут предпринять организации для выполнения своих обязательств?

Чтобы активно защищаться от рисков кибербезопасности, организации должны обеспечить:

компьютерные системы оснащены самой последней версией антивирусного программного обеспечения;

электронные письма фильтруются или помещаются в карантин;

резервные системы существуют и регулярно выполняются;

доступ к системам и интерфейсам надлежащим образом защищен соответствующими учетными данными или паролями;

они действуют эффективно и принимают упреждающие меры для защиты информации о потребителях; а также

воспитывать культуру соблюдения передовых методов кибербезопасности». ***(Rebecca Cameron, Alexandra Vrdoljak. Protect yourself and consumers against cyber-security risk // Scanlan Carroll (https://scanlancarroll.com.au/protect-yourself-and-consumers-against-cyber-security-risk/). 20.10.2022).***

***

«Федеральная торговая комиссия (FTC) принимает меры против онлайн-рынка алкоголя Drizly и его генерального директора Джеймса Кори Релласа в связи с утверждениями о том, что сбои в системе безопасности компании привели к утечке данных, в результате которой была раскрыта личная информация около 2,5 миллионов потребителей. Дризли и Реллас были предупреждены о проблемах безопасности за два года до взлома, но не предприняли шагов для защиты данных потребителей от хакеров. Предлагаемый приказ FTC требует от компании уничтожения ненужных данных, ограничивает данные, которые компания может собирать и хранить, и связывает Релласа с конкретными требованиями безопасности данных для его роли в управлении незаконными методами ведения бизнеса.

«Предлагаемый нами приказ против Drizly не только ограничивает то, что компания может удерживать и собирать в будущем, но также гарантирует, что генеральный директор столкнется с последствиями небрежности компании», — сказал Сэмюэл Левин, директор Бюро по защите прав потребителей Федеральной

торговой комиссии. «Генеральные директора, которые экономят на безопасности, должны принять это к сведению».

Бостонская компания Drizly, дочерняя компания Uber, управляет онлайн-рынком, где потребители, достигшие совершеннолетия, могут размещать заказы у розничных продавцов на покупку пива, вина и алкоголя с доставкой. Компания собирает и хранит в сервисе облачных вычислений Amazon Web Services широкий спектр личной информации от потребителей, такую как электронная почта, почтовые адреса, номера телефонов, уникальные идентификаторы устройств, информация о геолокации и данные, приобретенные у третьих лиц.

Согласно жалобе FTC, Дризли и Реллас были предупреждены о проблемах с процедурами безопасности данных компании после более раннего инцидента с безопасностью. В 2018 году сотрудник Drizly разместил информацию для входа в учетную запись облачных вычислений компании на платформе разработки программного обеспечения и хостинга GitHub. В результате этого нарушения безопасности хакеры смогли использовать серверы Drizly для майнинга криптовалюты, пока компания не изменила данные для входа в свою учетную запись облачных вычислений. Drizly не предприняла шагов для адекватного решения своих проблем безопасности, публично заявив, что у них есть соответствующие меры безопасности. Два года спустя хакер взломал учетную запись сотрудника, получил доступ к корпоративной регистрационной информации Drizly на GitHub, взломал базу данных компании, а затем украл информацию о клиентах.

В своей жалобе FTC утверждает, что Дризли и Реллас:

Не удалось реализовать основные меры безопасности: FTC утверждала, что, несмотря на заявления о том, что компания использовала соответствующие методы безопасности для защиты данных потребителей, Дризли и Реллас не приняли разумных мер безопасности для защиты личной информации, которую она собирала и хранила. От сотрудников не требовалось использовать двухфакторную аутентификацию для GitHub, ограничивать доступ сотрудников к личным данным, разрабатывать адекватные письменные политики безопасности или обучать сотрудников этим процедурам.

Сохранение важной информации базы данных на незащищенной платформе. Согласно жалобе FTC, Drizly хранил учетные данные для входа на GitHub вопреки собственному руководству платформы и широко разрекламированным инцидентам безопасности, связанным с GitHub. Например, в своей жалобе на Uber в 2018 году Федеральная торговая комиссия (FTC) специально обнародовала и описала плохие методы обеспечения безопасности, связанные с использованием учетной записи Uber на GitHub, которые способствовали утечке данных, связанной с приложением для совместного использования.

Пренебрежение мониторингом сети на предмет угроз безопасности: Федеральная торговая комиссия заявила, что Дризли не назначил старшего руководителя ответственным за обеспечение безопасности своих данных, а также не отслеживал свою сеть на предмет несанкционированных попыток доступа или удаления личных данных.

Предоставление клиентов хакерам и похитителям личных данных: после утечки данных компании личная информация, которую Дризли собрал о

потребителях, была выставлена на продажу на двух разных общедоступных сайтах в даркнете, где преступники публикуют и продают данные, украденные хакерами. Похитители личных данных и другие злоумышленники могут использовать такие данные для открытия мошеннических кредитных линий или совершения других видов мошенничества. Когда несанкционированные счета открываются на их имя, потребители могут понести финансовый ущерб, влезая в долги и нанося ущерб своему кредиту, утверждает FTC.

Правоприменительные меры

Предлагаемый приказ в отношении Дризли и Релласа включает несколько требований, направленных на то, чтобы они предприняли шаги для решения проблем, изложенных в жалобе FTC. Согласно предлагаемому распоряжению Федеральной торговой комиссии, Дризли и Реллас обязаны:

Уничтожение ненужных данных: Drizly обязан уничтожить все собранные персональные данные, которые не нужны для предоставления продуктов или услуг потребителям. Он также должен документировать и сообщать Комиссии, какие данные он уничтожил.

Ограничьте сбор данных в будущем: в дальнейшем Drizly должен воздерживаться от сбора или хранения личной информации, за исключением случаев, когда это необходимо для конкретных целей, указанных в графике хранения. Он также должен публично указать на своем веб-сайте информацию, которую он собирает, и почему такой сбор данных необходим.

Внедрить программу информационной безопасности: Drizly должен внедрить комплексную программу информационной безопасности и установить меры безопасности для защиты от инцидентов безопасности, изложенных в жалобе. Это включает в себя такие меры, как обучение сотрудников безопасности; назначение сотрудника высокого уровня для наблюдения за программой информационной безопасности; внедрение контроля над тем, кто может получить доступ к персональным данным; и требование к сотрудникам использовать многофакторную аутентификацию для доступа к базам данных и другим активам, содержащим данные о потребителях.

Примечательно, что приказ распространяется лично на Релласа, который руководил слабой практикой защиты данных Дризли в качестве генерального директора. В современной экономике руководители корпораций часто переходят из компании в компанию, несмотря на недостатки в их послужном списке. Признавая эту реальность, предложенный Комиссией приказ будет следовать Релласу, даже если он покинет Дризли. В частности, Релласу потребуется внедрить программу информационной безопасности в будущих компаниях, если он перейдет к бизнесу, собирающему информацию о потребителях от более чем 25 000 человек, и где он будет мажоритарным владельцем, генеральным директором или старшим должностным лицом, отвечающим за информационную безопасность.

Это действие является частью агрессивных усилий FTC, направленных на то, чтобы компании защищали данные потребителей, а небрежные руководители извлекали уроки из своих сбоев в обеспечении безопасности данных. В прошлом году Комиссия получила свой первый заказ, требующий от фирмы свести к минимуму сбор данных, и работала над последующими заказами, чтобы компании

собирали только то, что им нужно для ведения бизнеса. Комиссия также предпринимает шаги по укреплению безопасности на всем рынке, в том числе путем завершения обновлений Правил о гарантиях, выпуска заявления о политике в отношении Правил уведомления о нарушениях здоровья и инициирования предварительного уведомления о предлагаемом нормотворчестве в отношении коммерческого наблюдения и слабых методов обеспечения безопасности данных.

FTC проголосовала 4-0 за подачу предложенной административной жалобы и принятие соглашения о согласии с Дризли и Релласом. Комиссар Кристин Уилсон проголосовала за, но частично не согласилась с включением Релласа в качестве отдельного ответчика и выступила с отдельным заявлением. Председатель Лина М. Хан и комиссар Альваро Бедойя опубликовали совместное совпадающее заявление, а комиссар Ребекка Келли Слотер опубликовала отдельное совпадающее заявление.

FTC вскоре опубликует описание пакета соглашения о согласии в Федеральном реестре. Соглашение будет подлежать общественному обсуждению в течение 30 дней после публикации в Федеральном реестре, после чего Комиссия примет решение о том, сделать ли предложенный приказ о согласии окончательным...» ***(FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers // The Federal Trade Commission (https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million). 24.10.2022).***

***

«Расследование августовской смишинг-атаки на Twilio выявило связь с более ранней вишинг-атакой. Похоже, что виновнику августовского взлома Twilio также удалось проникнуть в компанию в июне в ходе отдельного инцидента, который раскрыл гораздо меньший объем контактной информации клиентов.

Два взлома Twilio за три месяца связаны с одним и тем же злоумышленником

Августовский взлом Twilio был связан с кампанией, которая засыпала сотрудников SMS-сообщениями, в конечном итоге убедив одного из них посетить мошенническую страницу входа. Расследование этого инцидента было недавно завершено, и компания обнаружила, что тот же злоумышленник был ответственен за более мелкое нарушение в июне. Однако в том более раннем инциденте использовался другой подход; вишинг-атака (голосовой фишинг), которая смогла убедить сотрудника компании отказаться от своих учетных данных для входа по телефону.

Сообщается, что июньское окно вишинговой атаки длилось всего около 12 часов и предоставило злоумышленникам доступ к «ограниченному» объему информации о клиентах. Те, кто пострадал, были уведомлены в июле, но связь с августовской атакой является новой. Взлом Twilio в августе, по-видимому, был запущен вскоре после того, как клиенты были уведомлены о первой атаке, когда хакер изменил свой подход, выдавая себя за сотрудника ИТ-отдела компании, и пытался заставить сотрудников вводить учетные данные на поддельном портале входа в систему Okta.

Окончательный отчет также включает некоторую новую информацию об августовском инциденте. Хотя более поздний взлом Twilio считался гораздо более разрушительным, расследование показало, что он также затронул относительно небольшое количество клиентов; всего 209 из 270 000 учетных записей компании и 93 из примерно 75 миллионов конечных пользователей службы Authy. Самым заслуживающим внимания сообщением о взломе Twilio в августе стало последующее нарушение Signal, но служба обмена сообщениями о конфиденциальности сообщила, что наблюдала только один успешный случай перерегистрации учетной записи на новом устройстве (и всего три случая были атакованы). этим способом).

С тех пор Twilio сбросила учетные данные всех сотрудников, которые были скомпрометированы в результате любой из атак, и находится в процессе распространения аппаратных ключей безопасности FIDO2 среди всех своих сотрудников в качестве метода двухфакторной аутентификации. Компания также заявила, что добавляет уровни защиты к своей корпоративной VPN и переоснащает некоторые административные функции и приложения, интегрированные с Okta, и что атаки smishing и vishing не предоставили злоумышленникам доступ к учетным данным клиентов или токенам аутентификации.

Вишинг-атаки становятся все более популярными среди хакеров

Виновника взлома Twilio называют «0ktapus» (иногда его также называют «Scatter Swine») из-за того, что он сосредоточен на краже логинов Okta в качестве начальной точки входа. Пока мало что известно об этих злоумышленниках, но взломы Twilio были частью более крупной продолжающейся кампании, нацеленной на 130 организаций. В то время как 0ktapus в этой кампании в основном использовал SMS-сообщения, ведущие на поддельные страницы входа в Okta, его спорадическое использование вишинг-атак является частью общего всплеска преступных хакеров, стремящихся к прибыли, которые возвращаются к телефонным звонкам и старомодной социальной инженерии.

Как SMS-атаки, так и вишинг-атаки отнимают часть рынка у фишинговых электронных писем, которые на сегодняшний день, как правило, были основным методом, используемым вымогателями и другими преступными группировками для первого контакта с целями. По иронии судьбы, одной из движущих сил этой тенденции является более широкое использование двухфакторной аутентификации и запросов на подтверждение входа в систему, отправляемых на телефоны сотрудников. Организации, как правило, больше полагаются на текстовые сообщения в качестве средства связи, поскольку доля удаленной работы значительно увеличилась за последние два года, а злоумышленники пользуются тем, что сотрудники привыкают видеть текстовые сообщения компании, связанные с вопросами безопасности. появляются на их телефонах.

Недавнее исследование, проведенное KnowBe4, показало, что вишинг-атаки подскочили на 625% с первого квартала 2021 года по второй квартал 2022 года, а другое исследование, проведенное Proofpoint, показало, что 69% компаний в настоящее время сталкивались с попытками атаки такого рода (по сравнению с 54% в 2020 году). Этому росту способствуют несколько факторов. Одним из них является рост популярности поддельных схем трудоустройства, которые, как известно,

использовали поддерживаемые государством хакеры Северной Кореи, чтобы получить доступ к сети блокчейна Ronin и украсть более 600 миллионов долларов. Инженеры и ИТ-персонал с привилегированным доступом потенциально могут быть заманены хорошо продуманным фальшивым предложением о работе, которое в некоторых случаях доходит до фальшивых собеседований.

Атаки Vishing также добавляют более сложные «гибридные» элементы, которые, по-видимому, повышают вероятность успеха преступников. Одним из примеров является использование поддельного электронного письма от какого-либо надежного бренда или источника с контактным номером в теле, при этом субъекты угрозы ждут, чтобы сыграть роль агента по обслуживанию клиентов, когда звонят по этому номеру.

Оливер Пинсон-Роксбург, генеральный директор Defense.com, отмечает, что для организаций важно быть в курсе этих все более сложных тенденций в области социальной инженерии, поскольку преступники будут многократно использовать проверенный метод: что люди должны быть настороже не только в подозрительных электронных письмах или текстовых сообщениях. Хакеры легко адаптируются и будут использовать множество различных платформ для психологического манипулирования пользователями, чтобы они передавали доступ к конфиденциальной информации. Атаки социальной инженерии, подобные этой, остаются для хакеров очень экономичным и действенным способом вывести сотрудников из равновесия и взломать системы компании; все, что нужно, это один человек, чтобы попасться на него, чтобы сделать это стоит их времени. Хотя это было лишь незначительное нарушение прав нескольких сотен пользователей, Атаки социальной инженерии потенциально могут представлять гораздо большую угрозу для бизнеса. Он нацелен на самое слабое место киберзащиты любой организации — человеческий фактор. Самые передовые технологии, защищающие вашу цифровую инфраструктуру, становятся практически бесполезными, если сотрудники недостаточно осведомлены об опасностях атак социальной инженерии и о том, как их избежать. Люди на всех уровнях любой организации должны быть осведомлены о киберугрозах и бдительны к ним. Если это так, самая большая слабость может быстро стать лучшей линией обороны». Самые передовые технологии, защищающие вашу цифровую инфраструктуру, становятся практически бесполезными, если сотрудники недостаточно осведомлены об опасностях атак социальной инженерии и о том, как их избежать. Люди на всех уровнях любой организации должны быть осведомлены о киберугрозах и бдительны к ним. Если это так, самая большая слабость может быстро стать лучшей линией обороны». Самые передовые технологии, защищающие вашу цифровую инфраструктуру, становятся практически бесполезными, если сотрудники недостаточно осведомлены об опасностях атак социальной инженерии и о том, как их избежать. Люди на всех уровнях любой организации должны быть осведомлены о киберугрозах и бдительны к ним. Если это так, самая большая слабость может быстро стать лучшей линией обороны». ***(Scott Ikeda. Culprit Behind Twilio Hack Traced to Earlier Vishing Attack That Nabbed Employee Credentials // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/culprit-behind-twilio-hack-traced-to-earlier-vishing-attack-that-nabbed-employee-credentials/). 31.10.2022).***

***

«Meta обнародовала отчет о внутренней безопасности, в котором говорится, что приложения, предназначенные для кражи информации для входа в Facebook, широко распространены в обоих крупных магазинах приложений. Компания заявляет, что она обнаружила более 400 вредоносных приложений такого рода между Android и iOS, которым удается оставаться на плаву благодаря сочетанию профессионального искусства и поддельных положительных отзывов, чтобы придать им видимость легитимности.

Однако при работе с приложениями, предназначенными для кражи данных для входа в Facebook, есть один явный недостаток; все они встраивают кнопку Facebook на стартовые экраны и требуют, чтобы жертва ввела свои учетные данные для использования приложения.

Кластер вредоносных приложений специально нацелен на учетные данные Facebook и сумел обойти защиту магазина приложений.

Вредоносные приложения, похоже, остаются вне поля зрения службы безопасности Google и Apple, поскольку не используют подход установки вредоносных программ или клавиатурных шпионов; вместо этого они просто запрашивают информацию для входа в Facebook в качестве условия запуска приложения, и если пользователь предоставляет ее, злоумышленник крадет ее. Мобильные приложения нередко имеют встроенные функции Facebook, но для них необычно требовать от пользователя предоставления учетных данных перед запуском приложения.

Meta сообщает, что сообщила о своих выводах непосредственно в Apple и Google и обращается к потенциально затронутым пользователям Facebook, и что приложения были удалены до публикации отчета.

Нет оценок того, сколько пользователей могли получить данные для входа в систему с помощью этих вредоносных приложений. Похоже, что приложения не используют двухфакторную аутентификацию (2FA), ориентируясь на пользователей, которые входят в Facebook только с базовым именем пользователя и паролем. Конечно, даже если пользователи защитили свои учетные записи с помощью 2FA, ничто не мешает злоумышленникам попробовать учетные данные в различных других службах, чтобы увидеть, использовались ли они повторно.

Кампания по краже информации для входа в Facebook выглядит хорошо организованной и охватывает широкий спектр различных категорий приложений. Наиболее распространенными из этих вредоносных приложений являются простые фоторедакторы, обычно предлагающие некоторые бесполезные функции, такие как превращение изображений пользователя в мультфильмы или возможность надевать одежду поверх селфи. Поддельные фоторедакторы составили более 42% всех обнаруженных вредоносных приложений. Другие основные категории включают бизнес-утилиты (часто обещающие доступ к функциям и информации, которые не предлагают другие подобные бесплатные приложения), телефонные утилиты, такие как вызовы VoIP, видеоигры и поддельные VPN. Есть несколько других типов приложений, таких как гороскопы, персональные психологические пособия, медиаплееры и коллекции обоев.

Вредоносные приложения также используют несколько методов, чтобы вызвать доверие. Они используют простую, но профессионально выглядящую графику и, кажется, активно публикуют поддельные положительные отзывы, пытаясь заглушить неизбежные отрицательные отзывы, когда пользователи понимают, что они не предлагают все обещанные функции и функции.

Meta отмечает, что к приложениям, которые запрашивают данные для входа в Facebook при запуске, следует относиться с подозрением, и рекомендует пользователям включить 2FA в своей учетной записи в качестве дополнительного уровня защиты. Он также рекомендует внимательно читать обзоры на наличие признаков вредоносной активности и обещанных функций, которые на самом деле не включены или не работают. Вредоносные приложения, о которых идет речь, по-видимому, в лучшем случае обеспечивали лишь небольшую часть обещанной функциональности.

Преступники все чаще интересуются данными для входа в социальные сети

Киберпреступники проявляют новый интерес ко всем основным платформам социальных сетей, рассматривая захват учетных записей как относительно легкую форму киберпреступности с низким уровнем риска. Традиционно считалось, что эти учетные записи ничего не стоят, если они не принадлежат кому-то известному или с крупной платформой, но хакеры находят творческие применения для большого количества учетных записей.

Существует множество различных приложений для кражи данных для входа в социальные сети, но одно из них, популярность которого в последнее время, кажется, растет, — это использование их (и их списков контактов) для обмана законных рекламных программ. Недавняя афера на Facebook привела к тому, что злоумышленники захватили учетную запись, а затем попытались перенаправить весь список контактов человека на URL-адрес, показывающий законную рекламу, от которой преступники получают доход. Аналогичные кампании разгораются в магазинах приложений с 2020 года, в них участвуют преступники, создающие вредоносные приложения, которые захватывают пользовательские устройства для аналогичных видов мошенничества с рекламой.

Киберпреступники также используют украденные учетные записи в социальных сетях для передачи вредоносных программ доверчивым друзьям и подписчикам или для мошенничества с криптовалютой. Также существует торговля учетными записями в социальных сетях, имена пользователей которых содержат общие слова или несколько символов, поскольку они часто являются самыми старыми учетными записями на платформе и имеют определенную ценность престижа». ***(Scott Ikeda. Meta Found More Than 400 Malicious Apps Designed To Steal Facebook Login Information on Official App Stores // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/meta-found-more-than-400-malicious-apps-designed-to-steal-facebook-login-information-on-official-app-stores/). 17.10.2022).***

***

«Согласно отчету, опубликованному во вторник компанией, занимающейся кибербезопасностью, обмен медиафайлами с высоким

разрешением в Интернете может непреднамеренно раскрыть конфиденциальные биометрические данные.

Это может быть особенно опасно, как отмечается в 75-страничном отчете Trend Micro, поскольку люди не знают, что раскрывают информацию.

В отчете, в качестве примера, приводится хэштег #EyeMakeup в Instagram с почти 10 миллионами постов и #EyeChallenge в TikTok с более чем двумя миллиардами просмотров, раскрывающие узоры радужной оболочки, достаточно хорошие, чтобы пройти сканеры радужной оболочки.

«Публикуя определенные виды контента в социальных сетях, мы даем злоумышленникам возможность получить наши биометрические данные», — поясняется в отчете. «Публикуя наши голосовые сообщения, мы раскрываем голосовые паттерны. Публикуя фото- и видеоконтент, мы раскрываем наши лица, сетчатку, радужную оболочку, формы ушей, а в некоторых случаях — ладони и отпечатки пальцев».

«Поскольку такие данные могут быть общедоступными, мы имеем ограниченный контроль над их распространением», — добавил он. «Поэтому мы не знаем, кто уже получил доступ к данным, и мы не знаем, как долго данные будут храниться или для каких целей».

Не панацея

В отчете рассказывается, какие виды биометрических данных могут быть раскрыты в социальных сетях, и описываются более двух десятков сценариев атак.

«Отчет показывает, что биометрическая идентификация не является панацеей, — отмечает Уилл Даффилд, политический аналитик Института Катона., аналитического центра в Вашингтоне, округ Колумбия.

«Разрабатывая системы идентификации, мы должны быть в курсе технологий, которые выходят из строя, и потенциальных злоупотреблений в реальном мире», — сказал он TechNewsWorld.

«Trend Micro вызывает некоторые обоснованные опасения, но эти опасения не новы для профессионалов в области биометрии», — сказал TechNewsWorld Сами Эльхини, специалист по биометрии из Cerberus Sentinel, консалтинговой компании по кибербезопасности и тестированию на проникновение в Скоттсдейле, штат Аризона.

Он отметил, что существуют различные способы атак на биометрические системы, в том числе описанные в отчете «презентационные» атаки, подменяющие биометрический элемент фотографией или другим объектом.

Чтобы противостоять этому, продолжил он, необходимо определить «живость», чтобы убедиться, что представленные биометрические данные принадлежат живому человеку, а не «воспроизведению» ранее захваченных биометрических данных.

Ави Тургеман, генеральный директор и соучредитель IronVest, компании по обеспечению безопасности учетных записей и личных данных в Нью-Йорке, согласился с тем, что «живость» является ключом к предотвращению атак на биометрическую защиту.

«Отчет Trend Micro вызывает обеспокоенность по поводу мошеннических биометрических данных, созданных с помощью контента социальных сетей», —

сказал он TechNewsWorld. «Настоящий секрет защищенной от мошенничества биометрии заключается в обнаружении живости, чего нельзя воссоздать с помощью фотографий и видео, собранных в социальных сетях».

Одного фактора недостаточно

Даже при тестировании на живучесть биометрические данные все еще слишком легко обойти, считает Эрих Крон, сторонник осведомленности о безопасности для KnowBe4, поставщика услуг по обучению осведомленности о безопасности в Клируотере, штат Флорида.

«Если держать телефон перед лицом человека во время сна, он может разблокировать устройство, особенно если он используется с настройками по умолчанию, а сбор отпечатков пальцев — несложная задача», — сказал он TechNewsWorld.

«Еще более тревожным является то, что если биометрический фактор скомпрометирован, его нельзя изменить, как пароль», — добавил он. «Вы не можете изменить свои отпечатки пальцев или структуру лица в долгосрочной перспективе, если их взломают».

Если отчет Trend Micro что-то и иллюстрирует, так это необходимость многофакторной аутентификации, даже если один из этих факторов является биометрическим.

«При использовании в качестве единственного фактора аутентификации важно отметить, что биометрические данные могут быть подвержены сбоям или манипуляциям со стороны злоумышленника, особенно когда эти биометрические данные общедоступны в социальных сетях», — сказал Даррен Гуччионе, генеральный директор Keeper Security. компания по управлению паролями и онлайн-хранилищу, базирующаяся в Чикаго.

«Поскольку возможности злоумышленников по захвату учетных записей с помощью биометрической аутентификации по голосу или лицу продолжают расти, крайне важно, чтобы все пользователи внедрили несколько факторов аутентификации и надежные уникальные пароли для своих учетных записей, чтобы ограничить радиус взрыва, если один метод аутентификации нарушена», — сказал он TechNewsWorld.

Проблемы метавселенной

«Я не люблю класть все яйца в одну корзину, — добавил вице-президент Trend Micro по инфраструктурным стратегиям Билл Малик. «Биометрия — это хорошо и полезно, но наличие дополнительного фактора аутентификации придает мне гораздо больше уверенности».

«Для большинства приложений биометрические данные и PIN-код подходят», — сказал он TechNewsWorld. «Когда биометрические данные используются отдельно, их очень легко подделать».

Сбор биометрических данных станет еще большей проблемой, когда метавселенная станет более популярной.

«Когда вы попадете в метавселенную, все станет еще хуже», — сказал он. «Вы надеваете эти очки за 1500 долларов, которые не только дают вам реалистичное представление о мире, но и постоянно отслеживают ваши микровыражения, чтобы выяснить, что вам нравится и не нравится в мире, который вы видите».

Тем не менее, он не беспокоится о том, что дополнительные биометрические данные используются цифровыми головорезами для создания клонов дипфейков. «Хакеры ленивы, и они получают почти все, что им нужно, с помощью простых фишинговых атак», — заявил он. «Поэтому они не собираются тратить много денег на суперкомпьютер, чтобы кого-то клонировать».

Биометрия, привязанная к устройству

Другой способ обеспечить биометрическую аутентификацию — привязать ее к аппаратному обеспечению. Если биометрические данные зарегистрированы на конкретном устройстве, их можно использовать только на этом устройстве для аутентификации пользователя.

«Вот как сегодня работают биометрические продукты Apple и Google — при использовании Face ID проверяются не только биометрические данные», — сказал Рид МакГинли-Стемпель, соучредитель и генеральный директор Stytch, компании по аутентификации без пароля в Сан-Франциско.

«Когда вы фактически выполняете проверку Face ID на своем iPhone, это проверяет, соответствует ли текущая биометрическая проверка биометрической регистрации, которая хранится в защищенном анклаве вашего устройства», — сказал он TechNewsWorld.

«В этой модели, — продолжил он, — угроза того, что кто-то сможет получить доступ к вашим фотографиям или вашим отпечаткам пальцев, не поможет им, если они также не контролируют ваше физическое устройство, что является очень крутым прорывом для злоумышленников».

Потеря контроля над нашими данными

Как пользователи, мы теряем контроль над нашими данными и их будущим использованием, а риски, связанные с платформами, которые мы используем каждый день, не совсем понятны рядовым пользователям, отмечается в отчете Trend Micro.

Данные из социальных сетей уже используются правительствами и даже стартапами для извлечения биометрических данных и создания моделей идентификации для камер наблюдения.

Тот факт, что наши биометрические данные нельзя изменить, означает, что в будущем такая сокровищница данных будет все более полезной для преступников, добавил он.

Будь то будущее на пять или 20 лет вперед, данные доступны уже сейчас, говорится в сообщении. Мы обязаны перед собой в будущем принять меры предосторожности сегодня, чтобы защитить себя в мире завтрашнего дня». ***(John P. Mello Jr. Report Finds Biometric Data Threatened by Social Media // ECT News Network, Inc. (https://www.technewsworld.com/story/report-finds-biometric-data-threatened-by-social-media-177270.html). 19.10.2022).***

***

«Многие дома в США набиты умными домашними гаджетами, что удобно с точки зрения удобства, но в меньшей степени с точки зрения безопасности. Известно, что устройства «умный дом» и «интернет вещей» (IoT) имеют проблемы с безопасностью, и правительство США обращает на это внимание. Начиная со следующего года, сотрудники государственных учреждений начнут программу по образцу Energy Star для маркировки продуктов, которые соответствуют определенным стандартам безопасности.

Белый дом объявил об этом после встречи с производителями устройств, такими как Google, Samsung и Amazon, а также с представителями ассоциаций потребительских товаров. Со стороны правительства присутствовали председатель FCC Джессика Розенворсел, национальный директор по кибербезопасности Крис Инглис и сотрудник Белого дома по кибербезопасности Энн Нойбергер. Это последовало за объявлением в 2021 году о том, что Белый дом поручил NIST и FCC изучить пилотную программу для меток кибербезопасности.

Речь идет не только о обеспечении безопасности вашей домашней сети — уязвимости IoT могут оказывать влияние на безопасность Интернета в целом. Они могут позволить онлайн-преступникам завладеть устройствами, которые они затем используют для запуска атак типа «отказ в обслуживании» (DoS) на веб-сайты и службы, в том числе находящиеся под управлением правительства.

Первоначально маркировка будет сосредоточена на устройствах, которые считаются наиболее потенциально опасными, таких как маршрутизаторы и камеры видеонаблюдения. Если любое из этих устройств проникнет, злоумышленник может собрать огромное количество информации и шпионить за домом. Позже программа будет расширена до большего количества устройств IoT, даже самые простые из которых могут предоставить поверхность атаки для того, чтобы кто-то мог получить доступ к вашей домашней сети. Конечно, умные колонки будут на дорожной карте — эти устройства должны нажимать на определенные фразы пробуждения, но их можно использовать для прослушивания чего угодно, если они будут скомпрометированы серьезной уязвимостью в системе безопасности.

Программа маркировки будет контролироваться Национальным институтом стандартов и технологий (NIST) и Федеральной торговой комиссией (FTC), которые будут работать над разработкой стандартов, которые будут использоваться для тестирования гаджетов для умного дома. Этикетки будут «признаны во всем мире», что бы это ни значило. Для людей, которые хотят приобрести продукт, на который распространяется схема маркировки, будет штрих-код, который вы можете отсканировать, чтобы получить подробную информацию о стандартах оценки, шифровании/безопасности данных и защите от уязвимостей». ***(Ryan Whitwam. US to Begin Giving IoT Devices a Cybersecurity Rating Starting in 2023 // Ziff Davis, LLC (https://www.extremetech.com/electronics/340417-us-to-begin-giving-iot-devices-a-cybersecurity-rating-starting-in-2023). 24.10.2022).***

***

«Автомобильная промышленность начиналась как механический бизнес и существует уже более 100 лет. Однако за последнее десятилетие в отрасли произошла цифровая трансформация, которая включает в себя всплеск подключенных транспортных средств, уникальные ADAS и функции безопасности, а также появление автономных и электрических транспортных средств. Транспортные средства, которые когда-то были строго механическими, теперь имеют больше строк кода, чем Boeing 747, что, по сути, делает их iPhone на колесах.

«Ни в какой другой отрасли не происходит таких быстрых технологических изменений, как в автомобильной, — говорит Зоран Филипи, заведующий кафедрой автомобильного машиностроения Международного центра автомобильных исследований Университета Клемсона. «Это обусловлено необходимостью соблюдения надвигающихся, еще более строгих норм выбросов CO2 и критериев, при этом поддерживая беспрецедентный темп прогресса в развитии автоматизации и информационно-развлекательных систем, а также оправдывая ожидания клиентов в отношении производительности, комфорта и полезности».

Потребительский спрос и цифровая трансформация, происходящая на многих рынках, стимулируют разработку чрезвычайно сложных транспортных средств, состоящих из множества электронных блоков управления, миллионов строк кода и сложных автоматизированных функций, которые никогда не были характерны для старых автомобилей. Всего десять лет назад в дорогих автомобилях было около 100 ЭБУ с примерно 100 миллионами строк кода. Сегодня такие автомобили, как BMW 7-й серии, могут иметь 150 ЭБУ, встроенных по всему автомобилю.

Эта проблема усугубляется всплеском разработки электромобилей, которые еще более уязвимы для кибератак, чем автомобили на топливе, поскольку они имеют более широкую поверхность атаки. Потребность в кибербезопасности для защиты электромобилей становится все более серьезной проблемой, поскольку речь идет не только об автомобиле, но и о защите всей экосистемы, включая автомобиль, зарядную станцию и сеть, которые очень уязвимы для вредоносных атак.

«Поскольку новые автомобили и электромобили стали более подключенными и автоматизированными, чем когда-либо прежде, они также подвергаются более высокому риску кибератак. Транспортные средства EV не обязательно должны подвергаться большему риску, чем современные автомобили с ДВС — просто транспортное средство EV для максимизации своих характеристик, естественно, будет использовать самую современную электрическую архитектуру, включая все виды подключения, которые по своей природе могут создать более высокий уровень риска», — говорит Стив МакЭвой, вице-президент автомобильного подразделения Expleo.

Поскольку подключение и программное обеспечение значительно повышают ценность автомобиля, потребители могут задаться вопросом, почему защита кибербезопасности не является приоритетом при покупке нового автомобиля. Ведь никто не оставит компьютер или телефон уязвимыми для кибератак. Транспортное средство требует еще большей киберзащиты, учитывая катастрофические последствия фактического взлома и количество людей, которые могут пострадать, если транспортное средство потеряет управление на дороге.

Кибербезопасность подключенных транспортных средств — непростая тема; разработка автомобиля состоит из множества сложных этапов, включающих проектирование, разработку, испытания, производство и постпроизводство. Реализация безопасности на каждом из этих этапов требует различных инструментов, решений и команд от разных заинтересованных сторон и часто выполняется вручную. Защита каждой из этих фаз обычно осуществляется изолированно, посредством утомительных ручных процессов, которые подвержены человеческим ошибкам. Кроме того, при разработке автомобиля многие компании несут ответственность за один аспект автомобиля и часто неэффективно взаимодействуют друг с другом, что создает множественные разрозненности и делает автомобиль уязвимым для кибератак.

Проблема заключается в разрозненных процессах обеспечения безопасности, из-за которых легко пропустить угрозу безопасности и невозможно получить полный обзор всего ландшафта безопасности. Это все равно, что иметь ручную сборочную линию по сравнению с автоматизированным оборудованием, которое производит автомобиль. Кроме того, работа в силосах довольно затратна, поскольку требует много ручной работы, что позже отражается на ценах, которые платят потребители.

Сегодня этот процесс кибербезопасности стал автоматизированным с помощью инструментов управления кибербезопасностью, которые устраняют разрыв между фазами и различными командами и защищают всю экосистему автомобиля. Вся автомобильная экосистема быстро осознает важность единой автоматизированной и централизованной платформы DevOps для обеспечения кибербезопасности, которая способствует делегированию полномочий и совместной работе, чтобы преодолеть разрозненный барьер и управлять кибербезопасностью во всей экосистеме с помощью прозрачного единого подхода.

Сто лет назад никто бы не предсказал, что в наших автомобилях будет больше программного обеспечения, чем почти в любой другой технологии, которую мы используем сегодня, или что промышленность сдвинется в сторону электрификации. Но за передовыми технологиями автомобильного мира должно стоять решение по обеспечению безопасности, которое могло бы защитить прорывной прогресс, к которому мы стремимся». ***(Roy Fridman. Cybersecurity Risks Facing Connected and Electric Vehicles // Informa USA, Inc. (https://www.wardsauto.com/industry-news/cybersecurity-risks-facing-connected-and-electric-vehicles). 31.10.2022).***

***

Кіберзлочинність та кібертероризм

«Офіційний гаманець платформи невзаємозамінних токенів (NFT) LiveArtX зламали хакери, а випущена нею серія NFT Seven Treasures впала в ціні на 84% за 24 години. Про це у своєму Твіттер повідомив китайський журналіст Колін Ву.

Журналіст також нагадав, що раніше LiveArtX отримала понад $4.5 млн у вигляді стратегічних інвестицій на чолі з Animoca Brands, BNB Chain Fund і KuCoin.

На момент публікації жодних нових оголошень LiveArtX у Twitter або Telegram не було. Команда платформи заявила, що докладає всіх зусиль для зниження негативних наслідків злому.

Метаморфічного описують як «генеративний арт-проект, який відправляє вас у подорож природою».

NFT-колекція Seven Treasures художника Хуан Юсіна, що складається з 997 невзаємозамінних токенів, була випущена у вересні 2022 року. Ще 15 жовтня її середня ціна становила 1.14 ETH (приблизно $1 500), але на поточний момент вартість впала до 0.36 ETH.

Раніше володар премії «Оскар» Ентоні Хопкінс випустив та розпродав свою дебютну колекцію невзаємозамінних токенів, що складалася з 1 000 NFT». ***(Писаренко Максим. Хакери зламали гаманець NFT-платформи LiveArtX // cryptomisto.com (https://cryptomisto.com/khakery-zlamaly-hamanets-nft-platformy-liveartx/). 17.10.2022).***

***

«Компанія ESET представляє рейтинг найбільш поширених кіберзагроз за травень-серпень 2022 року. За цей період зросла кількість загроз для Android та число фішингових листів на тему доставки. Крім цього, Україна опинилася у п'ятірці країн, на які була націлена найбільша кількість атак програм-вимагачів.

На поширення загроз у цей період значно вплинуло стрімке падіння курсів криптовалют. Зокрема кіберзлочинці почали частіше викрадати криптовалюту замість її прихованого майнінгу, на що вказує зростання кількості фішингових листів на тему криптовалюти та загроз для її крадіжки.

Також різко знизилася кількість атак на протокол віддаленого робочого столу (RDP). Навіть попри падіння найбільше RDP-атак відбувалося з російських IP-адрес.

Програми-вимагачі продовжують атакувати Україну

Незважаючи на загальне зменшення активності програм-вимагачів, спостерігалося кілька піків їх активності. Один з них у червні був частково спричинений розповсюдженням в Україні версій шкідливої програми MSIL/Filecoder. Ця загроза є першою програмою-вимагачем з відкритим кодом. Також Україна опинилася на 5 місці серед кількості атак програм-вимагачів після США, Китаю, Ізраїлю та росії.

Зловмисники маскуються під відомі компанії для обману користувачів

Кількість фішингових листів на тему доставки зросла у 6 разів порівняно з попереднім періодом. Також зловмисники використовували тему фінансів та соцмереж для поширення фішингових загроз. За даними ESET, найчастіше хакери маскувались під компанію Facebook, зокрема використовуючи Messenger для надсилання небезпечних посилань. Таким чином кіберзлочинці заманювали користувачів на фішингові сторінки, переконуючи їх ввести облікові дані свого акаунту.

Загалом кількість унікальних фішингових URL-адрес, які продукти ESET блокували щодня, у середньому досягала 38 000 за період травень-серпень 2022 року.

Хакери викрадають банківські дані та криптовалюту

Серед загроз для викрадення даних збільшилась кількість банківських шкідливих програм майже на 10%. Найпоширенішою шкідливою програмою у цій категорії є Magecart, яка здатна викрадати дані банківських карток у онлайн-покупців. Тоді як серед загроз для викрадення інформації найбільш активним залишилося саме шпигунське програмне забезпечення.

Крім цього, зловмисники все частіше вдаються до викрадення криптовалюти, а не до її незаконного майнінгу на пристроях жертв. Зокрема на 50% зросло число загроз для крадіжки цифрових коштів. Очікується, що і надалі їх активність буде рости разом з випадками прихованого майнінгу в браузері під час відвідування торент-сайтів та піратських ресурсів.

Шпигунські програми атакують користувачів Android та macOS

За даними телеметрії ESET, загальна кількість загроз для Android збільшилась на 9,5%. Найактивнішими на цій операційній системі були шпигунські програми та приховані додатки.

Це зростання спричинено доступністю наборів шпигунських програм для Android на різноманітних онлайн-форумах. Таким чином навіть зловмисники-аматори можуть безкоштовно знайти трояни та розгорнути їх без певного рівня технічних навичок.

Незважаючи на зменшення активності загроз для macOS, атаки на користувачів цієї платформи продовжуються. Зокрема спеціалісти ESET виявили новий бекдор для macOS під назвою CloudMensis, який шпигує за користувачами. Загроза використовує виключно публічні служби хмарних сховищ для обміну даними зі своїми авторами.

Зловмисники продовжують використовувати уразливості

Активність ботнета Mozi, який використовує застарілі уразливості, а в минулому році до складу якого входило близько 600 000 ботів, почала повільно зменшуватися. Це спричинило появу нових ботнетів на базі Mirai, які стають дедалі потужнішими та поширенішими, експериментуючи з новими та відомими уразливостями. Саме тому регулярне оновлення всіх пристроїв є досить важливим для захисту від подібних атак.

Загалом, щоб не стати жертвою будь-якого виду кіберзагроз, варто дотримуватись базових правил кібербезпеки, зокрема використовувати складні паролі та багатофакторну автентифікацію, подбати про безпеку мобільного пристрою, а також забезпечити надійний захист ноутбука та пристроїв Інтернету речей. ***(Герман Богапов. Україна опинилася у п'ятірці цілей програм-вимагачів // HiTech.Expert (https://expert.com.ua/152752-ukra%d1%97na-opinilasya-u-pyatirci-cilej-program-vimagachiv.html). 06.10.2022).***

***

«В 21 веке произошло резкое увеличение количества и изощренности угроз кибербезопасности. Вот 7 самых больших угроз, о которых должны знать предприятия и частные лица.

Программы-вымогатели как услуга

В последние несколько лет программы-вымогатели стали одним из самых популярных инструментов киберпреступников. Программы-вымогатели как услуга

(RaaS) — это новая бизнес-модель, которая позволяет любому, у кого практически нет технических знаний, запускать собственные атаки программ-вымогателей. Все, что им нужно, это зарегистрироваться на платформе RaaS и заплатить комиссию (обычно процент от выкупа, который они собирают).

RaaS представляет собой растущую угрозу, потому что он позволяет любому начать атаки. Киберпреступники могут атаковать любую организацию, независимо от ее размера и ресурсов. А поскольку платформы RaaS обычно берут на себя все технические детали, атаки программ-вымогателей можно запускать без особых усилий.

За последние несколько лет произошло несколько громких атак программ-вымогателей, которые попали в заголовки. В мае 2017 года атака программы-вымогателя WannaCry затронула более 200 000 компьютеров в 150 странах. Атака нанесла ущерб на миллиарды долларов и нарушила работу критически важной инфраструктуры, такой как больницы и банки. В декабре 2017 года атаке вируса-вымогателя NotPetya подверглись более 10 000 организаций в более чем 60 странах. Атака нанесла ущерб на миллиарды долларов и нарушила работу критически важной инфраструктуры, такой как больницы и банки.

Атаки программ-вымогателей стали более изощренными и целенаправленными. Киберпреступники теперь используют платформы RaaS для запуска целевых атак против определенных организаций. Эти атаки часто называют атаками «целевого фишинга», поскольку они используют тщательно составленные электронные письма, чтобы заставить людей переходить по вредоносным ссылкам или открывать вложения, которые устанавливают на их компьютеры программы-вымогатели.

Организации любого размера должны знать об угрозе программ-вымогателей и принимать меры для своей защиты. Это включает в себя наличие надежного плана резервного копирования и восстановления на случай атаки.

Интернет вещей

Интернет вещей (IoT) — это сеть физических устройств, транспортных средств, бытовой техники и других предметов, в которые встроена электроника, программное обеспечение, датчики и средства связи, позволяющие этим объектам подключаться и обмениваться данными.

Интернет вещей — это растущий рынок, и с каждым днем все больше и больше устройств подключаются к Интернету. Однако это также создает новые риски безопасности. Поскольку устройства IoT часто подключены к Интернету, их можно взломать и использовать для проведения атак.

В октябре 2016 года была запущена массовая распределенная атака типа «отказ в обслуживании» (DDoS) против службы Dyn DNS с использованием сети IoT-устройств, зараженных вредоносным ПО Mirai. Атака вызвала массовые сбои в работе интернета и отключила основные веб-сайты, такие как Twitter и Netflix.

Интернет вещей представляет собой уникальную проблему для безопасности, поскольку существует множество различных типов устройств, которые могут быть подключены к Интернету. У каждого типа устройств есть свои риски безопасности и уязвимости. И по мере того, как количество устройств IoT продолжает расти, увеличиваются и возможности киберпреступников для их использования.

Облачная безопасность

Облако стало неотъемлемой частью бизнеса для многих организаций. Он предлагает ряд преимуществ, таких как гибкость, масштабируемость и экономия средств. Однако облако также создает новые риски безопасности.

Одна из самых больших угроз безопасности, связанных с облаком, — это утечка данных. Поскольку данные хранятся удаленно на серверах, они более уязвимы для атак. Кроме того, поставщики облачных услуг часто имеют доступ к данным клиентов, что создает еще одну потенциальную точку входа для хакеров.

Еще одна угроза безопасности, связанная с облаком, — это злоумышленники. Поскольку поставщики облачных услуг имеют доступ к данным клиентов, они потенциально могут использовать эти данные не по назначению или продать их третьим лицам.

Кроме того, сотрудники поставщиков облачных услуг также могут быть принуждены к предоставлению хакерам доступа к данным клиентов.

Организации должны знать о рисках безопасности, связанных с облаком, и предпринимать шаги для собственной защиты. Сюда входит шифрование данных при передаче и хранении, а также использование многофакторной аутентификации.

Вредоносное ПО для майнинга криптовалют

Вредоносное ПО для майнинга криптовалюты — это тип вредоносного ПО, которое заражает компьютеры и использует их ресурсы для добычи криптовалюты. Это может замедлить работу зараженного компьютера и потреблять много электроэнергии. В некоторых случаях это может даже повредить компьютер.

Вредоносное ПО для майнинга криптовалюты часто доставляется через фишинговые электронные письма или вредоносные веб-сайты. После того, как вредоносное ПО установлено на компьютер, его может быть трудно удалить.

Организации должны знать об угрозе вредоносных программ для майнинга криптовалюты и принимать меры для защиты своих компьютеров. Это включает в себя использование антивирусного программного обеспечения и отказ от перехода по ссылкам или открытия вложений из неизвестных источников.

Внутренние угрозы

Внутренняя угроза — это угроза организации, исходящая изнутри. Это может быть сотрудник, подрядчик или третье лицо с авторизованным доступом к системам и данным организации.

Внутренние угрозы могут возникать, когда кто-то со злым умыслом получает доступ к системам и данным организации. Они также могут возникать, когда кто-то с авторизованным доступом злоупотребляет своими привилегиями.

Организации должны знать об угрозе внутренних угроз и предпринимать шаги, чтобы защитить себя. Это включает в себя мониторинг активности пользователей, требование многофакторной аутентификации и обучение сотрудников безопасности.

Квантовые вычисления

Квантовые вычисления — это тип вычислений, использующий квантово-механические явления, такие как суперпозиция и запутанность, для выполнения операций с данными. Квантовые компьютеры способны решать определенные задачи гораздо быстрее, чем классические компьютеры.

Развитие квантовых компьютеров представляет угрозу для традиционной криптографии. Это связано с тем, что квантовые компьютеры могут легко разложить на множители большие числа, что является основой многих криптографических алгоритмов.

Организации должны знать об угрозе квантовых вычислений и предпринимать шаги для защиты своих данных. Это включает в себя использование квантово-устойчивой криптографии и хранение данных в нескольких местах.

DDoS-атаки

DDoS-атака — это тип атаки, направленный на то, чтобы сделать компьютер или сетевой ресурс недоступным для пользователей. Это делается путем переполнения цели трафиком из нескольких источников.

DDoS-атаки могут быть невероятно разрушительными и нанести значительный ущерб организации. От них также может быть трудно защититься, поскольку злоумышленник может использовать несколько компьютеров или устройств для генерации трафика.

Организации должны знать об угрозе DDoS-атак и принимать меры для своей защиты. Это включает в себя наличие плана защиты от DDoS-атак и работу с надежным поставщиком защиты от DDoS-атак.

Вывод

Угрозы кибербезопасности постоянно развиваются, и организациям необходимо быть в курсе последних угроз, чтобы защитить себя. Киберпреступность и кража данных в настоящее время представляют собой серьезную глобальную проблему, и ставки только растут. По мере того, как мы движемся в будущее, очень важно, чтобы организации предпринимали шаги для защиты от этих угроз». ***(Anas Baig. 7 Biggest Cybersecurity threats of the 21st century // AT&T Cybersecurity Services (https://cybersecurity.att.com/blogs/security-essentials/7-biggest-cybersecurity-threats-of-the-21st-century). 06.10.2022).***

***

«Последняя сессия парламента в Словакии была прервана на значимость после проникновения с кибербезопасностью, которая выявила ущерб ИТ-системам органов.

В четверг спикер парламента Борис Коллар провел телевизионный брифинг, как выяснилось, что голосование будет опубликовано в связи с проведением расследования.

«Мы обнаруживаем объекты представдяющие опасность… Из каких-то точек поглощают сигнал, который блокирует наши системы, компьютеры, мы даже не можем обслуживать законодателей в нашей столовой», — сказал Коллар журналистам на телевизионном брифинге.

Позже Управление национальной безопасности (NSB) опубликовало заявление, подтверждающее, что оно получило отчет об «инциденте кибербезопасности», который произошел в Национальном совете.

Они отказались предоставить более подробную информацию о ситуации и не ответили на запросы о комментариях.

Официальные лица предоставили противоречивую информацию об инциденте, отметив, что Нацсовет «сообщил, что утром зафиксировал перебои в работе ИТ-сервисов», которые прервали заседания. Но представитель НБУ Питер Хабара предупредил, что инцидент мог не быть кибератакой, а мог быть просто сбоем, объяснив, что кибератака является «преднамеренным действием».

«Первоначальный анализ этого инцидента кибербезопасности показал, что сетевое соединение ведет себя ненормально. В результате пострадала функциональность всех компонентов, в том числе устройств для голосования, работающих в сетевой инфраструктуре СР СР», — заявила пресс-секретарь TASR Михаэла Юрцова.

Правоохранительные органы страны сейчас работают с Бюро национальной безопасности над расследованием.

Коллар назвал инцидент «очень серьезным» и отменил все заседания до 8 ноября, отметив, что если бы вопрос был решен быстрее, парламент мог бы собраться на следующей неделе.

Некоторые оппозиционные партии в Словакии поставили под сомнение решения и сам инцидент. Оппозиционный политик Анна Земанова сказала Euractiv, что отсрочка до 8 ноября была «абсурдной», и заявила, что нападение могло быть инсценировано, потому что несколько политиков от правящей партии отсутствовали, когда они пытались протолкнуть важный закон.

Словакия стала последней страной, столкнувшейся с кибератаками на свой парламент после инцидентов в Румынии, Италии, Литве, Норвегии, Польше, Финляндии и Латвии. На прошлой неделе также были атакованы правительственные веб-сайты Болгарии, причем официальные лица связывали инцидент с пророссийской хакерской группой. Агентство Reuters сообщило, что парламент Польши также подвергся кибератакам в четверг». ***(Jonathan Greig. Votes in Slovakia's parliament suspended after alleged 'cybersecurity incident' // The Record by Recorded Future (https://therecord.media/votes-in-slovakias-parliament-suspended-after-alleged-cybersecurity-incident/). 31.10.2022).***

***

«Федеральное управление кибербезопасности Германии предупредило во вторник, что программы-вымогатели, политический взлом и другие угрозы кибербезопасности, с которыми сталкивается страна, «выше, чем когда-либо».

В своем годовом отчете ведомство заявило, что за уровень угрозы отвечает продолжающаяся преступная деятельность, наряду с атаками, связанными с российским вторжением в Украину, но также предупредил, что одним из факторов является недостаточное качество ИТ и программного обеспечения.

Хотя «всеобъемлющая кампания нападения на немецкие цели не была очевидна», заявило Федеральное управление информационной безопасности (BSI), в Германии произошло «накопление мелких инцидентов и кампаний хактивизма в связи с агрессивной войной России против Украины».

Среди них кибератака на спутниковую компанию Viasat, которая произошла за час до вторжения России 24 февраля. Соединенные Штаты, Великобритания и Европейский Союз приписали нападение России — хотя они не задействовали

конкретное агентство в стране — в то время как ЕС и член НАТО Эстония приписали это ГРУ, главному разведывательному управлению российской армии.

Атака на Viasat была направлена на то, чтобы ухудшить способность украинского правительства и военных общаться, однако она также заблокировала маршрутизаторы для систем удаленного обслуживания, используемых немецкими ветряными турбинами, отключив 5800 из них. Viasat заявила, что десятки тысяч ее терминалов были непоправимо повреждены и нуждались в замене.

«Атака хактивистов на немецких дилеров нефтепродуктов с российской материнской компанией» также упоминается BSI, предположительно ссылаясь на мартовских анонимных хакеров, укравших информацию у немецкой дочерней компании государственной российской нефтяной компании «Роснефть».

Годовой отчет публикуется на фоне скандала в BSI, который последовал за сатирическим телешоу, в котором высказывались обвинения в адрес ныне отстраненного от должности главы агентства Арне Шенбома, утверждавшего, что он связан с бизнесом, связанным с российскими спецслужбами.

Хотя не было представлено никаких доказательств того, что работа офиса была каким-либо образом скомпрометирована или что Шёнбом действовал ненадлежащим образом, министерство внутренних дел Германии заявило, что обвинения «навсегда подорвали необходимое доверие общественности к нейтральности и беспристрастности поведения его офиса как Президент самого важного немецкого органа по кибербезопасности», объясняя свое отстранение.

По данным BSI, инциденты с программами-вымогателями и кибервымогательством остаются наиболее серьезной угрозой для Германии. «Платежи как в виде выкупа, так и за молчание» продолжают расти, поскольку накануне российского вторжения произошла волна инцидентов, затронувших нефтяной и химический сектор страны, а также ее соседей, что вызвало опасения, что они были частью преступной деятельности. кампания, координируемая российской разведкой. Бельгийский чиновник преуменьшил для The Record опасения, что атаки были связаны между собой.

Атака программы-вымогателя на муниципалитет Ангальт-Биттерфельд также вынудила региональные власти объявить чрезвычайное положение и призвать немецкие вооруженные силы для поддержки. «Услуги, связанные с гражданами, были недоступны или доступны лишь частично более 207 дней», — сообщает BSI.

Д-р Герхард Шабхюзер, вице-президент BSI, в настоящее время исполняющий обязанности Шенбома, сказал: «Ситуация с угрозами в киберпространстве напряженная, динамичная и разнообразная и поэтому выше, чем когда-либо. В цифровом мире благополучие населения больше, чем когда-либо, зависит от того, насколько хорошо мы подготовлены к инцидентам в области ИТ-безопасности».

Нэнси Файзер, министр внутренних дел, которая обязалась расширить BSI до центрального офиса, добавила: «Ситуация с киберугрозами, которая продолжает нарастать после агрессивной войны России в Украине, требует стратегической перестройки и значительных инвестиций. в нашей кибербезопасности». ***(Alexander Martin. German cyber agency warns threat situation is 'higher than ever' // The Record by Recorded Future (https://therecord.media/german-cyber-agency-warns-threat-situation-is-higher-than-ever/). 25.10.2022).***

***

«Enercity, один из крупнейших поставщиков муниципальной энергии в Германии, подтвердил, что в среду утром он подвергся кибератаке.

Ганноверская компания заявила, что ее системы безопасности «отреагировали немедленно» и что «большего ущерба компании» удалось избежать.

Enercity подтвердила, что продолжит поставлять энергию клиентам, пояснив, что ее операционные технологии и критическая инфраструктура не пострадали. «Наши сети и электростанции стабильны, и безопасность поставок гарантирована», — заявили в компании.

Однако атака повлияла на обслуживание клиентов, доступность которого ограничена. В компании добавили: «Не все ИТ-системы в настоящее время можно использовать в полной мере, а это значит, что у них могут быть незначительные ограничения».

Атака произошла через несколько дней после того, как федеральное управление кибербезопасности Германии предупредило, что угроза, с которой столкнулась страна, «выше, чем когда-либо»…

Бельгийский чиновник преуменьшил обеспокоенность The Record по поводу того, что атаки были связаны, однако в обвинительных актах против российских киберпреступников, таких как Максим Якубец, утверждается, что Федеральная служба безопасности России время от времени обращалась к отечественным киберпреступникам для зарубежных операций». ***(Alexander Martin. Major German energy supplier hit by cyberattack // The Record by Recorded Future (https://therecord.media/major-german-energy-supplier-hit-by-cyberattack/). 27.10.2022).***

***

«Второй по объему производитель меди в мире заявил, что восстанавливается после кибератаки, которая вынудила его несколько ИТ-систем.

Немецкая фирма Aurubis не ответила на запрос о цене, но в пятницу опубликовала заявление, в котором говорилось, что компания столкнулась с кибератакой, которая «очевидно, была частью более крупной атаки на металлургическую и горнодобывающую промышленность».

«В результате многие системы на объектах Aurubis пришлось отключить и отключить от Интернета в качестве превентивной меры. Производство в значительной степени может быть сохранено», — заявили в компании. «В настоящее время оценивается степень воздействия на Группу. Кроме того, Aurubis тесно сотрудничает со следственными органами».

Аурубис не может сказать, когда возобновится работа систем производства и закупок сырья.

Но компания смогла сохранить в рабочем состоянии производственные и природоохранные объекты на плавильных площадках и отметила, что начала обрабатывать процессы, связанные с входящими и исходящими товарами, вручную.

«В настоящее время внедряются переходные решения, чтобы со следующей недели снова предоставить бизнес-партнерам полный спектр услуг компании», — пояснили в компании.

Аурубис не ответил на вопросы о том, была ли это атака программы-вымогателя.

Кибератака произошла всего через два дня после того, как атаке подверглась Enercity, один из крупнейших муниципальных поставщиков электроэнергии в Германии.

В Германии произошло несколько кибератак и инцидентов с программами-вымогателями, затронувшими промышленные компании.

Фирма по кибербезопасности Dragos на прошлой неделе опубликовала отчет, в котором говорится, что в третьем квартале 2022 года в Европе было совершено не менее 42 атак промышленных программ-вымогателей.

Анализируя атаки на производственный сектор, исследователи Dragos обнаружили, что компании, связанные с металлическими изделиями, лидировали в 12 атаках программ-вымогателей». ***(Jonathan Greig. World's second largest copper producer recovering from cyberattack // The Record by Recorded Future (https://therecord.media/worlds-second-largest-copper-producer-recovering-from-cyberattack/). 31.10.2022).***

***

«Национальный парламент Греции завершил расследование использования шпионского ПО службами безопасности. Только не спрашивайте законодателей, каковы общие выводы.

Политические партии поздно вечером в понедельник представили результаты специального парламентского расследования, которое было организовано для расследования шпионского скандала, охватившего правительство с тех пор, как появились обвинения в том, что правительство шпионит за политической оппозицией.

Споры начались в августе, когда правительство признало, что оно прослушивало телефон лидера оппозиции Никоса Андрулакиса — шаг, который он назвал законным, но неправильным. Два высокопоставленных правительственных чиновника, начальник аппарата правительства и глава Национальной разведывательной службы (ЕНС) страны, потеряли свои должности. Затем он быстро превратился в шпионский триллер, в котором скандальная шпионская программа Predator была установлена на телефоны постоянно расширяющейся сети политиков и журналистов. Но правительство заявило, что не имеет отношения к этим более широким делам или даже не знает о них.

После нескольких недель слушаний правящая партия «Новая демократия» на этой неделе заявила, что считает вопрос закрытым, удвоив свои аргументы в защиту того, что слежка была признана законной по результатам расследования.

«Новая демократия» также заявила, что слушания доказали отсутствие связи между шпионским ПО Predator, обнаруженным в телефонах оппозиционеров и журналистов, с одной стороны, и шпионской службой страны, с другой. «Обвинения оппозиции в скандале вокруг юридической слежки за телефоном Андрулакиса и

деятельности Национальной разведывательной службы (ЕНС) развалились, как карточный домик», — говорится в их заключении.

Но оппозиционные партии, в том числе партия Андрулакиса «Пасок» и левая партия СИРИЗА, категорически не согласились, обвинив правительство в серьезном сокрытии в попытке отмахнуться от доказательств, изложенных в ходе расследования.

СИРИЗА обвинила партию «Новая демократия», которая имеет большинство в расследовании, в том, что она не позволила явиться на слушания ключевым свидетелям, в том числе журналистам, чьи телефоны были прослушаны или которые расследовали этот вопрос, а также государственным чиновникам из полиции и греческой тайной полиции. оказание услуг. Главной заботой правительства была «не правда и раскрытие дела, а сокрытие и исчезновение улик, которые могли привести к привлечению не только политической, но и возможной уголовной ответственности».

«Необходимо дальнейшее расследование дела как греческим парламентом всеми доступными парламентскими средствами, включая комитет предварительного расследования, так и системой уголовного правосудия», — заявила СИРИЗА». ***(Nektaria Stamouli. Greek spyware inquiry ends in stalemate // POLITICO (https://www.politico.eu/article/greek-spyware-inquiry-ends-in-stalemate/). 11.10.2022).***

***

«Новости полны историй о нарушениях кибербезопасности на всех уровнях правительства, и федеральные агентства являются особенно популярной мишенью. Фактически, отчет Microsoft Digital Defense показал, что 46 процентов всех кибератак на уровне государства за год были направлены на организации США, а 48 процентов атак были направлены на правительственные учреждения.

К сожалению, эти атаки становятся все более опасными и дорогостоящими. В отчете IBM «Стоимость утечки данных за 2022 год» поясняется, что средняя стоимость взлома в государственном секторе составляет 2,07 миллиона долларов. Более того, среднее время обнаружения и локализации нарушения составило 277 дней, что привело к увеличению расходов и увеличению рисков.

Сотрудники федерального агентства и отраслевые эксперты постоянно обсуждают, как наилучшим образом защитить государственные системы от постоянной угрозы кибератак, особенно по мере того, как поверхность атаки расширяется, а агентства становятся более уязвимыми. И хотя существует множество аспектов проблем, с которыми сталкиваются организации, универсального решения не существует. Однако ясно одно: федеральному правительству пора переосмыслить свой подход к кибератакам и взломам с помощью более устойчивой стратегии.

Запоздалый сдвиг мышления

Агентства часто имеют дело с кибератаками и взломами по мере необходимости. Когда ИТ-персонал обнаруживает нарушение, специалисты по кибербезопасности мобилизуются, чтобы заблокировать атаку и смягчить ущерб. Этого подхода было достаточно в те дни, когда кибератаки были относительно

редкой проблемой. Но сегодняшние федеральные агентства уязвимы и находятся под постоянными атаками.

Хотя наши средства защиты предназначены для предотвращения доступа или проникновения большинства угроз в правительственные системы (вспомните средства защиты периметра, такие как брандмауэры, виртуальные частные сети и т. д., которые пытаются не допустить злоумышленников), неизбежной реальностью нашего сверхсвязанного мира является то, что некоторые атаки нарушают через.

Агентства должны переключить свое мышление, политику и процедуры с невыполнимой задачи предотвращения всех нарушений на поиск способов ограничения ущерба от успешных атак. Вместо того, чтобы тратить время и деньги исключительно на предотвращение нарушений, агентства должны сосредоточиться на том, чтобы предполагать, что они произойдут, и сдерживать их, чтобы предотвратить их распространение, тем самым уменьшая ущерб и операционные последствия, которые они могут вызвать. Агентства должны изменить свое мышление, чтобы «предполагать нарушение». Это потребует значительных культурных изменений.

Агентства часто сосредотачиваются на соблюдении, соблюдении правил и отметке каждого пункта в контрольном списке — например, выполнении требований оценочной карты Федерального закона о реформе приобретения информационных технологий (FITARA). Вместо этого эксперты выступают за упреждающий подход, при котором агентства определяют области, в которых кибербезопасность является самой слабой, и выделяют ресурсы для повышения устойчивости в этой области.

Это требует, чтобы федеральное правительство заранее инвестировало больше средств в такие возможности, как прозрачность, чтобы они могли лучше понимать риски, с которыми сталкивается их инфраструктура, сети и системы, и принимать более обоснованные инвестиционные решения на раннем этапе. Однако сегодня большинство агентств не выявляют эти недостатки до тех пор, пока не произойдет нарушение. К тому времени часто бывает слишком поздно. Ни одна система не совершенна; уязвимые места есть в каждой организации. Но если агентство не подготовилось к нарушениям и не разработало стратегию их превентивного сдерживания, то отсутствие подготовки может привести к более серьезным последствиям.

Заблаговременное планирование с упреждающим подходом

Чтобы снизить риск и повысить устойчивость к неизбежным нарушениям, агентства должны планировать заранее. Им необходимо более активно подходить к киберфинансированию, учитывая сложный процесс закупок и бюджетирования, которым они должны управлять, и постоянно тратить деньги на кибербезопасность. Этот процесс никогда не будет завершен. Каждый год агентства должны определять области для улучшения и включать их в бюджетные планы. Это делает непрерывным улучшение кибербезопасности частью культуры каждого агентства.

Даже если группы кибербезопасности не уверены, что им нужно будет исправить или какие решения они внедрят, они должны убедиться, что деньги все еще выделены в бюджете. Таким образом, у них будут доступные ресурсы, если они обнаружат брешь в своей защите или если им придется соблюдать требования нового

мандата, такого как исполнительный указ о кибербезопасности (EO) от мая 2021 года.

В EO администрация Байдена отметила, что в течение 60 дней руководители агентств должны «разработать план внедрения архитектуры нулевого доверия… и описать любые такие шаги, которые уже были выполнены, определить действия, которые окажут самое непосредственное влияние на безопасность, и включить график их реализации». Обязательство повсеместно внедрять Zero Trust — лишь один из примеров того, как правительство настаивает на более активном подходе к кибербезопасности (к этому также призывали CISA и OMB).

Zero Trust предполагает, что даже внутреннему сетевому трафику нельзя доверять без предварительной авторизации и аутентификации пользователя и устройства. Это подход к безопасности по принципу «никогда не доверяй, всегда проверяй». С помощью инструментов и технологий с нулевым доверием, таких как сегментация с нулевым доверием (т.е. микросегментация), федеральные агентства могут предотвращать распространение кибератак, изолировать программы-вымогатели и, в конечном итоге, сокращать операционные последствия и денежные потери. Zero Trust с самого начала сокращает поверхность атаки, облегчая федеральным агентствам борьбу с современным развивающимся ландшафтом угроз, максимально увеличивая свой бюджет.

Хотя у агентств есть много способов противостоять современным угрозам кибербезопасности, наиболее устойчивый и устойчивый курс действий — действовать на опережение. Нарушения будут происходить, поэтому предположим, что они уже находятся внутри вашей сети, и внедрите стратегии нулевого доверия, чтобы сдерживать их заранее. Это снижает риск и повышает устойчивость, чтобы агентства могли поддерживать критически важную инфраструктуру, операции и активы в рабочем состоянии и в безопасности». ***(Gary Barlet. PERSPECTIVE: How Expecting Breaches Can Help Federal Agencies Combat Cyberattacks // Homeland Security Today (https://www.hstoday.us/featured/perspective-how-expecting-breaches-can-help-federal-agencies-combat-cyberattacks/). 28.10.2022).***

***

«До атак с помощью квантовых вычислений, которые, как опасаются, полностью сломают современное шифрование в Интернете, остается все еще около десяти лет. Однако многие считают их неизбежностью, и это не помешало злоумышленникам подготовиться заблаговременно. Новый опрос, проведенный Deloitte, показал, что существует непосредственный и значительный киберриск, связанный с атаками типа «собери сейчас, расшифруй позже» (HNDL), когда злоумышленники крадут зашифрованную информацию и просто сидят с ней до тех пор, пока достижения в области квантовых вычислений не сделают взлом ее тривиальной задачей.

Среди прочего, немногим более половины опрошенных ИТ-специалистов говорят, что их организации в настоящее время подвержены риску атак HNDL. Но менее половины в настоящее время занимаются анализом этого возникающего кибер-риска, и около 11% говорят, что должен произойти кибер-инцидент (точка,

когда уже слишком поздно), прежде чем их руководство будет вынуждено что-то предпринять. об угрозе.

Кажущийся далеким кибер-риск уже на ранних стадиях эксплуатации

В опросе Deloitte приняли участие более 400 ИТ-специалистов, работающих в организациях, которые активно рассматривают преимущества квантовых вычислений, хотя и не обязательно новый уровень киберриска, который им сопутствует. Только немногим более 26% сказали, что на данный момент они завершили оценку рисков. 18% планируют сделать это в этом году, а 16% говорят, что сделают это в ближайшие два-пять лет. 13% говорят, что либо не планируют этого более пяти лет, либо вообще не собираются этого делать.

Примерно столько же организаций, которые планируют провести оценку киберриска задолго до того, как квантовые вычисления станут угрозой, чуть более половины всех респондентов, также считают, что HDL представляет собой непосредственную угрозу для их организации. 21% не считают это угрозой, а 28% не знают.

Что может подтолкнуть некоторые из наиболее сопротивляющихся организаций серьезно отнестись к угрозам квантовых вычислений? 27% респондентов заявили, что потребуется давление регулирующих органов. 20 % считают, что руководство необходимо убедить потребовать изменений, 15 % считают, что изменения будут вызваны, если увидят, как это делают конкуренты, а 11 % заявили, что потребуется не что иное, как атака с помощью квантовых вычислений, чтобы сдвинуть иглу с места. организация. Чуть менее 7% считают, что требования клиентов или акционеров будут иметь значение.

Взлом квантовых вычислений ожидается примерно в 2030 году

Эксперты по кибербезопасности расходятся во мнениях по этому вопросу, но большинство считает, что угроза квантовых вычислений появится всего через пять лет и, вероятно, не более чем через 15. Это означает, что организации должны разумно рассчитывать на наличие средств защиты к концу текущего года. самое позднее десятилетие.

Хотя шифрование является жизненно важной частью программы защиты данных, файлы, зашифрованные с помощью современных алгоритмов, скорее всего, в какой-то момент будут взломаны за считанные секунды с помощью инструментов квантовых вычислений. Если эти зашифрованные файлы будут украдены сейчас, злоумышленникам потребуется всего несколько лет, чтобы получить к ним свободный доступ. Таким образом, угроза HNDL требует немедленного внимания, но пока осознание ее отстает (не говоря уже о значимых действиях).

Тем не менее, некоторые эксперты предупреждают, что организациям не следует слишком сильно тянуть в противоположном направлении и делать панические шаги, чтобы изменить криптоалгоритмы в одночасье. Ожидается, что новые стандарты полностью не появятся в NIST до 2024 года, и у большинства ИТ-отделов есть множество нерешенных проблем с киберрисками, которые гораздо более полезны для улучшения состояния безопасности.

Риск также неравномерно распределен по отраслям и организациям. Нынешние субъекты угроз HNDL — это почти исключительно злоумышленники из национальных государств, которые ищут государственные секреты и

конфиденциальную информацию, которую они могут разблокировать позже. Эти группы также почти наверняка являются злоумышленниками среди ограниченной группы людей, имеющих ранний доступ к стабильным квантовым вычислениям, как только они станут реальностью. Недостаточно стабильный квантовый компьютер Google Sycamore стоит миллионы долларов, прежде чем вы доберетесь до сотен специализированных кабелей связи, которые стоят по 1000 долларов за каждые два фута длины, должны быть размещены в специальной холодильной установке, способной постоянно поддерживать чрезвычайно точную температуру. и может выйти из строя, если слишком долго отключается для ремонта оборудования.

На данный момент с угрозой HNDL лучше всего бороться, не пуская злоумышленников в сети и конфиденциальные файлы. Проведение инвентаризации «долгоживущих» информационных активов, которые, как ожидается, не изменятся или не устареют в ближайшие несколько лет, таких как номера банковских счетов, также может помочь в качестве немедленного шага; к этим высокочувствительным данным потенциально можно обращаться с помощью современных средств, таких как смена ключей». ***(Scott Ikeda. Quantum Computing Attacks Still Years Off, but "Hack Now Decrypt Later" Presents Immediate Cyber Risk // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/quantum-computing-attacks-still-years-off-but-hack-now-decrypt-later-presents-immediate-cyber-risk/). 07.10.2022).***

***

Діяльність хакерів та хакерські угруповування

«Компанія ESET виявила та проаналізувала набір шкідливих інструментів, які використовувалися відомою APT-групою Lazarus наприкінці 2021 року. Атаки починалися з фішингових повідомлень із небезпечними документами, а головною метою зловмисників було перехоплення даних.

Цілями кіберзлочинців стали співробітник аерокосмічної компанії у Нідерландах та політичний журналіст у Бельгії. Обом жертвам надіслали пропозиції про роботу: перший отримав вкладення у повідомленнях LinkedIn, а другий — електронною поштою відповідно. Атаки почалися після відкриття цих документів. Зловмисники розгорнули в системі кілька шкідливих інструментів, зокрема дропери, завантажувачі, повнофункціональні бекдори HTTP(S) та завантажувачі HTTP(S).

Найпомітнішим інструментом був модуль режиму користувача, який дозволяв зловмисникам читати та записувати пам'ять ядра через уразливість CVE-2021-21551 у легітимному драйвері Dell. Використання цієї уразливості кіберзлочинцями було зафіксовано вперше. Варто зазначити, що у травні 2021 року компанія Dell випустила оновлення системи безпеки.

«Зловмисники використали доступ до запису в пам'ять ядра, щоб вимкнути 7 механізмів, які операційна система Windows застосовує для моніторингу своїх дій, таких як реєстр, файлова система, створення процесів, відстеження подій тощо. Таким дуже загальним та надійним способом хакерам вдалося обійти рішення з безпеки, — пояснює Пітер Калнаї, дослідник ESET. — Це було зроблено не лише в

просторі ядра, але й з використанням ряду маловідомих компонентів Windows. Безсумнівно, це вимагало глибоких досліджень, розробки та навичок тестування».

Група Lazarus також використовувала повнофункціональний бекдор HTTP(S), відомий як BLINDINGCAN. Дослідники ESET вважають, що цей троян віддаленого доступу (RAT) має складний серверний контролер із зручним інтерфейсом, за допомогою якого зловмисники можуть контролювати та досліджувати скомпрометовані системи. Більше двох десятків доступних команд включають завантаження, перезапис та видалення файлів, а також створення знімків екрана.

У Нідерландах атака була спрямована на комп'ютер на базі Windows 10, підключений до корпоративної мережі. Файл Word з назвою «Amzon_Netherlands.docx», який було надіслано жертві в електронному листі, є лише макетом документа з логотипом Amazon. Дослідникам ESET не вдалося отримати віддалений шаблон, але, ймовірно, він міг містити пропозицію про роботу для космічної програми Amazon Project Kuiper. Це метод, який кіберзлочинці застосовували у кампаніях Operation In(ter)ception та Operation DreamJob, спрямованих на аерокосмічну та оборонну галузь.

«У цій, а також у багатьох інших атаках групи Lazarus багато інструментів було розподілено навіть для однієї цільової робочої станції в мережі, яка представляє інтерес для зловмисників. Без сумніву, група, яка відповідальна за атаку, є досить великою, систематично організованою та добре підготовленою», – коментує дослідник ESET.

Спеціалісти ESET з високою достовірністю приписують ці атаки групі Lazarus. Різноманітність, кількість та оригінальність у реалізації атак, а також здійснення кібершпигунства, кіберсаботажу та отримання фінансової вигоди вказують на цю групу. Варто зазначити, що група Lazarus, також відома як HIDDEN COBRA, діє принаймні з 2009 року та відповідальна за кілька відомих інцидентів.

Персонал великих компаній часто стає ціллю кіберзлочинців, які використовують витончені методи, щоб заманити співробітника у пастку та отримати доступ до корпоративної мережі. Саме тому варто подбати про обізнаність працівників щодо правил кібербезпеки, зокрема попередити про небезпеку відкриття невідомих листів та документів у корпоративній мережі. Крім того, організаціям слід забезпечити всебічний захист робочих станцій, розширений аналіз загроз, виявлення та реагування, а також запобігання втраті конфіденційних даних». ***(ESET виявила нові атаки групи Lazarus // Компьютерное Обозрение (https://ko.com.ua/eset_viyavila_novi_ataki_grupi_lazarus_142237). 03.10.2022).***

***

«Anonymous та інші глобальні хакерські групи беруть участь у багатоплановій кібер-атаці на Іран, приєднуючись до боротьби з протестувальниками на місцях, які виступають проти суворих законів про носіння хіджабу в країні.

Тисячі хакерів-любителів організували онлайн кібератаки на іранських чиновників і установи, а також поділилися порадами про те, як обійти обмеження доступу до Інтернету за допомогою інструментів для підвищення конфіденційності.

Доступ до Інтернету в Ірані був вкрай обмежений в останні тижні після того, як спалахнули протести через смерть Махси Аміні, 22-річної іранської курдської жінки.

Аміні померла в лікарні в Тегерані за підозрілих обставин 16 вересня після того, як її затримала так звана «поліція моралі» Ірану за нібито порушення суворого ісламського дрес-коду країни, надто вільно одягнувши хіджаб.

Очевидці кажуть, що Аміні побила поліція. Влада Ірану заперечує будь-які правопорушення та стверджує, що Аміні помер від серцевого нападу.

Міністерство закордонних справ Ірану не відповіло на запит CNBC про коментар. У понеділок верховний лідер Ірану, аятолла Алі Хаменеї, зробив свої перші публічні зауваження щодо протестів, підтримавши поліцію та звинувативши в заворушеннях «іноземне втручання» з боку США та Ізраїлю.

Doxing і DDoS-атаки

25 вересня Anonymous, міжнародний колектив хактивістів, заявив, що зламав базу даних парламенту Ірану, отримавши особисту інформацію законодавців.

Обліковий запис YouTube, який нібито пов'язаний з групою, повідомив, що іранську асамблею було зламано.

«Парламент Ірану підтримує диктатора, коли він повинен підтримувати людей, тому ми оприлюднюємо особисту інформацію всіх них», — сказали вони, змінивши голос у типовий для кібербанди спосіб.

У додатку для обміну повідомленнями Telegram Atlas Intelligence Group, інша хакерська група, каже, що вона злила номери телефонів і адреси електронної пошти іранських чиновників і знаменитостей, тактика, відома як «доксінг».

Він також запропонував продати дані про явне місцезнаходження Корпусу вартових ісламської революції, гілки збройних сил Ірану, повідомляє Check Point, яка документувала зусилля хактивістів в Ірані.

Афілійовані з Anonymous групи кажуть, що вони також оприлюднили дані, які нібито надійшли від різних державних служб, міністерств і відомств, а також університету, і взяли на себе відповідальність за хакерські атаки на президентство Ірану, центральний банк і державні ЗМІ.

Хоча важко перевірити заяви хакерів, експерти з кібербезпеки заявили, що вони бачили численні ознаки зриву в Ірані з боку пильних хакерів.

«Ми помітили кілька ознак того, що урядові веб-сайти були виведені з ладу хакерами», — сказав CNBC Ліад Мізрахі, експерт із безпеки Check Point Research. «Здебільшого ми бачили, як це відбувається через атаки розподіленої відмови в обслуговуванні (DDoS).»

Під час DDoS-атаки хакери перевантажують веб-сайт великою кількістю трафіку, щоб зробити його недоступним.

«Mandiant може підтвердити, що кілька служб, які, як стверджується, були порушені, були в автономному режимі в різні моменти часу, а в деяких випадках залишалися недоступними», — сказав CNBC Еміель Хегеберт, аналітик з аналізу загроз компанії з кібербезпеки.

«Загалом ці операції DDoS і доксинг можуть посилити тиск на уряд Ірану, щоб він вніс зміни в політику», — сказав він.

Щодо участі Anonymous, Хегеберт зазначив, що воно «відповідає діяльності», яку раніше приписували філіям організації. Раніше цього року Anonymous здійснили низку кібератак на російські організації у відповідь на неспровоковане вторгнення Москви в Україну.

Обхід інтернет-обмежень

Хакерські групи заохочують громадян Ірану обходити інтернет-блокування Тегерана за допомогою VPN (віртуальної приватної мережі), проксі-серверів і темної мережі — методів, які дозволяють користувачам маскувати свою онлайн-ідентичність, щоб їх не могли відстежувати інтернет-провайдери (ISP).

У додатку для обміну повідомленнями Telegram група з 5000 членів ділиться деталями про відкриті сервери VPN, щоб допомогти громадянам обійти інтернет-блокування Тегерана, повідомляє компанія з кібербезпеки Check Point, яка документує зусилля хакерів в Ірані.

Окрема група з 4000 членів розповсюджує посилання на освітні ресурси про використання проксі-серверів, які тунелюють трафік через спільноту комп'ютерів, що постійно змінюється, якою керують волонтери, щоб ускладнити режимам обмеження доступу.

У міру того, як в Ісламській Республіці зростало незгода, уряд швидко придушив підключення до Інтернету та заблокував доступ до соціальних медіа-сервісів, таких як WhatsApp та Instagram, очевидно намагаючись зупинити публікацію в Інтернеті кадрів жорстокості поліції.

За даними незалежної та неурядової Іранської правозахисної групи, станом на неділю під час репресій уряду Ірану було вбито щонайменше 154 людини. Уряд повідомив про 41 смерть.

Фірма веб-безпеки Cloudflare і група інтернет-моніторингу NetBlocks задокументували численні приклади збоїв у телекомунікаційних мережах в Ірані.

«Було дуже важко підтримувати зв'язок із друзями та родиною за межами Ірану. Інтернет тут поганий, тому іноді ми не можемо спілкуватися днями», — сказав CNBC один молодий спеціаліст із Тегерана в Instagram, побажавши залишитися анонімним через страх за свою безпеку.

«У мене обмежений доступ до Instagram, тому я поки що використовую його, щоб зв'язатися з людьми»,- сказав він, додавши, що він і його друзі покладаються на VPN для доступу до платформ соціальних мереж.

Вважається, що це одне з найгірших відключень Інтернету в Ірані з листопада 2019 року, коли уряд обмежив доступ громадян до Інтернету на тлі масових протестів проти підвищення цін на пальне.

«ВОНИ ЗАКРИВАЮТЬ ІНТЕРНЕТ, ЩОБ ПРИХОВАТИ ВБИВСТВО. БУДЬТЕ НАШИМ ГОЛОСОМ», — йдеться в кількох відео та дописах, якими широко поширювалися іранські активісти в соціальних мережах, а також кадри вуличних протестів і насильства з боку поліції.

Активісти за цифрову свободу також намагаються навчити іранців, як отримати доступ до браузера Tor, який дозволяє користувачам підключатися до звичайних веб-сайтів анонімно, щоб їхні провайдери не могли визначити, що вони переглядають. Tor часто використовується для доступу до «темної мережі»,

прихованої частини Інтернету, до якої можна отримати доступ лише за допомогою спеціального програмного забезпечення.

«Це не перший раз, коли ми бачимо акторів, залучених до іранських справ», — сказав CNBC Амін Хасбіні, директор із глобальних досліджень і аналізу фірми з кібербезпеки Kaspersky.

Відомо, що Lab Dookhtegan, антиіранська хакерська група, витікає дані, які, як стверджується, належать іранським кібершпигунським операціям у Telegram, наприклад. Минулорічний звіт Check Point детально розповідав про те, як іранські хакерські групи атакували дисидентів за допомогою зловмисного програмного забезпечення, щоб стежити за ними». ***(Дмитро Сизов. Хактивісти прагнуть допомогти протестуючим в Ірані // nternetua (https://internetua.com/haktivisti-pragnut-dopomogti-protestuuacsim-v-irani). 04.10.2022).***

***

«Північнокорейське хакерське угруповування Lazarus розсилає фішингові електронні листи працівникам японських криптовалютних бірж. Мета — заразити комп'ютери шкідливим програмним забезпеченням та викрасти кошти. За останні роки від такої схеми постраждали декілька компаній. Так у 2018 хакери зламали криптобіржу Zaif, а у 2019 — платформу Bitpoint Japan. Загалом зловмисники вивели криптовалюти на суму ¥6.7 та ¥3.5 мільярдів.

Національна поліція та Агентство фінансових послуг Японії у спільній заяві звернулися до локальних компаній, які працюють з криптовалютою, і попросили про пильність та додаткові заходи з кібербезпеки всередині фірм. Щоправда, ні влада країни, ні правоохоронці поки не розкрили подробиць про те, які криптокомпанії були цілями або зламані в результаті цих фішингових атак.

Останніми місяцями Японія демонструє все більшу лояльність до криптовалютної галузі, хоче ще зовсім нещодавно країну вносили до списку держав, де власникам цифрових активів нема чого очікувати. На початку жовтня прем'єр-міністр Японії заявив, що на розвиток у сфері блокчейну з державного бюджету Японії щороку виділятимуть $ 7 мільярдів. У країні збираються звільнити від податків місцеві криптовалютні компанії, а для іноземців знизити податкову ставку з 55% до 20%...». ***(Найвідоміші хакери світу атакували японські криптовалютні біржі // No worries! (https://noworries.news/najvidomishi-hakery-svitu-atakuvaly-yaponski-kryptovalyutni-birzhi/). 17.10.2022).***

***

«Хакери із групи Black Reward опублікували документи про ядерну програму Ірану, повідомляє Iran International.

Хакери заявили, що зламали систему електронної пошти іранської компанії Nuclear Power Production and Development. Вони вимагали звільнити всіх політв'язнів та затриманих учасників протесту, інакше вони пригрозили опублікувати близько 50 гігабайт даних про ядерну програму. Але влада Ірану проігнорувала їхні вимоги, тому хакери почали публікувати дані.

«Опубліковані документи містять контракти іранської компанії з виробництва та розвитку атомної енергії з вітчизняними та зарубіжними партнерами, графіки

управління та експлуатації Бушерської АЕС, ідентифікаційні дані та платіжні квитанції інженерів та співробітників компанії, а також паспорти та візи іранських та російських фахівців Бушерської електростанції», - йдеться у повідомленні.

Крім того, хакери Black Reward вламали електронну пошту керівників та співробітників Press TV, міжнародного урядового англомовного каналу новин…» ***(Людмила Садловська. Хакери опублікували документи ядерної програми Ірану // Korrespondent.net (https://ua.korrespondent.net/world/4528573-khakery-opublikuvaly-dokumenty-yadernoi-prohramy-iranu). 23.10.2022).***

***

«…17 октября хакеры связались с Kyiv Post, которые указали, что они являются сторонниками российской Национальной стрелковой ассоциации. Как ранее сообщал Kyiv Post, NRA – это организация российских оппозиционеров, стремящихся к свержению путинского режима, в том числе с применением насильственных средств.

Члены NRA сообщили Kyiv Post, что они взломали несколько крупных российских технологических компаний, которые в настоящее время предоставляют услуги, критически важные для национальной безопасности российского правительства. Хакеры предоставили Kyiv Post эксклюзивный доступ к большому объему документов и фотографий, которые, по их словам, были получены с внутренних серверов компаний, которые, по мнению хакеров NRA, делают возможной войну России.

Сообщается, что одним из взломанных предприятий является «Техносерв» — крупнейший российский системный интегратор, который работает в разных странах в качестве консультанта». ***(Russians Against Putin: NRA Claims Massive Hack of Russian Government Contractors' Computers // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/russians-against-putin-nra-claims-massive-hack-of-russian-government-contractors-computers/). 23.10.2022).***

***

«Коллектив хактивистов Anonymous, который с момента вторжения в Украину проводил кибероперации против России и поддерживающих организаций, теперь нацелился на ФИФА, предупредив, что организация должна запретить Ирану участвовать в чемпионате мира в следующем месяце за поставку смертоносных дронов-камикадзе, которые терроризируют украинцев.

«ФИФА должна запретить #Иран после приостановки #России. Хаменеи снабжает Россию беспилотниками-камикадзе и поддерживает путинский хаос», — написал во вторник один из аккаунтов Anonymous в Твиттере. «Исключение Ирана из чемпионата мира имеет решающее значение для иранцев, украинцев и остального мира, чтобы разоблачить режим мулл».

Клятва согласуется с инициативой #OpIran от хакеров в поддержку более чем месячных протестов в Иране, вызванных смертью Маши Амини, которая умерла во время содержания под стражей в полиции 16 сентября, через три дня после ее ареста и предполагаемого избиения за неправильное ношение. хиджаб в Тегеране.

«Если ФИФА не исключит #Иран из чемпионата мира, он будет вовлечен в ужасающие бойни, совершенные Исламской Республикой», — написал один из аккаунтов Anonymous в Твиттере. «Заглушить голоса борцов за свободу равносильно их убийству».

Пресс-секретарь Пентагона, бриг ВВС. Генерал Пэт Райдер заявил журналистам в четверг, что министерство обороны установило, что «иранцы находились на территории Украины, чтобы помочь России в операциях с беспилотниками».

«Итак, с точки зрения того, что это означает, очевидно, опять же, мы по-прежнему видим, что Иран причастен к экспорту террора не только в регион Ближнего Востока, но теперь и в Украину», — добавил Райдер…

В видео, опубликованном во вторник, Anonymous обратились к «руководителям ФИФА и футбольной бюрократии».

«Мы анонимны, и у нас есть сообщение для вас. Иран будет исключен из чемпионата мира по футболу в этом году и заменен Украиной из-за предполагаемого использования Россией иранских беспилотников в войне против Киева», — говорится в видео.

«Пока иранские лидеры будут развлекаться, наблюдая за игрой своей национальной сборной на чемпионате мира, украинцев будут убивать иранские беспилотники и иранские ракеты», — говорится в сообщении Сергея Палкина, генерального директора украинского футбольного клуба «Шахтер Донецк». на Facebook.

«Иранский народ будет по-прежнему подвергаться преследованиям — женщины, мужчины, дети, которые борются за свои свободы, будут по-прежнему заключены в тюрьму и убиты режимом Исламской Республики, в то время как лидеры смотрят, как их команда играет на чемпионате мира 2022 года», — продолжается видео. «Кровь невинных будет продолжать литься, пока продолжается игра кровожадных убийц».

«Каждый из них (беспилотников) был произведен, доставлен иранскими властями, иранскими инструкторами, а военные непосредственно обучали и осуществляли запуски дронов, которые разрушали дома, музеи, университеты, офисы, спортивные и детские площадки и, самое главное, убивали украинцы», — говорится в видео со ссылкой на Палкина.

«Мы, Анонимные, присоединяемся к протестам и призываем ФИФА и все международное сообщество немедленно запретить сборной Ирана играть на чемпионате мира за прямую причастность страны к терактам против украинцев. Мы просим заменить Иран на Украину. Замена Ирана Украиной была бы исторически и спортивно оправдана».

В сообщении Anonymous говорится, что операция «Чемпионат мира», #OpWorldCup, «активирована, и просят всех присоединиться к давлению на футбольную бюрократию, чтобы спровоцировать изгнание сборной Ирана с чемпионата мира в Катаре 20 ноября».

«Ваш выбор — немедленно исключить сборную Ирана из ЧМ-2022 или подождите нас», — подчеркнули хактивисты.

Сегодня утром анонимные аккаунты в Твиттере сообщили, что они отключили веб-сайты офиса связи правительства Катара, обещая «больше новых целей», и Al Daffa Aluminium, Upvc & Steel Works в Дохе. «Катар, вас предупредили, замените команду Исламского режима на Украину», — отметил один из аккаунтов Anonymous. «Вы должны были ожидать Нас».

Другой анонимный аккаунт перечислил корпоративных спонсоров и партнеров чемпионата мира, добавив: «#OpWorldCup принимает это во внимание, потому что вы видите, что их молчание доказывает, что военные преступления, преступления против человечности и нарушения прав человека спонсируются #OpFifa !»…» ***(Bridget Johnson. Anonymous Warns FIFA to Expel Iran from World Cup Over Deadly Drone Attacks on Ukraine // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/anonymous-warns-fifa-to-expel-iran-from-world-cup-over-deadly-drone-attacks-on-ukraine/). 26.10.2022).***

***

Вірусне та інше шкідливе програмне забезпечення

«Исследователи обнаружили невиданное ранее кроссплатформенное вредоносное ПО, которое заразило широкий спектр устройств Linux и Windows, включая небольшие офисные маршрутизаторы, компьютеры с FreeBSD и крупные корпоративные серверы.

Black Lotus Labs, исследовательское подразделение охранной фирмы Lumen, называет вредоносное ПО Chaos — слово, которое постоянно встречается в именах функций, сертификатах и именах файлов, которые оно использует.

Хаос возник не позднее 16 апреля, когда заработал первый кластер серверов управления. С июня по середину июля исследователи обнаружили сотни уникальных IP-адресов, представляющих скомпрометированные устройства Chaos. Промежуточные серверы, используемые для заражения новых устройств, за последние месяцы выросли как грибы с 39 в мае до 93 в августе. На прошлой неделе их число достигло 111.

Black Lotus наблюдал за взаимодействием с этими промежуточными серверами как со встроенных устройств Linux, так и с корпоративных серверов, включая один в Европе, на котором размещался экземпляр GitLab. В дикой природе насчитывается более 100 уникальных образцов». ***(Never-Before-Seen Malware Infected Hundreds Of Linux, Windows Devices // MITechNews.com (https://mitechnews.com/cyber-defense/never-before-seen-malware-infected-hundreds-of-linux-windows-devices/). 09.10.2022).***

***

«Злоумышленники используют Internet Information Services — расширяемое программное обеспечение веб-сервера Microsoft — для доставки ранее недокументированного дроппера, который используется для установки нового бэкдора и других инструментов.

По словам исследователей Symantec, хакерская группа под названием Cranefly, также известная как UNC3524, использует новый бэкдор под названием Danfuan, используя другой дроппер под названием Geppei.

«Техника чтения команд из журналов IIS — это не то, что исследователи Symantec до сих пор видели в реальных атаках», — говорят исследователи.

Cranefly был впервые задокументирован Mandiant в мае, и группа фокусируется на адресной электронной почте сотрудников, занимающихся корпоративным развитием, слияниями и поглощениями, а также крупными корпоративными транзакциями.

У злоумышленников, стоящих за Cranefly, было долгое время ожидания, и они проводили не менее 18 месяцев в сетях жертв, используя устройства, которые не поддерживали инструменты безопасности.

Исследователи Mandiant обнаружили, что злоумышленники установили бэкдоры на средства безопасности, такие как массивы SANS, балансировщики нагрузки и контроллеры беспроводных точек доступа.

Технические подробности

Первоначально исследователи Symantec наблюдали вредоносную активность дроппера Trojan.Geppei на машине-жертве с помощью PyInstaller, преобразующего скрипт Python в исполняемый файл.

Geppei имеет возможность считывать команды из законного журнала IIS, который предназначен для записи данных из IIS, таких как веб-страницы и приложения.

«Злоумышленники могут отправлять команды на скомпрометированный веб-сервер, маскируя их под запросы доступа к сети. IIS регистрирует их как обычно, но Trojan.Geppei может читать их как команды», — говорят исследователи.

Исследователи говорят, что команды, считываемые Geppei, содержат вредоносные закодированные файлы.ashx, которые сохраняются в «произвольной папке, определяемой параметром команды, и работают как бэкдоры».

Такие строки, как Wrde, Exco и Cllo, не отображаются в файлах журнала IIS и используются Geppei для анализа вредоносных HTTP-запросов.

«Наличие этих строк побуждает дроппер выполнять действия на машине», — говорят исследователи. «Злоумышленники могут использовать фиктивный URL-адрес или даже несуществующий URL-адрес для отправки этих команд, потому что IIS по умолчанию регистрирует 404 в том же файле журнала».

На следующем этапе бэкдор сбрасывает два дроппера Hacktool.Regeorg и Trojan.Danfuan. ReGeorg — это известное вредоносное ПО, веб-оболочка, которая может создавать прокси-сервер SOCKS, а Danfuan — ранее неизвестное вредоносное ПО, представляющее собой DynamicCodeCompiler, который компилирует и выполняет полученный код C#.

«Похоже, он основан на технологии динамической компиляции.NET. Этот тип динамически компилируемого кода не создается на диске, а существует в памяти. Он действует как лазейка в зараженных системах», — говорят исследователи.

Исследователи Symantec говорят, что использование новой техники и специализированных инструментов, а также дополнительные шаги, предпринятые

для сокрытия его следов от компьютеров-жертв, показывают, насколько квалифицированы агенты Cranefly.

Исследователи говорят, что не наблюдали случаев кражи данных с компьютеров-жертв. Развернутые инструменты и усилия, предпринятые для сокрытия этой деятельности, указывают на то, что группа занимается «сбором разведданных». ***(Prajeet Nair. Espionage Hackers Use Microsoft IIS to Plant Malware // Information Security Media Group, Corp. (https://www.govinfosecurity.com/espionage-hackers-use-microsoft-iis-to-plant-malware-a-20363). 29.10.2022).***

***

«Группа исследования угроз Cequence опубликовала отчет о безопасности API за первую половину 2022 года, в котором показано, что почти треть вредоносных запросов нацелена на теневой API.

Команда проанализировала более 16,7 миллиарда транзакций API и обнаружила, что 31% или 5 миллиардов вредоносных запросов были нацелены на неизвестные, неуправляемые или незащищенные API, называемые теневыми API. Согласно Cequence, теневой API был ведущим источником угроз безопасности API, за ним следовали злоупотребления API или OWASP API10+ и «Нечестивая троица» вставки учетных данных, теневого API и раскрытия конфиденциальных данных.

Cequence отметила, что широкое распространение API привлекло последующие действия злоумышленников, что расширило спектр угроз. Исследователи отметили, что API популярны среди разработчиков из-за их гибкости, скорости и простоты использования, в отличие от веб-сервисов. Кроме того, их гибкость обусловлена тем, что они не требуют конфигурации брандмауэра веб-приложений или сторонних шлюзов API. Их популярность привела к тому, что многие современные приложения, такие как торговые и финансовые приложения, полагаются на API-интерфейсы для транзакций и бесшовной интеграции.

Однако API-интерфейсы также популярны среди злоумышленников, потому что хакеры могут легко находить ошибки в коде, чтобы использовать их или развертывать ботов для их проверки и атаки. Кроме того, хакеры могут быстро развернуть эфемерные мошеннические API-интерфейсы в скомпрометированных общедоступных облачных средах для раскрытия конфиденциальных данных и атак с использованием учетных данных.

Угроза безопасности API №1: Злоупотребление теневым API (OWASP API9)

В отчете о защите Cequence API обнаружено, что злоупотребление теневым API резко возросло в 2022 году и увеличилось в течение года. Фирма выявила различные сценарии, в которых злоумышленники использовали теневой API.

«От очень объемных кроссовочных ботов, пытающихся взломать новейшие модели Dunk или Air Jordan, до скрытных злоумышленников, пытающихся провести медленную струйку мошенничества с проверкой карт на украденных кредитных картах, до кампаний по заполнению учетных данных с использованием грубой силы».

Теневые API особенно проблематичны в организациях, где отсутствует надлежащее управление запасами, обеспечение качества или системы управления версиями.

Впоследствии злоумышленники могут быстро обнаружить теневой API, когда конечные точки закодированы так, чтобы принимать параметры или ввод с подстановочными знаками из URI. Они могут изменять входные данные от хорошо защищенных API, чтобы обнаруживать другие конечные точки API или разные версии одних и тех же API под другими именами хостов. Злоумышленники также могут легко автоматизировать и монетизировать процесс с помощью торговых ботов и заполнения учетных данных.

Угроза безопасности API № 2: Злоупотребление API правильно закодированными конечными точками (OWASP API10+)

Злоумышленники также нацелены на идеально закодированные конечные точки API, процесс, называемый «злоупотребление API», сопоставленный с OWASP API10+.

Согласно отчету Cequence о защите API, эта угроза заняла второе место с 3,6 миллиардами заблокированных вредоносных запросов, в том числе:

Вредоносные запросы API покупок, нацеленные на кроссовки или предметы роскоши (3 миллиарда)

Вредоносная проверка подарочных карт (290 миллионов)

Создание поддельных учетных записей для мошенничества с романтическими отношениями, торговых ботов и т. д. (237 миллионов)

Спам-запросы комментариев на важных платформах взаимодействия с бизнес-клиентами (37 миллионов).

Cequence отметила, что злоупотребление API или угроза безопасности API10+ были причиной взаимосвязи безопасности API и предотвращения ботов.

Фирма указала, что боты для очистки контента предшествовали сценариям злоупотребления API, таким как боты для покупок и атаки с подарочными картами.

Некоторые тактики, используемые злоумышленниками для компрометации должным образом закодированных API, включают злоупотребление авторизацией на нарушенном функциональном уровне (API15), чтобы позволить автоматизировать покупки с использованием украденных данных кредитной карты.

Угроза безопасности API № 3: «Нечестивая троица» вброса учетных данных, теневых API и раскрытия конфиденциальных данных

Хотя этот риск безопасности API бледнеет по сравнению (100 миллионов) со злоупотреблением теневым API и неправомерным использованием API, он по-прежнему представляет собой серьезную угрозу.

Этот эксплойт использовал несколько недостатков безопасности API, таких как нарушенная аутентификация пользователя (API2), чрезмерное раскрытие данных (API3) и неправильное управление активами (API9).

По словам исследователей, комбинация доказала, что «злоумышленники проводят подробный анализ того, как работает каждый API, как они взаимодействуют друг с другом и каковы ожидаемые результаты».

Ключевые результаты включают заполнение учетных данных, обнаружение теневого API и раскрытие конфиденциальных данных. Заполнение учетных данных

происходит из-за нарушенной аутентификации пользователя с использованием API-интерфейсов с функциями проверки, которые создают данные, которые могут быть украдены после аутентификации, а обнаружение теневых API-интерфейсов является результатом неправильного управления активами. Раскрытие конфиденциальных данных произошло из-за того, что API-интерфейсы программы проверки возвращали больше данных, чем необходимо, или когда разработчики довольствовались процессом аутентификации.

Хотя теневые API были невидимы для групп безопасности, злоумышленники могли использовать известные шаблоны для обнаружения API и выполнять последующую подстановку учетных данных или раскрытие данных.

Партнерские экосистемы и риск теневого API

В отчете говорится, что сторонние API также создают потенциальные риски безопасности, поскольку они обычно внедряются без ведома групп безопасности. Кроме того, они создают единую цифровую цепочку поставок, на которую злоумышленники могут нацеливаться, чтобы получить множество жертв.

Злоумышленники также понимали связь «один ко многим» между центральными учреждениями и их партнерами. Вместо того, чтобы атаковать центральный институт, они могут атаковать партнерскую экосистему и, в основном, самих партнеров.

Кроме того, хотя сторонние API могут быть правильно закодированы, они могут иметь недостатки реализации, которые делают их уязвимыми для злоумышленников, скрывающихся у всех на виду.

Cequence выявила и заблокировала не менее 50 миллионов вредоносных запросов за неделю, направленных на партнерские экосистемы. Атаки были совершены с 250 000 IP-адресов прокси-серверов Bulletproof на Ближнем Востоке, в Северной Африке, Корее, России, Филиппинах и Индонезии. Иногда запросы исходили из регионов, где у цели практически нет транзакций.

Обнаружение и защита API является приоритетом

В исследовании отмечается, что API стали краеугольным камнем бизнеса, поэтому защита API стала приоритетом.

«Защита API должна рассматриваться комплексно, с единым подходом, который начинается с обнаружения, идентификации и инвентаризации вашего следа API», — написали они.

Они рекомендовали обнаружение API, непрерывную оценку рисков для исправления раскрытия данных, нарушенной аутентификации и ошибок кодирования, применение контрмер и постоянное тестирование для устранения рискованных API». ***(Alicia Hope. Shadow API is the Leading API Security Threat With Over 5 Billion Attacks, Says API Protection Report // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/shadow-api-is-the-leading-api-security-threat-with-over-5-billion-attacks-says-api-protection-report/). 10.10.2022).***

***

«Банда вымогателей LockBit за последний месяц еще больше укрепила свои позиции в качестве самой активной группы онлайн-вымогателей.

Операция «вымогатель как услуга» стала самой продуктивной группой в начале этого года, уступив первое место Conti после того, как эта банда уничтожила большую часть ее инфраструктуры в мае. Эксперты по кибербезопасности говорят, что члены Conti, предпринявшие дерзкие атаки на правительство Коста-Рики и другие высокопоставленные лица, вероятно, разделились на более мелкие группы, чтобы избежать обнаружения.

LockBit был связан с 82 атаками в августе, в результате чего общее число жертв достигло 1111, согласно данным, собранным Recorded Future с сайтов-вымогателей, правительственных агентств, новостных сообщений, хакерских форумов и других источников. Французская полиция заявила, что эта группа стояла за нападением на больницу примерно в часе езды к юго-востоку от Парижа в прошлом месяце, что нарушило работу медицинских изображений, прием пациентов и другие службы. По данным фирмы по кибербезопасности Dragos, около трети атак программ-вымогателей, нацеленных на промышленные системы во втором квартале, были приписаны LockBit.

Группа наблюдала всплеск активности с июня, когда она запустила новую версию — то, что она называет «LockBit 3.0», — которая якобы включала технические улучшения и программу вознаграждения за обнаружение ошибок, которая предлагала вознаграждение за способы улучшения работы программы-вымогателя…» ***(ADAM JANOFSKY. Ransomware tracker: the latest figures [October 2022] // The Record by Recorded Future (https://therecord.media/ransomware-tracker-the-latest-figures/). 11.10.2022).***

***

«С августа 2022 года программа-вымогатель Venus компрометирует службы удаленного рабочего стола (RDP).

Основными целями зловреда являются незащищенные Windows-устройства с общедоступным RDP.

Успешная программа-вымогатель Venus блокирует доступ пользователей к важным файлам и требует оплаты в криптовалюте.

Что каждая организация должна знать о программе-вымогателе Venus и каковы некоторые из лучших методов кибербезопасности для предотвращения и борьбы с этим типом вредоносного ПО?

Прежде чем мы предпримем меры предосторожности и рекомендации для тех, кто уже пострадал, давайте определим признаки последней версии программы-вымогателя.

Как распознать Venus Ransomware?

Программа-вымогатель Venus шифрует файлы, переименовывает их и уведомляет жертв примечанием на экране.

Жертвы понимают, что на них повлияли, когда на их экране появляется записка с условиями и требованиями. После блокировки доступа к файлам

злоумышленник уведомляет пользователя с помощью файла README.txt и обоев рабочего стола.

Сообщение на экране подтверждает наличие вредоносной активности и отображает инструкции о том, как вернуть файлы и заплатить выкуп. В этом случае пользователь должен связаться с преступником для получения дальнейших инструкций в течение пяти дней.

Хакеры сообщают, что все файлы жертвы были зашифрованы и сообщат полученную информацию общественности, если требования не будут выполнены.

Еще одним очевидным признаком того, что программа-вымогатель Venus затронула файлы, является расширение имени файла. Заблокированные файлы, которые невозможно открыть, имеют дополнительный суффикс «Венера».

Всемирная угроза, нацеленная на общедоступный RD

Любое глобальное устройство Windows с общедоступными компонентами удаленного рабочего стола восприимчиво к программам-вымогателям Venus. RDP — это точка доступа, которая используется при атаке.

В случае успешного взлома пострадает база данных серверов и приложения Office, поскольку киберпреступник получает контроль над процессами.

Некоторые из возможностей хакеров после успешной атаки включают удаление журналов событий и предотвращение выполнения данных.

На зараженных устройствах программа-вымогатель шифрует данные, генерирует заметки о выкупе (скорее всего, также зашифрованные ключи описания) и меняет обои для отображения другого (в основном идентичного) сообщения о выкупе.

Меры кибербезопасности для предотвращения программ-вымогателей

В большинстве случаев сложно расшифровать файлы и перепроектировать программу-вымогатель, если вредоносная программа не имеет конкретной ошибки. Даже при удалении вредоносного ПО уже зараженные файлы не будут расшифрованы.

Поэтому важно установить превентивные меры для защиты активов от кибер-вымогательства.

Как можно подготовиться к очень реальной возможности программы-вымогателя Venus?

Критическая уязвимость, которая делает возможной программу-вымогатель Venus, — это общедоступные службы удаленных рабочих столов. Поэтому лучшие меры кибербезопасности включают использование виртуальной частной сети (VPN) при доступе к службам удаленных рабочих столов.

Убедитесь, что RDP недоступен для публики, и защитите такие службы с помощью брандмауэра.

Согласно последним данным, эта программа-вымогатель стала возможной благодаря фишинговым кампаниям по электронной почте, торрент-сайтам и рекламе, пронизанной вредоносными программами.

Хакеры отправляют зараженное вложение по электронной почте или внедряют вредоносный код в рекламу в Интернете.

Знание и понимание этих методов распространения необходимо для предотвращения программ-вымогателей Venus. Более сложные фильтры

электронной почты и блокировка доступа к таким сайтам, как торрент-страницы и рекламное ПО, — отличное начало.

Некоторые инструменты специально разработаны для обнаружения признаков вредоносных программ (например, шифрования).

Помимо такого защитного программного обеспечения, необходимо защищать инфраструктуру многоуровневой защитой, состоящей из различных программ и протоколов.

То есть кибербезопасность должна быть надежной и всеобъемлющей — охватывать все устройства, подключенные к удаленной сети, и блокировать любые пути, которые хакеры могут попытаться использовать для получения денежной выгоды.

В дополнение к этим мерам кибербезопасности важно создавать резервные копии данных на отдельных серверах, к которым нельзя получить удаленный доступ. Это позволяет вашим командам не отставать от своих повседневных задач, даже если часть сети скомпрометирована и недоступна.

Файлы уже зашифрованы программой-вымогателем Venus?

Что делать, если злоумышленники уже потребовали выкуп? Есть ли способ разблокировать файлы, и стоит ли платить?

Под давлением многие организации рассматривают и часто платят выкуп.

Например, выкуп Венеры сопровождается запиской, призывающей жертву не связываться со сторонней помощью, которая может попытаться расшифровать файлы. В противном случае они навсегда потеряют файлы, даже если выкуп будет уплачен.

Тем не менее, оплата не является решением, поскольку это действие подтверждает злоумышленникам, что атака была успешной, и нет никакой гарантии, что они выполнят свою часть сделки.

Простая истина в глазах закона заключается в том, что вы финансируете дальнейшую преступную деятельность.

Хотя оплата кажется менее затратной, чем восстановление инфраструктуры с нуля, нет никакой гарантии, что преступники все равно не утекут данные или не одолжат вам ключ для шифрования файлов.

Более того, платить выкуп незаконно — вместо этого сообщите о преступной деятельности.

Также не рекомендуется связываться и общаться с преступной организацией.

Заключительное слово

Хотя программа-вымогатель Venus активна с августа 2022 года, многие организации и отдельные лица по-прежнему могут быть подвержены угрозе и не иметь надлежащих инструментов для обнаружения и устранения последствий.

Вредоносное ПО является напоминанием о том, как трудно отсеять программы-вымогатели.

За последние пару лет количество таких эксплойтов увеличилось. Помимо увеличения количества атак программ-вымогателей, он превратился в более сложные варианты.

Новые версии могут не только шифровать файлы — они могут заблокировать пользователя в системе, загружать данные из уязвимых файлов, удалять данные, отключать различные функции с помощью удаленных команд и многое другое.

Надлежащая защита от программ-вымогателей и надежная архитектура кибербезопасности необходимы для любого бизнеса, который хочет избежать опасных и дорогостоящих записок о выкупе». ***(Evan Morris. Cybersecurity Measures Can Protect Windows Devices From Venus Ransomware // TechTarget, Inc. (https://www.datasciencecentral.com/cybersecurity-measures-can-protect-windows-devices-from-venus-ransomware/). 30.10.2022).***

***

«Согласно новому отчету, почти четверть предприятий пострадали от атак программ-вымогателей, пятая часть которых произошла за последние 12 месяцев.

Отчет Hornetsecurity 2022 Ransomware Report, в котором приняли участие более 2000 ИТ-руководителей, показал, что 24% из них стали жертвами атак программ-вымогателей, причем 20% атак произошли в прошлом году.

Кибератаки происходят все чаще. Прошлогодний опрос программ-вымогателей показал, что 21% компаний подверглись атаке; в этом году он вырос на три процента до 24 процентов.

«Атаки на бизнес участились, и ИТ-специалисты поразительно не осведомлены и не подготовлены», — сказал генеральный директор Hornetsecurity Дэниел Хофманн. «Наш опрос показывает, что у многих в ИТ-сообществе ложное чувство безопасности. По мере того, как злоумышленники разрабатывают новые методы, компании, подобные нашей, должны делать все возможное, чтобы выйти вперед и защитить бизнес по всему миру».

Пользователи Microsoft 365 стали мишенью злоумышленников

В отчете о программах-вымогателях за 2022 год подчеркивается недостаток знаний о безопасности, доступной для бизнеса. Четверть 25% ИТ-специалистов либо не знают, либо не думают, что данные Microsoft 365 могут быть затронуты атакой программ-вымогателей.

Не менее тревожно и то, что 40% ИТ-специалистов, использующих Microsoft 365 в своей организации, признались, что у них нет плана восстановления на случай, если их данные Microsoft 365 будут скомпрометированы атакой программы-вымогателя.

Недостаточная готовность бизнеса

Реакция отрасли показала повсеместное отсутствие готовности со стороны ИТ-специалистов и предприятий. Увеличилось количество предприятий, не имеющих плана аварийного восстановления, если они все же поддаются повышенной угрозе кибератаки.

В 2021 году 16% респондентов сообщили об отсутствии плана аварийного восстановления. В 2022 году этот показатель вырос до 19 процентов, несмотря на рост атак.

Опрос также показал, что 21% предприятий, подвергшихся атакам, либо заплатили, либо потеряли данные. У хакеров есть стимул проводить эти атаки

программ-вымогателей, потому что есть неплохая вероятность того, что они получат зарплату — 7 процентов ИТ-специалистов, чья организация подверглась атаке, заплатили выкуп, а 14 процентов признали, что они потеряли данные в результате атаки…» ***(Mike Brennan. Survey: Ransomware Attacks Increasing: 20 Percent Of All Attacks In Last 12 Months // MITechNews.com (https://mitechnews.com/cyber-defense/survey-ransomware-attacks-increasing-20-percent-of-all-attacks-in-last-12-months/). 04.10.2022).***

***

«В 2020 году польский разработчик игр CD Projekt Red (CDPR) столкнулся с экстремальным примером закона Мерфи. Вскоре после выпуска Cyberpunk 2077, одной из самых ожидаемых видеоигр за последние пять лет, CDPR подверглась атаке программы-вымогателя, в результате которой активы были заморожены и похищены. Время было выбрано как нельзя хуже: студия столкнулась с негативной реакцией критиков и коммерсантов на свой крупный релиз, а анонимные хакеры угрожали продать с аукциона часть ее наиболее важной интеллектуальной собственности, включая исходные коды для многих из ее крупнейших видеоигр.

Столкнувшись со всем этим, CDPR сделал нечто неожиданное. Он отказался платить какой-либо выкуп. В течение дня после того, как стало известно о взломе, разработчик опубликовал копию записки о выкупе и публичное сообщение, в котором заявил об отказе платить, подтолкнув хакеров к угрозам продать украденные данные.

У отказа были последствия. Новости об атаке привели к падению курса акций, исходные коды самых популярных игр и личная информация сотрудников стали появляться в открытом доступе, и CDPR признал, что утечка может затронуть и будущие проекты.

Ни одно из этих последствий не было неожиданным или трудно предсказуемым. Так как же CDPR мог так быстро и решительно отказать хакерам? Если бы я был тренером по взлому в кресле, я бы предположил, что CDPR мог сказать «нет», потому что это была организация, которая была достаточно подготовлена для выявления и оценки последствий атаки программ-вымогателей. И CDPR не единственная, кто отказывается играть в игры с злоумышленниками.

После неуклонного роста платежей в раннюю эру программ-вымогателей все больше и больше организаций начали отказываться от требований о выкупе. Частично это может быть связано с растущим недоверием к тому, что оплата может гарантировать безопасное и надежное восстановление операций, но это также может быть связано с растущей уверенностью организаций в собственной устойчивости к восстановлению после взлома.

Теперь не каждая организация может просто сказать «нет» требованию выкупа. Больница должна учитывать совсем другие факторы, чем химчистка. Но все организации должны действовать упреждающе, чтобы они были в состоянии 1) действовать проворно при реагировании на нарушение, 2) уменьшать ущерб и 3) сохранять возможность уйти от угрозы.

Вот шесть вещей, которые организации могут сделать сегодня, чтобы стать более устойчивыми к киберугрозам:

Поддерживайте актуальную ИТ-среду и надежные решения для резервного копирования. Организации должны будут сбалансировать затраты и риски при определении того, что им подходит. Как минимум обеспечение того, чтобы персонал соблюдал передовой опыт при использовании оборудования организации и скорейшее исправление известных эксплойтов, может значительно снизить риск того, что организация вообще пострадает от инцидента. Разделение различных аспектов бизнес-операций также может помочь ограничить ущерб, который может нанести взлом.

Убедитесь, что весь персонал ознакомлен с передовыми методами обеспечения безопасности. Цепь настолько прочна, насколько прочно ее самое слабое звено. Социальная инженерия остается чрезвычайно эффективным способом проникновения хакеров в системы. Организации должны активно информировать всех, кто имеет доступ к ее ИТ-среде, о распространенных красных флажках, которые могут помочь пресечь попытку взлома или, по крайней мере, пометить подозрительное поведение, которое необходимо отследить.

Определите драгоценности короны. Знайте, что организация не может позволить себе потерять или раскрыть (например, информацию о сотрудниках, интеллектуальную собственность и другие проприетарные активы), и обеспечьте отдельное хранение и резервное копирование этих данных. Если публичное раскрытие может иметь юридические или коммерческие последствия (например, коммерческая тайна или незапатентованные изобретения), это следует учитывать в любом плане реагирования на инциденты.

Иметь страховое покрытие. В частности, политики, которые применяются к инцидентам кибербезопасности. Организации должны будут определить приемлемый для них уровень риска (и соответствующие надбавки), но хорошая политика должна учитывать прямые и косвенные расходы, включая расходы на судебно-медицинских экспертов и юристов. Также важно знать требования для активации политики. Некоторые полисы требуют, чтобы страховая компания подписывала основные решения, включая юридическую консультацию, и это может стать препятствием во время кризиса, если это не ожидается заранее.

Определите соответствующие заинтересованные стороны. Знайте, кого нужно информировать о происшествии. Часто возникают обязательства по предоставлению отчетности, связанные с конфиденциальностью, которые могут варьироваться в зависимости от юрисдикции. Также могут быть договорные требования с поставщиками или клиентами, чтобы информировать их о любых нарушениях. Наличие актуального списка того, о чем нужно сообщать и кому, может сэкономить критическое время кризисного реагирования для организации.

Имейте дорожную карту кризиса. Все вышеперечисленные шаги должны быть учтены в дорожной карте кризиса. Имейте сценарий, определяющий первоначальные шаги реагирования, включая четкую структуру принятия решений, которая позволит вам быстро продвигаться вперед в выдаче разрешений и принятии ключевых решений по реагированию на инцидент. Многие решения должны быть

приняты после инцидента, который не является частью обычной деятельности бизнеса, и риск паралича может быть очень реальным…

Борьба с атакой программы-вымогателя может быть сюрреалистичным опытом, похожим на ограбление призраком под дулом пистолета. Организации, которые привыкли принимать решения в течение нескольких дней или недель, должны быть в состоянии действовать в течение нескольких часов. Наличие дорожной карты на случай кризиса и способность быстро сканировать и определять, что произошло, может значительно повысить способность организации реагировать на угрозу, как бы она ни проявлялась.

CDPR уже через день знал, что откажется (и может) платить выкуп. Это не могло быть легким решением, но оно требовало уравновешивания рисков и выгод от кражи бесценной и конфиденциальной информации с деловой целесообразностью восстановления систем и активов путем уплаты выкупа.

Важно отметить, что организациям, которые пострадали от взлома, не нужно постоять за себя. Существует целая индустрия услуг, которая выросла в ответ на рост числа инцидентов в области кибербезопасности. Тренеры по взлому (которые часто являются юристами), а также судебные следователи и участники переговоров могут предложить немедленный совет и опыт организациям и помочь им сориентироваться в кризисной ситуации. Правоохранительные органы и регулирующие органы также часто готовы предложить помощь, когда их об этом просят. Есть много ресурсов, включая юристов, которые также могут помочь организациям действовать на опережение, включая разработку дорожной карты, определение рисков и проведение кабинетных учений. Чем лучше организация может быть подготовлена к кризису, тем легче ей понять, когда просто сказать «нет». ***(Kavi Sivasothy. THE "NO WAY" KNOW-HOW: BRACING FOR RANSOMWARE ATTACKS // Gowling WLG International Limited (https://gowlingwlg.com/en/insights-resources/articles/2022/bracing-for-ransomware-attacks/). 31.10.2022).***

***

«…По данным IAPP, почти половина всех утечек данных в 2022 году началась с кражи учетных данных, а ущерб от программ-вымогателей, как ожидается, в 2023 году во всем мире превысит 30 миллиардов долларов. В программах-вымогателях есть три новых разработки, которые делают их более опасными, чем в предыдущие годы. К ним относятся следующие:

Утечка данных и «двойное вымогательство»

Брокеры начального доступа (IAB)

Программы-вымогатели как услуга (RaaS)

1. Утечка данных и «двойное вымогательство»

Многие предприятия используют корпоративные резервные копии для восстановления данных в случае атаки. В результате группы вымогателей больше не просто требуют выкуп за расшифровку важных данных. Они также требуют выкуп, чтобы предотвратить утечку ваших данных.

Атакующие группы теперь сливают конфиденциальные файлы, документы, базы данных и другую информацию, когда компании не платят. Следовательно, термин «двойное вымогательство» определяет первоначальное требование выкупа

за расшифровку файлов и последующее требование выкупа за предотвращение утечки ваших данных.

2. Брокеры начального доступа (IAB)

Рынок начальных брокеров доступа (IAB) переживает бум в даркнете. Рынок IAB обычно предлагает учетные данные по цене, зависящей от типа учетных данных, уровня доступа к учетным данным и размера организации. IAB позволяют атакующим группам программ-вымогателей получать доступ к законным учетным данным высокого уровня для целевых предприятий. Имея доступ к законным учетным данным, атакующие группы могут просто «зайти в сеть» без особых усилий и начать эксфильтрацию данных, чтобы подготовиться к требованию двойного вымогательства.

3. Программы-вымогатели как услуга (RaaS)

Ransomware-as-a-Service (RaaS) — еще одна разработка, ведущая к увеличению числа атак. RaaS сделал атаки программ-вымогателей доступными, так что любой человек с небольшим техническим опытом может провести атаку.

Злоумышленники могут использовать службы программ-вымогателей, не беспокоясь о разработке кода или обслуживании базовой инфраструктуры.

Защита от взлома пароля имеет решающее значение

Атаки программ-вымогателей часто начинаются со взлома учетных данных. Что компании могут сделать, чтобы защитить себя? Большинство органов кибербезопасности согласны с тем, что устаревших политик паролей недостаточно.

Политика паролей, найденная в Active Directory, не имеет встроенной защиты от взлома паролей и ограничена в возможностях фильтрации паролей. Вы можете загрузить бесплатный инструмент Specops Password Auditor, который сканирует вашу Active Directory и выявляет уязвимости, связанные с паролями. Из-за того, что многие нарушения происходят из-за скомпрометированных паролей, утечка паролей является точкой входа для злоумышленников, и этот инструмент сканирует и проверяет список из более чем 875 миллионов паролей.

Specops Password Policy расширяет функциональные возможности групповой политики и упрощает управление детализированными политиками паролей. Он также блокирует использование более 2 миллиардов известных взломанных паролей, полностью настраивается с помощью черных списков и словарей и обеспечивает динамическую обратную связь с конечным пользователем при смене пароля. Если вы ищете долгосрочное решение для слабых учетных данных в Active Directory, вы можете протестировать его бесплатно и посмотреть, подходит ли оно для вашей организации». ***(Breached Credentials Remain the Key Entry Point Behind Rising Ransomware Attacks // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/breached-credentials-remain-the-key-entry-point-behind-rising-ransomware-attacks/).*** 25.10.2022).

***

«Жертвы атак программ-вымогателей в сфере производства и производства платят самые большие выкупы, при этом средний размер выплаченного требования составляет чуть более 2 миллионов долларов.

Программы-вымогатели — это серьезная проблема кибербезопасности, затрагивающая все сектора. Но, согласно анализу атак, проведенному компанией Sophos, занимающейся кибербезопасностью, программы-вымогатели обходятся дороже всего в производстве и производстве.

Среди жертв, которые заплатили киберпреступникам выкуп, чтобы получить ключ дешифрования для извлечения зашифрованных файлов и серверов, и раскрыли, сколько они за это заплатили, средний выкуп составил 2 036 189 долларов.

Это более чем вдвое превышает общий средний размер выкупа, сделанный теми, кто детализировал платеж, который составил 812 360 долларов.

Производство является заманчивой целью для групп вымогателей из-за важной роли, которую оно играет в цепочках поставок, а производственное предприятие, находящееся в автономном режиме в течение значительного периода времени, будет чрезвычайно дорогим и окажет эффект домино для других отраслей, предприятий и потребителей.

Это означает, что некоторые жертвы требуют выкупа, а в некоторых случаях киберпреступники требуют значительных выкупов, потому что они знают, что жертвы отчаянно пытаются восстановить нормальную работу.

Многие производственные предприятия работают на старых компьютерных системах и промышленных «операционных технологиях» или OT, а это означает, что трудно применять исправления безопасности, если они вообще доступны.

«Производство является привлекательным сектором для киберпреступников из-за привилегированного положения, которое оно занимает в цепочке поставок. Устаревшая инфраструктура и отсутствие видимости в среде OT предоставляют злоумышленникам легкий путь и стартовую площадку для атак внутри взломанной сети», — сказал Джон Шир, старший советник по безопасности Sophos.

«Конвергенция ИТ и OT увеличивает поверхность атаки и усугубляет и без того сложную среду угроз», — добавил он.

Из тех, кто заплатил выкуп — несмотря на предупреждения — 37% респондентов в конечном итоге заплатили более 100 000 долларов, а 8% заплатили более 1 миллиона долларов за ключ дешифрования.

Но, в то время как жертвы могут полагать, что удовлетворение требования о выкупе — это самый быстрый способ восстановить свои данные, согласно анализу инцидентов в производственном секторе, в среднем только 59% данных были восстановлены после уплаты выкупа — это ниже, чем 61% данных. % данных, восстановленных в среднем по всем секторам.

Одной из основных рекомендуемых мер защиты от атак программ-вымогателей является использование автономных резервных копий, а также их регулярное обновление и тестирование, чтобы в случае атаки программ-вымогателей можно было восстановить сети без уплаты выкупа. Тем не менее, отчет предупреждает, что производство имеет один из самых низких показателей использования резервного копирования в разных секторах.

Другие рекомендации по защите сетей от атак программ-вымогателей и других киберугроз включают обеспечение применения исправлений и обновлений безопасности, а также то, что, если обновления безопасности не могут быть

применены, устройство или система должны быть отделены от остальной части сети и удалены от лицом к Интернету.

Согласно исследованию, 38% попыток атак программ-вымогателей на производство и производство были остановлены до того, как данные могли быть зашифрованы, и Sophos рекомендует, чтобы активный поиск злоумышленников в сети имел решающее значение для обнаружения потенциальных инцидентов до того, как они произойдут…» ***(Danny Palmer. These ransomware victims are making the highest ransom payments // ZDNET, A Red Ventures company (https://www.zdnet.com/article/these-ransomware-victims-are-making-the-highest-ransom-payments/). 26.10.2022).***

***

«Более половины атак программ-вымогателей в настоящее время начинаются с того, что преступники используют уязвимости в удаленных и подключенных к Интернету системах, поскольку хакеры пытаются воспользоваться неисправленными проблемами кибербезопасности.

Согласно анализу инцидентов с программами-вымогателями за последний год, проведенному исследователями компании Secureworks, занимающейся безопасностью, 52% атак были начаты злоумышленниками, использующими удаленные сервисы.

Уязвимости в приложениях, подключенных к Интернету, стали наиболее распространенным вектором атаки программ-вымогателей. Часто эти интернет-приложения являются стандартными для корпоративных сред по всему миру, что делает их очень заманчивой мишенью для злоумышленников.

Эти приложения и службы могут быть подключены к Интернету, потому что организации нуждаются в них, чтобы сотрудники могли работать удаленно, или организации могут даже не знать, что эти приложения вообще доступны в Интернете.

По данным Secureworks, некоторые из уязвимостей, которые использовались для запуска атак программ-вымогателей, включают уязвимости в Microsoft Exchange Server., уязвимости в Fortinet VPN, уязвимость в Zoho ManageEngine ADSelfService Plus и многое другое — все они имеют официальные исправления, доступные от поставщиков.

Но даже когда исправления безопасности стали доступны, многие организации остаются уязвимыми для эксплойтов, потому что обновление не применяется.

Это особенно актуально, когда уязвимость обнаруживается недавно, и киберпреступники стараются как можно быстрее использовать ее до того, как будут выпущены исправления и организации смогут их применить.

«Даже там, где существует патч, процесс исправления уязвимости в корпоративной среде намного сложнее и медленнее, чем процесс использования злоумышленниками или разработчиками OST [наступательного инструмента безопасности] общедоступного кода эксплойта», — предупреждает отчет.

Установка исправлений может быть трудоемким и громоздким процессом, но по-прежнему жизненно важно защититься от атак программ-вымогателей и других

вредоносных программ, нацеленных на уязвимости в службах, доступных в Интернете.

Хотя более половины исследованных инцидентов с программами-вымогателями начались с того, что злоумышленники использовали уязвимости в Интернете, скомпрометированные учетные данные — имена пользователей и пароли — были отправной точкой для 39% инцидентов.

Существует несколько способов кражи имен пользователей и паролей, включая фишинговые атаки или заражение пользователей вредоносной программой для кражи информации. Злоумышленники также часто взламывают слабые или распространенные пароли. с помощью атак грубой силы.

Другие методы, которые киберпреступники использовали в качестве начальной точки входа для атак программ-вымогателей, включают заражение вредоносным ПО, фишинг, загрузку с диска и использование неправильных конфигураций сети.

Независимо от того, какой метод используется для инициирования кампаний программ-вымогателей, отчет предупреждает, что «программы-вымогатели остаются серьезной угрозой, которая питается пробелами в системах контроля безопасности».

Несмотря на проблемы, которые могут быть связаны с подготовкой к программам-вымогателям и другим злонамеренным киберугрозам, особенно в крупных корпоративных средах, исследователи Secureworks предполагают, что применение исправлений безопасности является одним из ключевых действий, которые организации могут предпринять для защиты своих сетей.

Еще одна форма защиты, которую, по мнению исследователей, следует применять для предотвращения атак программ-вымогателей, — это многофакторная аутентификация (MFA).

Применяя MFA, особенно к приложениям и учетным записям, имеющим доступ к критически важным службам, киберпреступникам становится намного сложнее входить в сеть и перемещаться по сети, даже если у них есть правильный пароль. Подобные шаги могут стать значительной силой в предотвращении атак программ-вымогателей еще до того, как они начнутся». ***(Danny Palmer. Ransomware: This is how half of attacks begin, and this is how you can stop them // ZDNET, A Red Ventures company (https://www.zdnet.com/article/ransomware-this-is-how-half-of-attacks-begin-and-this-is-how-you-can-stop-them/). 05.10.2022).***

***

«URSNIF, вредоносное ПО, также известное как Gozi, которое пытается украсть учетные данные для онлайн-банкинга с компьютеров жертв с Windows, развивается для поддержки программ-вымогателей.

Как один из старейших банковских троянов, появившийся в середине 2000-х годов, эта вредоносная программа имеет несколько вариантов и получила несколько прозвищ, включая URSNIF, Gozi и ISFB. Его пути пересекались с другими семействами вредоносных программ, с 2016 года дважды происходила утечка его исходного кода, и, по словам Mandiant, теперь это не единое семейство вредоносных программ, а «набор родственных братьев и сестер».

Он также видел, как его предполагаемые вдохновители предстали перед судами США. Последний из них был экстрадирован в этом году из Колумбии, куда он сбежал после освобождения под залог после ареста в Румынии в 2012 году.

Те, кто все еще стоит за URSNIF, идут по пути, проложенному разработчиками других семейств вредоносных программ, таких как Emotet, TrickBot и Qakbot, которые избавились от своего прошлого в краже банковской информации, чтобы стать бэкдорами на зараженных машинах, которые злоумышленники могут использовать для доставки программ-вымогателей и полезные нагрузки для кражи данных.

В отчете на этой неделе исследователи Mandiant Сандор Немес, Сулиан Лебег и Джесса Вальдес написали, что разновидность версии RM3 URSNIF больше не является банковским трояном, а является универсальным бэкдором, похожим на недолговечный вариант Saigon.

Этот бэкдор можно использовать для запуска программ-вымогателей, кражи данных и другой ужасной хрени на взломанных компьютерах.

«Это значительный отход от первоначальной цели вредоносного ПО, заключавшейся в совершении банковского мошенничества, но он соответствует более широкому ландшафту угроз», — написали исследователи, добавив, что, по их мнению, «за этим, вероятно, стоят те же субъекты угрозы, которые использовали вариант URSNIF для RM3». the] LDR4 [вариант]. Учитывая успех и изощренность RM3, которые ранее были у RM3, LDR4 может быть очень опасным вариантом, способным распространять программы-вымогатели, за которым следует внимательно следить».

Программы-вымогатели, а теперь и вымогательство данных, когда злоумышленники крадут файлы у жертв и угрожают их утечкой, если требуемые деньги не будут выплачены, сейчас повсюду. Только за первые три квартала этого года компания Intel 471, специализирующаяся на анализе угроз, обнаружила более 1500 заражений программами-вымогателями.

Атака программы-вымогателя может стоить компаниям и их страховым компаниям миллионы долларов, поэтому неудивительно, что авторитетные группы киберпреступников будут двигаться в этом направлении. URSNIF со своим последним вариантом LDR4, похоже, делает именно это.

Mandiant впервые обнаружил LDR4 в дикой природе 23 июня после анализа подозрительного электронного письма, которое напоминало сообщения, используемые RM3 годом ранее. В электронном письме есть ссылка на вредоносный веб-сайт, который перенаправляет жертву на сайт, выглядящий как законный бизнес, с вызовом CAPTCHA для загрузки документа Microsoft Excel, предположительно связанного с содержимым электронного письма. Если электронное письмо посвящено предложению о работе, считается, что документ содержит информацию об этом.

Нажатие на документ приводит к загрузке и выполнению полезной нагрузки LDR4, как только отметка следует данным инструкциям для запуска макросов в файле.

«Одной из самых заметных вещей во время анализа было то, что разработчики упростили и очистили различные части кода по сравнению с предыдущими

вариантами», — написали исследователи. «В частности, его банковские функции были полностью убраны».

URSNIF в свое время как банковское вредоносное ПО доставил множество проблем финансовым учреждениям и их клиентам. После экстрадиции в Америку Михая Ионута Паунеску, 37-летнего румына, обвиняемого в создании URSNIF, представители правоохранительных органов США заявили, что вредоносное ПО заразило более миллиона компьютеров Windows по всему миру, в том числе в США. По их оценкам, правительственные учреждения, организации и частные лица нанесли ущерб в десятки миллионов долларов.

Пользователи ПК в таких странах, как Германия, Великобритания, Польша, Италия и Турция, также пострадали от вредоносного ПО, которое могло регистрировать нажатия клавиш жертвы и красть учетные данные для входа в их банковские онлайн-счета.

Однако в 2020 году у варианта RM3 начались проблемы. Распределение и серверные части, особенно в Европе, рухнули, а затем не смогли воспользоваться сбоями, вызванными TrickBot и Emotet, для увеличения их использования.

«Одним из крупнейших победителей в этом стало семейство вредоносных программ ICEDID, которому удалось использовать сокращающуюся конкуренцию среди банковских вредоносных программ, поставив RM3 в затруднительное положение», — написала команда Mandiant, добавив, что это было необычно для варианта ISFB URSNIF, который породил другие варианты, в том числе RM3 — чтобы перестать получать обновления после июня 2020 года.

«Некоторые исследователи выдвинули гипотезу, что единственный способ вернуть это банковское вредоносное ПО — это серьезно обновить его код».

Последним шагом к падению RM3 стало удаление Microsoft Internet Explorer из Windows в июне. Вариант зависел от этого браузера для сетевого взаимодействия.

Аналитики Mandiant назвали LDR4 «смесь рефакторинга кода, регрессий и интересных стратегий упрощения». Он больше не использует пользовательский формат исполняемого файла PX, который впервые появился в RM3, а инструмент стеганографии под названием FJ.exe, который использовался в ISFB для сокрытия нескольких файлов в одной полезной нагрузке, либо ушел, либо был переработан.

Затем следует переход к новой стратегии — переход от банковского мошенничества к лазейке для других вредоносных программ.

«Кончина варианта RM3 в начале этого года и решения авторов значительно упростить свой код, включая удаление всех функций, связанных с банковскими операциями, указывают на радикальное изменение их ранее наблюдаемых TTP [тактики, методы и процедуры.]», — написала команда.

«Эти сдвиги могут отражать повышенное внимание злоумышленников к участию в операциях с программами-вымогателями или их разрешению в будущем».

Это подтвердилось, когда в этом году аналитики Mandiant увидели киберпреступника в подпольных сообществах, ищущего партнеров для распространения новой программы-вымогателя и варианта RM3, похожего на LDR4». ***(Jeff Burt. Good news, URSNIF no longer a banking trojan. Bad news, it's now a backdoor // The Register***

(https://www.theregister.com/2022/10/21/ursnif_trojan_shift_ransomware/). 21.10.2022).

***

«Digital Shadows стверджує, що в третьому кварталі 2022 кількість атак з використанням програм-вимагачів дещо знизилася. У звіті зазначається, що це є результатом перегрупування та переорієнтації зловмисників після напруженого початку року. Але при цьому наголошується, що гучні атаки все ще мали місце. У третьому кварталі найпоширенішою групою вірусів-вимагачів була LockBit, яка зайняла домінувала, в той час, як атаки вірусів-здирників Conti відійшли на другий план.

Головною особливістю атак шифрувальників в третьому кварталі стало розмивання кордонів між фінансово і політично мотивованими атаками. Як державні, так і приватні компанії стали об'єктами атак.

Компанія Digital Shadows зафіксувала зниження кількості атак з використанням програм-вимагачів на 10,5% порівняно з другим кварталом. Основними факторами цього стали закриття Conti та запуск LockBit 3.0. Зокрема, серпень був спокійним, але у вересні кількість атак з вимогами знову неухильно зростала.

На частку LockBit припадає 35,1% всіх атак з вимогою викупу в цьому кварталі, в порівнянні з 32,8% в попередньому кварталі. У вересні частка LockBit перевищила 40%, попри певний скептицизм серед хакерів щодо якості LockBit 3.0.

Зростання LockBit розглядається детальніше у звіті. При цьому дослідники Digitial Shadow стверджують, що успіх групи має свою ціну – зокрема, обурення з боку конкуруючих груп загроз і попер

«LockBitSupp часто, і сумнозвісно, вступає в публічні суперечки з іншими представниками програм-вимагачів, в тому числі з Conti й Alphv, – пояснюється у звіті. – Цілком можливо, що конкуруюча група націлилася на LockBit під виглядом помсти за злом Entrust».

Кульмінацією обурення проти LockBit стало поширення завантажувача LockBit 3.0 через Twitter у вересні. У відповідь LockBit заявила, що не була зламана, і звинуватила у витоку колишнього розробника. Дослідники Digital Shadows зазначають, що незалежно від джерела, код виглядає легітимним, що призведе до можливих наслідків у четвертому кварталі, якщо інші суб'єкти загрози використають його у власних цілях.

Особливо помітною також є політизація програм-вимагачів у цьому кварталі. Так, з'явилася інформація, що колишні члени групи Conti націлилися на Україну. Це підтверджує зростаючу тенденцію перетину між політичними та фінансово мотивованими гравцями. Якщо минулі атаки Conti на українські готельні організації можна пояснити фінансовими мотивами, то рішення націлюватися на українські державні структури майже напевно пов'язане з російсько-українською війною.

Надзвичайно руйнівні атаки на Чорногорію та Албанію також є прикладами викликів, пов'язаних з політично вмотивованими програмами-вимагачами. Атака на Чорногорію, в якій спочатку звинувачували росію, була здійснена з Куби.

Аналогічна історія сталася з Албанією, в якій звинувачували росію, а потім з'ясувалося, що атака була здійснена з Ірану.

У звіті робиться висновок, що банди й групи, які вимагають викуп, всупереч зниженню кількості атак в третьому кварталі, поширені як ніколи. Digital Shadows відстежує 97 сайтів-вимагачів і сайтів витоку даних, з яких 44 є активними». ***(Евгений Куликов. Натиск вірусів-вимагачів дещо ослаб // Компьютерное Обозрение (https://ko.com.ua/natisk_virusiv-vimagachiv_deshho_oslab_142489). 31.10.2022).***

***

Програми-трояни

«Одна из старейших и наиболее успешных форм банковского вредоносного ПО была перепрофилирована в троян-бэкдор, который был описан как «чрезвычайно опасный» и, вероятно, будет использоваться для атак программ-вымогателей.

Новый вариант вредоносного ПО Ursnif, также известный как Gozi, был подробно описан исследователями компании Mandiant, занимающейся безопасностью, которые предполагают, что он был специально создан для поддержки программ-вымогателей и атак с целью кражи данных.

Первое воплощение вредоносного ПО, предназначенное для кражи банковских реквизитов, появилось в 2006 году и нанесло убытки в десятки миллионов долларов, причем ФБР назвало его «одним из самых финансово разрушительных компьютерных вирусов в истории». С тех пор первоначальный исходный код просочился, что породило несколько новых вариантов, которые до сих пор досаждают жертвам.

Эти версии Ursnif застряли с целью исходного вредоносного ПО — кражи банковских реквизитов. Но, согласно анализу Mandiant, ситуация изменилась с появлением нового варианта, получившего название LDR4, который перепрофилировал Ursnif во вредоносное ПО в стиле Trickbot и Emotet.

Злоумышленники, использующие вредоносное ПО, могут похитить данные или использовать бэкдор для установки программы-вымогателя, что может нанести гораздо больший и серьезный ущерб, чем кража банковских реквизитов, и обеспечить злоумышленникам гораздо большую зарплату.

«LDR4 может быть очень опасным вариантом — способным распространять программы-вымогатели — за которым следует внимательно следить», — предупредил Мандиант в своем блоге.

Новый вариант был впервые замечен в июне этого года и распространяется с использованием того же метода, что и предыдущие кампании Ursnif и многие другие атаки вредоносных программ, через фишинговые электронные письма.

Некоторые из этих фишинговых писем якобы отправлены рекрутером с предложением новой возможности. В сообщениях утверждается, что из-за Общего регламента по защите данных они не могут раздавать информацию по электронной почте, поэтому жертве предлагается загрузить документ, чтобы узнать больше.

Другие распространяются в сообщениях, в которых утверждается, что в них содержится счет, который необходимо срочно просмотреть.

Независимо от того, как выглядит приманка, если пользователь следует инструкциям в фишинговом электронном письме, это приведет к загрузке полезной нагрузки Ursnif, которая предоставляет злоумышленникам удаленный доступ к машине.

«Это значительный отход от первоначальной цели вредоносного ПО, заключавшейся в совершении банковского мошенничества, но он соответствует более широкому ландшафту угроз», — заявили исследователи Mandiant.

Хотя это потенциально опасное вредоносное ПО, стать жертвой этой последней версии Ursnif далеко не неизбежно. Поскольку они приходят через фишинговые электронные письма, организации должны сделать все возможное, чтобы обеспечить наличие средств защиты для выявления и блокировки вредоносного спама.

Они также должны информировать пользователей о рисках, связанных с фишинговыми сообщениями, и информировать их о типах тем, которые используются для заманивания жертв». ***(Danny Palmer. This old malware has been rebuilt with new features to use in ransomware attacks // ZDNET, A Red Ventures company (https://www.zdnet.com/article/this-old-malware-has-been-rebuilt-with-new-features-to-use-in-ransomware-attacks/). 20.10.2022).***

***

Фішингові атаки

«…Фишинг ничего не подозревающих энтузиастов и новичков NFT по-прежнему является популярной схемой мошенничества, используемой онлайн-хакерами и мошенниками, которые успешно ограбили тысячи потребителей, имитируя или взламывая цифровые форумы, веб-сайты и учетные записи в социальных сетях известных проектов NFT, чтобы заманить ничего не подозревающих жертв в покупка поддельных NFT. В одном случае хакеры взломали официальную страницу чрезвычайно популярной коллекции NFT в социальных сетях и поделились ссылками на поддельный аирдроп. Последователи, которые нажимали на мошеннические ссылки, были заманены подключением и авторизацией доступа к своим цифровым кошелькам, неосознанно позволяя хакерам выкачивать все средства из них. Мошенники нацелились на еще один долгожданный запуск NFT, используя поддельные веб-сайты и имена пользователей в популярной платформе обмена сообщениями в социальных сетях, чтобы обманным путем общаться с ничего не подозревающими энтузиастами и побуждать их к покупке поддельных NFT. Вводить покупателей в заблуждение, заставляя их поверить, что они общаются с брендом, — опасно простой и эффективный способ обмануть жертв. Такие транзакции после совершения не могут быть отменены. Покупатели NFT должны сохранять бдительность и принимать меры предосторожности, такие как повторная проверка URL-адресов торговых площадок и других каналов социальных сетей бренда на наличие соответствующих обновлений, прежде чем завершать

какие-либо покупки. Аналогичным образом, бренды и торговые площадки цифровых активов могут публиковать уведомления и раскрытия информации, предупреждающие потребителей о таких рисках и подготавливающие их к тому, как реагировать на них.

Инсайдерская торговля

Торговые площадки NFT также уязвимы для инсайдерской торговли, когда сотрудники используют инсайдерскую информацию для покупки эксклюзивных NFT до того, как они станут общедоступными, а затем продают их с прибылью после скачка цен. Министерство юстиции США (DOJ) недавно предъявило обвинение бывшему сотруднику торговой площадки NFT и его сообщникам в мошенничестве с использованием электронных средств связи и отмывании денег «в связи со схемой совершения инсайдерской торговли». Министерство юстиции утверждало, что бывший сотрудник использовал конфиденциальную информацию об определенных NFT, выбранных для продвижения на рынке NFT, чтобы приобрести их заранее и получить выгоду от соответствующего увеличения стоимости NFT после продвижения.

Чтобы предотвратить инсайдерскую торговлю, торговые площадки NFT могут внедрять формальные политики, которые формулируют запрещенное поведение, проводят обучение сотрудников, отслеживают покупки и продажи, требуют периодической отчетности, устанавливают периоды блокировки для транзакций сотрудников, предоставляют горячие линии для анонимных сообщений и создают брандмауэры. Такие политики должны быть разработаны заранее, чтобы информировать сотрудников о правовых рисках, связанных с инсайдерской торговлей, и предотвращать инсайдерскую торговлю.

Отмывание денег и финансирование незаконной деятельности

«Рынок NFT является главной мишенью для финансовых преступлений, включая отмывание денег, финансирование терроризма и мошенничество», по данным аналитической компании Elliptic, которая недавно сообщила, что с 2017 года через торговые площадки NFT было отмыто более 8 миллионов долларов незаконных средств. Один из методов отмывания — «самоотмывание» — является особенно распространенным и включает в себя покупку физическими лицами NFT за незаконные средства, а затем создание последующих повторных транзакций с собой или связанными сторонами с использованием многочисленных уникальных открытых ключей для «очистки» средств путем запутывания поток транзакций и, следовательно, их связь с преступной деятельностью к концу цикла.

НФТ также могут быть связаны с коррупционной финансовой деятельностью из-за присущих НФТ характеристик, которые можно использовать для облегчения преступлений. Такие характеристики включают в себя различные уровни анонимности, доступные для транзакций блокчейна, и возможность мгновенного расчета транзакций по всему миру. Например, аналитики блокчейна и представители разведки заметили, что Исламское Государство Ирака и Сирии (ИГИЛ) использовало NFT для вербовки и финансирования, и что NFT на тему ИГИЛ был виден по крайней мере на одном торговом веб-сайте NFT. Это недавнее открытие иллюстрирует жизнеспособность использования NFT для финансирования незаконной деятельности не только из-за их возможностей по сбору средств, но и

потому, что их неизгладимый характер делает практически невозможным их удаление или цензуру, в отличие от других инструментов онлайн-вербовки и обмена сообщениями.

Биржи и торговые площадки NFT могут принимать меры для предотвращения отмывания денег, такие как внедрение надлежащих процедур «знай своего клиента» и борьбы с отмыванием денег, мониторинг торговли и активности интернет-протокола среди пользователей, а также запрет и удаление контента, связанного с незаконной деятельностью. Однако, поскольку NFT записываются в неизменной цепочке блоков, их будет трудно (если не невозможно) полностью устранить.

Манипуляции рынком

Как и в случае с самоотмыванием, злоумышленники нашли способы манипулировать рынками NFT, искусственно увеличивая стоимость определенных NFT посредством «фиктивной торговли» — практики создания большого объема торгов для манипулирования рыночными ценами в свою пользу. Мошенническая торговля создает иллюзию того, что NFT пользуется большим спросом, тогда как на самом деле все транзакции исходят от одного человека или между связанными лицами, использующими разные кошельки, чтобы скрыть тот факт, что такие транзакции связаны. Этот тип сфабрикованного спроса может заставить ничего не подозревающих покупателей поверить в то, что NFT более ценен, чем он есть на самом деле, и может быть очень прибыльным для тех, кто занимается такими незаконными действиями. Например, в одном отчете было обнаружено, что ложная торговля принесла десяткам трейдеров около 8,9 миллионов долларов в совокупности.

Хотя такие методы бывает трудно установить, потребители должны опасаться их, прежде чем покупать NFT. Покупатели NFT должны уделять пристальное внимание активности в социальных сетях и участвовать в других мероприятиях по осмотрительности, чтобы определить, действительно ли конкретный NFT высоко ценится. Торговые площадки и бренды также могут принимать меры для защиты потребителей, используя инструменты аналитики блокчейна для мониторинга активности транзакций NFT, чтобы выявлять и блокировать действия злоумышленников, пытающихся участвовать в фиктивной торговле.

Эксплойты платформы

Уязвимости платформы и эксплойты могут привести к значительным финансовым потерям для пользователей платформы. Недавний пример этого произошел, когда крупная глобальная платформа NFT непреднамеренно способствовала продаже «неактивных» списков NFT опытным покупателям, которые поняли, что опытные держатели NFT часто переводят NFT «голубых фишек» в другие кошельки, которые они контролируют, вместо того, чтобы исключить их из листинга (что требуют ручной отмены за отдельную плату). Перемещая NFT между кошельками, держатели NFT смогли удалить публичный листинг и избежать платы, связанной с его отменой.

Однако этот процесс просто обновил список с «активного» на «неактивный», что позволило осведомленным покупателям приобретать неактивные NFT через смарт-контракт, а не через пользовательский интерфейс биржевой платформы. Согласно сообщениям, одна популярная платформа NFT была вынуждена

возместить до 1,8 миллиона долларов пользователям, которые по незнанию продали свои NFT по ценам, намного ниже рыночной стоимости, из-за проблемы с пользовательским интерфейсом платформы.

Недостатки безопасности также могут быть обнаружены во внутренней архитектуре торговых площадок NFT, которые, если их не устранить, могут привести к значительным потерям для пользователей торговых площадок. Например, одному популярному маркетплейсу NFT недавно было предложено обновить внутреннюю кодировку, чтобы исправить уязвимость в системе безопасности, обнаруженную сторонней фирмой по обеспечению безопасности. Если бы злоумышленники заметили и воспользовались уязвимостью серверной части, они смогли бы отправить владельцам NFT вредоносные ссылки, которые при нажатии на них потенциально могли бы предоставить полный доступ к кошелькам пользователей и NFT или другим цифровым активам, расположенным в них.

В то время как эти конкретные эксплойты были устранены в одном случае постфактум, а в другом случае до того, как какой-либо эксплойт произошел, торговые площадки NFT уведомлены о необходимости планировать и разрабатывать продукты и пользовательские интерфейсы, которые защищают потребителей от непреднамеренного воздействия риска.

Вывод

Ежедневно происходят взаимозаменяемые и невзаимозаменяемые транзакции цифровых активов на миллиарды долларов. Таким образом, пользователи и платформы должны сохранять бдительность, чтобы защитить себя от мошенничества, взломов и других незаконных действий, и принимать меры для минимизации этих рисков. Группы BakerHostetler по технологиям блокчейна и реагированию на инциденты, связанные с безопасностью цифровых активов и данных, состоят из десятков опытных специалистов, в том числе юристов, которые работали в Министерстве юстиции, и многих других, обладающих обширным опытом работы во всех секторах рынка блокчейнов и криптовалют, от расследований до реагирования на инциденты. и кибербезопасность, соблюдение Закона о банковской тайне / противодействии отмыванию денег, налогообложение, конфиденциальность, транзакции, интеллектуальная собственность, а также разработка средств массовой информации и технологий в соответствии с федеральным законодательством, надзором Конгресса, расследованиями и государственной политикой. Пожалуйста, не стесняйтесь обращаться к любому из наших опытных специалистов, если у вас есть вопросы об этом предупреждении». ***(Veronica Reynolds, Robert A. Musiala Jr., Sally Kim, and Reem Chehade. Top NFT-Related Cybersecurity, Phishing, Hacking and Other Risks in 2022 // Baker & Hostetler LLP (https://www.bakerdatacounsel.com/data-breaches/top-nft-related-cybersecurity-phishing-hacking-and-other-risks-in-2022/#page=1). 26.10.2022).***

***

«Согласно исследованию, проведенному Avanan, компанией Check Point, киберпреступники усовершенствовали свою способность проводить специальные фишинговые атаки по электронной почте, чтобы обойти защиту электронной почты Microsoft.

Рассматривая Microsoft 365 как важнейшую начальную точку входа для многих организаций, злоумышленники разрабатывают и тестируют каждую фишинговую атаку, чтобы убедиться, что она обходит средства защиты безопасности Microsoft по умолчанию.

Аванан пояснил, что Microsoft не смогла остановить угрозы электронной почты не потому, что ее функции безопасности электронной почты ухудшились, а потому, что хакеры стали лучше и быстрее разрабатывать уклончивые атаки.

Платформа безопасности электронной почты проанализировала три миллиона электронных писем, полученных ее клиентами, которые используют этот инструмент в качестве последней линии защиты от угроз, которые обходят стандартные инструменты безопасности Microsoft.

Больше фишинговых атак по электронной почте обходят Microsoft Exchange Online Protection (EOP) и Defender.

Аванан обнаружил, что инструменты безопасности электронной почты Microsoft позволили почти пятой части (18,8%) фишинговых сообщений достичь своих целей.

Согласно исследованию, способность Microsoft Exchange Online Protection (EOP) и Defender останавливать фишинговые атаки по электронной почте снизилась на 74% по сравнению с 2020 годом, когда уровень отказов составлял всего 10,8%.

Однако процент промахов увеличился до 42%, когда киберпреступники разработали специальные фишинговые атаки по электронной почте против финансов целей, например, поддельные счета-фактуры и переводы биткойнов.

Microsoft Defender также пропустил 22 % атак с использованием олицетворения бренда, 21 % попыток сбора учетных данных и 12 % атак с использованием социальной инженерии.

Уровень обнаружения Microsoft еще больше снизился для более крупных организаций: 50-70% фишинговых писем достигают почтовых ящиков своих целей. И наоборот, предыдущее исследование Аванана показало, что уровень обнаружения не коррелирует с размером организации в 2020 году, при этом в некоторых более крупных компаниях показатель промахов составляет 2,6%.

Аванан выделил одну крупную организацию с более чем 53 000 сотрудников, где ИТ-персонал предотвратил только 59 из 910 фишинговых сообщений, что составляет всего 7%. Компания заявила, что ей требуется 16 штатных сотрудников для борьбы с фишинговыми атаками по электронной почте, о которых сообщают пользователи. Аванан также обнаружил, что ручное реагирование на проблемы безопасности занимает 23% времени сотрудников.

Кроме того, исследователи обнаружили организацию, которая тратила 2500 часов или 104 дня на реагирование на сообщения пользователей о попытках фишинга. Впоследствии утечка времени подорвала другие приоритеты и вызвала выгорание технических специалистов и сотрудников службы безопасности.

Погружение в мусорные контейнеры приводит к успешным фишинговым атакам по электронной почте

Исследование, проведенное платформой безопасности электронной почты, показало, что Microsoft Defender отправляет 7% фишинговых писем в папку «Нежелательная почта».

Отправка обнаружений в папку «Нежелательная почта» может привести к тому, что сотрудники могут получить к ним доступ через «поиск в мусорных баках». Многие организации предпочли отправлять помеченные сообщения в папку нежелательной почты, чтобы избежать блокировки законных электронных писем.

«Конечные пользователи привыкли копаться в папке «Спам» в поисках законных сообщений». — сказали исследователи. «Пользователи могут по ошибке действовать с фишинговым электронным письмом, и многие электронные письма могут быть найдены в папке нежелательной почты без различия между сокровищами и мусором».

Microsoft преуспела в блокировании атак BEC и вложений вредоносного ПО

Однако Microsoft преуспела в других областях, таких как блокировка сообщений о компрометации деловой электронной почты (BEC) на 93% и вложений вредоносных программ на уровне 90%.

Исследователи заявили, что большинство фишинговых атак по электронной почте были нацелены на Microsoft. Хотя технологический гигант проигрывал борьбу в некоторых областях, снижение эффективности не было референдумом по его методам обеспечения безопасности.

«Это представляет собой не снижение эффективности Microsoft, а скорее увеличение целевых атак, направленных непосредственно на обход Microsoft. Другими словами, хакеры активизировали свою игру».

Хакеры используют такие тактики, как избегание источников вредоносных ссылок, используя законные службы, маскируя URL-адреса и избегая вложений, чтобы обойти защиту от фишинга.

Исследователи Avanan предсказали, что злоумышленники продолжат изобретать способы обхода стандартных функций безопасности электронной почты и дополнительных уровней». ***(Alicia Hope. Study Shows Attackers Designing Email Phishing Attacks To Bypass Microsoft Email Defenses, and They Are Winning // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/study-shows-attackers-designing-email-phishing-attacks-to-bypass-microsoft-email-defenses-and-they-are-winning/). 14.10.2022).***

***

«По данным Check Point, DHL является брендом, который злоумышленники чаще всего используют, когда речь идет о фишинговых электронных письмах.

Мошенники чаще всего использовали торговую марку в своих попытках украсть личную и платежную информацию с марок в период с июля по сентябрь 2022 года, при этом на долю гиганта судоходства приходится 22 процента всех попыток фишинга во всем мире, перехваченных подразделением кибербезопасности.

DHL предупредила клиентов, что 28 июня стала целью «крупного глобального мошенничества и фишинговой атаки», и отметила, что «прилагает все усилия, чтобы заблокировать мошеннические веб-сайты и электронные письма».

Злоумышленники использовали проверенное поддельное сообщение в попытках фишинга, ложно предупреждая клиентов о том, что их посылка не может

быть доставлена, и запрашивая личную и платежную информацию для продолжения доставки.

Как мы видели на примере недавней киберпреступности Oktapus, эти типы срочных запросов — сменить пароль или, в данном случае, информацию о доставке или оплате — особенно эффективны для кражи учетных данных.

Не нажимайте на это

Одно фишинговое письмо, обнаруженное Check Point с попыткой выдать себя за DHL, было отправлено с адреса «info@lincssourcing[.]com». Мошенники подделали его так, чтобы он выглядел так, как будто отправителем был «DHL Express», как отмечается в отчете компании по безопасности.

Строка темы электронного письма «Недоставленная DHL (посылка / доставка)» и сообщение также пытались обмануть жертву, заставив ее щелкнуть вредоносную ссылку, утверждающую, что им необходимо обновить свой адрес доставки, чтобы получить посылку.

Конечно, URL-адрес на самом деле не направляет пользователя на веб-сайт DHL. Вместо этого они переходят на поддельный веб-сайт, контролируемый злоумышленниками, с формой, предлагающей жертве ввести свое имя и пароль, которые затем перехватываются мошенниками.

Эти украденные учетные данные затем можно использовать для получения другой информации об учетной записи, такой как платежные реквизиты, или их можно просто продать другим похитителям личных данных на форумах темной сети.

В то время как DHL возглавляет список поднятых брендов, Check Point сообщает, что Microsoft находится на втором месте по фишинговым мошенничествам в третьем квартале, что составляет 16 процентов всех кампаний, направленных на получение прибыли за счет узнаваемости бренда. LinkedIn, который возглавлял список как в первом, так и во втором квартале этого года, опустился на третье место с 11 процентами.

Жертвы с большей вероятностью нажмут на вредоносную ссылку, которая выглядит так, как будто она была отправлена из надежного бренда, что поддерживает фишинговый пул. Это недорогое преступление с высокой окупаемостью для мошенников.

Фишинговые атаки были, безусловно, наиболее частыми киберпреступлениями, о которых сообщалось в прошлом году: в ФБР было сообщено о 323 972 атаках, которые обошлись жертвам в 44,2 миллиона долларов.

В другом примере фишинга с подделкой бренда Check Point подробно описал, как преступники использовали поддельную электронную почту OneDrive, чтобы попытаться украсть информацию об учетной записи пользователя Microsoft. В этом конкретном мошенничестве сообщение было отправлено с адреса «websent@jointak[.]com[.]hk», с использованием «OneDrive» в качестве фальшивого имени отправителя и содержало тему: «Документ под названием «Предложение» был передан ты на Onedrive».

Подобно подделке DHL, фишинг под брендом Microsoft пытается заманить жертву, чтобы она щелкнула вредоносную ссылку, которая подделывает страницу входа в веб-приложение Microsoft, а затем ввела пароль своей учетной записи.

Не то чтобы нам нужно было говорить вам об этом, но, как правило, не доверяйте электронным письмам, особенно тем, которые запрашивают личную информацию или данные кредитной карты, предупредил Check Point. Кроме того, «подумайте дважды, прежде чем открывать вложения электронной почты или ссылки, особенно электронные письма, которые якобы принадлежат таким компаниям, как DHL, Microsoft или LinkedIn». ***(Jessica Lyons Hardcastle. DHL named most-spoofed brand in phishing // The Register (https://www.theregister.com/2022/10/24/dhl_phishing_scams/). 24.10.2022).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Человеку, стоящему за вредоносным программным обеспечением Raccoon, предназначенным для кражи информации, грозит экстрадиция в Соединенные Штаты и перспектива более чем 20 лет тюремного заключения.

Голландские власти арестовали 26-летнего гражданина Украины Марка Соколовского в марте, что свидетельствует о недавно раскрытом обвинительном заключении федеральной прокуратуры Техаса.

Арест Соколовского был приурочен к международной операции правоохранительных органов по демонтажу инфраструктуры, поддерживающей Raccoon в то время. В заявлениях, размещенных на криминальных форумах вскоре после операции, говорилось, что троянец больше не будет доступен, что предполагает закрытие как-то связано с продолжающимся вторжением России в Украину.

С тех пор неназванные сообщники Соколовского возобновили операцию с переписанным трояном, говорится в исследовании фирмы по кибербезопасности Sekoia.

Соколовский обжалует сентябрьское решение голландского суда, разрешающее его экстрадицию в США.

Raccoon завоевал популярность среди онлайн-преступников с момента своего появления в 2019 году. Доступ к панели администрирования и обслуживанию клиентов стоит пользователям 200 долларов в криптовалюте в месяц или 75 долларов в неделю. Анализ вредоносного ПО, проведенный CyberArk, показал, что это «не самое сложное вредоносное ПО, доступное кибер-злоумышленникам, но оно оказалось весьма эффективным». Киберпреступники могли настроить конфигурацию и похитить данные почти из 60 приложений.

Прокуроры говорят, что пользователи заражали жертв трояном удаленного доступа через фишинговые электронные письма. CyberArk также обнаружил его распространение с помощью наборов веб-эксплойтов, исследующих уязвимые браузерные приложения. Французская фирма по кибербезопасности Sekoia обнаружила, что Raccoon распространяется как предположительно взломанные приложения для потенциальных пиратов программного обеспечения.

Прокуратура утверждает, что данные миллионов жертв, включая личную и финансовую информацию, а также пароли, были украдены через Raccoon. Агенты ФБР говорят, что они идентифицировали более 50 миллионов уникальных учетных данных и форм идентификации, таких как банковские счета и криптовалютные адреса, полученные пользователями Raccoon. Бюро создало веб-сайт, на котором любой желающий может проверить, есть ли его электронная почта в базе данных жертв Raccoon. Те, кто получит совпадение, получат электронное письмо с подтверждением, содержащее дополнительную информацию.

Соколовскому предъявлены четыре уголовных обвинения, включая сговор с целью совершения мошенничества с использованием электронных средств и отмывания денег, а также сговор с целью совершения мошенничества в связи с компьютерами. Его онлайн-клиенты включают Photix, raccoonstealer и black21jack77777». ***(David Perera. US Indicts Ukrainian for Role in Raccoon Malware Scheme // Information Security Media Group, Corp. (https://www.govinfosecurity.com/us-indicts-ukrainian-for-role-in-raccoon-malware-scheme-a-20329). 25.10.2022).***

***

Технічні аспекти кібербезпеки

«Исследователи компьютерной безопасности говорят, что они разработали управляемую искусственным интеллектом систему, которая может за секунды угадывать пароли компьютеров и смартфонов, исследуя тепловые сигнатуры, которые кончики пальцев оставляют на клавиатуре и экранах при вводе данных.

Исследователи из Школы компьютерных наук Университета Глазго под названием ThermoSecure разработали систему, чтобы показать, как падение цен на тепловизионные камеры и расширение доступа к алгоритмам машинного обучения и искусственного интеллекта (ИИ) открывают новые возможности для того, что они называют термические атаки.

Взглянув с помощью тепловизионной камеры на клавиатуру компьютера, экран смартфона или клавиатуру банкомата, можно сделать снимок, показывающий недавнюю тепловую сигнатуру пальцев, касающихся устройства.

Чем ярче область на тепловом изображении, тем раньше к ней прикасались. Это означает, что изображение можно использовать для взлома пароля или пин-кода путем анализа того, где и когда касались клавиатуры или экрана.

Более раннее исследование термальных атак, проведенное Университетом Глазго, показало, что люди, не имеющие опыта, могут угадывать пароли, глядя на тепловые изображения, а теперь, благодаря добавлению искусственного интеллекта, специалисты-взломщики могут взламывать пароли еще быстрее.

Используя ThermoSecure для анализа изображений с помощью ИИ, 86% паролей были раскрыты, когда тепловые изображения были сделаны в течение 20 секунд, 76% паролей можно было угадать с помощью изображений в течение 30 секунд, а 62% можно было обнаружить через 60 секунд.

Чем длиннее пароль, тем сложнее было его раскрыть, но в большинстве случаев это все же удавалось. ThermoSecure может взломать две трети паролей длиной до 16 символов, и по мере того, как пароли становятся короче, система добивается большего успеха: 12-символьные пароли угадываются в 82% случаев, а восьмизначные пароли угадываются до 93 раз. % времени.

Пароли, состоящие из шести или менее символов, успешно взламывались в 100% случаев, что делало PIN-коды банкоматов или более короткие коды, используемые для защиты смартфонов, особенно уязвимыми для атак.

Используя эту умную технику, злоумышленник, наблюдающий за потенциальными жертвами, может сделать тепловое фото клавиатуры, смартфона или банкомата и использовать его для подбора паролей. В некоторых случаях им также потребуется физический доступ к устройству, но также возможно, что цель может оставить свой компьютер без присмотра.

Также существует вероятность того, что злоумышленник уже может знать имя пользователя онлайн-учетной записи своей цели или потенциально может использовать тепловую атаку, чтобы раскрыть и это.

Статья о ThermoSecure, написанная доктором Мохамедом Кхамом из Университета Глазго, доктором Джоном Уильямсоном и Норой Алотаиби, была опубликована в надежде, что она показывает потенциальный риск, связанный с термальными атаками, поскольку технология, используемая для их питания, становится все дешевле и больше. широко доступный.

«Доступ к тепловизионным камерам стал более доступным, чем когда-либо — их можно найти менее чем за 200 фунтов стерлингов — и машинное обучение также становится все более доступным. Это делает весьма вероятным, что люди во всем мире разрабатывают системы по аналогии с ThermoSecure для кражи паролей», — сказал д-р Мохамед Хамис, преподаватель компьютерных наук Университета Глазго, руководивший разработкой ThermoSecure.

«Важно, чтобы исследования в области компьютерной безопасности шли в ногу с этими разработками, чтобы найти новые способы снижения рисков, и мы продолжим развивать нашу технологию, чтобы попытаться быть на шаг впереди злоумышленников», — добавил он.

Но хотя исследование демонстрирует некоторые передовые методы, которые можно использовать для взлома паролей, пользователи могут защитить свои учетные записи, выполнив одну относительно простую вещь — используя более надежные пароли...» ***(Danny Palmer. This 'thermal attack' can read your password from the heat your fingertips leave behind // ZDNET, A Red Ventures company (https://www.zdnet.com/article/this-thermal-attack-can-read-your-password-from-the-heat-your-fingertips-leave-behind/). 10.10.2022).***

***

«Одной из самых популярных уязвимостей системы безопасности среди киберпреступников за последние несколько месяцев является программная уязвимость в Microsoft Office, которой более пяти лет, и она продолжает использоваться, поскольку, несмотря на давно доступное обновление безопасности, многие предприятия до сих пор не применили его.

Согласно анализу, проведенному исследователями кибербезопасности из Digital Shadows, наиболее часто обсуждаемой киберпреступниками на подпольных форумах за последние три месяца уязвимости является CVE-2017-11882 — уязвимость в безопасности Microsoft Office, впервые обнаруженная в 2017 году.

При успешном использовании эта уязвимость позволяет киберпреступникам удаленно выполнять код в уязвимой системе Windows, предоставляя злоумышленникам возможность тайно установить вредоносное ПО на машину.

Вредоносное ПО, используемое для атак с использованием CVE-2017-11882, включает Formbook, который тайно предоставляет злоумышленникам возможности удаленного доступа, регистрацию нажатий клавиш и возможность делать снимки экрана, подвергая жертв риску кражи имен пользователей и паролей.

Уязвимость также связана с доставкой Redline — вредоносного ПО, которое крадет имена пользователей, пароли, данные кредитных карт и содержимое криптовалютных кошельков, а также содержимое журналов чатов.

Атаки с целью использования CVE-2017-11882 часто начинаются с фишинговых писем, предназначенных для того, чтобы заманить жертв открыть вредоносные документы, которые вызывают ошибку.

Хотя исправление безопасности для CVE-2017-11882 доступно уже несколько лет, уязвимость по-прежнему достаточно распространена, чтобы ею могли воспользоваться киберпреступники…

Второй по популярности уязвимостью за отчетный период стала Follina (CVE-2022-30190) — уязвимость нулевого дня высокой степени опасности в Microsoft Word, возникшая ранее годом.

Follina позволяет злоумышленникам выполнять удаленный код и развертывать вредоносное ПО для получения доступа к системам; эта уязвимость активно использовалась поддерживаемыми государством хакерскими группами и бандами киберпреступников. Доступен патч для исправления этой уязвимости.

Третьей по популярности уязвимостью является CVE-2022-2294, уязвимость нулевого дня в Google Chrome, впервые обнаруженная и исправленная в июле. Однако многие пользователи еще не установили обновление для системы безопасности, поэтому оно остается популярным методом атаки для пользователей Google Chrome.

Хотя регулярное применение обновлений безопасности для всех типов программного обеспечения в корпоративной сети может быть сложной задачей, это одна из лучших вещей, которую предприятия могут сделать, чтобы помочь защитить свою сеть и пользователей от кибератак, особенно если они сосредоточены на

исправлении некоторых из наиболее часто используемые уязвимости…» ***(Danny Palmer. These cybersecurity vulnerabilities are most popular with hackers right now - have you patched them? // ZDNET, A Red Ventures company (https://www.zdnet.com/article/these-cybersecurity-vulnerabilities-are-most-popular-with-hackers-right-now-have-you-patched-them/). 27.10.2022).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Стартап в области кибербезопасности Protexxa привлек начальное финансирование в размере 4 млн канадских долларов. Компания стремится устранить риски для бизнеса, возникающие из-за пробелов в личной кибербезопасности как для компаний, так и для отдельных лиц.

Раунд начального финансирования возглавлял BKR Capital, который инвестирует в революционные компании и многообещающих основателей технологий Black. В раунде также приняли участие Ангелы Firehood и несколько ангелов-инвесторов, в том числе Джефф Феттс, Аннетт Вершурен и Лин Ли.

Средства будут использованы для создания платформы кибербезопасности с технологией вспомогательного исправления, облегчения пилотных проектов с глобальными клиентами и подготовки к масштабированию ее операций. В настоящее время компания находится в процессе подачи нескольких патентов.

Protexxa — детище мирового лидера в области информационных технологий и руководителя службы кибербезопасности Клодетт Макгоуэн. До прихода в Protexxa Макгоуэн занимал должность глобального исполнительного директора по кибербезопасности в TD Bank. Поскольку она увлечена продвижением женщин в области технологий, 70% инвесторов Protexxa — женщины.

Персонализированная платформа защиты от кибербезопасности Protexxa

Половина из 4,95 миллиарда пользователей Интернета во всем мире являются жертвами киберпреступлений, и большинство из них даже не осознают, что их взломали. Protexxa обращается к человеческому элементу кибербезопасности, соединяя точки между личной кибергигиеной и бизнес-рисками.

Используя искусственный интеллект (ИИ), платформа Protexxa выявляет, оценивает, прогнозирует и решает распространенные кибер-проблемы. Поскольку 43% кибератак нацелены на малый бизнес, кибер-решения для предприятий любого размера нужны сейчас как никогда.

Персонализированная платформа защиты от кибербезопасности Protexxa в настоящее время тестируется в нескольких отраслях, включая правительство, научные круги и здравоохранение…» ***(Protexxa raises $4 million to remediate gaps in cybersecurity for companies and individuals // Help Net Security (https://www.helpnetsecurity.com/2022/10/30/protexxa-funding/). 30.10.2022).***

***

«Программа кибербезопасности Cochise College прошла проверку Агентством национальной безопасности (АНБ) и группой академических коллег до 2027 года. Проверка является требованием для Национального центра академического превосходства (CAE) в программах, предназначенных для кибербезопасности. Программа CAE направлена на создание совместной образовательной программы по кибербезопасности с общественными колледжами и университетами, которая устанавливает стандарты для учебных программ и академических достижений. Это включает в себя развитие компетенций среди студентов и преподавателей, ценит работу с сообществом и лидерство в профессиональном развитии, интеграцию практики кибербезопасности в учебном заведении по академическим дисциплинам и активное участие в решении проблем образования в области кибербезопасности.

«Ваша способность удовлетворять растущие требования программы валидации сослужит хорошую службу стране, способствуя защите национальной информационной инфраструктуры», — говорится в письме о валидации. «Высококвалифицированная рабочая сила в области кибербезопасности является стратегическим преимуществом в области национальной безопасности. Правительство Соединенных Штатов продолжит инвестировать и совершенствовать программы, направленные на формирование внутреннего кадрового резерва, от начального до высшего образования».

Любой студент, который получает степень младшего специалиста по кибербезопасности в колледже, будет иметь подтвержденную степень NSA, что делает их востребованными при трудоустройстве. «Подтверждение нашей программы АНБ является важным отличием, поскольку это национальное признание достигнутого нами уровня совершенства», — добавила Мишель Хиггс, директор программы кибербезопасности в Cochise College. «Это очень интересно для нас. Наш следующий шаг — работать над тем, чтобы АНБ назначило его Национальным центром академического мастерства в области кибербезопасности». Проверка АНБ — это первый этап превращения Cochise College в Центр академического мастерства в области киберзащиты». ***(Cybersecurity program receives validation from NSA // Cochise College (https://www.cochise.edu/cybersecurity-program-received-validation-from-nsa/). 27.10.2022).***

***

«Отчет Egress приоткрыл завесу над трудностями, с которыми сталкиваются лидеры в области безопасности при выборе стека безопасности своих организаций из-за маркетинговой тактики поставщиков кибербезопасности «змеиного масла».

Отчет Cybersecurity Hype: Как управлять ожиданиями и реальностью показал, что лидеры в области безопасности изо всех сил пытаются преодолеть шум и внедрить подходящие решения для своих компаний.

Тони Пеппер, генеральный директор и соучредитель Egress, сказал, что индустрия кибербезопасности виновна в продаже «змеиного масла», результаты которого часто отличаются от первоначальных ожиданий.

«Отрасль представляет собой переполненный очаг стартапов и признанных игроков, внедряющих инновации в одних и тех же пространствах и постоянно пытающихся как выровнять, так и дифференцировать себя друг от друга. Несмотря на шум создания категорий, запусков продуктов, модных словечек и аббревиатур, покупатели кибербезопасности продолжают инвестировать в механизмы снижения рисков».

Ажиотаж вокруг кибербезопасности затуманивает суждения лидеров безопасности и расширяет поверхность атаки

Согласно отчету о кибербезопасности, запутанные маркетинговые стратегии поставщиков сбили с толку большинство лидеров безопасности. Впоследствии 91% лиц, принимающих решения, столкнулись с трудностями при выборе поставщиков кибербезопасности из-за неясного маркетинга их конкретных предложений.

Кроме того, 49 % руководителей служб безопасности заявили, что их организации страдают от разрастания поставщиков, что приводит к увеличению поверхности для атак.

Следовательно, 92% организаций реализуют стратегию глубокоэшелонированной защиты и должны управлять от 10 до 30 различных продуктов безопасности. Глубокая защита направлена на создание большего количества технологических уровней для обнаружения, предотвращения, сдерживания, устранения и восстановления после атак.

На шумном рынке, наполненном необоснованными заявлениями, пользователи не могут точно предсказать эффективность разрекламированных решений, да и времени на это у них нет. Таким образом, они предпочитают несколько уровней безопасности, надеясь по возможности остановить атаки, а затем определить, что не удалось.

«Покупатели сталкиваются с переполненным и сложным рынком, которым необходимо постоянно внедрять новые продукты безопасности в свою среду для обеспечения глубокой защиты, оценивать новые и появляющиеся технологии искусственного интеллекта и постоянно реинвестировать в SA&T».

Неудивительно, что поставщики извлекли выгоду из этой стратегии, убедив руководителей ИТ-отделов и специалистов по безопасности в том, что их продукты внесут огромный вклад в эшелонированную защиту.

Egress предупредил, что увеличение количества продуктов для кибербезопасности не всегда выгодно с учетом соотношения риска и затрат, разногласий между бизнесом и пользователями, а также ресурсов и времени в области ИТ/безопасности.

Ажиотаж вокруг кибербезопасности усложняет стек безопасности

Компания по обеспечению безопасности обнаружила, что шумиха вокруг кибербезопасности усложняет стек безопасности организаций и увеличивает накладные расходы на управление. Почти половина (49%) руководителей ИТ-отделов и специалистов по безопасности считают, что их стек безопасности слишком сложен, а 48% считают, что им сложно управлять.

Точно так же сложный стек безопасности создавал потенциальные коммерческие риски при подключении нескольких поставщиков, особенно стартапов, склонных к финансовым неудачам. Эта ситуация вряд ли изменится,

поскольку стартапы, доминирующие в индустрии кибербезопасности, оцениваются в 139,77 млрд долларов в 2021 году и, по прогнозам, достигнут 155,83 млрд долларов в 2022 году и 376,32 млрд долларов к 2029 году.

Неясные результаты и маркетинг продуктов безопасности на основе ИИ

В отчете Egress содержится информация о том, поддерживает ли ИИ кибербезопасность, чтобы обнаруживать новые неизвестные угрозы, а также ускорять и повышать точность расследования инцидентов.

По данным исследователей, 77% ИТ-лидеров уже использовали продукт безопасности со встроенными функциями искусственного интеллекта для улучшения обнаружения. Однако только 66% полностью понимают, как ИИ сделал их продукты безопасности более эффективными, и только 52% считают, что поставщики «очень четко» продвигают возможности ИИ.

Кибербезопасность является вторичной по отношению к осведомленности и обучению безопасности

Отчет о шумихе в области кибербезопасности показал, что 96% респондентов считают, что осведомленность и обучение в области безопасности (SA&T) могут привести к долгосрочным положительным изменениям в поведении сотрудников. Однако Egress предупредил, что такие высокие ожидания могут быть неосуществимы на основании имеющихся данных.

«Несмотря на эти убеждения, другие данные, которые мы обнаружили, свидетельствуют о том, что эти ожидания могут быть оторваны от реальности, а завышенные ожидания в отношении SA&T могут усугубляться поставщиками».

Egress также обнаружил, что большинство организаций отдают приоритет SA&T не только безопасности. Например, 67 % респондентов назвали соблюдение нормативных требований ключевым фактором для SA&T, а 62 % внедрили SA&T для выполнения требований киберстрахования. Только 32% респондентов указали «создание культуры безопасности» в качестве основной цели повышения осведомленности и обучения в области безопасности.

Неудивительно, что SAT часто терпел неудачу: 84% респондентов сообщили об успешных фишинговых атаках, несмотря на то что 98% организаций внедрили программы SAT.

Преодоление ажиотажа в области кибербезопасности и навигация по сложному стеку безопасности

Чтобы преодолеть ажиотаж вокруг кибербезопасности и победить сложный стек безопасности, Egress рекомендовал следующее:

оценка результатов вместо деятельности;

Индивидуальное обучение по индивидуальному заказу; а также

Сочетайте SA&T с подталкиваниями, вмешательствами и обучаемыми моментами в режиме реального времени в момент риска, когда пользователь собирается выполнить потенциально опасное действие.

Между тем, Egress обнаружил, что 40% организаций уже сочетают SA&T с вмешательствами в реальном времени, такими как оповещения непосредственно перед тем, как пользователь совершит ошибку, например ответ на фишинговое электронное письмо». ***(Alicia Hope. Study Shows Cybersecurity Hype Complicates the Security Stack, Expands the Attack Surface // Rezonen Pte. Ltd.***

(https://www.cpomagazine.com/cyber-security/study-shows-cybersecurity-hype-complicates-the-security-stack-expands-the-attack-surface/). 27.10.2022).

***

«SE Labs протестировала CrowdStrike Falcon против ряда атак программ-вымогателей, предназначенных для вымогательства у жертв. Эти нападения были реалистичными, с использованием той же тактики и методов, которые применялись против жертв в последние месяцы.

Тестируйте как хакеры-вымогатели

Тестеры атаковали целевые системы, защищенные CrowdStrike Falcon. Наши тестировщики в лаборатории действовали так же, как мы наблюдаем, как группы программ-вымогателей ведут себя в Интернете.

Атаки были инициированы с самого начала цепочки атак с использованием фишинговых ссылок электронной почты и вложений, как только два примера. Каждая атака проводилась с самого начала до ее очевидного завершения, что означает попытку украсть, зашифровать и уничтожить конфиденциальные данные в целевых системах.

Программы-вымогатели — это наиболее заметная и наиболее понятная киберугроза, затрагивающая сегодня бизнес. Парализованные компьютерные системы означают остановку бизнеса и потерю доходов. Вдобавок ко всему, требование выкупа обеспечивает четкую, исчисляемую ценность угрозы. Спрос на «миллион долларов!» легче поддается количественной оценке, чем возможная утечка интеллектуальной собственности конкуренту.

Учитывая глобальный интерес и ужас вокруг программ-вымогателей, мы разработали комплексный тест, который показывает, насколько эффективны продукты безопасности при столкновении со всем спектром угроз, исходящих от самих программ-вымогателей и преступных групп, действующих в тени.

В этом отчете мы использовали два основных подхода к оценке того, насколько хорошо продукты могут обнаруживать и защищать от программ-вымогателей.

Глубокие атаки программ-вымогателей

В первой части этого теста мы проанализировали распространенную тактику банд вымогателей и создали две пользовательские банды, которые используют более широкий набор методов. Во всех случаях мы запускаем атаку с самого начала, в том числе пытаемся получить доступ к целям с украденными учетными данными или другими способами. Затем мы перемещаемся по системе, а иногда и по сети, прежде чем развернуть программу-вымогатель в качестве окончательной полезной нагрузки.

В первых двух атаках для каждой группы мы получаем доступ и сразу же развертываем программу-вымогатель на цель. В третьей, четвертой и пятой атаках мы перемещаемся по сети и развертываем программу-вымогатель на цели глубже в сети. Полезные нагрузки программ-вымогателей, использованные в этой части отчета, представляли собой известные файлы из пяти семейств, перечисленных в разделе «Хакеры против целей».

Этот тест показывает способность продукта отслеживать движение злоумышленника по всей цепочке атаки. Мы отключаем функции защиты продукта и полагаемся на его режим обнаружения в этой части теста. Результаты демонстрируют, как группы реагирования на инциденты могут использовать этот продукт для получения информации об атаках программ-вымогателей.

Прямые атаки программ-вымогателей

Во второй части теста используется широко распространенное известное вредоносное ПО и добавляются варианты, призванные избежать обнаружения. Мы перечислили семейства программ-вымогателей, используемых в разделе «Хакеры против целей». Мы отправили каждую из этих полезных нагрузок программ-вымогателей непосредственно в целевые системы, используя реалистичные методы, такие как атаки социальной инженерии по электронной почте. Это полная, но короткая цепочка атак.

В этой части теста мы проверяем, включены ли в продукте все функции защиты. Если продукты могут обнаруживать известные версии каждого из этих файлов и защищать от них, все в порядке. Но если они также обнаружат и заблокируют две разновидности каждой программы-вымогателя, то мы можем сделать вывод, что доступная защита является более активной, чем простое реагирование на вчерашних незадачливых жертв.

Программы-вымогатели протестированы

В этом подробном отчете рассматривается обнаружение программ-вымогателей во время полной сетевой атаки; и защита от известных атак программ-вымогателей и их неизвестных вариантов. Для получения подробной информации о том, как продукт справился с различными типами атак, см. разделы 3. Подробности реагирования (глубокие атаки программ-вымогателей)». ***(Deep and Direct Ransomware Testing // SE Labs Ltd (https://blog.selabs.uk/2022/10/deep-and-direct-ransomware-testing/). 10.2022).***

***

«Кибер-злоумышленники придумывают все более изощренные методы для кражи конфиденциальной информации пользователей, шифрования документов для получения выкупа или повреждения компьютерных систем. В результате ученые-компьютерщики пытаются создать более эффективные методы обнаружения и предотвращения кибератак.

Многие детекторы вредоносных программ, разработанные в последние годы, основаны на алгоритмах машинного обучения, обученных автоматически распознавать шаблоны или сигнатуры, связанные с конкретными кибератаками. Хотя некоторые из этих алгоритмов добились замечательных результатов, они, как правило, уязвимы для атак злоумышленников.

Состязательные атаки происходят, когда злоумышленник незаметно искажает или редактирует данные, чтобы алгоритм машинного обучения неправильно классифицировал их. В результате этих незаметных возмущений алгоритм может классифицировать вредоносное ПО, как если бы оно было безопасным и обычным программным обеспечением.

Исследователи из Инженерного колледжа в Пуне, Индия, недавно провели исследование уязвимости детектора вредоносных программ, основанного на глубоком обучении, к атакам со стороны злоумышленников. В их статье, предварительно опубликованной на arXiv, особое внимание уделяется детектору на основе преобразователей, классу моделей глубокого обучения, которые могут по-разному взвешивать разные части входных данных.

«Было предложено множество моделей, основанных на машинном обучении, для эффективного обнаружения широкого спектра вредоносных программ», — пишут в своей статье Яш Джахотия, Херамб Патил и Джугал Ролани.

«Многие из этих моделей оказались восприимчивыми к состязательным атакам — атакам, которые работают путем создания преднамеренно разработанных входных данных, которые могут привести к неправильной классификации этих моделей. Наша работа направлена на изучение уязвимостей в современных современных детекторах вредоносных программ для состязательных атак».

Чтобы оценить уязвимость детекторов вредоносных программ, основанных на глубоком обучении, к атакам злоумышленников, Jakhotiya, Patil и Rawlani разработали собственную систему обнаружения вредоносных программ. Эта система состоит из трех ключевых компонентов: модуль сборки, модуль статической функции и модуль нейронной сети.

Модуль ассемблера отвечает за вычисление функций языка ассемблера, которые позже используются для классификации данных. Используя те же входные данные, которые подаются в модуль сборки, модуль статических функций создает два набора векторов, которые также будут использоваться для классификации данных.

Модель нейронной сети использует функции и векторы, созданные двумя моделями, для классификации файлов и программного обеспечения. В конечном счете, его цель — определить, являются ли файлы и программы, которые он анализирует, безопасными или вредоносными.

Исследователи проверили свой детектор вредоносных программ на основе трансформаторов в серии тестов, в ходе которых они оценили, как на его производительность повлияли атаки со стороны. Они обнаружили, что он был склонен к неправильной классификации данных почти в 1 случае из 4.

«Мы обучаем детектор вредоносных программ на основе Transformers, проводим состязательные атаки, в результате которых уровень ошибочной классификации составляет 23,9%, и предлагаем средства защиты, которые снижают этот уровень ошибочной классификации до половины», — написали Джахотия, Патил и Равлани в своей статье.

Недавние результаты, полученные этой группой исследователей, подчеркивают уязвимость детекторов вредоносных программ на основе трансформаторов тока для атак со стороны злоумышленников. Основываясь на своих наблюдениях, Джахотия, Патил и Ролани предлагают ряд стратегий защиты, которые могут помочь повысить устойчивость трансформеров, обученных обнаруживать вредоносное ПО, от атак злоумышленников.

Эти стратегии включают в себя обучение алгоритмов на враждебных выборках, маскирование градиента модели, уменьшение количества функций, на

которые обращают внимание алгоритмы, и блокирование так называемой переносимости нейронных архитектур. В будущем эти стратегии и общие результаты, опубликованные в недавней статье, могут помочь в разработке более эффективных и надежных детекторов вредоносных программ на основе глубокого обучения». ***(Ingrid Fadelli. The vulnerability of transformers-based malware detectors to adversarial attacks // Science X Network (https://techxplore.com/news/2022-10-vulnerability-transformers-based-malware-detectors-adversarial.html). 18.10.2022).***

***

«Шифрование диска — абсолютная магия для большинства нематематиков. И как любая сложная технология, приводит к неудобным вопросам.

Снижает ли шифрование диска возможность восстановления данных с помощью утилит после сбоя? Повышает ли шифрование диска вероятность возникновения ошибок и сбоев? Затрудняет ли шифрование диска перенос на загрузочный диск большего размера? Каковы плюсы и минусы для среднего пользователя ПК дома или в малом бизнесе без штатного ИТ-отдела?

Не заблуждайтесь, шифрование диска — мощная мера безопасности. Использование надежного шифрования диска означает, что ваши данные находятся под вашим контролем и только под вашим контролем. Неавторизованный злоумышленник, который может получить доступ к этим зашифрованным данным, но не имеет надлежащих учетных данных для входа (вашего имени пользователя и пароля) или ключа восстановления, может увидеть то, что выглядит как чистая тарабарщина. И методы грубой силы неэффективны. Даже с активами самых могущественных спецслужб мира могут потребоваться годы или даже столетия, чтобы взломать этот код и расшифровать лежащие в его основе данные.

На ПК, предназначенных для Windows 10 и Windows 11, системный диск зашифрован по умолчанию, но для этого шифрования используется открытый ключ. Шифрование не защищает ваши данные, если вы не входите в систему с учетной записью Microsoft, которая защищает данные, а также сохраняет ключ восстановления в OneDrive. На компьютерах с версиями Windows Pro и Enterprise вы можете включить шифрование диска BitLocker, которое способно шифровать любой диск, включая съемные диски, такие как USB-накопители.

Современные компьютеры Mac также предлагают встроенное шифрование с использованием функции FileVault.

А теперь плохие новости: если вы забудете пароль или кодовую фразу, необходимые для расшифровки этих данных, программное обеспечение для шифрования не сможет отличить вас от враждебного злоумышленника, а это означает, что вы заблокированы для доступа к зашифрованным данным.

Это не баг, это фича. Бэкдор, который позволит вам восстановить ваши данные без ключа дешифрования, также будет доступен злоумышленнику, что сделает защиту данных бесполезной.

Но это единственная разница между зашифрованным диском и тем, где данные хранятся в открытом виде. Если ваш диск или контроллер выходит из строя, что приводит к повреждению данных, не имеет значения, зашифрованы данные или нет;

вам понадобится резервная копия для восстановления поврежденных файлов. А на современном оборудовании шифрование и дешифрование по стандарту AES происходит в ЦП, а значит, какое-либо влияние на скорость передачи данных незначительно.

Это означает, что ваша самая большая проблема — убедиться, что у вас есть доступ к резервному ключу шифрования для вашего устройства, чтобы использовать его только в случае чрезвычайной ситуации. На Mac, использующем шифрование Apple FileVault, вы можете хранить ключ восстановления в iCloud или локально...

Убедитесь, что вы сохранили этот ключ восстановления в надежном месте. Если вы можете предоставить этот ключ по запросу, у вас есть полный доступ к данным на зашифрованном диске». ***(Ed Bott. Does disk encryption slow down your PC? // ZDNET, A Red Ventures company (https://www.zdnet.com/article/does-disk-encryption-slow-down-your-pc/). 26.10.2022).***

***

«Компанія Eset повідомляє про вихід нової 16 версії продуктів для SOHO користувачів операційної системи Windows. В ній реалізовано новітню технологію для виявлення загроз, а також вдосконалено функції для захисту конфіденційних даних, зокрема від атак методом підбору паролів та під час здійснення онлайн-платежів.

В новій версії продуктів Eset реалізовано підтримку апаратної технології Intel TDT для виявлення шкідливого програмного забезпечення. Вона використовується в процесорах Intel Core для посилення захисту від програм-вимагачів, зокрема у випадках, коли ці загрози намагаються уникнути виявлення в пам’яті. Також у новій версії було покращено функцію «Захист онлайн-платежів», який тепер має режим «Захист усіх браузерів», що активується автоматично для всіх сумісних браузерів.

Крім того, було покращено функцію «Інспектор мережі», яка сканує роутер та усі підключені до нього пристрої на наявність уразливостей для забезпечення максимального рівня безпеки пристроїв Інтернету речей, які стали невіддільною частиною життя багатьох користувачів.

Як зазначається, всі продукти з портфоліо рішень Eset для користувачів Windows – базовий захист (NOD32 Antivirus), комплексний захист (Internet Security) та преміум-захист (Smart Security Premium) – забезпечують високий рівень безпеки пристроїв на усіх рівнях та відрізняються тільки додатковими функціями.

Для більш ефективного управління безпекою домашніх пристроїв було оновлено платформу Eset Home, яка дозволяє централізовано поновлювати та змінювати ліцензії, а також віддалено перевіряти безпеку пристроїв. Зокрема тепер користувачі можуть бачити поточні статуси захисту на головному екрані. Також було додано двофакторну автентифікацію для входу в обліковий запис для підвищення рівня конфіденційності.

На додаток до продуктів для комп’ютерів було оновлено Eset Mobile Security – рішення для користувачів смартфонів та планшетів Android, яке захищає дані користувачів від втрат, витоків та несанкціонованого доступу, а також дозволяє безпечно переглядати вебсторінки. Крім оновленого дизайну головної інформаційної панелі, користувачі версії 8 отримають розширені можливості

функції «Антифішинг», яка тепер забезпечує захист від потенційно небезпечних посилань в SMS-повідомленнях та сповіщеннях». ***(Захисні рішення Eset отримали підтримку технології Intel TDT для виявлення шкідливого ПЗ // Компьютерное Обозрение (https://ko.com.ua/zahisni_rishennya_eset_otrimali_pidtrimku_tehnologiyi_intel_tdt_dlya_viyavlennya_shkidlivogo_pz_142464). 27.10.2022).***

***