**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

№ 5 (травень)

Київ – 2023

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., 2023.– №5 (травень) . – 197 с.

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

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

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

ЗМІСТ

«Ще задовго до повномасштабного вторгнення росія посилила кібератаки на держоргани, оборонно-промисловий комплекс, інфраструктурні об'єкти, IT-мережі та ЗМІ в Україні.

Кіберборотьба й кіберзахист стали одними із ключових елементів гібридної війни. Наші фахівці та хакери-волонтери не лише успішно протистоять нападам, а й завдають дошкульних ударів у відповідь. Торік зафіксовано понад 1,25 мільйона DDoS-атак на російську інфраструктуру (це 8,4% від усіх кібератак у світі). За оцінками керівника служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО Наталії Ткачук, Україна – єдина держава, яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії рф.

Проте маємо усвідомлювати: про остаточну перемогу наразі не йдеться. Ворог удосконалюється, маневрує, змінює вістря ударів. Нинішній тренд - інтелектуальні атаки задля виявлення слабких місць в інфраструктурі. І світовий досвід доводить: надійна робота систем кіберзахисту залишатиметься актуальною і в мирний час.

Державна політика

Формуванням і реалізацією державної політики у сфері кіберзахисту, захисту об'єктів критичної інфраструктури та державних інформаційних ресурсів у кіберпросторі в нашій країні опікується Держспецзв'язку (Державна служба спеціального зв'язку та захисту інформації України). Вона також відповідає за підготовку фахівців у цих напрямах, що потребує особливої гнучкості, аби нові кадри відповідали мінливим вимогам сьогодення. Для цього існує лише два шляхи.

Перший – впровадження змін у систему вищої освіти. Зараз абітурієнтам, яких цікавить робота, пов'язана із захистом інформації, доступна лише одна опція – спеціальність 125 "Кібербезпека" у галузі знань 12 "Інформаційні технології". Однак її стандарти не забезпечують майбутнім фахівцям увесь спектр знань та навичок, необхідних на сучасному ринку праці. Вихід – розширення переліку освітніх можливостей у співпраці з МОН. Однак кооперація з іншою державною структурою ускладнює процес і розтягує його в часі, а зміни необхідні вже зараз.

Другий шлях – імплементувати міжнародні стандарти та кращі світові практики і розробити кваліфікаційну рамку професій у галузі кібербезпеки. Простими словами – розширити перелік можливих посад для кіберспеціалістів в українському Класифікаторі професій, а також створити для них відповідну систему оцінювання фаху. Саме у цьому напрямі Держспецзв'язку наполегливо працює останні роки. У результаті кількість професій галузі кіберзахисту та захисту інформації збільшилася із 2 до 27. Ще однією ініціативою є створення кваліфікаційних центрів, де фахівці з кібербезпеки і дотичних спеціальностей зможуть складати професійні іспити. Це дасть їм можливість виходити на ринок праці як вузькопрофільні спеціалісти, а роботодавцям знаходити саме ті кадри, яких вони потребують. Крім влаштування профільних іспитів, кваліфікаційні центри зможуть також надавати освітні послуги. Тому Держспецзв'язку всіляко підтримує ініціативи навчальних закладів та приватних компаній щодо заснування на їхній базі сертифікаційних центрів та отримання ними акредитації відповідно до чинного законодавства.

«Очевидно, що Держспецзв'язку не може лише власними силами розбудувати ринок праці. Ми як державний орган і регулятор – чи радше медіатор – можемо задавати орієнтовний напрямок руху для подальшого розвитку в галузі кіберзахисту та захисту інформації. Проте без підтримки вищих навчальних закладів, роботодавців, приватних компаній, які надають освітні послуги, побудувати систему професійної сертифікації та ринку праці просто неможливо», – вважає заступник Голови Держспецзв'язку Олександр Потій.

Працевлаштування і кар'єра

Цього року в Україні запрацювала бета-версія метчингової платформи для підбору професіоналів у галузі кібербезпеки – CyberPeople. Вона працює за принципом відповідності навичок фахівців запитам потенційних роботодавців та орієнтована у першу чергу на інтереси кандидатів. На відміну від рекрутингових платформ, таких як LinkedIn, де одразу видно всі попередні місця роботи, трудову історію та фото власника профілю, CyberPeople захищає кіберспеціалістів від оціночних суджень і неетичної поведінки з боку рекрутерів.

«Я хочу зробити платформу такою, щоб вона була на боці професіоналів. Там будуть закриті профілі, а оцінювання відбуватиметься тільки за скілами (набутими навичками претендента на вакансію, - ред.). Зараз компанії кажуть, що на ринку немає достатньої кількості кваліфікованих працівників. Я із цим не зовсім згодна. Тож якщо ми запропонуємо компаніям зазначити навички, за якими вони шукають людей на ті чи інші позиції, і платформа сама їх оцінить, у підприємств не буде можливості сказати, що їм це не підходить. За результатами такого підбору компанії зможуть попросити кандидата відкрити свій профіль, а спеціаліст уже самостійно вирішуватиме, чи підходить йому пропозиція і чи хоче він проходити співбесіду», – розповіла співзасновниця CyberPeople Ольга Насібулліна.

Наступним кроком розробки проєкту стане співпраця з навчальними платформами, яка дозволить фахівцям підтверджувати свої скіли та отримувати сертифікати відповідного рівня. Крім цього, платформа зможе запропонувати кіберспеціалістам побудову індивідуального кар'єрного треку, наприклад від джуніора (початківця) до мідла (фахівця зі стажем).

Загалом, говорячи про кар'єрні можливості та працевлаштування у галузі кіберзахисту, варто зазначити, що за останні кілька років підхід роботодавців до підбору нових працівників дещо змінився. Вимоги до практичних навичок кандидатів стали жорсткішими, при цьому суттєву роль у виборі найкращих претендентів стали відігравати їхні особистісні якості.

Своє бачення ситуації під час нещодавньої експертної дискусії на тему «Професії та кар'єра у сфері кібербезпеки» висловив керівник відділу IT-безпеки Raiffeisen Bank Євген Балютов: «Ще рік тому я б сказав: «якщо у вас горять очі, ви хочете щось робити і маєте базовий технічний бекграунд – окей, пограймо в цю гру. Нехай це буде півроку та personal development план, якщо у вас є амбіції – рушаймо!». Зараз я скажу інакше. Коли команда вже збалансована, доводиться дуже акуратно ставитися до нових людей, що приносять нову культуру, нові цінності і якісь нові знання. Тому для мене важливий не тільки технічний бекграунд, а й здатність кандидата поділяти цінності команди, сформовані за роки. Наприклад, якщо весь колектив не проти гнучкого графіка та необхідності попрацювати ніч,

коли горить дедлайн, а для когось одного це погано, то зазвичай це не дуже добре і для всієї організації. Тож ми намагаємося збалансувати роботу всіх членів колективу».

Крім цього, змінилися пріоритети компаній у підготовці фахівців. З'явилася потреба саме у вузькопрофільних спеціалістах, котрі віртуозно володітимуть знаннями та навичками у своїй галузі. «Наприклад, у нашій компанії обов'язковою вимогою є англійська мова та рівень спеціалістів вище середнього. Зараз ми шукаємо фахівців з дуже глибокими точковими знаннями. Тобто універсали вже не такі цікаві, оскільки нам потрібні люди, які зможуть за рахунок своїх унікальних знань підсилити команду», – зазначила Security Service Delivery Manager компанії EPAM Мирослава Стременецька.

Навіть попри те, що сфера кібербезпеки є глибоко технічною і потребує специфічного набору практичних умінь, тут так само високо цінуються навички спілкування, як і в багатьох інших галузях. А оскільки цей критерій здається не настільки очевидним при підборі фахівців, на ньому окремо акцентують уже досвідчені представники галузі кіберзахисту.

«Найприємніше шукати потрібних людей у ком'юніті (професійній спільноті), адже це ті, кого ми знаємо, і бачимо, як вони спілкуються. Технічні навички (hard skills) можна підтягнути, крім цього, їх легше перевірити. Соціально-комунікативні навички (soft skills) значно важче протестувати, а розвинути їх іноді неможливо. Тож коли ми зустрічаємо людину у ком'юніті і спостерігаємо її взаємодію з іншими, вже можна зрозуміти, як такий спеціаліст спілкуватиметься з клієнтами, замовниками, чи зможе він, наприклад, пояснити програмістам, як їм виконувати завдання, чи зможе вибудувати комунікацію з менеджментом. Важливим є те, як людина вміє презентувати себе, свій продукт або свою роботу. Адже безпека – невидима. Її потрібно презентувати, щоб компанії, усвідомлюючи свої вразливості, прагнули над цим працювати», – наголосила Security Software Engineer компанії Cossack Labs Юлія Межер.

Освітні можливості

З початком повномасштабного вторгнення стало зрозуміло, що кібербезпека є одним з пріоритетних і критично важливих напрямів розвитку країни. Звичайно, різні освітні ініціативи для підготовки майбутніх фахівців у цій сфері існували й раніше. Проте останній рік ознаменувався появою нових навчальних проєктів і можливостей, створених не лише для молоді, а й для тих, хто наважився на повну професійну переорієнтацію.

Так, у березні Міністерство цифрової трансформації України започаткувало освітній проєкт re/start in cyber. Програма складається з двох етапів. Перший – проходження онлайн-курсу з основ кібербезпеки на базі Toronto Metropolitan University, що передбачає набуття теоретичних знань та практичних навичок. Другий – підготовка до майбутнього працевлаштування за участі рекрутингової компанії BazaIT, під час якої учасники дізнаються про правила написання CV (професійного резюме) та проходження співбесіди з роботодавцями. Для участі у програмі є певні вимоги:

українське громадянство;

досвід роботи в будь-якій галузі, крім кібербезпеки, не менш ніж півтора року;

володіння англійською мовою на рівні не нижче В2.

Результатом успішного проходження курсу стане отримання всесвітньо визнаного сертифіката GIAC Foundational Cybersecurity Technologies (GFACT).

Багато українських абітурієнтів також бачать своє професійне майбутнє у галузі кібербезпеки, тож обирають відповідну спеціальність для вступу до вищих навчальних закладів. Як зазначає координатор освітнього напряму «Кібербезпека» на факультеті інформатики Національного університету «Києво-Могилянська Академія» Трохим Бабич, для навчання у цій галузі не потрібно нічого особливого, крім стійких знань з математики і англійської мови, а також певної рамки мислення, яка допоможе студентові розуміти специфіку роботи з тими чи іншими технологіями. «Якщо саме по собі програмування – це вміння будувати будинок, то кібербезпека для мене – це певна ревізія будинку, яка дозволяє знаходити в ньому зайві двері та вікна», – пояснив Бабич.

Загалом рівень зацікавленості кібербезпекою в українському суспільстві підвищується. А враховуючи стрімкі темпи зростання галузі, треба розуміти, що нині питання захисту інформації стосується абсолютно всіх. На цьому акцентував співзасновник CyberSchool Єгор Аушев: «Елементарними знаннями з кібергігієни зараз повинна володіти кожна людина. Ми намагаємося пояснювати компаніям, що співробітники мають приділяти кіберзахисту хоча б кілька хвилин на тиждень. Таким чином з'являється human firewall, тобто вибудовуються стіни всередині організації, які захищають її від 80% хакерських атак. Є різні рівні навчання у кібербезпеці, починаючи від школярів та студентів і закінчуючи колективами компаній. Ми як CyberSchool готові співпрацювати з університетами, хочемо ділитися досвідом та рухати багато проєктів. Адже цей human firewall всередині нашої держави також має будуватись. Чим обізнаніше суспільство у кібербезпеці, тим міцнішою буде наша країна».

Нині Україна перебуває на передовій кібервійни. І хоча ці обставини негативно впливають на наше життя, їх можна використати для тестування нових ідей та технологій у галузі захисту інформації. Досвід, який ми здобуваємо в боротьбі з ворогом, робить наших кіберспеціалістів лідерами галузі на світовому ринку. Крім цього, починає формуватися попит на українські освітні проєкти серед фахівців за кордоном. Із цього можемо зробити висновок, що галузь кіберзахисту у нашій державі й надалі активно зростатиме та залучатиме нові таланти, і настане час, коли ми зможемо повноцінно поділитися набутим знаннями зі світом». ***(Анастасія Кириченко. Кібербезпека в Україні: шляхи розвитку та можливості // Укрінформ (https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html). 03.05.2023).***

***

«Національний координаційний центр кібербезпеки при РНБО України провів XIX засідання Національного кластера кібербезпеки на тему «Кібербезпека у сфері охорони здоров'я та медицини: основні виклики та загрози», під час якого учасники обговорили питання захисту медичних даних та протидію кібератакам в інформаційних системах сфери охорони здоров'я.

Про це повідомляє Апарат Ради національної безпеки і оборони України.

Відкриваючи засідання, керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО Сергій Прокопенко зазначив, що ворожі атаки рф мають дві мети — руйнування інфраструктури та доступ до персональних даних громадян.

«Захист персональних та медичних даних дуже важливий, особливо коли наша країна перебуває у стані війни. російські хакери постійно намагаються викрасти дані українців для кібератак та інформаційних кампаній. Тому ми повинні приділяти особливу увагу питанням кібербзепеки на стратегічному, організаційному та технічному рівнях. Адже будь-хто в державному та приватному секторах може стати елементом атаки на ланцюг постачання», — зазначив Сергій Прокопенко.

Заступниця міністра охорони здоров'я Марія Карчевич розповіла, що за останні роки цифровізація охорони здоров'я стрімко зростає.

«В Україні затверджена п'ятирічна Концепція розвитку електронної охорони здоров'я. Щороку затверджується відповідна «дорожня карта» цифрових проєктів, яка цього року включає 107 проєктів. З-поміж них важливе місце займає кібербезпека та заходи, що вживаються для підвищення її рівня», — сказала Марія Карчевич.

Понад 200 представників з 80 організацій взяли участь у заході у форматі онлайн. Ключовими спікерами заходу були представники МОЗ України, Національної служби здоров'я України (НСЗУ), eHealth, CISA та інших організацій, відповідальних за цифровізацію та кібербезпеку галузі.

«Сфера охорони здоров'я потребує особливої уваги в розбудові надійного кіберзахисту в нашій країні. Насамперед це безпека персональних даних кожного пацієнта. Завдяки Національному кластеру кібербезпеки ми можемо обговорювати всі нагальні питання та виробляти комплексний підхід, захистити кожну галузь і всю країну», — наголосив керівник з операційної діяльності CRDF Global Михайло Верич». ***(Питання кіберзахисту у сфері охорони здоров'я обговорили на Національному кластері кібербезпеки // АрміяInform (https://armyinform.com.ua/2023/05/26/pytannya-kiberzahystu-u-sferi-ohorony-zdorovya-obgovoryly-na-naczionalnomu-klasteri-kiberbezpeky/). 26.05.2023).***

***

Правове забезпечення кібербезпеки в Україні

«В Апараті РНБО України відбулося засідання робочої групи з питань удосконалення нормативно-правової бази у сфері кібербезпеки.

Про це повідомляє прес-служба Ради національної безпеки і оборони України.

Учасники обговорили законопроєкт, який стосується підвищення ефективності боротьби з кіберзлочинністю на об'єктах критичної інфраструктури в умовах дії воєнного стану.

«Ефективне розслідування кіберзлочинів є однією з важливих складових кіберстійкості і правопорядку держави. Реалізація кіберзагроз національній безпеці відбувається не лише через злочинні дії зловмисників, але й через нехтування відповідальними особами правил із захисту критичних для держави інформаційних

систем, що є неприпустимим в умовах воєнного стану. На вирішення цієї проблеми і спрямований зазначений законопроект. Впевнена, що спільними зусиллями ми досягнемо консенсусу у цьому питанні та досягнемо необхідного результату», — наголосила Наталія Ткачук.

Зазначається, що у заході взяли участь фахівці Апарату РНБО України, Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України та ін». ***(У РНБО обговорили, як посилити національну систему кібербезпеки // АрміяInform (https://armyinform.com.ua/2023/05/19/u-rnbo-obgovoryly-yak-posylyty-naczionalnu-systemu-kiberbezpeky/). 19.05.2023).***

***

«Кабінет Міністрів ухвалив постанову, яка забезпечить встановлення механізму запуску програм Bug Bounty, що підвищить рівень кіберзахисту інформаційних систем.

Як передає Укрінформ, про це повідомляє прессслужба Міністерства цифрової трансформації.

«Кабінет Міністрів України ухвалив постанову, розроблену Держспецзв'язку, яка визначає порядок пошуку та виявлення потенційних вразливостей в електронних системах. Це дасть змогу запустити повноцінну програму національних Bug Bounty, щоб тестувати інформаційні системи на вразливості, вчасно виявляти ризики і підвищувати захищеність систем», - йдеться в повідомленні.

Зауважується, що запуск програм Bug Bounty дозволить: підвищити рівень кіберзахисту інформаційних систем; протидіяти несанкціонованому доступу до інформаційних систем; підвищити кіберстійкість інформаційних систем до інцидентів.

Bug Bounty - це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Процедура широко застосовується у всьому світі. Проте в Україні проведення Bug Bounty для державних систем було неприйнятним…» ***(В Україні запустять програму Bug Bounty для посилення кіберзахисту // Укрінформ (https://www.ukrinform.ua/rubric-technology/3711354-v-ukraini-zapustat-programu-bug-bounty-dla-posilenna-kiberzahistu.html). 19.05.2023).***

***

Кібервійна проти України

«Украинские сети подвергались жестоко изощренным и новаторским кибератакам со стороны России почти десятилетие, и Украина все чаще наносила ответные удары, особенно после прошлогоднего вторжения Кремля. На фоне всего этого и активности других правительств и хактивистов исследователи из охранной фирмы Malwarebytes говорят, что они отслеживают новую хакерскую группу, которая с 2020 года проводит шпионские операции против как проукраинских целей в центральной Украине, так и пророссийских. объекты на востоке Украины.

Malwarebytes приписывает пять операций в период с 2020 года по настоящее время группе, которую она назвала Red Stinger, хотя исследователи имеют представление только о двух кампаниях, проведенных в прошлом году. Мотивы и лояльность группы пока не ясны, но цифровые кампании примечательны своей настойчивостью, агрессивностью и отсутствием связей с другими известными акторами.

Кампания, которую Malwarebytes называет «Операция четыре», была нацелена на одного из украинских военных, который работает с критической украинской инфраструктурой, а также на других лиц, чья потенциальная разведывательная ценность менее очевидна. В ходе этой кампании злоумышленники скомпрометировали устройства жертв, чтобы получить скриншоты и документы и даже записать звук с их микрофонов. В ходе пятой операции группа нацелилась на нескольких чиновников избирательных комиссий, проводивших российские референдумы в спорных городах Украины, включая Донецк и Мариуполь. Одна цель была советником Центральной избирательной комиссии России, а другая занимается транспортом — возможно, железнодорожной инфраструктурой — в регионе.

«Мы были удивлены тем, насколько масштабными были эти целевые операции, и они смогли собрать много информации», — говорит Роберто Сантос, исследователь угроз в Malwarebytes. Сантос сотрудничал в расследовании с бывшим коллегой Хоссейном Джази, который первым обнаружил деятельность Red Stinger. «Мы видели прошлую целенаправленную слежку, но тот факт, что они собирали настоящие микрофонные записи жертв и данные с USB-накопителей, увидеть необычно».

Исследователи из охранной фирмы «Лаборатория Касперского» впервые опубликовали информацию об «Операции 5» в конце марта, назвав группу, стоящую за ней, Bad Magic. Касперский также видел, что группа сосредоточилась на правительственных и транспортных целях на востоке Украины, а также на сельскохозяйственных целях.

«Вредоносное ПО и методы, использованные в этой кампании, не отличаются особой сложностью, но эффективны, а код не имеет прямого отношения к каким-либо известным кампаниям», — пишут исследователи «Лаборатории Касперского».

Кампании начинаются с фишинговых атак для распространения вредоносных ссылок, которые ведут к зараженным ZIP-файлам, вредоносным документам и специальным файлам ссылок Windows. Оттуда злоумышленники развертывают базовые сценарии, которые действуют как бэкдор и загрузчик для вредоносных программ. Исследователи Malwarebytes отмечают, что Red Stinger, похоже, разработала собственные хакерские инструменты и повторно использует характерные сценарии и инфраструктуру, в том числе определенные вредоносные генераторы URL-адресов и IP-адресов. Исследователи смогли расширить свое понимание операций группы после обнаружения двух жертв, которые, по-видимому, заразили себя вредоносным ПО Red Stinger во время его тестирования.

«В прошлом случалось, что разные злоумышленники заражали самих себя, — говорит Сантос. «Я думаю, что они просто обленились, потому что их не замечали с 2020 года».

Red Stinger в настоящее время активен. Теперь, когда подробности о ее операциях становятся достоянием общественности, группа может изменить свои методы и инструменты, пытаясь избежать обнаружения. Исследователи Malwarebytes говорят, что, публикуя информацию о действиях группы, они надеются, что другие организации будут развертывать средства обнаружения для операций Red Stinger и искать в собственной телеметрии дополнительные указания на то, что хакеры делали в прошлом и кто стоит за группой». ***(Lily Hay Newman. A Mysterious New Hacker Group Is Lurking in Ukraine's Cyberspace // Condé Nast (https://www.wired.com/story/red-stinger-russia-ukraine-apt/). 10.05.2023).***

***

«Черговий огляд активності APT-груп, який охоплює період з жовтня 2022 року до кінця березня 2023, представила компанія Eset. Зокрема аналітики констатують, що російські APT-групи були особливо активними в Україні та країнах ЄС, використовуючи для атак програми для знищення даних та фішингові листи. Серед основних цілей кіберзлочинців – організації у галузі оборони та енергетики, а також медіакомпанії.

APT-групи зазвичай об'єднують кваліфікованих хакерів, діяльність яких часто спонсорується певною державою. Їх метою є отримання конфіденційних даних урядових установ, високопоставлених осіб або стратегічних компаній та уникнення при цьому виявлення. Такі групи кіберзлочинців мають великий досвід та використовують складні шкідливі інструменти та експлойти невідомих раніше уразливостей.

Однією з найактивніших APT-груп, спрямованих на Україну з метою викрадення конфіденційної інформації, залишається Gamaredon. Спеціалісти Eset виявили також поширення фішингових листів, націлених на урядові установи в кількох країнах ЄС. Зловмисники використовують відому тактику – електронні листи з вкладеним шкідливим HTML-документом, який після відкриття зберігає архів з небезпечним файлом.

Інша група Sandworm продовжує атакувати різні організації в Україні, зокрема державні установи, енергетичний сектор та медіа. У січні фахівці виявили розгортання групою Sandworm програми для знищення даних в Україні під назвою SwiftSlicer. В той самий час CERT-UA опублікував повідомлення про кібератаку Sandworm на інформаційне агентство України.

У першому кварталі спеціалісти також виявили поширення шкідливих повідомлень, націлених на дипломатів у країні ЄС. Зокрема фішингові електронні листи, замасковані під повідомлення від міністерства закордонних справ Чеської Республіки, містили посилання на сторінку для завантаження шкідливого ZIP-архіву.

Крім того, останніми місяцями група кіберзлочинців Winter Vivern була досить активною у Європі з атаками на українських та польських держслужбовців. Зловмисники надсилали електронні листи з посиланням на вебсайт, де жертви можуть завантажити підроблений антивірус, який потім встановлює спеціальний бекдор PowerShell.

В інших випадках ціллю кіберзлочинців було викрадення облікових даних пошти. Наприклад, у лютому група Winter Vivern використала уразливість на порталі Zimbra для спроби атаки урядових організацій в Європі. У разі введення облікові дані відправлялися на віддалений сервер зловмисників, а жертвам відображалася звичайна сторінка вебпошти.

Атаки APT-груп досить витончені та небезпечні, тому важливо забезпечити максимальний захист завдяки комплексному підходу до безпеки. Тому компаніям варто подбати про потужний захист пристроїв, зокрема за допомогою розширеного виявлення та реагування на загрози, розширеного аналізу у хмарі та шифрування даних тощо, а також розуміти можливі вектори атак та особливості діяльності певних груп». ***(Євген Куліков. Хакери рф прагнуть знищувати дані організацій в Україні та Європі // Компьютерное Обозрение (https://ko.com.ua/hakeri_rf_pragnut_znishhuvati_dani_organizacij_v_ukrayini_ta_yevropi_144075). 10.05.2023).***

***

«Российско-украинская война многому научила нас в кибервойне. В конце концов, это первый случай, когда кибердержава мирового класса одновременно ведет кинетическую войну. Но прежде чем мы сможем в полной мере усвоить уроки, извлеченные за последний год, мы должны сначала понять, какую роль киберпространство играет в активной кинетической войне, а также критерии, определяющие его эффективность.

Разрушение кибербезопасности в войне

Основные роли кибербезопасности в военных действиях включают: 1) шпионаж, 2) саботаж, 3) пропаганду и 4) сбои, обычно вызываемые распределенными атаками типа «отказ в обслуживании» (DDoS), нацеленными на правительственные, электрические и экономические/финансовые учреждения. Я считаю, что кибервойна состоит из двух частей: информационной войны с использованием кибертактики и методов и одной части — кибервойны с реальным разрушением.

Кибератаки со стратегическими или военными последствиями могут включать в себя манипулирование программным обеспечением, данными, знаниями и мнениями с целью снижения производительности и создания политических или психологических последствий. Внесение неуверенности в сознание противоборствующих командиров или политических лидеров является поддающейся расчетам военной задачей. Манипулирование общественным мнением с целью нанести ущерб легитимности и авторитету оппонента как внутри страны, так и за рубежом также ценно. Некоторые действия могут иметь только символический эффект, направленный на внутреннюю аудиторию, но и это ценно для нации, находящейся в состоянии войны.

Итак, как мы можем судить об эффективности кибератак? Мой более чем двадцатилетний опыт работы агентом ФБР научил меня тому, что критерии успеха в применении тактики кибернаступления лежат в пяти областях:

Создание хаоса

Сбор информации

Использование нарративов для формирования мнений (дезинформация)

Нанесение ущерба данным или экосистемам

Кража/эксфильтрация данных жертв для вымогательства и/или продажи криминальным брокерам данных

Кибервойна в российско-украинском конфликте

Россию часто называют «агрессором» в конфликте с Украиной. Но важно помнить, что, поскольку кибернетика не знает границ, любая страна или группа хактивистов могут безнаказанно присоединиться к битве — это один из способов фундаментального отличия кибернетики от традиционной войны, и динамика, от которой выиграли обе стороны. стал жертвой.

Россия придерживается широкой дефиниционной концепции информационной войны, которая включает в себя разведку, контрразведку, обман, дезинформацию, радиоэлектронную борьбу, ослабление связи, деградацию навигационного обеспечения, психологическое давление, деградацию информационных систем и пропаганду.

Кибермощь, используемая российскими военными, является ключевым аспектом гибридной войны и важным фактором российской политической стратегии, направленной на противодействие расширению и сплочению НАТО. Кибератаки могут быть направлены конкретно на уничтожение ключевых сетей и с целью их уничтожения, но также могут использоваться как инструмент для усиления тумана войны путем внесения путаницы в сети управления и контроля. Если местные политические и военные лидеры не могут опередить и дать точную оценку быстро развивающимся событиям, могут быть выиграны критические часы или даже дни, в течение которых противник может создать на местах факты, которые нелегко обратить вспять. В рамках своей военной кампании Россия провела множество кибератак на компьютеры в Киеве, Польше, Европейском парламенте и Европейской комиссии, прежде чем переправить танки через украинскую границу.

Вот лишь несколько примеров тактики кибервойны, использованной в российско-украинском конфликте:

Русские атаковали Viasat, американскую компанию спутниковой связи, которая оказывала поддержку украинским военным, с помощью вредоносного ПО, предназначенного для стирания ее данных перед отключением. Русские не ограничили масштаб вредоносного ПО, и оно затронуло другие компоненты наземных спутников, в результате чего сотни тысяч людей за пределами Украины потеряли электроэнергию и подключение к Интернету.

Кибератака на городской совет Одессы, крупного украинского портового города, расположенного на берегу Черного моря, была приурочена к атаке крылатыми ракетами, которая должна была помешать ответу Украины на российские войска, атакующие на юге.

Кибератаки также были предприняты против многих частей украинской инфраструктуры, правительственных и гражданских сетей, включая больницы.

Украинские военные подразделения создали поддельные сайты знакомств для российских солдат в сочетании с платформами социальных сетей, чтобы заманить российские войска использовать свои личные мобильные устройства — после чего

украинские военные триангулируют свое местоположение, чтобы они могли использовать беспилотник, чтобы сбросить бомбу на геолокацию. позиции.

Несмотря на то, что Россия считается одним из самых опасных игроков в киберпространстве, использование тактики кибервойны против Украины в преддверии и в настоящее время во время неспровоцированной войны, длившейся год, показывает, что наступательные киберметоды, когда они используются в качестве отдельного области ведения боевых действий, не обязательно предлагает волшебные решения и чудесные короткие пути для достижения стратегических военных целей. Подобно тому, как российская армия развернула кибератаки против Грузии в 2008 году и Сирии после этого вооруженного конфликта, когда российско-украинская война закончится, у нас будет еще один исторический пример, чтобы судить об эффективности российских кибервойн.

Уроки, извлеченные на данный момент

Кибервойна реальна, и она разыгрывается на различных театрах военных действий по всему миру — некоторые из них видны, как в российско-украинском конфликте, а другие — закулисно. Из этих действий можно извлечь много уроков, но вот несколько выводов, которые мы уже сделали:

Последствия кибератак трудно сдержать, если они не сопровождаются кинетической военной деятельностью. Эффекты чаще всего распространяются далеко за пределы намеченной цели и могут использоваться больше как стратегическое оружие, а не как тактическое или высокоточное оружие.

Установить атрибуцию кибератак сложно, и ее легче опровергнуть. Кибервойна находится в серой зоне, поскольку ее могут использовать как государственные, так и негосударственные субъекты с меньшими запретами, чем кинетические удары.

При использовании негосударственных или патриотических прокси кибератаки менее трудоемки, чем кинетические атаки, но, безусловно, требуют больше навыков для подготовки и выполнения и могут быть столь же разрушительными для инфраструктуры жертвы.

Нет никаких сомнений в том, что кибермощь используется в качестве стратегического оружия наряду с применением кинетической силы в российско-украинском конфликте. А кибервойна позволяет демократизировать власть и силу и продавать их в темной паутине, доступной для всех, кто обладает техническими навыками — независимо от границ, властей или принадлежности. Из-за этого мы должны начать думать заранее об угрозе и разрабатывать стратегии для реагирования на эти вызовы в масштабе». ***(James Turgal. Cyber Warfare Lessons From the Russia-Ukraine Conflict // Informa PLC (https://www.darkreading.com/attacks-breaches/cyber-warfare-lessons-from-russia-ukraine-conflict). 22.05.2023).***

***

«Департамент кіберполіції НПУ за п’ять місяців цього року отримав понад 15 тисяч звернень від громадян, постраждалих від фішингових атак.

Про це повідомив головний інспектор Департаменту кіберполіції Роман Сочка на пресконференції «Баланс безпеки – як захистити українських користувачів інтернету від фішингових атак?» у Медіацентрі Україна - Укрінформ.

«Від фішингових атак страждають громадяни не лише фінансово, від цих атак, у тому числі страждають їхні персональні дані. Крім того, страждають органи державної влади, бо спецслужби країни-агресора отримують їхні дані, використовуючи фішингові атаки, і це дійсно питання нацбезпеки. Що стосується наслідків для звичайних громадян, то на сьогодні за 5 місяців ми отримали понад 15 тисяч звернень щодо потерпілих від цих атак, і сума матеріальних збитків становить мільйони гривень», - сказав він.

Сочка висловив думку, що фільтрація фішингових сайтів має здійснюватися в найкоротші терміни, «оскільки ми не можемо чекати, поки зареєструється кримінальне впровадження, поки слідчий суддя дасть ухвалу суду на блокування ресурсу, поки інтернет-провайдер заблокує той чи інший ресурс». Він уточнив, що насамперед ідеться не про блокування, а про фільтрацію ресурсів, які вважаються фішинговими.

Представник кіберполіції навів приклад: коли Інтерпол у Європі формує базу даних таких сайтів і відправляє інтернет-провайдерам, їх блокують у найкоротші терміни…» ***(Кіберполіція цьогоріч отримала понад 15 тисяч звернень про фішингові атаки // Укрінформ (https://www.ukrinform.ua/rubric-society/3711669-kiberpolicia-cogoric-otrimala-ponad-15-tisac-zvernen-pro-fisingovi-ataki.html). 20.05.2023).***

***

«Протягом багатьох років російські урядові хакери використовували прикриття, щоб приховати сліди своїх кібератак і спробувати обдурити дослідників у галузі безпеки та урядові відомства, аби вони переклали провину за їхні дії на інших зловмисників. Про це йдеться в аналітичній публікації TechCrunch, переказ якої пропонує Foreign Ukraine.

Зокрема, російські хакери вдавали з себе румунського хактивіста-одинака на ім’я Guccifer 2.0, коли зламали Національний комітет Демократичної партії США; випустили руйнівне шкідливе програмне забезпечення, яке виглядає як пересічна програма-вимагач; ховались на серверах, які використовуються іранською хакерською групою; вдавали із себе ісламістську хакерську групу під назвою «Кібер-халіфат»; зламали зимові Олімпійські ігри 2018 року, залишивши «сліди», що вказують на Північну Корею та Китай; і підсунули хибні докази у документах, опублікованих як операція зі злому та витоку, імовірно проведена групою хактивістів під назвою «Кібер-Беркут».

Наразі дослідники у сфері кібербезпеки у BlackBerry стверджують, що виявили нову кібератаку російського уряду під прикриттям. Тепер вони прикриваються групою кіберзлочинців, відомою як Cuba Ransomware, що раніше була пов’язана зі штамом шкідливого програмного забезпечення, відомим як RomCom RAT. За словами дослідників, насправді це група, яка працює на російський уряд і атакує українські військові частини та місцеві органи влади.

«Атрибуція, яка вводить в оману. Схоже, це просто ще один підрозділ, який працює на російський уряд», – зазначив Дмитро Бестужев, старший директор групи розвідки кіберзагроз у BlackBerry, маючи на увазі зв'язок між RomCom RAT і Кубою.

Зазначимо, що RomCom RAT – це троян для віддаленого доступу, який вперше виявлений Unit 42, дослідницькою групою Palo Alto Networks, у травні 2022 року. За даними американського агентства з кібербезпеки CISA, зловмисне програмне забезпечення пов'язали з угрупованням Cuba, яке використовувало програми для кібератак у таких секторах, як «фінансові послуги, державні установи, охорона здоров'я, критичне виробництво та інформаційні технології».

Назва Cuba пояснюється тим, що група використовувала ілюстрації Фіделя Кастро та Че Гевари на своєму веб-сайті у даркнеті, хоча жоден дослідник так і не знайшов доказів того, що група має якийсь стосунок до «Острова свободи».

RomCom RAT використав підроблені версії популярних додатків для атаки, зокрема менеджер паролів KeePass, інструмент IT-адміністрування SolarWinds, Advanced IP Scanner та Adobe Acrobat Reader. За останні кілька місяців, RomCom RAT також завдавав кіберударів по українським військовим частинам, місцевим органам влади та українському парламенту.

Команда Бестужева відстежувала групу RomCom RAT протягом року та виявила її сліди через Інтернет. В рамках свого розслідування дослідники спостерігали за тим, як хакери використовували різноманітні цифрові сертифікати для реєстрації підроблених доменів, щоб встановити шкідливі програми.

Дослідники стали свідками того, як 23 березня 2023 року, за тиждень до звернення президента України Володимира Зеленського до австрійського парламенту по відеозв'язку, хакери створили цифровий сертифікат Австрії, щоб підписати вебсайт-пастку.

Також хакери RomCom RAT імітували веб-сайт SolarWinds у листопаді 2022 року, приблизно у той час, коли українські війська увійшли до Херсона. Хакери імітували Advanced IP Scanner у липні 2022 року, коли Україна розпочала використання ракет HIMARS. А у березні 2023 року хакери імітували Remote Desktop Manager приблизно в той час, коли українські пілоти навчалися на винищувачах F-16, а Польща та Словаччина вирішили надати Україні військові технології.

Багато експертів, а також сам український уряд досі не переконані, що RomCom RAT і Cuba Ransomware насправді є хакерами російського уряду.

Доель Сантос, старший науковий співробітник Palo Alto Networks Unit 42, вважає, що група, яка стоїть за шкідливим ПЗ RomCom RAT, «витонченіша, ніж традиційні групи хакерів», оскільки використовує спеціальні інструменти.

«Unit 42 зафіксував кібератаки проти України. У цьому є шпигунський аспект і тому вони можуть отримувати вказівки від певної держави. Проте, ми не знаємо ступеня цього зв'язку. Це виходить за рамки звичайної діяльності групи хакерів», – пояснює Сантос.

Проте, «деякі групи займаються заробітчанством, щоб отримати додаткові прибутки — це може бути те, що ми спостерігаємо у цьому випадку».

Бестужев та його команда розглядали цю можливість, але виключили її через наполегливість хакерів, час та цілі кібератак, які вказують на те, що їхня справжня мета — шпигунство, а не злочин.

Представник Державної служби спеціального зв'язку України повідомив, що одна з операцій RomCom RAT в Україні була націлена на користувачів спеціального програмного забезпечення під назвою DELTA, і «судячи з цільового та шкідливого програмного забезпечення, яке використовується, можна припустити, що метою кібератаки був збір розвідувальних даних від українських військових».

Бестужев та його група не планує публікувати всі технічні подробиці своїх знахідок, щоб не дозволити хакерам RomCom RAT змінити стратегії та методи.

Хто насправді стоїть за RomCom RAT та Cuba Ransomware, ще остаточно не відомо, але Бестужев та дослідники з інших компаній продовжать стежити за цими групами». ***(Володимир Тиравський. Російські урядові хакери атакують українські військові частини та органи влади під прикриттям – дослідження // Foreign Ukraine (https://foreignukraines.com/2023/05/24/russian-government-hackers-are-attacking-ukrainian-military-units-and-authorities-under-cover/). 24.05.2023).***

***

Боротьба з кіберзлочинністю в Україні

«Фігурант розробив програму для віддаленого керування даними на серверах потерпілих. Свою розробку він продавав на форумах і надалі з її використанням хакери здійснювали атаки на різні компанії та установи. Правопорушнику оголосили підозру.

Протиправну діяльність 27-річного жителя Чернівців викрили співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції.

Чоловік розробив програму за типом Obfuscated Web Backdoor для шифрування програмного коду та модифіковане шкідливе забезпечення для віддаленого контролю над вебресурсами. Таким чином розробка фігуранта дозволяла приховати шкідливе програмне забезпечення на ураженому ресурсі та залишати контроль над ним непомітним для власника.

Шкідливу програму він продавав на тематичних форумах. Надалі розробку використовували інші хакери для атак іноземних кампаній та подальшого скоєння кіберзлочинів.

Паралельно фігурант застосовував іншу програму, яка штучно підвищувала рейтинг та пошукову видачу вебсторінки в обхід правил використання та просування вебресурсів пошукових систем.

В оселі фігуранта працівники поліції провели обшук, вилучили комп'ютерну техніку, яку передали на експертизу.

Чоловіку оголосили підозру у вчинені кримінального правопорушення, передбаченого ч. 2 ст. 361-1 (Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Підозрюваному може загрожувати до п'яти років позбавлення волі». ***(Кіберполіцейські викрили жителя***

Чернівців у розробці та збуті шкідливого програмного забезпечення // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-vykryly-zhytelya-chernivcziv-u-rozrobczi-ta-zbuti-shkidlyvogo-programnogo-zabezpechennya-6053/). 01.05.2023).

***

Міжнародне співробітництво у галузі кібербезпеки

«У вівторок, 16 травня, Україна офіційно приєдналася до Центру передових технологій кібероборони НАТО (NATO CCDCOE). Про це повідомляє Міністерство закордонних справ України у Twitter.

«Сьогодні у штаб-квартирі Центру передового досвіду спільного кіберзахисту НАТО в Таллінні офіційно піднято Державний прапор України», — пише пресслужба.

У дипломатичному відомстві зазначили, що це означає офіційне приєднання нашої країни до Об'єднаного центру передових технологій з кібероборони НАТО.

«Ми дякуємо країнам-спонсорам Центру передових технологій з кібероборони НАТО за запрошення України та висловлюємо особливу подяку уряду Естонії за їх підтримку та допомогу на шляху до Центру передових технологій з кібероборони НАТО!», – йдеться у публікації.

Що таке Об'єднаний центр передових технологій кібероборони НАТО?

Один із центрів Північноатлантичного альянсу, який забезпечує боротьбу з кібератаками та кіберзахист інформаційних систем, а також навчання та підготовку профільних фахівців з кіберзахисту НАТО.

Центр є одним з основних елементів системи Альянсу з розвитку можливостей у сфері кібернетичної оборони.

Нагадаємо, 15 травня президент України Володимир Зеленський підсумував результати турне країнами Європи. За його словами, Україна отримала підтримку своєї формули миру, а також вступу до ЄС та НАТО.

Цього ж дня генеральний секретар Альянсу Єнс Столтенберг заявив, що на цей момент немає сенсу обговорювати вступ України до НАТО, оскільки Росія ще не програла війну повністю». ***(Україна приєдналася до Центру передових технологій з кібероборони НАТО: що він робить // Фокус (https://focus.ua/uk/ukraine/566712-ukraina-prisoedinilas-k-centru-peredovych-tehnologiy-po-kiberoborone-nato-chto-on-delaet). 16.05.2023).***

***

Світові тенденції в галузі кібербезпеки

«HackerOne опубликовала результаты своего нового исследования, которое показывает, что половина опрошенных организаций столкнулись с повышенными уязвимостями кибербезопасности в прошлом году, поскольку

они столкнулись с сокращением бюджета безопасности и увольнениями. HackerOne — крупнейшее в мире сообщество этичных хакеров.

TechRepublic посетила недавнее мероприятие HackerOne, на котором руководители компании, а также этичные хакеры и руководители GitLab и Sumo Logic обсудили экономические последствия кибербезопасности. Эксперты на мероприятии рассказали о шагах, которые некоторые компании предпринимают, чтобы делать больше с меньшими затратами, подчеркнув решающую роль, которую DevSecOps, машинное обучение и искусственный интеллект могут сыграть во время экономического спада.

Опрос HackerOne показывает, что экономические сокращения, такие как сокращение бюджета, увольнения и замораживание новых сотрудников и инвестиций, связанные с безопасностью, негативно сказываются на способности эффективно управлять кибербезопасностью для 75% опрошенных компаний. Однако сокращение инвестиций в кибербезопасность из-за экономического спада может иметь разрушительные последствия для компаний в долгосрочной перспективе.

Киберпреступность увеличивается во время рецессий и кризисов, как показывают отчеты ФБР за 2008 год и пандемию соответственно., к 2023 году средняя стоимость утечки данных вырастет до рекордно высокого уровня и превысит 5 миллионов долларов. По словам Acronis. Кроме того, риски несоблюдения нормативных требований растут в связи с постоянно меняющейся нормативно-правовой базой.

«Всякий раз, когда наступают периоды сильного беспокойства, такие как экономический спад, вызванный пандемией, плохие деятели проявляют себя наилучшим образом», — сказал Джордж Герчоу, директор по безопасности и старший вице-президент по информационным технологиям в Sumo Logic, во время круглого стола в Мероприятие HackerOne.

«Я видел несколько компаний, пострадавших от ужесточения бюджетных ограничений, но могу сказать вам, что в Sumo этого не произошло. Мы, вероятно, инвестируем больше, чем когда-либо. Я думаю, что это настоящая ошибка, когда компании начинают урезать свой бюджет на кибербезопасность, особенно в наше время».

Недавний отчет GitLab показывает, что 85% опрошенных лидеров безопасности говорят, что у них такой же или меньший бюджет, чем в 2022 году.

«Организации во всем мире ищут способы сделать больше с меньшими затратами, — сказал Дэвид ДеСанто, директор по продуктам GitLab.

Марк Лавлесс, штатный инженер по безопасности в GitLab, объяснил, что на компанию повлиял экономический спад, и он внес коррективы, усилив внимание к DevSecOps.

«Мы используем наше программное обеспечение для написания программного обеспечения», — сказал Лавлесс.

«Многое из того, что мы делаем, — это попытки ускорить процесс и сделать его более эффективным, и это помогло», — добавил Лавлесс.

Размышляя о том, было ли сокращение бюджета хорошим планом, Лавлесс использовал аналогию с банком.

«Если вы собираетесь сократить персонал банка, вы хотите сократить всех охранников, которые охраняют хранилище? Возможно нет.»

Этичные хакеры и охотники за ошибками Херан Малхотра, представитель бренда HackerOne, и Джозеф (который не назвал свою фамилию) сказали, что с их стороны влияние было низким, поскольку они все еще активно взаимодействуют со многими компаниями. Малхотра добавил, что из-за сложной экономической ситуации многие предприятия переходят в онлайн, а сотрудники получают доступ к приложениям и инфраструктуре компаний, используя общедоступные сети или другие небезопасные средства.

«Там необходимо повысить уровень кибербезопасности, — сказал Малхотра.

Отчет HackerOne показывает, что, хотя 84% компаний заметили увеличение числа уязвимостей и обеспокоены финансовым и репутационным ущербом от взломов, они все еще планируют или уже провели увольнения и сокращения бюджета, которые затронут команды безопасности.

По данным опроса HackerOne, за последний год 39% компаний сократили штат сотрудников службы безопасности, а 40% планируют сделать это в ближайшие 12 месяцев. Герчоу объяснил, что эти действия имеют прямые и косвенные последствия, которые часто упускают из виду.

Герчоу сказал, что, хотя многие компании не обязательно увольняют сотрудников, они заморозили численность персонала, несмотря на то, что у них есть планы увеличить количество отделов безопасности из-за нагрузки. Затем службы безопасности вынуждены брать на себя повышенную нагрузку, что, в свою очередь, повлияет на производительность и эффективность и может привести к выгоранию. Этичные хакеры добавили, что нехватка сотрудников службы безопасности может дать злоумышленникам возможность найти новые уязвимости в менее защищенных системах.

Экономический ландшафт, сокращение бюджета и увольнения заставляют многих в индустрии кибербезопасности изучать тенденции, которые включают DevSecOps, искусственный интеллект, машинное обучение, автоматизацию, программы вознаграждения за обнаружение ошибок и консолидацию решений безопасности.

Благодаря DevSecOps компании осознают тесную связь между разработкой программного обеспечения, безопасностью и эксплуатацией, а также внедряют меры безопасности на более ранних этапах жизненного цикла разработки программного обеспечения или сдвигаются влево. Эта стратегия позволяет группам разработки, безопасности и эксплуатации работать совместно, а не изолированно.

Опрос GitLab показывает, что этот сдвиг в DevSecOps увеличивается: 38% специалистов по безопасности сообщают, что являются частью межфункциональной команды, занимающейся вопросами безопасности, по сравнению с 29% в 2022 году.

Опрос GitLab также показывает, что ведущие компании обращаются к ИИ и машинному обучению, чтобы повысить производительность и эффективность жизненного цикла программного обеспечения.

AI и ML стали важнейшими компонентами рабочих процессов DevSecOps. % разработчиков используют AI-ML для тестирования — или будут использовать в

ближайшие три года — и 62% используют эту технологию для проверки кода. Согласно опросу GitLab, 65

Такой подход к интеграции принят далеко не всеми компаниями и ведет к ненужным затратам. По данным опроса HackerOne, треть организаций признают, что тратят деньги впустую из-за неэффективности своего технологического стека и процесса обеспечения безопасности жизненного цикла разработки программного обеспечения.

Количество компаний, занимающихся кибербезопасностью, предлагающих ИИ и консолидацию, продолжает расти. Некоторые из наиболее признанных поставщиков и решений включают Falcon Complete MDR от CrowdStrike, Advanced Threat Protection от Tessian, Cloud Security Automation от Palo Alto Networks и PREVENT, DETECT & RESPOND и HEAL от Darktrace.

AI и ML позволяют компаниям увеличивать свои ресурсы, повышать производительность и укреплять безопасность. Инструменты автоматизации и консолидация также сокращают расходы, позволяя командам сосредоточиться на критически важных задачах.

Руководители признают, что специалисты по кибербезопасности, эксперты и этичные хакеры пользуются большим спросом. Команды безопасности обнаруживают уязвимости с более высоким риском, реагируют, пресекают атаки и проводят расследования. Они заполняют пробелы, которые оставляет за собой автоматизация, и используют инновационные технологии, такие как ИИ, в качестве инструмента, а не замены.

Еще одна область, в которой эксперты по безопасности начинают использовать ИИ и новые технологии, такие как ChatGPT, — это программы вознаграждения за обнаружение ошибок и тестирование на проникновение.

…компаниям дешевле запускать программы вознаграждения за обнаружение ошибок, чем нанимать собственные группы безопасности, занимающиеся исключительно поиском слабых мест.

Все эксперты круглого стола HackerOne согласились с тем, что искусственный интеллект и такие инструменты, как модели ChatGPT, меняют правила игры, но они также признали, что отрасль только начинает раскрывать свой потенциал.

Согласно отчету HackerOne, 37% опрошенных компаний уверены, что на ИИ можно «в некоторой степени полагаться».

Правительство и государственный сектор США также пострадали: многие респонденты опроса GitLab говорят, что они развертывают программное обеспечение медленнее или с той же скоростью, что и в прошлом году. Даже на федеральном, правительственном, аэрокосмическом и оборонном уровнях более половины хотят усилить и консолидировать свой инструментарий.

Консолидация служб безопасности и поставщиков — еще одна тактика, привлекательная для компаний, стремящихся сократить бюджет. Например, такие компании, как Check Point Software Technologies, используя облачную аналитику угроз и автоматизацию на основе ИИ, недавно представили Infinity Global Services. комплексное решение…

В индустрии кибербезопасности ясно одно: сокращение собственного бюджета на безопасность без плана или пренебрежение новыми инструментами и

стратегиями, такими как DevSecOps, ИИ, автоматизация и программы вознаграждения за обнаружение ошибок, представляют собой серьезный риск в 2023 году». ***(Ray Fernandez. HackerOne: How the economy is impacting cybersecurity teams // TechnologyAdvice (https://www.techrepublic.com/article/hackerone-cybersecurity-teams-economic-impact/). 04.05.2023).***

***

«Kubernetes» — это слово, которое предприятия слышат все чаще и чаще, но большинство за пределами сферы ИТ и безопасности, вероятно, не имеют четкого представления о том, что оно означает. Само слово по-гречески означает «рулевой» или «пилот», что на самом деле дает хорошее представление о том, что такое Kubernetes.

По сути, Kubernetes — это система с открытым исходным кодом, используемая для автоматизации развертывания программного обеспечения, которая очень хорошо справляется с управлением и масштабированием контейнерных приложений. Он, так сказать, управляет кораблем разработчиков программного обеспечения, работающих в масштабах, требуемых сегодняшним технологическим ландшафтом.

Это может показаться техническим, и это так. Но по мере распространения Kubernetes бизнес-руководителям потребуется более полное понимание того, как он используется в их организации. Те, кто не входит в команду разработчиков, могут даже не знать, что Kubernetes вообще используется, что создает серьезную проблему. По мере того, как Kubernetes становится все более популярным, киберпреступники обращают свое внимание на Kubernetes, а организации, не разбирающиеся в Kubernetes, рискуют оставить значительную часть своей среды незащищенной.

Kubernetes стал стандартом де-факто для автоматизации масштабирования, развертывания и управления контейнерными приложениями. Есть ряд факторов, способствующих его внедрению, но в основном это сводится к тому, чтобы дать возможность разработчикам. Самое простое объяснение того, как работает Kubernetes, состоит в том, что вместо того, чтобы разработчики развертывали код непосредственно на сервере, они могут упаковать код в контейнер, который затем можно развернуть практически где угодно.

Kubernetes похож на шеф-повара, который следит за тем, чтобы все на кухне были на своих местах и делали то, что должны делать. Это абстрагирует типичные проблемы разработчиков, такие как дисковое пространство или количество копий приложения, которое им может понадобиться. Вместо этого им нужно думать только о том, достаточно ли ресурсов в их кластере Kubernetes для работы.

В прошлом разработчики обычно создавали монолитное приложение с массивной кодовой базой и развертывали его непосредственно на огромных серверах. Это работает какое-то время, но по мере роста бизнеса требования к этому серверу будут увеличиваться — и, в конечном счете, на решение проблемы можно задействовать только определенное количество ЦП и памяти.

В конце концов, у серверов есть ограничения. Это позволяет легко понять, почему Kubernetes стал популярным: он позволяет компаниям масштабироваться горизонтально. Вместо вертикального масштабирования (за счет покупки все более

мощных серверов) они могут просто добавлять дополнительные экземпляры приложения по мере необходимости. Это создает другую парадигму масштабирования бизнеса, которая невероятно ценна, особенно для стартапов.

Также стоит отметить, что Kubernetes вводит уровень абстракции между разработчиками, пишущими код, и развертыванием и запуском этого кода. Это означает, что разработчики могут сосредоточиться на написании кода, а Kubernetes позаботится о его масштабировании и обслуживании. Раньше для этого требовалась специальная группа сотрудников, наблюдающая за этими приложениями, отслеживающая сбои и добавляющая при необходимости больше памяти, серверов или ЦП. Kubernetes облегчает эту боль — и это еще одна причина, по которой он стал чрезвычайно популярным.

Хотя Kubernetes отлично подходит для разработчиков, существуют и проблемы, особенно в том, что касается безопасности. Поскольку Kubernetes все еще (относительно) нов, может быть трудно найти специалистов по безопасности с опытом работы с Kubernetes.

В настоящее время спрос на этих экспертов по понятным причинам высок, а это означает, что небольшим компаниям и стартапам может быть сложно привлечь их. При этом по мере того, как Kubernetes становится все более распространенным, эта база знаний будет расти, а также появятся партнеры и сервисные компании. могут обратиться, если сами не смогут привлечь необходимую экспертизу.

Для организаций важно рассматривать Kubernetes как расширение существующей инфраструктуры. Для этого требуются те же уровни контроля, мониторинга и реагирования, что и в традиционной среде разработки. Как и любая другая кибербезопасность, защита Kubernetes — это скорее путешествие, чем пункт назначения, но важно как можно раньше начать внедрять элементы управления.

Организации должны оценить, где они находятся с точки зрения безопасности по сравнению с тем, где они хотели бы быть, а затем начать думать о необходимых шагах, чтобы достичь этого. Это может быть пугающим — некоторые компании тратят годы на создание своей инфраструктуры безопасности, и это может показаться началом с нуля — но это не обязательно.

Во-первых — и, возможно, самое главное — одна из самых больших ошибок организаций, когда речь идет о безопасности Kubernetes, заключается в том, что они полагают, что могут просто купить продукт, который решит эту проблему за них. Это почти никогда не бывает, когда речь идет о безопасности. Все инструменты безопасности требуют зрелого понимания того, как они будут развернуты, как они будут использоваться и поддерживаться, и какие ожидаемые результаты они принесут. Как бы хорошо это ни было, не существует единого продукта, который просто «решает вопросы безопасности» для всех сред Kubernetes.

Вместо этого лучший первый шаг — это взаимодействие с инженерами и командами DevOps, которые действительно используют Kubernetes. Никто не может лучше объяснить не только свои цели, но и потенциальные риски, связанные с ними. Крайне важно объединить команды разработчиков и специалистов по безопасности, чтобы обсудить, где могут находиться существующие уязвимости и как их можно учесть без ущерба для производительности. Эти идеи могут помочь определить, какие решения необходимы, что приведет к принятию более эффективных решений

о покупке и более эффективному контролю. Если все сделано правильно, безопасность может быть встроена в среду Kubernetes с самого начала.

Обеспечение безопасности Kubernetes может быть непростой задачей, но сегодняшним организациям необходимо заняться ею как можно раньше. Поскольку все больше разработчиков обращаются к Kubernetes, чтобы обеспечить более простую и масштабируемую разработку программного обеспечения, защита сред Kubernetes становится все более важной.

Бизнес-лидеры могут получить быстрый старт, поговорив с разработчиками и инженерами, изучив основные принципы Kubernetes и работая над получением более полной картины потенциальных рисков и связанных с этим проблем. Проще говоря, это 2023 год — Kubernetes будет становиться все более распространенным, и важно знать, что ваши среды безопасны». ***(Dan Whalen. It's 2023: Do you know if your Kubernetes environments are safe? // VentureBeat (https://venturebeat.com/programming-development/its-2023-do-you-know-if-your-kubernetes-environments-are-safe/). 06.05.2023).***

***

«…Аналитика киберугроз включает в себя сбор, анализ и интерпретацию сведений о потенциальных или реальных угрозах кибербезопасности. Эти сведения могут включать данные из различных источников, таких как аналитика с открытым исходным кодом, мониторинг даркнета, социальные сети и другие каналы информации об угрозах. Затем эта информация анализируется для выявления и понимания характера и масштабов потенциальных или реальных кибератак.

Разведка киберугроз (CTI) — это не решение кибербезопасности само по себе, а важнейший компонент любой архитектуры безопасности, позволяющий организациям получить представление о мотивах, целях и поведении субъектов угроз.

Преимущества CTI для бизнеса

Информация о киберугрозах имеет решающее значение для компаний, стремящихся защитить себя от постоянно меняющихся кибератак. Некоторые преимущества, которые CTI предоставляет для бизнеса, включают:

Раннее обнаружение угроз

CTI может помочь компаниям выявлять потенциальные угрозы на ранних стадиях и предпринимать необходимые действия для защиты своих систем.

Лучшее понимание киберрисков

Анализ информации о киберугрозах позволяет компаниям лучше понять свои уязвимости и потенциальные риски, с которыми они сталкиваются. Это позволяет им принимать более обоснованные решения о своих стратегиях кибербезопасности.

Улучшенное реагирование на инциденты

Предприятия могут получать информацию о потенциальных угрозах в режиме реального времени с помощью аналитики киберугроз, что позволяет им быстро и эффективно реагировать на инциденты.

Повышенная безопасность

Аналитика киберугроз может улучшить общее состояние безопасности бизнеса, снижая вероятность успешных атак и сводя к минимуму последствия киберинцидентов.

Соблюдение правил

CTI может помочь предприятиям соблюдать отраслевые и нормативные стандарты кибербезопасности, такие как PCI DSS и HIPAA.

Конкурентное преимущество

CTI может помочь компаниям повысить уровень кибербезопасности, дав им конкурентное преимущество перед конкурентами и укрепив репутацию среди клиентов.

Экономия затрат

CTI может помочь предприятиям предотвращать киберпреступления и уменьшать влияние будущих инцидентов, экономя деньги на восстановлении и устранении недостатков в долгосрочной перспективе.

Ключевые проблемы при внедрении CTI

Внедрение программы анализа киберугроз может принести компаниям значительные преимущества. Однако предприятия также могут столкнуться с некоторыми проблемами при внедрении CTI.

Расходы

Создание программы анализа киберугроз может быть дорогостоящим, требуя значительных инвестиций в технологии, инструменты и персонал.

Нехватка навыков

Может быть трудно найти квалифицированный персонал с необходимыми навыками для анализа и интерпретации информации об угрозах.

Качество данных

Информация о киберугрозах хороша настолько, насколько хороши данные, которые она использует. Низкое качество данных, неполные наборы данных и неточная/устаревшая информация могут существенно повлиять на эффективность программы CTI.

Интеграция с существующими процессами

Внедрение программы CTI может потребовать значительных изменений в существующих процессах и системах, которые могут быть разрушительными и занимать много времени.

Ложные срабатывания

Информация о киберугрозах может генерировать много ложных срабатываний. Это может снизить эффективность программы и привести к утомлению бдительности.

Конфиденциальность и безопасность данных

Собранные данные могут включать в себя конфиденциальную информацию или информацию, позволяющую установить личность, что создает проблемы конфиденциальности и безопасности данных.

Отсутствие поддержки заинтересованных сторон

Создание успешной программы анализа киберугроз требует участия и поддержки со стороны заинтересованных сторон во всей организации, включая исполнительное руководство, ИТ и управление рисками.

Решения этих ключевых проблем

Предприятия могут рассмотреть следующие шаги для решения этих проблем:

1. Разработайте четкое экономическое обоснование программы CTI, чтобы обосновать затраты и объяснить преимущества для заинтересованных сторон.

2. Предоставить возможности обучения и развития существующему персоналу для повышения их навыков и знаний в области кибербезопасности и анализа угроз.

3. Убедитесь, что в аналитике угроз используются качественные и регулярно обновляемые данные.

4. Интегрируйте программу анализа киберугроз с существующими процессами и системами, где это возможно, чтобы свести к минимуму сбои.

5. Внедрите механизмы фильтрации и другие методы, чтобы уменьшить количество ложных срабатываний и предотвратить усталость от предупреждений.

6. Разработайте политики конфиденциальности и безопасности данных, чтобы гарантировать, что данные собираются и используются в соответствии с применимыми законами и правилами.

7. Убедитесь, что заинтересованные стороны в организации понимают важность программы анализа киберугроз и привержены ее успеху.

Как выбрать провайдера CTI

Реализация программы CTI может быть сложной и сложной задачей, требующей опыта в области кибербезопасности и анализа разведывательных данных. Вот почему многие компании рассматривают возможность партнерства со сторонним поставщиком CTI. Для тех, кто заинтересован в поиске поставщика CTI, вот несколько ключевых факторов, которые следует учитывать, прежде чем выбрать его.

Источники данных

Проверьте, есть ли у провайдера доступ как к аналитике с открытым исходным кодом, так и к мониторингу даркнета, а также к каким-либо специализированным каналам аналитики угроз.

Качество интеллекта

Убедитесь, что поставщики предлагают высококачественную и актуальную информацию, в том числе возможность предоставлять актуальную, своевременную и полезную информацию.

Аналитические возможности

Проверьте аналитические возможности поставщика, в том числе используйте ли они передовые инструменты, такие как машинное обучение и обработка естественного языка (NLP), для анализа и интерпретации данных.

Покрытие угроз

Покрытие угроз поставщиком — это еще одна вещь, которую следует учитывать, в том числе охватывают ли они широкий спектр субъектов угроз, векторов атак и отраслей.

Настройка

Убедитесь, что поставщики предлагают настраиваемые аналитические каналы для удовлетворения конкретных потребностей вашей организации.

Экспертиза

Ищите поставщика с командой опытных аналитиков, которые могут предоставить дополнительную информацию и рекомендации.

Подведение итогов

Аналитика киберугроз может развивать кибербезопасность бизнеса, чтобы не отставать от постоянно меняющихся кибератак. Несмотря на то, что внедрение может столкнуться с некоторыми проблемами, их преодоление может помочь вам опережать возникающие угрозы с помощью аналитики киберугроз в качестве секретного оружия для вашего бизнеса». ***(Rabiul Islam. Understanding Cyber Threat Intelligence For Business Security // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/05/04/understanding-cyber-threat-intelligence-for-business-security/?sh=16c232784908). 04.05.2023).***

***

«Сегодня бизнес сталкивается с двумя острыми проблемами – экономикой и киберпреступностью. Это вынуждает директоров по информационной безопасности принимать жесткие решения о расходах. Исследование нарушений кибербезопасности, проведенное правительством Великобритании в 2022 году, показало, что за последние 12 месяцев 39% британских предприятий выявили кибератаки, а 31% предприятий оценили, что они подвергались атакам не реже одного раза в неделю. В условиях этих растущих уровней угроз еще никогда не было так важно оставаться в безопасности, управляя бюджетными расходами.

Поскольку киберриски продолжают расти, бюджеты остаются на прежнем уровне — фактически, в отчете о защите от киберугроз за 2022 год подчеркивается, что бюджеты на безопасность в Великобритании не изменились с 2021 года. расходы являются такой монументальной проблемой. Реальность такова, что ИТ-директорам нужно делать больше с меньшими затратами. Организации должны оптимизировать исходящие расходы, где это возможно, чтобы оставаться экономичными и продуктивными — и, прежде всего, безопасными. При правильном планировании и эффективных процессах руководители могут сэкономить на расходах и внедрить средства контроля, которые могут снизить любую ненужную подверженность рискам.

Комплексный подход к киберзащите

Эффективные методы обеспечения безопасности не всегда должны нарушать бюджет. Целостный подход к киберзащите, охватывающий технологическую экосистему, может снизить риски любых пробелов в защите, которые в противном случае оставили бы организацию открытой для эксплуатации. Вот некоторые способы создания надежной системы кибербезопасности:

Управление активами

Это означает поддержание точной и централизованной инвентаризации всех ИТ-активов. Отслеживание срока службы каждого ИТ-актива необходимо для обеспечения актуальности исправлений и обновлений программного обеспечения. Специалисты по безопасности могут оптимизировать ресурсы, выявляя и выводя из эксплуатации любое старое оборудование или программное обеспечение, которые устарели или закончили свою жизнь.

Знание того, где находится инвентарь аппаратного и программного обеспечения и как оно защищено, позволяет выявлять неправильные конфигурации и устранять потенциальные пробелы в безопасности. Это также упрощает обеспечение соблюдения требований безопасности, идентификацию неуправляемых устройств и оценку того, какие пользователи, имеющие доступ к критически важным системам, не имеют средств защиты, таких как включенная многофакторная проверка подлинности.

Предоставление сотрудникам возможности стать первой линией обороны организации

Хотя это кажется еще одним вложением, обучение сотрудников может сыграть важную роль в сохранении бюджета безопасности. Поскольку человеческая ошибка становится основной причиной взломов программ-вымогателей — фактически, согласно Всемирному экономическому форуму, 95% всех проблем кибербезопасности можно отнести к человеческой ошибке — кибербезопасность стала не только технологической проблемой, но и проблемой людей. Сотрудник, который не знает о методах атаки, может открыть или щелкнуть электронное письмо, которое потенциально может загрузить вредоносное ПО или перенаправить на веб-сайты для кражи интеллектуальной собственности или денег, что подвергает их организацию риску.

Начальное время, стоимость и ресурсы, направляемые на упреждающую и непрерывную программу обучения, ничто по сравнению с потенциально разрушительными последствиями и затратами на успешное нарушение кибербезопасности. Обучение передовым методам и поведению в киберпространстве, а также сообщение о подозрительных или необычных действиях могут остановить потенциальную атаку.

Наиболее эффективный способ проведения обучения для более широкой рабочей силы — это обучение в реальном мире, в котором активно участвуют работники на основе реальных сценариев, основанных на рисках. Например, запуск симуляций и игровое интерактивное обучение может сделать процесс обучения более актуальным и полезным.

Делайте более разумный выбор в области безопасности

Из-за изощренных методов киберпреступников, которые часто позволяют им быть на шаг впереди специалистов по безопасности, сокращение инвестиций в кибербезопасность вызывает все большую озабоченность. Однако инвестиции в дорогостоящие инструменты безопасности могут оказаться неуместными, если организациям не удастся заложить прочную основу для обеспечения безопасности.

Систематически пересматривая такие процессы, как непрерывный мониторинг сети и многофакторная аутентификация, постоянно обновляя обновления и максимально используя ресурсы, а также уделяя особое внимание обучению, ИТ-директора повысят организационную устойчивость. Это повысит их цифровую защиту и общий уровень безопасности. Кроме того, развертывание специальных инструментов кибербезопасности укрепит эти передовые методы, оставаясь при этом экономически эффективным.

В трудные экономические времена необходимо пересмотреть приоритеты кибербезопасности, чтобы проанализировать все ограниченные ресурсы и

определить, где их лучше всего использовать. Слишком часто организации путают хорошие методы обеспечения безопасности с хорошими покупками средств защиты, а это означает, что усилия приводят к приобретению новых и ненужных инструментов безопасности, которые дублируют усилия и еще больше усугубляют проблемы управления командными ресурсами.

Киберустойчивость — это идеальное сочетание технологий и человеческого опыта.

Учитывая риски кибератаки, потенциально включая потерю данных, штрафы за несоблюдение требований, выкуп или долгосрочный ущерб репутации, профилактика лучше, чем лечение. Сосредоточение расходов на пересмотре таких методов, как управление активами, в стремлении свести к минимуму векторы атак, обеспечение того, чтобы политики безопасности были четко и широко сформулированы и реализованы, а также защита всех конечных точек будет иметь решающее значение.

Настоящая кибербезопасность означает сочетание автоматизации, человеческого опыта и круглосуточной поддержки для защиты от постоянно меняющегося ландшафта угроз. Программа обучения, предоставляющая всем сотрудникам возможность обнаруживать и компенсировать новейшие векторы угроз, создаст культуру кибербезопасности, обеспечивающую самую передовую, доступную и долгосрочную устойчивость». ***(Andy Swift. Optimising Cyber Security Costs In A Recession // ISBuzz Pty Ltd (https://informationsecuritybuzz.com/optimising-cyber-security-costs-in-a-recession/). 02.05.2023).***

***

«Согласно новому исследованию, почти две трети (61%) лиц, принимающих решения в области ИТ-безопасности (ITSDM), считают, что руководство их компании упускает из виду роль кибербезопасности в успехе бизнеса, что приводит к тому, что многие из них не соответствуют действительности.

Исследование Delinea более 2000 ITSDM в 23 странах показало, что несоответствие между кибербезопасностью и бизнес-целями имело негативные последствия практически в девяти из 10 (89%) случаев.

Согласно полученным данным, это привело к повышенному уровню угрозы кибератак, что поставило предприятия под угрозу, которой можно было бы избежать.

Более трети (36%) респондентов считали, что члены совета директоров и высшего руководства их компании рассматривают кибербезопасность только как необходимость соответствия и регулирования, при этом поразительные 17% не считают ее приоритетом.

То, что именно виновато, различается для каждой компании, однако некоторые из ключевых выводов касались задержек с инвестициями, задержек в принятии стратегических решений и ненужного увеличения расходов.

Забегая вперед, Delinea предложила несколько важных областей, на которые следует обратить внимание как компаниям, не достигшим поставленной цели, так и

тем, которые добились удовлетворительных результатов, потому что «все еще есть возможности для улучшения».

Регулярные встречи между командами и руководителями важны для обмена и распространения результатов, а включение сотрудников службы безопасности в различные бизнес-операции может привести к повышению эффективности кибербезопасности.

Все это сделано для того, чтобы не только предотвратить атаки, но и обеспечить соответствие требованиям и снизить стоимость инцидентов, связанных с безопасностью, что одинаково важно для участников опроса.

Главный научный сотрудник и консультант по информационной безопасности Джозеф Карсон объяснил: «Исполнительные руководители должны думать о кибербезопасности не только с точки зрения соблюдения требований или защиты компании, но и с точки зрения ценности, которую она может принести на более стратегическом уровне». соответствие между кибербезопасностью и бизнес-целями как «необходимое для успеха». ***(Craig Hale. Most firms aren't taking cybersecurity seriously enough - and it could come back to haunt them // Future US, Inc. (https://www.techradar.com/news/most-firms-arent-taking-cybersecurity-seriously-enough-and-it-could-come-back-to-haunt-them). 10.05.2023).***

***

«Цифровые технологии коренным образом меняют то, как работают отрасли и приносят пользу клиентам. Чтобы идти в ногу с разрушительными силами цифровой трансформации, предприятия должны быстро внедрять инновации, чтобы конкурировать. Однако эти инновации создают новые киберриски, поскольку предприятия внедряют новые технологии или используют существующие по-новому, создавая новые пути для кибератак. С ростом значения цифровых инноваций в бизнес-операциях, продуктах и услугах потенциальные риски и последствия успешной кибератаки продолжают расти, что делает ставки выше, чем когда-либо прежде.

Чтобы добиться успеха, компании должны обеспечить проактивную устойчивость своих продуктов, услуг и бизнес-операций к кибератакам, изменив роль кибербезопасности в цифровых инновациях.

Проактивная устойчивость

При строительстве горной дороги строители не просто принимают решение о размещении дороги и ждут, когда автомобили упадут со скалы, прежде чем внедрять меры безопасности, такие как ограждения. Вместо этого они анализируют характер дороги и связанные с ней риски и заранее принимают необходимые защитные меры.

Точно так же в успешных цифровых преобразованиях, таких как электронная коммерция, банки и розничные торговцы не внедряют средства для обмена конфиденциальной информацией или проведения транзакций, а принимают решение о применении защитных мер только после взлома. Вместо этого они заранее распознают потенциальные риски и активно внедряют меры кибербезопасности в качестве основы для защиты от них.

При разработке любого нового продукта или услуги крайне важно определить условия, необходимые для его успеха, безопасности и масштабируемости. В

контексте типичной деловой операции такие условия могут включать проверку личности как покупателя, так и продавца, защиту конфиденциальной информации и предоставление подтверждения оплаты. Можно установить эти цели заранее и предвидеть любые факторы, которые могут помешать их достижению.

Четко сформулировав эти цели для нового вида деятельности, можно определить и развернуть технологии кибербезопасности, необходимые для достижения этих целей, и эффективно управлять связанными с ними рисками.

Но традиционные подходы к кибербезопасности в значительной степени далеки от инноваций. Вместо встроенного обеспечения безопасности в новые продукты, услуги и бизнес-деятельность, традиционный подход заключается в реактивном применении элементов управления кибербезопасностью в соответствии с корпоративными политиками и стандартами безопасности. Под давлением необходимости «действовать быстро и ломать вещи» понятно, почему команды разработчиков иногда вообще опускают безопасность в начальных выпусках продукта.

Проблема с этим подходом заключается в том, что развертывание киберконтроля без детального понимания того, как работает конкретная бизнес-операция, неизменно оставит ее незащищенной и одновременно помешает ее эффективной работе. По сути, вы не можете защитить что-то, если не знаете, как это работает.

Хотя стандарты кибербезопасности и процессы управления, которые обеспечивают их применение, помогают поддерживать надлежащую гигиену кибербезопасности и защищать неизменные унаследованные методы ведения бизнеса, они оставляют новые продукты и услуги неадекватно защищенными и мешают требованиям цифровой трансформации.

Организации, проходящие цифровую трансформацию, сталкиваются с дилеммой: либо они не реализуют свои стратегии цифровой трансформации, необходимые для выживания компании, либо ставят под угрозу свою безопасность, подвергая себя неизвестным рискам, с которыми они не могут справиться, что может привести к катастрофическим последствиям.

Чтобы продукты, услуги и бизнес-операции были проактивно устойчивы к кибератакам, необходим фундаментальный сдвиг в роли кибербезопасности и ее отношениях с организацией. Кибербезопасность должна выйти за рамки своих традиционных обязанностей по защите компьютеров компании, чтобы стать неотъемлемой частью основных бизнес-инноваций, разделяя ответственность за защиту и создание ценности для бизнеса.

Интеграция кибербезопасности в дизайн

Первым шагом является включение кибербезопасности в первоначальный дизайн продуктов, услуг и других проектов, ориентированных на технологии. Чтобы удовлетворить требования традиционной разработки программного обеспечения с регулярными циклами выпуска, большинство крупных организаций создали формальные процессы управления, которые требуют проверки кибербезопасности на контрольных точках на протяжении всего жизненного цикла разработки и при тестировании на уязвимости после завершения разработки.

Проблема заключается в том, что уязвимости системы безопасности, обнаруженные на этих более поздних этапах цикла разработки продукта, часто возвращают проекты обратно на чертежную доску, в результате чего замедляется процесс разработки и возникает риск дорогостоящих изменений дизайна для включения функций безопасности, которые можно было бы ожидать как часть первоначальный дизайн. Интегрируя кибербезопасность на этапе проектирования, организации могут избежать этих недостатков и обеспечить необходимую скорость и гибкость, необходимые для удовлетворения требований цифровой трансформации.

Дополнительные обязанности

Инициирование процесса проектирования с помощью кибербезопасности является важным шагом, но он также требует значительного изменения мышления в отношении сотрудничества между командами кибербезопасности и проектировщиками. На практике продуктовые команды сосредотачиваются на создании отличных продуктов и функций и имеют понятную тенденцию рассматривать кибербезопасность как препятствие, которое нужно преодолеть, а в некоторых случаях вообще избежать. Между тем, группы кибербезопасности сосредоточены на управлении общими рисками для корпоративных компьютеров и оценке рисков, связанных с конечным продуктом в этом контексте.

Чтобы успешно включить кибербезопасность в разработку новых продуктов и услуг, как кибербезопасность, так и проектные группы должны взять на себя дополнительные обязанности. Персонал по кибербезопасности должен предоставлять консультации и поддержку по проектированию и архитектуре безопасности, что может потребовать новых возможностей и навыков. Для этого требуется культура сотрудничества, ориентация на услуги и способность оказывать помощь в проектировании кибербезопасности, что отличается от простой оценки соответствия стандартам и практикам безопасности.

С другой стороны, продуктовые группы должны достаточно подробно сформулировать требования к своим продуктам и услугам, чтобы облегчить сотрудничество с персоналом по кибербезопасности. Самая сложная часть оценки состояния кибербезопасности сложных систем — это определение того, как они работают и что они делают. Как только это будет понято, определение соответствующего набора элементов управления станет простым.

Определив основные элементы, необходимые для успеха их проекта, и последствия потенциальных сбоев, группы разработчиков и коллеги по кибербезопасности могут работать вместе, чтобы эффективно применять технологии кибербезопасности для безопасного достижения бизнес-целей.

Интегрируя кибербезопасность в постоянно меняющемся ландшафте цифровой трансформации в качестве важного элемента инноваций и поощряя общую ответственность за создание ценности для бизнеса, компании могут выйти за рамки стандартных оценок рисков своих компьютерных систем и заранее обеспечить устойчивость своих продуктов, услуг и бизнес-операций в целом к потенциальным кибератакам». ***(Jack J. Domet. Cybersecurity Needs to Be Part of Your Product's Design from the Start // Harvard Business School Publishing***

(https://hbr.org/2023/05/cybersecurity-needs-to-be-part-of-your-products-design-from-the-start). 09.05.2023).

***

«Вот отрезвляющая правда: 95% кибератак можно отнести к человеческим ошибкам. Чем больше у вас сотрудников, тем выше риск стать жертвой киберпреступления. Мы все представляем себе легионы хакеров, пытающихся взломать наши брандмауэры, и да, иногда некоторым это удается. Но гораздо более распространенная правда заключается в том, что ничего не подозревающие сотрудники непреднамеренно предоставляют этим киберпреступникам доступ к корпоративным системам и данным, или же эти хакеры подталкивают их к совершению сомнительных (или даже незаконных) действий.

Еще хуже преднамеренные мошеннические действия людей, сидящих между клавиатурой и стулом. Некоторые сотрудники сами пытаются обмануть систему, изменяя суммы, реквизиты банковского счета или другие данные, чтобы улучшить свое личное финансовое положение. Кроме того, есть другие внешние люди, которые не приносят пользы, например, когда поставщик или партнер отправляет компании поддельные или измененные документы, такие как счета-фактуры поставщика с поддельными реквизитами банковского счета или неправильными суммами.

Ни один из этих случаев не является обвинением руководителей компании, методов обеспечения безопасности или суждений. Они просто подчеркивают, что технологии сами по себе не могут остановить каждую кибератаку. Ключом к максимальной защите и минимизации подверженности этим атакам является сочетание технологий с человеческим прикосновением.

1. Безопасные данные начинаются и заканчиваются людьми

Многие кибератаки увенчались успехом благодаря простой, но предотвратимой человеческой ошибке или неправильной реакции на мошенничество. Например, сотрудник может раскрыть имена пользователей и пароли после перехода по ссылке в фишинговом письме. Они могут открыть вложение электронной почты, которое по незнанию устанавливает программу-вымогатель или другое не менее разрушительное вредоносное ПО в корпоративной сети. Или они могут просто выбирать легко угадываемые пароли. Это всего лишь несколько примеров, которые могут позволить кибер-ворам атаковать.

Чтобы свести к минимуму риски, связанные с человеческими ошибками, рассмотрите возможность принятия следующих мер, чтобы обеспечить надежную защиту вашего бизнеса.

Повышение осведомленности и обучение сотрудников: организуйте периодическое обучение передовым методам кибербезопасности, распознаванию фишинговых писем, предотвращению атак с использованием социальной инженерии и пониманию важности безопасной обработки данных. В 2022 году около 10% попыток кибератак были предотвращены, потому что о них сообщили сотрудники, но они могут сообщить о таких попытках только в том случае, если они их узнают.

Создавайте культуру безопасности: убедитесь, что каждый в своей роли активно защищает активы компании, способствуя открытому обмену информацией

о проблемах безопасности, признавая сотрудников, демонстрирующих надежные методы обеспечения безопасности, и включая безопасность в оценку производительности.

Используйте более строгий контроль доступа: контроль доступа ограничивает круг лиц, которые могут просматривать или изменять конфиденциальные данные и системы компании. Применение контроля доступа «принцип наименьших привилегий» и информирование сотрудников о рисках совместного использования учетных записей может ограничить несанкционированный доступ и утечку данных.

Используйте менеджеры паролей: надежные пароли сложно взломать, но сложно запомнить. Программное обеспечение для управления паролями может создавать и хранить сложные для угадывания пароли, при этом пользователям не приходится их «записывать».

Включите многофакторную аутентификацию (MFA): MFA добавляет дополнительный уровень безопасности, требуя дополнительный метод проверки — например, отпечаток пальца или одноразовый код — на случай, если злоумышленник украдет пароль сотрудника.

Внедрите процессы обнаружения мошенничества для входящих документов : эти процессы пытаются идентифицировать мошеннические документы (например, поддельные счета) при получении, прежде чем они смогут быть обработаны.

2. Уменьшите подверженность кибератакам и мошенничеству с помощью технологий и автоматизации.

Несмотря на то, что отсутствие осведомленности, обучения, распознавания и процессов является причиной успеха большинства кибератак, вам по-прежнему нужны технологические барьеры, чтобы попытаться не допустить проникновения решительных хакеров в ваши системы. Финансовые и бухгалтерские отделы являются главными целями для кибератак и мошенников, поэтому системы счетов к оплате (AP) являются главной целью, если они проникнут.

На самом деле, 74% компаний или с ними сталкиваются с попытками мошенничества с платежами. Мошенничество с кредиторской задолженностью использует системы AP и связанные с ними данные и документы с таким вредом, как:

Создание поддельных учетных записей поставщиков и поддельных счетов-фактур для них.

Изменение сумм платежа, банковских реквизитов или дат в действительных счетах-фактурах.

Подделка чеков.

Осуществление мошеннического возмещения расходов.

3. Не допускать плохих парней

Конечно, вы захотите, чтобы ваш ИТ-отдел использовал технологии для предотвращения несанкционированных попыток доступа к сети и системам. Помимо почтенного брандмауэра, некоторые надежные системы включают в себя:

Система обнаружения и предотвращения вторжений (IDPS) отслеживает сетевой трафик на наличие злонамеренных действий или нарушений политик и может автоматически блокировать или сообщать об этих действиях.

Искусственный интеллект (ИИ) играет важную роль в кибербезопасности, используя алгоритмы машинного обучения для анализа объемов данных, выявления закономерностей и прогнозирования потенциальных угроз. Он может определять векторы атак и быстро и эффективно реагировать на киберугрозы, с которыми люди не могут справиться.

Шифрование данных гарантирует, что только авторизованные стороны с правильным ключом дешифрования могут получить доступ к содержимому файла, защищая конфиденциальные данные в состоянии покоя (хранящиеся на устройствах) и при передаче (по сети).

4. Защита от мошенничества изнутри

Независимо от того, преодолевает ли киберпреступник все эти барьеры или недобросовестный сотрудник пытается совершить мошенничество с AP, различные типы автоматизации могут обнаружить и предотвратить успешную кибератаку.

Автоматизированный мониторинг действий сотрудников: это может помочь выявить подозрительное поведение и потенциальные риски безопасности. Программное обеспечение отслеживает действия пользователей, анализирует журналы на наличие признаков несанкционированного доступа и регулярно проверяет права доступа пользователей. Конечно, сотрудники должны знать, что за ними наблюдают и в какой степени.

Полная автоматизация процесса оплаты на одной платформе: исключает человеческую ошибку (и человеческий фактор), за исключением случаев, когда есть исключения. Зашифрованное получение/получение электронных счетов-фактур от поставщиков, автоматическое сопоставление счетов-фактур с заказами и электронные платежи — все без вмешательства человека — являются примерами того, как автоматизация устраняет возможность (и соблазн) совершать мошенничество с использованием AP.

Обнаружение изменений на уровне документов продвигает эту защиту еще на один шаг вперед: эта автоматизированная технология может обнаруживать, когда хитрый кибер-вор, имеющий доступ к базовым системам, предпринимает попытки несанкционированного доступа, модификации или удаления конфиденциальных документов, включая заказы, счета-фактуры и авторизации платежей. Эти инструменты оповещают администраторов и предоставляют подробные журналы аудита операций с документами, помогая обнаруживать и предотвращать мошенничество с точками доступа, независимо от того, происходит ли оно извне или изнутри.

Обнаружение необычных шаблонов данных: предупредите персонал AP, чтобы он еще раз проверил, прежде чем разрешить обработку и оплату счета. Используя машинное обучение и искусственный интеллект, автоматизированные системы могут сравнивать данные с историческими данными, отмечая подозрительные изменения в банковских реквизитах, официальном названии и адресе поставщика, а также необычные суммы платежей.

Почти невозможно полностью защитить себя от кибер-кражи и мошенничества с точками доступа, особенно когда большинство уязвимостей и провинностей связаны с людьми. Вы должны сосредоточить свои усилия по обеспечению безопасности на идеальном балансе между современными

технологиями и людьми между клавиатурой и креслом. Надлежащее и непрерывное обучение может уменьшить человеческие ошибки, которые позволяют кибератакам увенчаться успехом. А технологии и автоматизация могут помочь в первую очередь предотвратить попадание атак на людей. Но правильное сочетание этих двух факторов является ключом к победе над потенциальными мошенниками». ***(Francois Lacas. Cybercriminals Aren't Just Attacking Your Software — They're Coming for Your Employees. Level Up Your Company's Cybersecurity With These 4 Steps. // Entrepreneur Media, Inc. (https://www.entrepreneur.com/growing-a-business/overlooking-these-4-critical-measures-expose-your-company/451737). 10.05.2023).***

***

«…В последние годы наблюдается всплеск кибератак на бухгалтерские фирмы. Нарушение конфиденциальной финансовой информации может иметь тяжелые последствия для клиентов и репутации бухгалтерской фирмы. Чтобы противостоять этим угрозам, специалисты по бухгалтерскому учету должны принять надежные меры кибербезопасности, которые защищают их данные и инфраструктуру.

Основные шаги в области кибербезопасности, которые должны предпринять бизнес-лидеры, включают внедрение многофакторной аутентификации, проведение регулярных аудитов безопасности и обучение сотрудников передовым методам кибербезопасности. Однако сами по себе эти меры не могут защитить фирмы от постоянно развивающихся киберугроз.

Обоюдоострый меч цифровой трансформации

Хотя цифровая трансформация, несомненно, изменила правила игры в профессии бухгалтера, она также поставила новые задачи, причем киберугрозы являются одной из самых насущных проблем. Растущая зависимость от технологий и хранения конфиденциальных финансовых данных в цифровых форматах делает бухгалтерские фирмы привлекательными целями для киберпреступников. Несанкционированный доступ к этой информации может иметь серьезные последствия, включая финансовые потери, ущерб репутации и юридические последствия.

Чтобы ориентироваться в этом сложном ландшафте, бухгалтерские фирмы должны сбалансировать использование технологий для роста и инноваций, одновременно защищая свои системы и данные от киберугроз. В эпоху, когда киберриски развиваются, бухгалтеры должны оставаться в курсе и быть бдительными, принимая надежные меры кибербезопасности для защиты своих ценных цифровых активов.

Шаги для реализации правильной стратегии кибербезопасности

Следующие шаги могут помочь компаниям оценить свои потребности в безопасности, выбрать правильное программное обеспечение и создать комплексный план кибербезопасности.

1. Создайте письменную политику информационной безопасности.

Письменная политика информационной безопасности (WISP) — это официальный документ, в котором излагаются процедуры и протоколы компании

для защиты конфиденциальной информации. Этот документ следует регулярно обновлять, чтобы он отражал последние отраслевые стандарты и меры безопасности.

2. Внедрить двухфакторную аутентификацию.

Включите двухфакторную аутентификацию, чтобы добавить дополнительный уровень безопасности при доступе к конфиденциальным данным и системам. Этот метод аутентификации требует, чтобы пользователи предоставили две формы идентификации: пароль и одноразовый код, что сводит к минимуму несанкционированный доступ.

3. Установите исправления безопасности.

Поддерживайте программное обеспечение и системы в актуальном состоянии, регулярно применяя исправления безопасности. Это помогает снизить риск использования уязвимостей киберпреступниками.

4. Подумайте о программном обеспечении безопасности и управлении брандмауэром

Выберите правильное программное обеспечение для кибербезопасности и решения для брандмауэров, соответствующие потребностям вашей компании. При выборе решения для обеспечения безопасности сравнивайте различные решения, оценивайте поставщиков и учитывайте долгосрочную поддержку и масштабируемость.

5. Установите политику паролей.

Внедрите политику надежных паролей, которая требует от сотрудников создавать сложные уникальные пароли и регулярно их менять. Это снижает вероятность несанкционированного доступа из-за слабых или повторно используемых паролей.

6. Разработайте политику хранения данных.

Создайте политику хранения данных, в которой указано, как долго должна храниться конфиденциальная информация, и надлежащие процедуры удаления данных. Это помогает свести к минимуму риск несанкционированного доступа к устаревшим или ненужным данным.

7. Обеспечьте обучение сотрудников.

Проводите регулярное обучение сотрудников передовым методам кибербезопасности. Обучите персонал фишинговым атакам, безопасному управлению паролями и безопасному просмотру веб-страниц, чтобы снизить риск человеческой ошибки, приводящей к нарушениям безопасности.

Заключение

Цифровая трансформация произвела революцию в бухгалтерской отрасли, но также сделала кибербезопасность главным приоритетом. По мере развития киберугроз бухгалтерские фирмы должны активно улучшать свои меры кибербезопасности для защиты конфиденциальных данных и соблюдения отраслевых норм.

Выполняя описанные выше шаги и выбирая подходящего поставщика кибербезопасности, специалисты по бухгалтерскому учету могут сосредоточиться на предоставлении дополнительных услуг своим клиентам, гарантируя, что их системы и данные останутся в безопасности перед лицом постоянно растущих киберрисков». ***(Jatin Narang. How Accounting Firms Can Embrace And Implement***

The Right Cybersecurity Strategy // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/05/15/how-accounting-firms-can-embrace-and-implement-the-right-cybersecurity-strategy/?sh=694b1e026248). 15.05.2023).

***

«(ISC)² — крупнейшая в мире некоммерческая ассоциация сертифицированных специалистов по кибербезопасности и Королевский институт объединенных служб (RUSI), старейший в мире независимый аналитический центр по международной обороне и безопасности, сегодня опубликовали новое исследование. отчет под названием «Глобальные подходы к киберполитике, законодательству и регулированию».

Выводы из отчета подчеркивают растущую потребность в большей стандартизации и сотрудничестве для обеспечения более надежных и устойчивых платформ, поддерживающих совместное обучение и передовой опыт, в условиях быстро меняющихся политик и правил кибербезопасности во всем мире.

В отчете рассматривается законодательство и регулирование в области кибербезопасности в Канаде, Европейском союзе, Японии, Сингапуре, Соединенном Королевстве и Соединенных Штатах, а также определяются различные проблемы, формирующие киберполитику. Эти проблемы включают нехватку квалифицированных специалистов по кибербезопасности, сложности критической национальной инфраструктуры (CNI) и международное сотрудничество по разработке норм для киберпространства.

Объединяя идеи из разных юрисдикций и заинтересованных сторон, отчет показывает важность сотрудничества между частными и государственными заинтересованными сторонами и тот факт, что политики все чаще стремятся к гармонизации киберполитики.

Это особенно важно для Сингапура, поскольку его цифровая экономика и соответствующая киберэкосистема продолжают быстро расширяться. Хотя страна известна своим передовым регулированием и политикой в области кибербезопасности, в последние годы Сингапур пережил большое количество кибератак.

Например, в 2022 году в стране наблюдался приток SMS-мошенничества, нацеленного на клиентов банков. Агентство кибербезопасности Сингапура (CSA) зафиксировало увеличение на 54 % по сравнению с прошлым годом числа сообщений о программах-вымогателях в 2021.

«Хотя в отчете определяется ряд тенденций в киберполитике, выделяется растущая зависимость от обязательных обязательств по кибербезопасности для критически важных секторов национальной инфраструктуры и за ее пределами, но обязательства, налагаемые различными юрисдикциями для повышения киберустойчивости, различаются», — сказала Пиа Хюш. Аналитик-исследователь по кибербезопасности, технологиям и национальной безопасности в RUSI.

«Поэтому в отчете особое внимание уделяется необходимости лучше понять, какие политики эффективны для повышения киберустойчивости и как они влияют на бизнес и персонал, внедряющий их».

«Политики должны применять упреждающий, а не реактивный подход к политике кибербезопасности и сотрудничать между странами, отраслями и секторами, чтобы установить общие стандарты, протоколы и лучшие практики», — сказал Клар Россо, генеральный директор (ISC)².

«Результаты этого отчета дают ценную информацию об основных законодательных и нормативных приоритетах, что подчеркивает необходимость большей гармонизации между политиками, специалистами по кибербезопасности и другими заинтересованными сторонами для повышения киберустойчивости и решения насущных проблем кибербезопасности в 2023 году и в последующий период.

Чтобы защитить нашу национальную безопасность, экономику, критически важную инфраструктуру, а также данные и конфиденциальность наших граждан, нам нужны последовательные, строгие, перспективные и объединенные политики, которые позволят специалистам по кибербезопасности во всем мире оставаться сосредоточенными на наиболее важных аспектах. своих рабочих мест».

Отчет углубляется в несколько других ключевых заголовков, в том числе:

Приближаются новые правила; организации должны готовиться сейчас, а не позже.

Ни одна страна или правительство не застрахованы от нехватки навыков и рабочей силы в области кибербезопасности.

В то время как нехватка рабочей силы в сфере кибербезопасности в Сингапуре значительно сократилась в 2022 году, город-государство инвестирует в развитие рабочей силы в сфере кибербезопасности и принял ряд мер по привлечению высококвалифицированных работников, например, посредством визовых программ, таких как TechPass.

Глобальная стандартизация имеет решающее значение, и необходимо полное международное сотрудничество для защиты и соблюдения этических принципов и стандартов.

На этом фронте Сингапур активно взаимодействует с широким кругом действующих лиц, включая рабочие группы ООН. Он учредил Сингапурский центр кибербезопасности АСЕАН и проводит ежегодную Сингапурскую международную кибернеделю.

Укрепление критически важной инфраструктуры является главным приоритетом для всех юрисдикций, особенно с учетом большей взаимосвязанности и размытия «границ штатов».

Чтобы обеспечить дальнейшую устойчивость своей критической информационной структуры и цепочек поставок, Сингапур продолжает развивать регулирование, например, в форме Дополнительного свода правил (CCoP 2.0), предусматривающего меры и стандарты, применяемые предприятиями, которые являются частью критической информационной инфраструктуры.

Коллективная защита необходима между государственным и частным секторами и между юрисдикциями для поддержки разработки норм…

Королевский институт объединенных служб (RUSI) проводил это исследование с декабря 2022 г. по март 2023 г. Шесть изучаемых юрисдикций — Великобритания, ЕС, США, Канада, Япония и Сингапур — были выбраны потому,

что они определяют политику в области кибербезопасности и являются лидерами в области, либо как разработчики норм, либо из-за их технологических секторов. Исследование было сосредоточено в основном на политике, принятой или предложенной в период с 2019 по 2023 год. Исследование, лежащее в основе этой публикации, в основном основывалось на обзоре существующей литературы…» ***(Nonprofit, think tank call for global cybersecurity standards // Endeavor Business Media, LLC. (https://www.securityinfowatch.com/cybersecurity/press-release/53060116/isc-is-an-international-nonprofit-membership-association-nonprofit-think-tank-call-for-global-cybersecurity-standards). 10.05.2023).***

***

«Infoblox Inc., компания, предлагающая упрощенную облачную сетевую платформу и платформу безопасности для повышения производительности и защиты, опубликовала выводы своего Отчета о глобальном состоянии кибербезопасности за 2023 г. Компания определила тенденции в области безопасности и сетей, которые побуждают индустрию кибербезопасности следовать ее примеру в объединении команд, занимающихся сетями и безопасностью…

Результаты исследования 2022 года среди респондентов из ОАЭ выявили следующие тенденции:

1. С начала пандемии COVID-19 многие организации в ОАЭ ускорили цифровую трансформацию для поддержки удаленных сотрудников (61%), усилили поддержку клиентских порталов для поддержки своих сотрудников или клиентов (46%), а также сосредоточили средства контроля сети и безопасности на периферия — например, SASE, граничная служба безопасного доступа (44%).

2. В прошлом году большая часть организаций ОАЭ добавила удаленные мобильные устройства сотрудников и корпораций (59%) и облачные серверы DDI (DNS-DHCP-IPAM) (59%) для защиты своих сетей при управлении распространение и связанные с этим риски безопасности от более удаленных устройств в сети. Кроме того, 55% добавили смарт-киоски или аналогичные устройства для поддержки удаленных клиентов или клиентов.

3. В следующие 12 месяцев респонденты из ОАЭ заявили, что их организация будет больше всего обеспокоена утечкой данных (48%), облачными атаками (40%), а также атаками через сетевой IoT (29%).

4. Респонденты из ОАЭ считают, что их организация наименее подготовлена к защите сетей своей организации от внутренних угроз (15%), прямых атак через облачные сервисы (13%), утечки данных (13%), а также программ-вымогателей, цепочки поставок/третьих лиц. групповые атаки и атаки через сетевой IoT, которые упомянули по 11%. Похоже, они не были уверены в способности работников или поставщиков поддерживать высокие стандарты безопасности, особенно когда организации переходят от локальных служб к облачным.

5. В среднем организации ОАЭ обнаружили больше проблем, связанных с атаками по электронной почте/фишинговыми атаками, по сравнению с любым другим типом. Респонденты оценили, что их организация обнаружила проблемы, возникшие в результате примерно 27 атак по электронной почте/фишинга за последние 12 месяцев, а также 17 атак программ-вымогателей, 15 сетевых атак, 15

атак на устройства/конечные точки, 14 атак на приложения и 14 облачных атак за тот же период.

6. Две трети (66%) респондентов из ОАЭ сообщили об одном или нескольких нарушениях безопасности своей организации в результате кибератак, большинство из которых исходят от точек доступа Wi-Fi в результате удаленных сотрудников (41%), третьих лиц и/или поставщиков. сетевых провайдеров (39%), устройств или сетей IoT (38%) и облачной инфраструктуры или приложений (36%).

7. Фишинг был наиболее распространенным методом атаки на организации, подвергшиеся взлому, на его долю приходилось 62% методов атак в прошлом году, за ним следовали сложные угрозы (APT) (53%) и программы-вымогатели (51%).

8. В совокупности оценочная средняя стоимость организационных потерь ОАЭ, включая прямые и косвенные финансовые потери, а также ущерб репутации и расходы на восстановление, возникшие в результате нарушений в прошлом году, составила примерно 8 миллионов дирхамов ОАЭ (2,2 миллиона долларов США). Организации, ставшие жертвами взломов, чаще всего сталкивались с перебоями в работе или простоями системы (49%), блокировкой данных из-за программ-вымогателей (41%) и других вредоносных программ (39%) или манипулирования данными (38%).

9. Организации ОАЭ использовали различные средства контроля для защиты своих сетевых активов в локальных, облачных и гибридных (локальных и облачных) средах. Наиболее распространены средства управления VPN/доступом (29%) для локальных сетей; Безопасность DNS (48%) и брокеры безопасности доступа к облаку, шифрование данных и безопасная подготовка и удаление (по 44%) для облачных сред.

10. В среднем большинству организаций (69%) требуется до 24 часов на расследование угрозы, при этом многие полагаются на сторонние платформы или службы анализа угроз. Чтобы облегчить свои расследования или поиск угроз, группы безопасности в основном полагаются на информацию об уязвимостях (44%), DNS-запросы и ответы (43%), аналитику с открытым исходным кодом (39%) и данные о сетевых потоках (38%).

11. Система доменных имен (DNS) обеспечивает различные меры безопасности для защиты организаций и является ключевым компонентом практически всех стратегий безопасности организаций. Респонденты сообщили, что их организации чаще всего используют DNS в своей стратегии для решения следующих задач: защита от таких угроз, как туннелирование DNS, эксфильтрация данных и алгоритмы создания доменов, которые могут пропустить другие инструменты безопасности (61%); помощь в обнаружении активности вредоносных программ на более ранних этапах цепочки уничтожения (57%); блокировка известных неверных запросов к адресату для снижения нагрузки на защиту периметра (55 %); и информирование их об устройствах, отправляющих запросы на подключение к вредоносным ресурсам (51%).

12. Основные ожидаемые проблемы в области защиты от атак связаны с возможностью контролировать доступ удаленных сотрудников (38%), реагировать на оповещения (31%), нехваткой навыков ИТ-безопасности (30%) и ограниченным бюджетом (35%).

13. Большинство (62%) организаций ОАЭ указали, что их бюджеты на ИТ-безопасность увеличились в 2022 году, а 72% заявили, что ожидают увеличения бюджетов на безопасность в 2023 году для борьбы с известными и новыми угрозами.

14. Наиболее популярные запланированные закупки технологий включают мониторинг сетевого трафика/сетевое обнаружение и реагирование (NDR) и анализ угроз (по 50 %) для гибридных сред; защита от потери данных, брокеры безопасности облачного доступа (CASB) и безопасность DNS (по 39% каждый) для облачных систем; безопасная инициализация и деинициализация (27%), средства управления VPN/доступом (25%), а также обнаружение и реагирование конечных точек (24%) для локальной защиты». ***(Infoblox's 2023 Global State of Cybersecurity Report: 66% of UAE Organizations Report Data Breaches in the Past Year // MENAFN (https://menafn.com/1106238876/Infobloxs-2023-Global-State-of-Cybersecurity-Report-66-of-UAE-Organizations-Report-Data-Breaches-in-the-Past-Year). 12.05.2023).***

***

«Согласно недавно опубликованному Всемирному экономическому форуму (ВЭФ) отчету о глобальных рисках за 2023 год, широко распространенные киберпреступления и угрозы кибербезопасности входят в десятку основных угроз для частного и государственного секторов в ближайшие два года.

В отчете также предполагается, что к 2025 году киберпреступность может привести к ежегодным потерям для мировой экономики в размере 10,5 трлн долларов. В Англии и Уэльсе на случаи кибермошенничества в прошлом году приходилось 61% всех случаев мошенничества.

В сегодняшней меняющейся среде организации должны найти более эффективные меры для устранения этих угроз.

Однако при внесении этих корректировок также необходимо учитывать влияние на продажи и качество обслуживания клиентов.

Платформа автоматизации, оснащенная роботизированной автоматизацией процессов с минимальным кодом и машинным обучением, может удовлетворить финансовые требования, требования клиентов и репутации на протяжении всего процесса, одновременно повышая кибербезопасность.

Хотя сотрудники являются движущей силой организаций, они также могут быть самым слабым звеном в отношении предотвращения мошенничества и кибербезопасности.

В современном быстро меняющемся мире люди склонны быстро читать и медленно думать, особенно с учетом огромного количества сообщений, которые они ежедневно получают в виде текстовых сообщений, электронных писем и социальных сетей. Эта информационная перегрузка может привести к тому, что люди будут действовать на автопилоте, что приведет к отсутствию критического мышления и сделает их уязвимыми для мошенничества мошенников.

Даже если вы считаете, что никогда не станете жертвой попытки мошенничества, такое мышление может усугубить проблему. Люди часто считают,

что такие инциденты с ними никогда не произойдут, что еще больше усложняет обнаружение подозрительной активности.

Представьте, что вашу команду аккаунтов взломали, и, просканировав ранее отправленные электронные письма, хакеры знают, как написать письмо, чтобы убедить вас, что это действительно они. Или вы получаете письмо со знакомого адреса, но изменена только предпоследняя буква.

Вы уверены, что заметите эти нюансы, когда совершенно ничего не подозреваете и теряете бдительность? Есть причина, по которой фишинг является одним из наиболее распространенных и наиболее успешных типов кибератак.

Принятие низкого кода для защиты внутренних и внешних коммуникаций

Чтобы решить эту проблему, организации могут отказаться от использования исключительно электронной почты для цифрового общения, поскольку важна не сама электронная почта, а средство связи.

Этого можно достичь, разработав приложение с низким кодом.

Простота простого перетаскивания кода означает, что ваша организация может легко разработать приложение для обмена сообщениями и файлами. Такое приложение лишает киберпреступника возможности атаковать ваших сотрудников.

Конечно, электронная почта по-прежнему будет нужна в некотором качестве, поскольку сообщения от людей за пределами организации не смогут пройти через приложение.

Эти электронные письма сопровождаются неотъемлемыми рисками безопасности, например, возможностью фишинговых ссылок.

Тем не менее, сотрудника следует научить ожидать, что релевантные ссылки от коллег будут отправлены через приложение с низким кодом. Что касается электронных писем, дополнительное обучение должно сделать их осторожными с такими сообщениями и любыми вложениями или ссылками, которые они могут включать.

Любые принимаемые меры должны сопровождаться образовательным обучением, в ходе которого сотрудники узнают о передовом опыте и о том, на что следует обращать внимание в случае мошенничества.

Например, внутренние политики, которые требуют, чтобы сотрудники раскрывали личную или финансовую информацию только через корпоративный портал, который можно создать с помощью платформы с низким кодом, снижают вероятность того, что они будут делиться этой информацией по электронной почте.

Портал защищает не только организации и их сотрудников, но и тех, кого они обслуживают.

Например, если пациент хочет ввести медицинские данные для своего врача или проверить результаты своих анализов в больнице, он может сделать это через портал для пациентов, не беспокоясь о безопасности своей информации.

Устранение препятствий для повышения безопасности

Внедряя платформы с низким кодом, организации могут уменьшить количество барьеров на пути внедрения эффективной системы кибербезопасности.

Разработчики, не занимающиеся кодированием, могут быстро создавать безопасные приложения собственными силами, предоставляя экономичное решение,

которое выгодно командам по кибербезопасности с ограниченными бюджетами, обычно выделяемыми другим отделам.

Любое решение с низким кодом должно включать в себя функции контроля и управления, которые позволяют центральной ИТ-группе поддерживать надзор, поскольку внутренние разработчики с низким кодом могут не обладать знаниями для обеспечения соблюдения мер безопасности.

При правильном решении ИТ-специалисты могут поддерживать управление, контролируя разработку приложений и доступ.

Низкий уровень кода также способствует итеративной разработке, а это означает, что организации могут адаптировать свои приложения к изменяющимся обстоятельствам или требованиям безопасности.

Поддержание защиты с помощью RPA и ML

Сочетание низкого кода с роботизированной автоматизацией процессов (RPA) и машинным обучением (ML) может укрепить сети кибербезопасности организаций.

RPA помогает обнаруживать точные совпадения символов и согласовывать информацию с заранее определенными критериями, предоставляя сотрудникам помеченные электронные письма, которые требуют более тщательного изучения.

Кроме того, это помогает преодолеть недостаток критического мышления, возникающего при быстром просмотре электронных писем, тем самым укрепляя сеть кибербезопасности.

Машинное обучение особенно полезно, когда речь идет о больших объемах информации, например, об организациях здравоохранения, местных советах или корпорациях. Он может использовать эти обширные данные для выявления закономерностей и прогнозирования тенденций в области безопасности.

Благодаря тому, что RPA и ML предлагаются в тандеме с минимальным кодом на единой легко интегрируемой платформе, организации могут более эффективно разрабатывать безопасную инфраструктуру, поскольку эти передовые технологии работают вместе для оптимизации безопасности.

Платформа автоматизации позволяет добиться безопасности без компромиссов

Повышение безопасности часто является балансом между бюджетом и качеством обслуживания клиентов. Когда организация отдает приоритет безопасности, это может привести к замедлению процессов и снижению производительности, что негативно скажется на качестве обслуживания клиентов.

Но что, если бы организациям не пришлось жертвовать такими столпами, как гражданский опыт, безопасность и ограниченный бюджет?

Благодаря использованию платформы автоматизации меры аутентификации могут быть автоматизированы. Более того, RPA может перепроверять информацию на высоких скоростях, обеспечивая быструю защиту, которая способствует удовлетворенности клиентов и поддерживает большие объемы транзакций и взаимодействий.

Кибербезопасность является обязательной для всех организаций, поэтому важно найти способы управления рисками без ущерба для безопасности граждан и сотрудников.

Предоставив вашей организации эффективную платформу автоматизации с четко определенными политиками и процедурами безопасности, а также всестороннее обучение, руководители могут быть уверены, что человеческий фактор — их самый значительный риск безопасности — в значительной степени сведен к минимуму». ***(Richard Higginbotham. Automation platform mitigates employee cybersecurity risk // Adjacent Digital Politics Ltd (https://www.openaccessgovernment.org/automation-platform-mitigates-employee-cybersecurity-risk/158852/). 12.05.2023).***

***

«Компания Immersive Labs, лидер в области киберустойчивости, ориентированной на людей, сегодня объявила о своем отчете о тенденциях устойчивости сотрудников в киберпространстве за 2023 год, подготовленном Osterman Research. В отчете показано, что неуклонный рост кибератак и меняющийся ландшафт угроз приводят к тому, что все больше организаций обращают свое внимание на создание долгосрочной киберустойчивости; однако многие из этих программ терпят неудачу и не могут доказать реальные кибер-возможности команд. В отчете, в ходе которого были опрошены 570 руководителей высшего звена в области безопасности и управления рисками на предприятиях Великобритании, США и Германии со штатом не менее 1000 сотрудников, было обнаружено, что хотя 86% организаций имеют программу киберустойчивости, более половины (52%) респондентов говорят, что в их организации отсутствует комплексный подход к оценке киберустойчивости.

Укрепление кибер-возможностей возглавляет список стратегических приоритетов для организаций в 2023 году, при этом повышение кибер-устойчивости членов группы кибербезопасности (83%) и общей рабочей силы (75%) определено как две наиболее приоритетные области. Организации предприняли шаги по развертыванию программ киберустойчивости; однако 53% респондентов указали, что персонал организации плохо подготовлен к следующей кибератаке (любого рода), и чуть более половины заявили, что им не хватает комплексного подхода к оценке киберустойчивости. Эти статистические данные показывают, что, хотя киберустойчивость является приоритетом и программы существуют, их текущая структура и обучение неэффективны.

«Сегодня все думают о киберустойчивости на фоне постоянно меняющегося ландшафта угроз, когда программы-вымогатели, риски цепочки поставок и уязвимости являются главными проблемами лидеров безопасности. И хотя это обнадеживает, что организации и лидеры внедряют тактики и программы для повышения киберустойчивости, многие, к сожалению, все еще не достигают цели», — сказал Джеймс Хэдли, генеральный директор и основатель Immersive Labs. «Несмотря на все аудиторные занятия и сертификации, половина респондентов указали, что сотрудники, группы кибербезопасности и организация недостаточно подготовлены. Очевидно, что текущие программы необходимо реструктурировать, чтобы обеспечить успешную реализацию программы киберустойчивости».

Ниже приведены дополнительные ключевые выводы из исследовательского отчета, подчеркивающие необходимость в дополнительных и модернизированных

программах киберустойчивости в организациях, а не только для группы безопасности:

Организациям не хватает уверенности в том, что их основная рабочая сила будет знать, как реагировать на киберинцидент: каждые две из трех организаций не уверены, что 95% их сотрудников не будут знать, как восстановиться после киберинцидента. К высокоприоритетным задачам относятся поддержание бизнес-операций без доступности основных ИТ-систем, выполнение срочных задач с использованием ручных процессов и не усложнение процесса восстановления путем подключения скомпрометированных устройств к сети.

Организации ставят под сомнение надежность отраслевых сертификатов, аудиторных занятий и специальных путей обучения для повышения киберустойчивости: хотя почти все организации поощряют отраслевые сертификаты, только 32% говорят, что они эффективны в борьбе с киберугрозами. Обучение в классе предлагается слишком редко, чтобы быть эффективным, и только около четверти (27%) респондентов указали, что проходят ежемесячное обучение. Почти половина респондентов (46%) говорят, что их сотрудники не знали бы, что делать, если бы получили фишинговое электронное письмо, несмотря на многолетнее обучение по вопросам безопасности и тесты на фишинг.

Большинству компаний не хватает структуры с показателями для измерения и демонстрации киберустойчивости: наличие правильных показателей для подтверждения киберустойчивости среди команд важно, особенно когда советы директоров и руководители высшего звена ищут конкретные доказательства. Несмотря на это, почти половина (46%) старших руководителей по безопасности и рискам говорят, что у них нет показателей, необходимых для полной демонстрации устойчивости их сотрудников перед лицом кибератаки. Только около 6 % организаций используют информативные показатели, такие как время отклика, для устранения уязвимостей, отслеживания показателей вторжений, показателей внутренней потери данных и уровней возникновения различных типов угроз.

Коммуникация с Советом директоров и высшим руководством по вопросам киберустойчивости необходима для стимулирования изменений: за последние шесть месяцев запрос к группе безопасности о подтверждении киберустойчивости был направлен Советом менее чем в половине (46%) организаций. Для команды высшего руководства в 51% организаций. Повышение осведомленности о важности киберустойчивости — важный шаг к получению большей поддержки со стороны этих критически важных лидеров. При общении с Советом директоров и высшим руководством руководители по безопасности и рискам должны использовать обмен сообщениями о киберустойчивости, а не сосредотачиваться на статусе разрозненных входных данных, таких как развертывание новых решений кибербезопасности…» ***(New Osterman Research Report Finds Cyber Resilience Programs are Falling Short, With More Than Half of Security Leaders Revealing Their Workforce Is Not Prepared for A Cyberattack // Business Wire (https://www.businesswire.com/news/home/20230517005210/en). 17.05.2023).***

***

«Exactitude Consultancy, исследовательское и консалтинговое подразделение Ameliorate Digital Consultancy Private Limited, завершила и опубликовала окончательную копию подробного исследовательского отчета о рынке кибербезопасности.

Ожидается, что размер мирового рынка кибербезопасности вырастет на 10,6% в год с 2023 по 2029 год. Ожидается, что к 2029 году он превысит 850,17 млрд долларов США по сравнению со 159,65 млрд долларов США в 2022 году. Кибербезопасность стала серьезной проблемой в современном цифровом ландшафте. С ростом зависимости от технологий и взаимосвязанных систем необходимость защиты конфиденциальной информации от киберугроз как никогда актуальна. Рынок превратился в жизненно важную отрасль, предоставляющую решения и услуги для защиты организаций от злонамеренных атак. В этой статье мы рассмотрим рынок кибербезопасности, его эволюцию, ключевых игроков, типы решений, отраслевые вертикали, новые тенденции, проблемы и перспективы на будущее.

Во взаимосвязанном мире, где широко распространены утечки данных и кибератаки, кибербезопасность играет жизненно важную роль в защите конфиденциальной информации. Рынок кибербезопасности включает в себя широкий спектр продуктов, услуг и решений, предназначенных для защиты организаций от цифровых угроз. Все, от малого бизнеса до крупных корпораций, уязвимы для кибератак, что делает кибербезопасность первостепенной задачей». ***(With 10.6% CAGR, Cyber Security Market Size is Expected to Reach USD 850.17 Bn by 2029 // Cision US Inc. (https://www.prnewswire.com/news-releases/with-10-6-cagr-cyber-security-market-size-is-expected-to-reach-usd-850-17-bn-by-2029--301826065.html). 16.05.2023).***

***

«…Только в 2022 году произошло в общей сложности 4100 публично раскрытых утечек данных, в том числе около 22 миллиардов записей, которые были раскрыты. И все это несмотря на то, что в 2021 году организации по всему миру потратили на кибербезопасность рекордные 150 миллиардов долларов.

Меняется и само программное обеспечение. Рост искусственного интеллекта в целом и генеративного ИИ в частности коренным образом меняет то, как компании используют программное обеспечение. Растущее использование ИИ, в свою очередь, делает поверхности для атак программного обеспечения более сложными, а само программное обеспечение более уязвимым.

Как же тогда компании должны защищать свое программное обеспечение и данные?

Ответ заключается не в том, что кибербезопасность — это бессмысленное занятие — это далеко не так. Вместо этого то, чего компании стремятся достичь с помощью своих программ безопасности, должно развиваться, так же как эволюционировало то, как компании используют данные и программное обеспечение. Пришло время изменить и их усилия в области кибербезопасности.

В частности, компании могут адаптироваться к растущей ненадежности цифрового мира, внеся три изменения в способы укрепления своего программного обеспечения:

3 способа, которыми компании могут улучшить свою кибербезопасность

Во-первых, главной целью программ кибербезопасности больше не должно быть предотвращение сбоев.

Программные системы, ИИ и данные, на которые они все полагаются, настолько сложны и хрупки, что сбой на самом деле является особенностью этих систем, а не ошибкой. Так как системы ИИ сами по себе являются вероятностными, например, ИИ гарантированно иногда ошибается — в идеале, однако, в меньшей степени, чем люди. То же самое относится и к программным системам, но не потому, что они являются вероятностными, а потому, что по мере увеличения их сложности растет и их уязвимость. По этой причине программы кибербезопасности должны переключить свое внимание с попыток предотвратить инциденты на обнаружение и реагирование на сбои, когда они неизбежно происходят.

Принятие так называемых архитектур с нулевым доверием, основанных на предположении, что все системы могут или будут скомпрометированы злоумышленниками, является одним из многих способов распознать эти риски и отреагировать на них. У правительства США даже есть стратегия нулевого доверия, которую оно внедряет во всех департаментах и агентствах. Но принятие архитектур с нулевым доверием — это лишь одно из многих изменений, которые должны произойти на пути к принятию сбоев в программных системах. Компании также должны больше инвестировать в свои программы реагирования на инциденты, объединять свое программное обеспечение и ИИ для устранения различных типов сбоев путем моделирования потенциальных атак, укреплять внутреннее планирование реагирования на инциденты для традиционного программного обеспечения и систем ИИ и многое другое.

Во-вторых, компании также должны расширить свое определение «сбоя» для программных систем и данных, чтобы охватить больше, чем просто риски безопасности.

Цифровые сбои больше не связаны просто с безопасностью, а теперь связаны с множеством других потенциальных опасностей, начиная от ошибок производительности и заканчивая проблемами конфиденциальности, дискриминацией и многим другим. Действительно, с быстрым внедрением ИИ определение инцидента безопасности само по себе перестало быть четким.

Веса (обученные «знания», хранящиеся в модели) для генеративной модели искусственного интеллекта Meta LLaMA, например, стали достоянием общественности в марте, что дало любому пользователю возможность запустить модель с многомиллиардными параметрами на своем ноутбуке. Утечка, возможно, началась как инцидент безопасности, но она также породила новые опасения в отношении интеллектуальной собственности в отношении того, кто имеет право использовать модель ИИ (кража IP), и подорвала конфиденциальность данных, на которых была обучена модель (знание параметры могут помочь воссоздать его обучающие данные и, следовательно, нарушить конфиденциальность). И теперь, когда эта модель находится в свободном доступе, ее можно использовать более

широко для создания и распространения дезинформации. Проще говоря, злоумышленнику больше не нужно нарушать целостность или доступность программных систем; изменение данных, сложные взаимозависимости и непреднамеренное использование систем ИИ сами по себе могут привести к сбоям.

Таким образом, программы кибербезопасности не могут сводиться к сосредоточению внимания только на сбоях в системе безопасности; на практике это приведет к тому, что группы информационной безопасности со временем станут менее эффективными по мере роста масштабов программных сбоев. Вместо этого программы кибербезопасности должны стать частью более широких усилий, направленных на общее управление рисками — оценку возможных сбоев и управление ими, независимо от того, был ли сбой вызван злоумышленником или нет.

Это, в свою очередь, означает, что в состав групп по информационной безопасности и управлению рисками должен входить персонал с широким спектром знаний, выходящих за рамки только безопасности. Эксперты по конфиденциальности, юристы, инженеры по обработке данных и другие лица играют ключевую роль в защите программного обеспечения и данных от новых и развивающихся угроз.

В-третьих, мониторинг сбоев должен быть одним из самых приоритетных направлений работы всех групп кибербезопасности.

К сожалению, в настоящее время это не так. В прошлом году, например, компаниям потребовалось в среднем 277 дней или примерно 9 месяцев, чтобы выявить и локализовать нарушение. И слишком часто организации узнают о нарушениях и уязвимостях в своих системах не из собственных программ безопасности, а через третьих лиц. Нынешняя зависимость от посторонних для обнаружения сама по себе является молчаливым признанием того, что компании не делают всего, что должны, чтобы понять, когда и как их программное обеспечение дает сбой.

На практике это означает, что каждая программная система и каждая база данных нуждаются в соответствующем плане мониторинга и показателях потенциальных сбоев. Действительно, этот подход уже набирает обороты в мире управления рисками для систем ИИ. Национальный институт стандартов и технологий (NIST), например, выпустил свою концепцию управления рисками ИИ ранее в этом году (AI RMF), в которой четко рекомендуется, чтобы организации отображали потенциальный вред, который система ИИ может генерировать, и разработали соответствующий план для измерения и управления. каждый вред. (Полное раскрытие информации: я получил грант от NIST на поддержку разработки AI RMF.) Применение этой передовой практики к программным системам и базам данных в целом — это прямой способ подготовиться к сбоям в реальном мире.

Однако это не означает, что третьи стороны не могут играть важную роль в обнаружении инцидентов. Наоборот: третьи стороны играют важную роль в обнаружении сбоев. Такие мероприятия, как «награды за обнаружение ошибок», в которых вознаграждения предлагаются в обмен на обнаружение рисков, являются проверенным способом стимулирования обнаружения рисков, как и четкие способы для потребителей или пользователей сообщать о сбоях, когда они происходят. Однако в целом третьи стороны не могут продолжать играть основную роль в

обнаружении цифровых сбоев…» ***(Andrew Burt. The Digital World Is Changing Rapidly. Your Cybersecurity Needs to Keep Up // Harvard Business School Publishing (https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up). 16.05.2023).***

***

«…Количество пользователей, устройств и программ увеличивается в сочетании с растущим потоком данных, большинство из которых являются конфиденциальными, а потребность в кибербезопасности продолжает расти с каждым днем.

Проблема еще больше усугубляется увеличением изощренности кибер-злоумышленников и их методов атаки.

Тенденции кибербезопасности и технологий на 2022–2023 годы

Из-за цифровой революции глобальные предприятия, как малые, так и крупные корпоративные организации, а также государственные полугосударственные предприятия, так сильно зависят от компьютеризированных систем для управления всей своей повседневной деятельностью и, таким образом, делают кибербезопасность своим ключевым приоритетом для защиты своих данных от различных онлайн-атак или несанкционированного доступа. к их данным.

Поэтому непрерывные изменения в глобальных технологиях также означают параллельный сдвиг в тенденциях современных технологий кибербезопасности, новости об утечках данных и взломах стали нормой для регулярных действий. Ниже приведены основные тенденции кибербезопасности:

1. Новая цель мобильна

Современные тенденции в области технологий кибербезопасности в значительной степени обеспечивают разумный рост вредоносных программ или атак для мобильных банков в прошлые годы, что делает так много устройств потенциальной добычей для хакеров.

Все финансовые транзакции, электронная почта и сообщения несут в себе множество угроз для отдельных лиц и организаций. Вирусы для смартфонов или вредоносное ПО — еще одна вещь, которая привлекла внимание трендов кибербезопасности.

2. Рост числа взломов автоматизации

Так много современных автомобилей спроектированы с использованием автоматизированного программного обеспечения, которое обеспечивает беспрепятственное подключение водителей к управлению, двигателю, дверному замку, подушкам безопасности, хронометрированию и усовершенствованным системам помощи водителю.

Многие из этих транспортных средств используют технологии Bluetooth и WIFI для связи, что также дает им доступ к различным уязвимостям и хакерским угрозам.

Использование самоуправляемых транспортных средств или автономных транспортных средств использует более сложный механизм, который требует строгой технологии кибербезопасности.

3. Искусственный интеллект (ИИ)

Появление на рынке искусственного интеллекта и комбинации машинного обучения привело к большим изменениям в кибербезопасности.

ИИ был неотъемлемой частью построения автоматизированных систем безопасности, обработки естественного языка, автоматического обнаружения угроз, а также распознавания лиц.

ИИ также используется для создания интеллектуальных вредоносных программ и атак, которые обходят новейшие протоколы безопасности при контроле данных.

Искусственный интеллект позволяет системам обнаружения угроз предсказывать новые атаки или злоумышленников и мгновенно уведомлять администраторов об утечке данных.

4. Основная цель — утечка данных

Ключевой проблемой для каждой организации в мире являются данные. Основной целью как отдельных лиц, так и организаций является безопасность их данных.

Любая небольшая лазейка в системном браузере или программном обеспечении организации станет целью хакеров, чтобы легко получить доступ к информации такой организации или отдельного лица.

5. Облако — еще одна потенциально уязвимая среда

С созданием многих организаций в облаке безопасность данных требует постоянного мониторинга и регулярных обновлений, чтобы защитить данные от попадания в чужие руки.

Некоторые облачные приложения должным образом оснащены средствами безопасности со своей стороны, но пользовательская сторона всегда служит источником ошибок, фишинговых атак и вредоносных программ.

6. Автоматизация и интеграция

Учитывая скорость, с которой размер данных увеличивается ежедневно, важно интегрировать автоматизацию, чтобы обеспечить более совершенный контроль над информацией в Интернете.

Это также требует, чтобы инженеры и другие специалисты по безопасности предлагали профессиональные и быстрые решения. Нынешняя проблема безопасности делает автоматизацию более ценной, чем раньше.

Измерения безопасности объединяются в ходе гибкого процесса для создания более безопасного программного обеспечения во всех областях.

сложные и большие веб-приложения сложны, поэтому автоматизация и кибербезопасность являются основными понятиями в процессе разработки программного обеспечения.

7. Нацельтесь на программы-вымогатели

Это еще одна важная тенденция в области кибербезопасности, которую нельзя не заметить. В частности, в развитых странах мира они так сильно полагаются на определенное программное обеспечение для выполнения своей повседневной деятельности. Первопроходцы программ-вымогателей более сосредоточены.

8. Угрозы от инсайдера

Одна из основных причин ошибки данных. Любой тяжелый день или маленькая преднамеренная лазейка могут привести к краху организации с украденными данными на миллионы.

Статистика тенденций кибербезопасности показывает, что около 34% всех атак были прямо или косвенно связаны с вовлеченным сотрудником организации.

Чтобы защитить свои данные всеми возможными способами, вам необходимо повысить осведомленность своих сотрудников.

9. Конфиденциальность данных как дисциплина

Одной из основных тенденций технологий кибербезопасности является повышение конфиденциальности данных, это отдельная дисциплина. Одна из вещей, которая приводит к различным громким кибератакам, — это раскрытие личных информационных записей.

Организации, которые не соблюдают правила, рискуют получить штрафы и получить плохую огласку, а это приведет к потере доверия потребителей к организации. Конфиденциальность данных затрагивает все сферы деятельности организации.

Это заставляет все организации уделять больше внимания обеспечению конфиденциальности данных и обеспечению управления доступом на основе ролей, многофакторной аутентификации, сегментации сети, шифрования при передаче и хранении, а также внешней оценки для выявления областей улучшения.

10. Мобильная кибербезопасность

Использование мобильных телефонов растет с высокой скоростью из-за увеличения удаленной работы.

Удаленные работники, как правило, с комфортом переключаются между мобильными устройствами, такими как телефоны и планшеты, и используют как частные, так и общедоступные сети WIFI. Вот некоторые из мобильных угроз:

мобильные вредоносные программы с различными возможными приложениями, которые варьируются от кражи данных до SMS-спам-атак.

Хакеры используют или используют уязвимости безопасности в устройствах Android.

Специализированное шпионское ПО разработано специально для слежки за зашифрованными приложениями для обмена сообщениями.

Увеличение использования многофакторной аутентификации

Пароли остаются стандартом для кибербезопасности, поэтому многие компании с радостью примут многофакторную аутентификацию (MFA), чтобы всегда бороться с утечкой данных и вредоносными атаками.

MFA предполагает использование двух или более отдельных факторов для авторизованных пользователей для доступа к защищенным данным, заставляя людей и пользователей использовать более одного устройства для подтверждения своей личности.

Microsoft посоветовала пользователям отказаться от телефонной базы MFA, потому что злоумышленники могут получить доступ к открытому тексту, отправляемому на мобильные телефоны отдельных лиц и организаций. Это возможно, потому что SMS-сообщения не шифруются.

11. Аналитика поведения пользователей

Каждый раз, когда имя пользователя и пароль людей скомпрометированы, любой, кто имеет к ним доступ, может выйти в Интернет и совершить любое злонамеренное поведение.

Это может вызвать тревогу у защитников системы, если аналитика поведения пользователей. используется

Как только злоумышленник получает доступ к данным или информации организации, первое, что он делает, — это компрометирует учетные данные организации. UBA очень поможет идентифицировать настоящего пользователя от злоумышленников.

Заключение

Защита ваших данных и другой конфиденциальной и важной информации — это тенденция кибербезопасности в мире технологий.

Тенденции кибербезопасности в ближайшие годы обязательно заставят организации опасаться усиливать или удваивать свои стратегии безопасности.

Ожидается, что никакие деньги и время, потраченные на защиту ваших данных с помощью кибербезопасности, не будут слишком большими по сравнению с ущербом, утечкой или уязвимостью вашей информации, которые могут стоить вам намного больше, чем инвестиции в кибербезопасность». ***(Kevin James. Cybersecurity and Latest Technology Trends For 2022-2023 // Cybersecurity For Me (https://cybersecurityforme.com/cybersecurity-and-latest-technology-trends/). 16.05.2023).***

***

«В сегодняшнюю цифровую эпоху приложения финансовых технологий (FinTech) становятся все более популярными. Это связано с их простотой использования и удобством, когда дело доходит до управления финансами. Поскольку все больше людей полагаются на эти приложения для своих банковских нужд, они также должны учитывать важность кибербезопасности. Разработка безопасного приложения FinTech необходима для защиты данных пользователей и предотвращения злонамеренных атак со стороны хакеров. В этом сообщении блога мы обсудим, как разработчики могут обеспечить безопасность своих финтех-приложений для всех пользователей. Мы рассмотрим такие темы, как протоколы аутентификации, методы шифрования и другие передовые методы обеспечения безопасности, которые следует применять на протяжении всего процесса разработки. Следуя этим рекомендациям, разработчики могут создать эффективную защиту от потенциальных киберугроз, обеспечивая при этом положительный пользовательский опыт для клиентов, которые полагаются на их услуги.

1. Понять риски, связанные с приложениями FinTech

По мере развития технологий финансовая индустрия обращается к аутсорсингу разработки финансовых технологий для создания приложений, которые могут оптимизировать транзакции и способствовать более быстрым платежам. Однако существуют риски, связанные с созданием безопасного финтех-приложения из-за возможности утечки финансовых данных или кибератак. Разработчикам важно понимать риски, прежде чем начинать разработку любого финтех-приложения.

Существует несколько типов угроз безопасности, которые различаются в зависимости от типа создаваемого приложения, например манипулирование данными, несанкционированный доступ, внедрение вредоносного кода и атаки вредоносного программного обеспечения. Разработчики должны знать о различных методах, которые злоумышленники могут использовать для получения доступа к финансовым счетам и конфиденциальным данным. Для защиты от этих угроз разработчикам важно учитывать меры безопасности, такие как двухфакторная аутентификация, шифрование, надежные ключи API и системы контроля доступа при создании безопасного приложения FinTech. Кроме того, для обеспечения оптимальной защиты от внешних угроз необходимо регулярно устанавливать обновления безопасности.

2. Разработайте безопасную архитектуру для своего финтех-приложения

При разработке безопасной архитектуры для финтех-приложения важно подумать о том, как создать финтех-приложение, чтобы защитить его от потенциальных кибератак. Безопасная архитектура должна включать такие меры, как двухфакторная аутентификация, шифрование, надежные ключи API и системы контроля доступа.

Двухфакторная аутентификация добавляет дополнительный уровень безопасности, требуя от пользователей ввода дополнительной информации или использования биометрических методов, таких как распознавание лиц или сканирование отпечатков пальцев, прежде чем они смогут получить доступ к конфиденциальным финансовым счетам или данным. Шифрование данных также помогает добавить дополнительный уровень защиты, предотвращая доступ неавторизованных пользователей к данным без правильного ключа. Кроме того, надежные ключи API важны для обеспечения безопасной связи между серверами и веб-приложениями, а также для предотвращения вредоносных действий. Наконец, системы контроля доступа могут быть реализованы для ограничения доступа определенных пользователей к определенным областям приложения и предотвращения несанкционированного доступа.

3. Внедрить протоколы аутентификации и авторизации

Для обеспечения безопасности приложения FinTech протоколы аутентификации и авторизации абсолютно необходимы для разработчиков. Аутентификация позволяет пользователям уверенно подтверждать свою личность перед доступом к конфиденциальным данным или финансовым счетам. Без этих мер безопасности невозможно гарантировать безопасный доступ! Это можно сделать с помощью двухфакторной аутентификации, которая включает в себя требование от пользователя ввести дополнительную информацию или использовать биометрические методы, такие как распознавание лиц или сканирование отпечатков пальцев, прежде чем ему будет предоставлен доступ. Протоколы авторизации также важны для обеспечения безопасной связи между серверами и веб-приложениями, а также для предотвращения вредоносных действий. Посетите Jatapp.co для получения дополнительной информации. В дополнение к этим мерам инновации в финтехе могут помочь разработчикам внедрить более надежные системы контроля доступа, которые ограничивают доступ определенных пользователей к определенным областям приложения и быстро и точно обнаруживают потенциальные киберугрозы.

При правильной реализации протокола разработчики могут предоставить пользователям безопасную среду для безопасного и уверенного взаимодействия со своими финансами.

4. Используйте шифрование для защиты пользовательских данных

Шифрование — важная мера безопасности для любого финтех-приложения, обеспечивающая безопасность пользовательских данных и финансовых счетов. Шифрование помогает защититься от потенциальных кибератак путем кодирования данных, что затрудняет получение злоумышленниками доступа без правильного ключа. Чтобы эффективно использовать шифрование, разработчики должны использовать надежные алгоритмы, такие как AES или RSA, с большими размерами ключей, чтобы обеспечить высочайший уровень безопасности. Кроме того, следует внедрить криптографию с открытым ключом, чтобы обеспечить дополнительный уровень защиты пользовательской информации и финансовых счетов. Кроме того, разработчики должны убедиться, что все пароли и номера учетных записей, используемые в системе, полностью зашифрованы перед сохранением в базе данных. Используя методы шифрования, разработчики могут предоставить пользователям безопасную среду для уверенного проведения финансовых транзакций.

5. Регулярно обновляйте программные компоненты, чтобы уменьшить уязвимости

Чтобы держать злоумышленников в страхе, разработчикам важно регулярно обновлять свои приложения FinTech с помощью новейших программных компонентов. Это поможет снизить любые риски безопасности и предотвратить обнаружение уязвимостей в кодовой базе. Обновления должны состоять из исправлений ошибок, новых функций, улучшений производительности, а также патчей для известных слабых мест — все это делается регулярно, чтобы укрепить вашу защиту! Кроме того, важно, чтобы все команды разработчиков были осведомлены о последних протоколах и мерах безопасности, чтобы иметь возможность правильно реализовать их в приложении. Кроме того, разработчики должны регулярно контролировать и проверять свои системы, чтобы быстро и эффективно обнаруживать любые подозрительные действия или потенциальные киберугрозы. Регулярно обновляя программные компоненты, организации могут обеспечить безопасность своих финтех-приложений и защиту от потенциальных кибератак.

Заключительные слова

Принимая необходимые меры для защиты финтех-приложений, разработчики могут предоставить пользователям безопасную и надежную среду. Протоколы аутентификации, такие как двухфакторная аутентификация, помогают подтвердить личность пользователя, а методы шифрования защищают конфиденциальные данные от потенциальных киберугроз. Кроме того, регулярные обновления необходимы для уменьшения уязвимостей в кодовой базе и быстрого обнаружения любых подозрительных действий. Следуя этим шагам, разработчики могут обеспечить безопасность своих финтех-приложений и обеспечить пользователям спокойствие, когда дело доходит до проведения финансовых транзакций в Интернете. Приняв правильные меры безопасности, организации могут

использовать инновации в финтех-технологиях и создавать продукты, вызывающие доверие у клиентов». ***(SOC CSIRT. CyberSecurity in FinTech: How to Develop a Secure FinTech App // Soc Investigation (https://www.socinvestigation.com/cybersecurity-in-fintech-how-to-develop-a-secure-fintech-app/). 24.05.2023).***

***

«Стратегия кибербезопасности более чем когда-либо является основной частью бизнес-стратегии. Например, киберриск компании может напрямую повлиять на ее кредитный рейтинг.

Кредитно-рейтинговые агентства постоянно стремятся лучше понять риски, с которыми сталкиваются компании. Сегодня эти агентства все чаще включают кибербезопасность в свои оценки кредитоспособности. Это позволяет агентствам оценить способность компании погасить заемные средства с учетом риска кибератак.

Взлом влияет на кредитный скоринг

Согласно Wall Street Journal (WSJ), рейтинговые агентства уделяют больше внимания тому, как компании справляются с кибератаками. Кибербезопасность теперь стала частью оценки кредитоспособности. Аналитики S&P Global Ratings сообщили, что компании и государственные учреждения, пострадавшие от кибератак, были понижены в рейтинге из-за сбоев в работе ИТ, а также из-за финансовых последствий атак.

Moody's Investors Service и Fitch Ratings также подчеркнули опасность киберрисков. В случае кибератаки некоторые финансовые последствия могут быть очевидны сразу. Для реализации других могут потребоваться месяцы, и они могут повлиять на способность организации погашать свои долги.

Влияние кредитного рейтинга в реальном мире

После кибератаки на SolarWinds в 2020 году S&P понизило рейтинг компании с B+ до B. По данным WSJ, заместитель директора S&P по корпоративным рейтингам Минеш Шилотри похвалил SolarWinds за четкую коммуникацию и быстрое предоставление клиентам исправлений безопасности после атаки. Тем не менее, софтверная компания по-прежнему страдала от потери клиентов и увеличения расходов на безопасность.

Даже когда компании быстро реагируют на кибератаки, прозрачность и коммуникация имеют жизненно важное значение. Агентства кредитного рейтинга ожидают исчерпывающую информацию о любом кибер-инциденте. Любая задержка или двусмысленность в сообщении может повлиять на кредитоспособность в будущем.

Тем временем Хлоя Пикетт, заместитель директора S&P по рейтингам государственных финансов США, сообщила, что Принстонская общественная больница в Западной Вирджинии подверглась атаке программы-вымогателя в 2017 году. В результате этого инцидента центр на месяц перенаправил машины скорой помощи и потерял значительную сумму дохода.

Атака на Принстонскую общественную больницу стала фактором, способствовавшим решению S&P понизить рейтинг больницы с BBB+ до BBB в

2019 году. Наряду с пандемией Covid-19 и приобретением небольшой соседней больницы кибератака также была названа причиной для S&P негативный прогноз на 2021 год. Сбои, вызванные атакой, привели к тому, что больница оказалась в более слабом положении, чтобы справиться с другими изменениями в своей деятельности.

Руководство Всемирного банка по кибербезопасности

Всемирный банк также отметил влияние кибербезопасности и кредитной отчетности. В Руководстве Всемирного банка по кибербезопасности в кредитной отчетности говорится:

«Широкомасштабные киберинциденты могут побудить кредиторов сократить выдачу кредитов в ответ на опасения по поводу широкомасштабного мошенничества, которое может быть связано с такими инцидентами с данными. Полученное в результате нормирование кредита может затем повлиять как на совокупный спрос со стороны отдельных лиц, так и на прибыльность фирм».

Согласно отчету Всемирного банка, киберэкосистема кредитной отчетности в целом претерпевает заметные изменения. Это обусловлено изменениями в ландшафте кредитной отчетности. Появление новых поставщиков данных, появление новых технологий и расширение разнообразных наборов данных — все это влияет на то, как кредит оценивается во всем мире.

По данным Всемирного банка, меры безопасности обеспечивают конфиденциальность, целостность и доступность обрабатываемой, хранимой и передаваемой информации. И эти элементы управления должны соответствовать набору предопределенных требований безопасности.

Всемирный банк заявляет, что основные направления кибербезопасности должны включать:

Конфиденциальность данных
Осведомленность и образование
Обмен информацией и общение
Устойчивость
Управление идентификацией и доступом
Управление активами
Управление изменениями и конфигурациями
Безопасность программного обеспечения
Стороннее управление
Физическая охрана
Сетевая безопасность
Безопасность конечной точки
Защита данных
Управление угрозами и уязвимостями
Регистрация и мониторинг событий.

Шаги по разработке стратегии кибербезопасности и конфиденциальности данных

Хотя задача может показаться сложной, успех зависит от организованных усилий по продвижению вперед. Некоторые шаги (адаптированные для этой статьи), описанные в отчете Всемирного банка, включают:

Расставьте приоритеты для критически важных активов: создайте перечень ИТ-активов (данные, физические устройства, информационные системы и программное обеспечение), которые поддерживают критические бизнес-процессы. Определите потенциальное влияние (финансовое, операционное и репутационное) на организацию, если эти активы будут скомпрометированы. Присвойте рейтинг критичности каждому активу.

Понимание угроз (информация об угрозах): определите субъектов угроз (государственные организации, организованная преступность, хактивисты, злоумышленники и т. д.), имеющих отношение к организации. Ранжируйте их по возможностям и мотивации для компрометации критически важных активов.

Оценка текущего состояния. Проведите откровенную оценку текущих кибервозможностей и производительности с использованием признанной в отрасли киберсреды (например, NIST Cybersecurity Framework).

Определите будущее состояние: установите видение и долгосрочные цели для функции кибербезопасности с учетом стратегических целей организации. Эти цели должны определять курс кибербезопасности организации в будущем.

Создайте план реализации: проведите анализ разрыва между текущими кибервозможностями и желаемым будущим состоянием. Определите инициативы, которые помогут преодолеть разрыв. Оцените стоимость и уровень усилий для каждой инициативы, а также определите преимущества безопасности, которые каждая из них обеспечит. Создайте список инициатив на многолетней временной шкале, назначая высокий приоритет тем из них, которые обеспечивают благоприятное соотношение затрат/выгод/затраченных усилий.

Внедрение и отслеживание прогресса: назначьте необходимые ресурсы для реализации плана обеспечения безопасности. Отслеживайте ключевые показатели эффективности и регулярно сообщайте о прогрессе высшему руководству.

Стратегия кибербезопасности — это бизнес-стратегия

Влияние киберриска больше, чем когда-либо, продолжает влиять на процесс принятия основных бизнес-решений. Учитывая риски, регулирующие органы и кредитные агентства, вероятно, станут более активными в своих оценках. Недостаточно сообщать только о нарушениях. Всемирный банк упомянул «заранее определенные требования безопасности». Это может означать, что организации будут все чаще требовать соблюдения требований, когда дело доходит до оценки безопасности.

Такие законодательные акты, как DFARS (Дополнение к федеральному положению о закупках в сфере обороны), FISMA (Федеральный закон об управлении информационной безопасностью), HIPAA (Закон о переносимости и подотчетности медицинского страхования) и стандарты ISO, уже установили требования к обеспечению кибербезопасности. Аналогичные меры могут потребоваться в будущем для получения благоприятных кредитных рейтингов». ***(Jonathan Reed. Heads Up CEO! Cyber Risk Influences Company Credit Ratings // IBM (https://securityintelligence.com/articles/cyber-risk-influences-company-credit-ratings/). 25.05.2023).***

***

«…Киберустойчивость — это способность организации прогнозировать, оставаться наготове, выживать, восстанавливаться и адаптироваться к неблагоприятным условиям, таким как кибератаки или компрометация систем или устройств, которые используют ресурсы или активируются киберресурсами. Растет спрос на киберустойчивые бизнес-сети. Лидеры кибербезопасности поняли, что традиционные меры безопасности устарели по сравнению с текущим ландшафтом угроз. Традиционная защита от кибербезопасности больше не может защитить системы, данные и бизнес-сеть от компрометации.

Предприятия всех размеров, типов и отраслей нуждаются в гибкой стратегии кибербезопасности для обеспечения непрерывности бизнеса. Кроме того, использование гибкого подхода к кибербезопасности может дать множество преимуществ до, после и во время инцидента кибербезопасности. Ниже приведены некоторые преимущества внедрения устойчивой системы кибербезопасности.

Укрепление системы безопасности

Организации, обеспечивающие киберустойчивость, помогут им эффективно реагировать и пережить изощренную кибератаку. Кроме того, такой подход к кибербезопасности позволяет предприятиям повысить эффективность управления ИТ, усилить безопасность критически важных активов, оптимизировать усилия по защите данных и сократить количество ошибок, связанных с человеческим фактором.

Минимизируйте финансовые потери

Средняя стоимость утечки данных увеличивается из-за меняющихся законов о конфиденциальности во всем мире. Кроме того, другие финансовые затраты, связанные с ущербом для имиджа бренда и другими сбоями в бизнесе из-за нарушения кибербезопасности, невозможно даже рассчитать. Разработка и внедрение устойчивых к киберугрозам стратегий безопасности позволит организациям снизить затраты на восстановление и быстро устранить последствия атаки.

Укрепление позиции соответствия

В зависимости от отрасли, в которой работает бизнес, он должен соответствовать нескольким отраслевым стандартам, постановлениям регулирующего органа или правительства, а также другим законам о конфиденциальности данных, чтобы гарантировать право клиентов на конфиденциальность. Использование устойчивого к киберугрозам механизма безопасности позволит организациям любого размера, типа и отрасли укрепить свою позицию по соответствию требованиям.

Повышение производительности ИТ-команды

Внедрение устойчивой системы кибербезопасности — это эффективный способ оптимизации рабочих процессов для улучшения и оптимизации ежедневных ИТ-операций.

Повышение доверия клиентов к бренду

Еще одним преимуществом реализации стратегии кибербезопасности является то, что она помогает повысить доверие клиентов. Киберустойчивая система

безопасности эффективно реагирует на изощренные кибератаки и выдерживает их, сводя к минимуму влияние на отношения с клиентами организаций.

Получите конкурентное преимущество в отрасли

Организации, которые придерживаются киберустойчивой системы кибербезопасности, получат конкурентное преимущество перед своими конкурентами, которые не реализуют такие стратегии.

Проблемы, связанные с разработкой киберустойчивой системы безопасности

Достижение киберустойчивости может быть затруднено для предприятий, поскольку им не хватает информации о своей сети и критически важных активах в режиме реального времени. Большинству организаций не хватает информации об их критической инфраструктуре из-за эволюции ландшафта угроз.

Команды службы безопасности могут даже не иметь четкого представления о том, какие активы следует защищать, и о возможных способах, которыми киберпреступники могут использовать бизнес-сеть для достижения своих злонамеренных намерений. Более того, многие команды могут даже не понимать, достаточен ли их уровень безопасности, чтобы оставаться в безопасности в условиях текущей ситуации в области кибербезопасности или пробелов в их стратегии кибербезопасности. Группы безопасности не могут реагировать на угрозы в режиме реального времени, потому что они полагаются на ручные способы выявления и снижения рисков.

Команды службы безопасности должны оценить свои текущие возможности, а также угрозы или риски, которым они подвержены. Организация должна определить стратегию киберустойчивости, соответствующую ее потребностям. Команды по кибербезопасности должны реализовать стратегию киберустойчивости, основанную на оценке стратегий и методов, которые хакеры обычно используют при эксплуатации своих жертв.

Основные шаги по повышению киберустойчивости

Киберустойчивость не является традиционным подходом к кибербезопасности. Ниже приведены несколько шагов, которые руководители кибербезопасности могут рассмотреть для повышения киберустойчивости своих организаций.

Получите видимость всей бизнес-сети в режиме реального времени

Одним из начальных шагов на пути к киберустойчивой организации является получение информации обо всей ИТ-инфраструктуре в режиме реального времени. Команды службы безопасности могут лучше отслеживать свою бизнес-сеть, определяя все ИТ-активы и критически важные уязвимые активы, подверженные риску. Команды безопасности должны лучше понимать контекст актива с бизнес-операциями и другими связанными уязвимостями и рисками. Разработка и внедрение информационных панелей для количественной оценки киберрисков обеспечит лучшее представление о рисках предприятия с финансовой точки зрения. Такой подход позволит лицам, принимающим решения, расставить приоритеты в стратегиях снижения рисков с учетом их влияния на финансы и сбои в бизнесе.

Кроме того, эффективная информационная панель обеспечит лучшее представление об эффективности и действенности реализованных средств контроля безопасности.

Привлекайте членов правления к обсуждению киберустойчивости

Принятие киберустойчивой системы безопасности потребует значительных инвестиций, ресурсов и усилий. Информирование членов правления о потенциальных рисках взлома и их влиянии поможет привлечь их к разработке строгого плана кибербезопасности. Команды SecOps должны выделить достаточный бюджет и разумно использовать его для повышения устойчивости своей ИТ-инфраструктуры к сложным киберугрозам или рискам.

Привлекайте и удерживайте лучших специалистов по кибербезопасности

Большинству групп SecOps приходится сталкиваться с организационными проблемами, такими как нехватка квалифицированных кадров в области кибербезопасности для поддержки оперативной и технической деятельности. В отрасли кибербезопасности существует огромный пробел в навыках, и многие компании изо всех сил пытаются найти и удержать нужный ресурс. Один из лучших способов преодолеть нехватку кадров в области кибербезопасности — повысить квалификацию существующих ресурсов в соответствии с потребностями организации.

Кроме того, крайне важно внедрить правильные инструменты в стек технологий кибербезопасности, такие как искусственный интеллект (ИИ), автоматизация и машинное обучение (МО), чтобы снизить нагрузку на ресурсы и улучшить удержание сотрудников.

Достижение киберустойчивости может быть затруднено для многих организаций из-за меняющегося ландшафта угроз и растущей изощренности киберпреступников. Лидеры службы безопасности могут рассмотреть упомянутые выше стратегии для повышения устойчивости своей системы кибербезопасности». ***(Nikhil Sonawane. Strategies to Develop a Cyber-Resilient Security Posture // ITSecurityWire (https://itsecuritywire.com/featured/strategies-to-develop-a-cyber-resilient-security-posture/). 22.05.2023).***

***

«Сегодня конвергенция операционных технологий (ОТ) и ИТ-сетей ускоряется, поскольку организации могут использовать данные, собранные физическим оборудованием и устройствами промышленного Интернета вещей (IIoT), для выявления проблем и повышения эффективности. С менее разрозненными отделами ИТ и ОТ конвергенция снижает требования к пространству и физическому оборудованию. Другие преимущества включают более короткое время развертывания, экономию средств и более высокую производительность.

Однако конвергенция IT/OT также означает, что кибербезопасность становится еще более важной. Постоянно развивающиеся и разрушительные киберугрозы могут быть нацелены на ранее закрытые среды ОТ и не позволяют многим организациям в полной мере воспользоваться преимуществами интеграции сетей OT/IT.

Чтобы получить всестороннее представление о текущем состоянии ОТ и кибербезопасности, Fortinet завершила и опубликовала пятое издание нашего отчета о состоянии операционных технологий и кибербезопасности за 2023 год. Это ежегодное исследование предоставляет данные и результаты, основанные на

всемирном опросе 570 специалистов по операционным технологиям (OT), проведенном сторонней исследовательской компанией InMoment.

Улучшения и проблемы кибербезопасности

Новый отчет показывает обнадеживающую тенденцию. Многие организации OT добились значительных успехов в повышении своей кибербезопасности. Однако отчет также указывает на необходимость дальнейшего совершенствования. Глобальный обзор включает в себя несколько ключевых выводов.

OT по-прежнему часто становится мишенью киберпреступников. Хотя количество организаций, которые не подверглись вторжению в систему кибербезопасности, резко увеличилось по сравнению с прошлым годом (с 6% в 2022 году до 25% в 2023 году), все еще есть значительные возможности для улучшения. На самом деле, три четверти организаций OT сообщили как минимум об одном вторжении за последний год. Вторжения вредоносных программ (56%) и фишинг (49%) снова стали наиболее частыми инцидентами, о которых сообщалось, и почти треть респондентов сообщили, что они стали жертвами атак программ-вымогателей в прошлом году (32%, без изменений с 2022 года).

Специалисты по кибербезопасности переоценили свою зрелость безопасности OT. В 2023 году количество респондентов, считающих уровень безопасности OT в своей организации «очень зрелым», сократилось до 13 % с 21 % годом ранее. Это падение указывает на растущую осведомленность специалистов по OT и использование более эффективных инструментов для самооценки возможностей кибербезопасности их организаций. Респонденты также указали, что в случае кибератаки почти треть (32%) респондентов указали, что пострадали как ИТ-, так и OT-системы, по сравнению с 21% в прошлом году.

Взрывной рост подключенных устройств подчеркивает сложность проблем, стоящих перед организациями OT. Почти 80 % респондентов сообщили, что в их OT-среде имеется более 100 OT-устройств с поддержкой IP. Это число показывает, насколько серьезной задачей для специалистов по безопасности является обеспечение защиты от постоянно расширяющегося ландшафта угроз. Результаты опроса показали, что решения в области кибербезопасности продолжают способствовать успеху большинства (76%) профессионалов OT, в частности, за счет повышения эффективности (67%) и гибкости (68%). Однако данные отчетов также указывают на то, что разрастание решений затрудняет последовательное внедрение, применение и применение политик во все более конвергентной среде ИТ/OT. Устаревшие системы усугубляют проблему: большинство (74%) организаций сообщают, что средний возраст систем ICS в их организации составляет от 6 до 10 лет.

Согласование безопасности OT с CISO. Хотя почти каждая организация сталкивается с трудностями при поиске квалифицированных специалистов по безопасности из-за растущей нехватки навыков в области кибербезопасности, результаты отчета показывают, что организации OT продолжают уделять кибербезопасности приоритетное внимание. Ключевым показателем является то, что почти каждая (95%) организация планирует в ближайшие 12 месяцев возложить ответственность за кибербезопасность OT на главного сотрудника по информационной безопасности (CISO), а не на руководителя или группу по

эксплуатации. Выводы также показывают, что специалисты по кибербезопасности ОТ теперь занимают руководящие должности в сфере ИТ-безопасности, а не в управлении продуктами. Влияние на решения в области кибербезопасности переходит от операций к другим лидерам, особенно к ролям директоров по информационной безопасности и безопасности.

Глобальные тенденции и идеи

Тщательный анализ данных отчета за 2023 год позволяет выявить некоторые заметные глобальные тенденции.

Несмотря на то, что общее количество вторжений могло снизиться из-за меньшего количества внутренних нарушений, программы-вымогатели и фишинг по-прежнему остаются серьезными угрозами. И киберпреступники, похоже, применяют более целенаправленный подход.

Почти все организации возложили ответственность за кибербезопасность ОТ на директора по информационной безопасности, а не на руководителя или команду по эксплуатации.

Точечные продукты кибербезопасности и разрастание решений могут усложнить применение политик и их согласованное применение в конвергентной среде ИТ/ОТ.

Специалисты по ОТ теперь, похоже, имеют более реалистичную самооценку средств защиты от кибербезопасности ОТ в своей организации.

После пяти лет опроса специалистов по ОТ отчет этого года содержит положительные новости о том, что кибербезопасность ОТ теперь привлекает внимание руководителей предприятий и руководителей высшего звена. Но директорам по информационной безопасности и их организациям еще многое предстоит сделать в области кибербезопасности.

Защитите сети, применяя лучшие практики

Организации могут продолжать улучшать защиту своих сетей ИТ и ОТ, применяя передовые методы, изложенные в отчете Fortinet о состоянии ОТ и кибербезопасности за 2023 год.

Разработайте стратегию поставщика и платформы кибербезопасности ОТ. Консолидация снижает сложность и ускоряет получение результатов. Первым шагом является постепенное создание платформы путем партнерства с поставщиками, которые разрабатывают свои продукты с учетом интеграции и автоматизации, чтобы организации могли последовательно внедрять и применять политики во все более конвергентной среде ИТ/ОТ. Ищите поставщиков с широким портфелем решений, которые могут предоставить базовые решения для инвентаризации и сегментации активов, а также более продвинутые решения, такие как центр управления безопасностью ОТ (SOC) или возможность поддержки совместного ИТ/ОТ SOC.

Разверните технологию управления доступом к сети (NAC). Решение задач, связанных с защитой промышленных систем управления (ICS), диспетчерским управлением и сбором данных (SCADA), Интернетом вещей (IoT), использованием собственных устройств (BYOD) и другими конечными точками, требует расширенного контроля доступа к сети, который должен быть частью комплексная архитектура безопасности. Эффективное решение NAC также помогает поддерживать полный контроль над сетью организации, управляя новыми

устройствами, которые хотят подключаться или обмениваться данными с другими частями инфраструктуры организации.

Используйте подход к доступу с нулевым доверием. Реализуйте базовые этапы инвентаризации и сегментации активов и обеспечьте постоянную проверку всех пользователей, приложений и устройств, пытающихся получить доступ к критически важным активам.

Включите обучение и обучение по вопросам кибербезопасности. Обучение кибербезопасности остается критически важным, потому что битва за кибербезопасность потребует, чтобы все сотрудники обладали знаниями и осведомленностью, чтобы работать вместе, чтобы защитить себя и данные своей организации. Организациям следует рассмотреть возможность включения нетехнического обучения, предназначенного для всех, кто использует компьютер или мобильное устройство, — от удаленных работников до членов их семей». ***(The state of operational technology and cybersecurity // IDG Communications, Inc. (https://www.csoonline.com/article/3697753/the-state-of-operational-technology-and-cybersecurity.html). 26.05.2023).***

***

Сполучені Штати Америки і Канада

«Cox Business в среду опубликовала новые результаты опроса 500 владельцев малого бизнеса в США. В отчете под названием «Фактор ИТ: импульс малого бизнеса Cox для управляемых ИТ-услуг» показано, что, хотя угрозы кибербезопасности растут, управляемые ИТ-услуги вселяют во владельцев малого бизнеса уверенность в том, что они могут справиться с этими рисками.

Кибербезопасность является главным мотиватором для компаний, инвестирующих в управляемые ИТ. 42% владельцев бизнеса предпочитают аутсорсинг. 42% респондентов также опасаются вирусов для устройств, 38% беспокоятся о резервном копировании и аварийном восстановлении, а 35% опасаются фишинговых атак.

42% инвестируют в управляемые ИТ-услуги для своего бизнеса. Из этой группы 71% в этом году инвестируют больше, чем в 2022 году.

По мнению владельцев бизнеса, облачные услуги являются наиболее выгодным предложением управляемых ИТ, помимо кибербезопасности. Из тех, кто сегодня использует облачные сервисы (рабочий стол как услуга, миграция, мониторинг или инфраструктура как услуга), 84 % чувствуют себя более уверенно в сети своей компании, а 86 % — в хранении данных.

Опрос показал, что 74% тех, кто пользуется управляемыми ИТ-услугами, чувствуют себя «уверенными» или «чрезвычайно уверенными» в способности своей компании обеспечить кибербезопасность благодаря такой поддержке…» ***(Ariana Lynn. Three Quarters of US SMEs with Managed IT Services are Confident in Their Cyber Security, Says Cox Business // THE FAST MODE (https://www.thefastmode.com/market-trends/31876-three-quarters-of-us-smes-with-***

managed-it-services-are-confident-in-their-cyber-security-says-cox-business). 05.05.2023).

***

«Ранее в марте Белый дом опубликовал свою Национальную стратегию кибербезопасности до 2023 года, в которой рассматривается новый взгляд на угрозы кибербезопасности и защитные меры. Наличие первой национальной стратегии за пять лет позволяет исполнительной власти сигнализировать своим собственным агентствам, а также государственному и деловому секторам, на что ее внимание и ресурсы будут потрачены, а также сигнализирует о ее ожиданиях в отношении более строгого соблюдения и инвестиций частного сектора. Таким образом, анализ приоритетов стратегии должен позволить предприятиям рассмотреть влияние федерального правительства, использующего их существующие полномочия для усиления правоприменения, наряду с их ожиданием больших долгосрочных инвестиций со стороны частных компаний для обеспечения защиты их собственных сетей. их собственная технология неуязвима, и что они будут сотрудничать, когда возникнет проблема. Во время этого администрирования компании, которые не обновляют свою киберпозицию, подвергаются большему риску правоприменения, и в дополнение к критически важным компонентам инфраструктуры приоритет, вероятно, будет отдан тем компаниям, которые предоставляют технические решения или платформы как услугу.

Стратегия на период до 2023 года сосредоточена на пяти основных принципах и направлена на требование более тесного сотрудничества со стороны частного сектора, особенно между крупными предприятиями или теми, кто занимается данными о потребителях, а также сбором или хранением конфиденциальной личной информации. В Стратегии 2023 сделан акцент на усилении правоприменения с помощью существующих органов, включая выполнение требований об уведомлении, будь то в соответствии с FTC, HIPAA или другими регулирующими органами по обеспечению соблюдения данных и соответствующими нормативными актами. Общая цель двояка: сбалансировать ответственность оборонительного киберпространства, где должны действовать те, кто имеет наилучшие возможности для принятия мер, поскольку киберустойчивость всей страны не должна зависеть от самых маленьких и наиболее уязвимых организаций или отдельных граждан; и перестроить стимулы в пользу долгосрочных инвестиций в кибербезопасность, вознаграждая рыночные силы и государственные программы за создание более надежной, безопасной и разнообразной киберпрактики. Стратегия на период до 2023 года предусматривает, что федеральное правительство привержено «инвестициям поколений в инфраструктуру нашей страны, оцифровке и обезуглероживанию энергетических систем, обеспечению безопасности наших цепочек поставок полупроводников, модернизации наших криптографических технологий и обновлению наших приоритетов внешней и внутренней политики» и сделать это., предлагает следующие пять столпов:

1. Столп первый: защита критической инфраструктуры

Первый компонент Стратегии 2023 предлагает уделять больше внимания государственно-частному сотрудничеству между владельцами и операторами

критической инфраструктуры. Ожидается, что соответствующие предприятия будут следовать обновленным планам и процессам реагирования на инциденты федерального агентства, чтобы улучшить усилия по выявлению причин инцидентов безопасности и обеспечить более эффективные процессы реагирования для всех вовлеченных сторон.

2. Второй столп: подрыв и ликвидация угроз

Второй компонент Стратегии на период до 2023 года предлагает использовать дипломатические, информационные, военные, финансовые, разведывательные и правоохранительные возможности для закрепления успехов в борьбе с угрозами в киберпространстве и их ликвидации. Для реализации этого предложения Стратегия 2023 предлагает предприятиям работать вместе с федеральным правительством, чтобы прервать деятельность, чтобы сделать кибердеятельность убыточной, и удержать иностранные правительства и негосударственные субъекты от участия в такой деятельности.

3. Третий компонент: формирование рыночных сил для обеспечения безопасности и устойчивости

Третий компонент Стратегии 2023 предлагает сосредоточить ответственность на тех, кто лучше всего способен снизить риск. Для этого в Стратегии-2023 предусмотрено, что мы должны модернизировать нашу цифровую экономику и продвигать практики, повышающие цифровую безопасность. Ожидается, что бизнес будет следовать более жестким ограничениям, касающимся сбора личных данных, для обеспечения конфиденциальности данных.

4. Столп четвертый: инвестируйте в устойчивое будущее

Четвертый компонент Стратегии 2023 направлен на создание программного обеспечения, устройств и инноваций следующего поколения, которые реализуют надежные методы и функции безопасности. Цель состоит в том, чтобы превзойти в инновациях другие страны и оптимизировать критически важные и новые технологии.

5. Пятый столп: формирование международного партнерства для достижения общих целей

Пятый компонент Стратегии на период до 2023 года направлен на изменение способов функционирования киберпроцессов, чтобы ответственное поведение ожидалось и вознаграждалось, а безответственное поведение обходилось дорого. Стратегия 2023 направлена на взаимодействие с другими странами для создания широкой коалиции стран, работающих над достижением общей цели и обеспечением и поддержанием безопасного Интернета.

При реализации своей Стратегии до 2023 года федеральное правительство будет использовать подход, основанный на данных, для измерения реализации, результатов и эффективности. Ожидается, что исполнительная власть будет координировать свои действия с различными государственными агентствами и ведомствами, а также с частным и государственным сектором, чтобы устанавливать стандарты и внедрять новые процессы. Независимо от того, будет ли принято новое законодательство, предусматривающее дополнительные стимулы для повышения кибербезопасности, Стратегия 2023 г. сигнализирует о том, что правительство ожидает увеличения инвестиций частного сектора и сотрудничества в области

безопасности и намерено предпринять шаги, которые повысят способность федерального правительства выполнять свои основные функции. и защитить американскую общественность от кибератак». ***(Aloke S. Chakravarty, James P. Melendres, Gabrielle M. Morlock. 2023 National Cybersecurity Strategy: Businesses Are Asked To Bear More of the Burden // Snell & Wilmer L.L.P. (https://www.swlaw.com/publications/legal-alerts/2023-national-cybersecurity-strategy-businesses-asked-to-bear-more-of-the-burden). 03.05.2023).***

***

«Система голосования в США уже много лет является целью хакеров, спонсируемых иностранными государствами. Теперь двухпартийное предложение пытается ввести более строгие требования безопасности с помощью сертифицированных процедур тестирования на проникновение.

Законопроект, внесенный сенаторами Марком Р. Уорнером (D-VA) и Сьюзан Коллинз (R-ME), направлен на усиление кибербезопасности цифровой инфраструктуры выборов в США, предусматривая новые требования к тестированию машин для голосования, проходящих процесс сертификации на выборах. Комиссия содействия (EAC).

Законопроект, получивший прозвище SECURE IT или «Усиление кибербезопасности выборов для обеспечения уважения к выборам посредством независимого тестирования», требует, чтобы машины для голосования прошли надлежащую сертифицированную процедуру тестирования на проникновение.

По словам двух сенаторов, текущие правила Закона о помощи Америке в голосовании (HAVA) требуют, чтобы EAC проводил тестирование и сертификацию, отмену сертификации и повторную сертификацию аппаратного и программного обеспечения системы голосования через аккредитованные лаборатории. Тем не менее, HAVA по-прежнему явно не требует процедур пентеста для цифровых систем голосования.

По словам сенатора Коллинза, тщательная проверка безопасности аппаратных и программных конфигураций, используемых в процедурах голосования, необходима для того, чтобы убедить американских граждан и выборных должностных лиц в честности избирательного процесса. В конце концов, эксперты по безопасности и «белые хакеры» годами самостоятельно тестировали машины для голосования, обнаруживая опасные уязвимости и выявляя спонсируемых государством субъектов (из России, Ирана или других стран), активно работающих над подрывом выборов в США.

Предлагаемый законопроект внесет поправки в действующие правила HAVA, установив программу добровольного раскрытия информации об уязвимостях (Coordinated Vulnerability Disclosure Program), в рамках которой этичные, «проверенные» хакеры и исследователи получат доступ к коммерческим системам голосования, предоставляемым производителями. Уязвимости, обнаруженные в системах, будут раскрыты указанным производителям и EAC, при этом недостатки будут храниться в секрете в течение 180 дней, чтобы дать разработчикам достаточно времени для устранения проблем.

По словам сенатора Уорнера, если США собираются победить своих противников, «мы должны уметь думать так же, как они». Закон SECURE IT позволит исследователям взять на себя роль киберпреступников, обнаруживая уязвимости и недостатки, которые иначе невозможно было бы обнаружить. По словам Уорнера, иностранные и внутренние угрозы по-прежнему нацелены на американскую демократию, и новое актуальное законодательство, разработанное для использования «критической практики кибербезопасности» пентестинга в белых шляпах, поможет федеральному правительству защитить инфраструктуру выборов в США». ***(Alfonso Maruccia. A new bipartisan bill wants to improve cybersecurity of the US voting system // TechSpot, Inc. (https://www.techspot.com/news/98688-new-bipartisan-bill-wants-improve-cybersecurity-us-voting.html). 15.05.2023).***

***

«Ожидается, что ведущие американские компании, занимающиеся кибербезопасностью, сообщат о еще одном квартале уверенного роста, поскольку громкие взломы и изменение предпочтений клиентов в пользу более крупных игроков с более интегрированными предложениями помогают поддерживать их бизнес в условиях турбулентной экономики.

Palo Alto Networks, крупнейший игрок в отрасли по доле рынка и оценке, во вторник начнет отчетность по сектору, что, по оценкам аналитиков, опрошенных Refinitiv, увеличит квартальный доход почти на 24%.

Это сопоставимо с ростом почти на 26 процентов в предыдущем квартале и на 29 процентов годом ранее, что подчеркивает устойчивость спроса на услуги, которые считаются важными, несмотря на более широкое замедление расходов на технологии.

«Кибербезопасность стала важнее, чем когда-либо, в связи с быстрой цифровой трансформацией, происходящей во всех отраслях», — сказал Акшара Басси, аналитик Counterpoint Research.

Более частые случаи угроз безопасности также увеличили спрос. В последние месяцы Western Digital и Министерство транспорта США столкнулись с утечками информации, в результате которых была раскрыта информация о клиентах производителя микросхем памяти и 237 000 государственных служащих США.

Согласно данным аналитической компании International Data Corporation, мировые расходы на решения для кибербезопасности, как ожидается, вырастут на 12,1 процента и достигнут 219 миллиардов долларов в 2023 году.

Аналитики говорят, что корпоративные клиенты также объединяют своих поставщиков программного обеспечения для кибербезопасности, стремясь снизить сложность своих операций и защитить себя от атак.

Поставщики, предлагающие комплексные решения для кибербезопасности, помогают своим клиентам лучше анализировать данные о безопасности, а также интегрировать различные приложения, оптимизировать расходы и улучшать управление рисками.

По словам аналитика DA Davidson Руди Кессинджера, ведущие поставщики кибербезопасности Palo Alto Networks, CrowdStrike Holdings и Fortinet Inc, которые

предлагают ряд услуг, включая облачную защиту и защиту личных данных, получат выгоду от тенденции к консолидации.

Ожидается, что CrowdStrike и ZScaler Inc сообщат о росте выручки на 39% и 45%, когда они сообщат о доходах 31 мая и 1 июня соответственно.

Ранее в этом месяце Check Point Software Technologies и Fortinet Inc сообщили об оптимистичных результатах, поскольку спрос на брандмауэры и продукты для облачной безопасности оставался высоким». ***(Cybersecurity firms to gain from growing threat of hacks // AGBI, part of Link Media Corporation Ltd. (https://www.agbi.com/article/cybersecurity-firms-to-gain-from-growing-threat-of-hacks/). 23.05.2023).***

***

«Cisco опубликовала результаты своего индекса готовности к кибербезопасности. Результаты рисуют мрачную картину, поскольку в отчете говорится, что только 9% канадских организаций имеют «зрелый» уровень готовности к управлению рисками безопасности в гибридном мире. Проблема усугубляется нашей новой рабочей реальностью, в которой люди работают удаленно, используют несколько устройств, полагаются на облачные приложения и генерируют большие объемы данных.

Роб Бартон, технический директор Cisco Canada, пояснил: «Устойчивость к кибербезопасности стала одной из самых важных задач, стоящих перед предприятиями в Канаде и во всем мире».

«Чтобы помочь предприятиям понять, на каком уровне они находятся в своей готовности противостоять современным угрозам и смягчать их последствия, Cisco провела индекс готовности к кибербезопасности — двойной слепой опрос 6700 бизнес-лидеров, отвечающих за кибербезопасность, на 27 мировых рынках в 18 отраслях», — поделился Бартон. «Индекс измеряет готовность компаний по пяти основным направлениям, определяющим устойчивость бизнеса к кибербезопасности: идентификационные данные, устройства, сеть, рабочие нагрузки приложений и данные. Затем компании были разделены на четыре стадии возрастающей готовности: начинающие, формирующиеся, прогрессивные и зрелые».

«Выводы из Канады показали, что только 9% канадских организаций имеют «зрелый» уровень готовности к управлению рисками безопасности в гибридном мире — по сравнению со средним мировым показателем в 15%. При небольшом проценте компаний на стадии зрелости 57% канадских компаний попадают в стадию «начинающая» или «формирующаяся», что означает, что их готовность к современным угрозам кибербезопасности ниже среднего», — заявил Бартон.

«Поскольку 77% респондентов из Канады заявили, что ожидают, что инцидент с кибербезопасностью нарушит их бизнес в ближайшие год или два, этот опрос является тревожным сигналом для организаций, чтобы они действовали сейчас».

Бартон добавил: «Пандемия коренным образом изменила динамику безопасности. В настоящее время в организациях все чаще люди работают с нескольких устройств в разных местах, подключены к нескольким сетям, получают доступ к приложениям в облаке и в пути и генерируют огромные объемы данных».

Канадская готовность к кибербезопасности и основные показатели индекса

Бартон начал: «Киберугрозы и атаки растут во всем мире, и злоумышленники все чаще нацелены на Канаду — мы почти ежедневно видим это в новостях».

«Организациям необходимо действовать срочно, чтобы подумать о том, насколько они готовы к кибератакам, потому что мы должны исходить из предположения, что это вопрос «когда», а не «если», потому что цена самоуспокоенности значительна».

«На самом деле, 51% респондентов заявили, что за последние 12 месяцев у них был инцидент кибербезопасности, а 34% пострадавших заявили, что это стоило им не менее 500 000 долларов США. И это только тяжелая стоимость. Нам необходимо учитывать дальнейшее влияние на корпоративный бренд и репутацию».

Бартон резюмировал: «Наши данные показывают, что есть ключевые области, в которых необходимо добиться прогресса в отношении пяти столпов обороны:

Идентичность: здесь необходим прогресс, поскольку только 15% организаций оцениваются как «зрелые».

Устройства: здесь самый высокий процент компаний на стадии «Зрелые» — всего 33%.

Сетевая безопасность: компании отстают в этом отношении: 64% организаций находятся на стадиях «Начинающий» или «Формирующийся».

Рабочие нагрузки приложений: это столп, к которому компании наименее подготовлены: 73% организаций находятся на стадиях «Начинающий» или «Формирующийся».

Данные: это второе место по количеству компаний на стадии «зрелости» (всего 17%)».

Предупредил Бартон: «Результаты выявляют тревожный пробел в готовности к кибербезопасности, который будет только увеличиваться, если предприятия не будут действовать быстро».

Рекомендации по улучшению кибербезопасности бизнеса

Бартон предложил несколько предложений о том, как компании могут улучшить свою кибербезопасность.

«Кибератаки могут произойти в любое время, в любом месте и в отношении любого малого, среднего или крупного бизнеса», — признал Бартон. «Появление гибридной работы изменило ландшафт кибербезопасности и усложнило канадский бизнес».

«Создание надежной системы обеспечения безопасности требует времени. Тем не менее, есть шаги, которые предприятия могут начать предпринимать при создании инфраструктуры, от оценки текущего положения и развертывания решений до мониторинга и прогнозирования угроз. Канадские предприятия могут извлечь выгоду из пяти аспектов устойчивости системы безопасности:

Закройте пробелы в вашей системе, чтобы у вас была одна открытая платформа.

Смотрите больше и всегда следите.

Предугадывайте, что будет дальше, используя полезную информацию.

Расставьте приоритеты в самом важном.

Автоматизируйте свой ответ, чтобы вы могли быстро прийти в норму».

Также необходимы надежные технологии, быстрое реагирование, надежные цепочки поставок и устойчивость к внешним воздействиям.

«Во всех отраслях организациям необходима видимость для успешного внедрения этого подхода, потому что невозможно защитить то, чего вы не видите», — заметил Бартонг.

«Оборудуя сети правильной информацией, от приложений до конечных точек и всего, что между ними, мы можем видеть, что происходит, и защищать сети от угроз и атак», — сказал Бартон.

Далее Бартон пояснил: «Скорость и время отклика — это все, когда организация сталкивается с угрозой, а устойчивость системы безопасности позволяет компаниям лучше предвидеть угрозы и быстрее возобновлять работу, когда угроза становится реальной».

«Большинство организаций включают устойчивость в свои финансовые, операционные, организационные функции и функции цепочки поставок. Отказоустойчивость безопасности присутствует во всех них, позволяя компаниям проверять угрозы, понимать связи в организации и видеть полный контекст любой ситуации. Это позволяет командам расставлять приоритеты и гарантировать, что их следующее действие будет лучшим».

«Хорошая новость заключается в том, что лидеры в области безопасности осознают риски и готовы вкладывать средства в обеспечение готовности к кибербезопасности», — сказал Бартон. «Данные показывают, что 78% респондентов планируют увеличить свои бюджеты на безопасность как минимум на 10% в течение следующих 12 месяцев. Несмотря на положительную траекторию, крайне важно, чтобы это увеличение бюджета было осуществлено раньше, чем позже. Учитывая нынешние условия, 12-месячное ожидание — это слишком долго». ***(Yasmin Ranade. Cybersecurity Readiness Report Identifies Gaps for Canadian Businesses // WhatsYourTech.ca (https://whatsyourtech.ca/2023/05/23/cybersecurity-readiness-report-identifies-gaps-for-canadian-businesses/). 23.05.2023).***

***

«Поскольку кибератаки занимают центральное место в новостях, правительство США осознало необходимость принятия мер для обеспечения защиты данных своих граждан частными компаниями и государственными организациями. Добровольные меры, принятые компаниями в прошлом, оказались недостаточными или последовательными. Поэтому Комиссия США по ценным бумагам и биржам (SEC) и Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) вмешались и ввели новые правила кибербезопасности. Эти два федеральных агентства по-разному подходят к требованиям к организациям по защите частных и общедоступных данных. Давайте углубимся в Правило кибербезопасности SEC и Директиву CISA и посмотрим, как их можно интегрировать в стратегию безопасности данных организации.

Что такое правило кибербезопасности SEC?

Правило кибербезопасности SEC — это набор правил, которые регулируют безопасность и конфиденциальность информации о клиентах, хранящейся в финансовых учреждениях, регулируемых SEC. В соответствии с правилом, эти

организации должны иметь письменные политики и процедуры для защиты информации о клиентах, включая защиту от несанкционированного доступа или использования этой информации. Они также должны предоставить клиентам уведомления, объясняющие их политику конфиденциальности, и предоставить механизм отказа для клиентов, которые не хотят, чтобы их непубличная личная информация передавалась третьим лицам. Правило кибербезопасности SEC обновлялось с годами, чтобы отразить меняющуюся картину кибербезопасности и возникающие угрозы, а также упростить оценку практики кибербезопасности публичных компаний и отчетность об инцидентах.

Недавно предложенные SEC правила кибербезопасности уделяют больше внимания раскрытию информации до и после киберсобытия. Компании обязаны раскрывать информацию о том, есть ли в совете директоров специалисты по кибербезопасности; какие члены правления контролируют риски кибербезопасности и этот процесс; политики выявления и управления киберугрозами, а также то, как руководство будет реализовывать эти политики. Требования SEC к раскрытию информации о кибербезопасности также требуют от компаний раскрывать существенный инцидент кибербезопасности в течение четырех рабочих дней после его возникновения.

Что такое директива CISA?

Директива CISA использует более активный подход, предоставляя федеральным агентствам рекомендации и требования по улучшению их состояния кибербезопасности. В директиве изложен набор конкретных действий, которые федеральные агентства должны предпринять для усиления своей защиты от кибербезопасности, включая оценку уязвимостей, исправление критических уязвимостей и внедрение многофакторной аутентификации для привилегированных учетных записей.

Руководящие принципы CISA также устанавливают требования к планированию реагирования на инциденты, поиску угроз и возможностям центра управления безопасностью (SOC). Директива призвана помочь федеральным агентствам активно выявлять и устранять потенциальные киберугрозы до того, как они смогут нанести значительный ущерб федеральным системам и данным. Федеральные агентства обязаны соблюдать правила CISA и регулярно отчитываться перед CISA о своем прогрессе. Сроки для отчетов об инцидентах также сжаты, но, в отличие от нового правила SEC о кибербезопасности, отчеты CISA анонимизируют любые подробности о кибератаках до их публичного раскрытия.

Влияние правила кибербезопасности SEC и директивы CISA на экосистему соответствия требованиям безопасности

Обмен информацией имеет решающее значение в сфере кибербезопасности, и предлагаемые правила требуют более широкого раскрытия информации и прозрачности как для публичных компаний, так и для федеральных агентств в качестве средства защиты США от кибератак. Данные о последних злонамеренных тактиках могут помочь в разработке стратегии защиты, и эта информация также поможет правительственным учреждениям решить, как реагировать. Чем раньше будет раскрыта уязвимость, тем быстрее другие связанные компании и агентства смогут отреагировать, чтобы смягчить угрозу. Эти правила также расширяют

возможности инвесторов для оценки практики кибербезопасности публичных компаний и отчетности об инцидентах, что делает компании, которые следуют этим правилам, еще более привлекательными для рынка.

Хотя правительство должно сыграть значительную роль в достижении этих результатов, стратегия указывает, что частный сектор, как ожидается, активизируется для устранения своих собственных технологических уязвимостей. Однако из-за сжатых сроков и необходимых доказательств многим компаниям сложно выполнить требования законодательства без увеличения штата или передачи работы на аутсорсинг. Например, четырех дней может быть недостаточно, чтобы оценить угрозу и определить, какую информацию необходимо раскрыть. И даже если организация сможет уложиться в срок, публичное раскрытие уязвимостей до того, как эти бреши будут устранены, может увеличить риск. Организации оправданно нервничают по поводу принятия важных решений под давлением.

Государственные органы должны найти баланс. Тот, где можно быстро обмениваться информацией об инциденте, чтобы SEC и CISA могли защитить киберэкосистему, но при этом компании не опасались негативной реакции, слишком рано раскрывая слишком много информации.

Как подготовиться к изменениям правил кибербезопасности SEC и директивы CISA

Вместо того, чтобы ждать окончательной доработки правил, организации уже могут предпринять шаги для подготовки к этим изменениям, создав стратегию кибербезопасности, которая соответствует подходам Правил кибербезопасности SEC и Директивы CISA. Вот некоторые предложения:

Проведите оценку рисков

Организации должны провести всестороннюю оценку рисков, чтобы выявить потенциальные угрозы и уязвимости кибербезопасности, понять финансовые последствия этого риска и разработать стратегии по снижению этих рисков. Это может помочь организациям расставить приоритеты в своих усилиях по кибербезопасности, рассчитать рентабельность инвестиций в сравнении с затратами на устранение рисков и эффективно распределять ресурсы.

Разработайте программу кибербезопасности с постоянным мониторингом

Организации должны разработать и внедрить комплексную программу кибербезопасности, которая состоит из следующего:

регулярная оценка рисков

мониторинг безопасности

планирование реагирования на инциденты и

выявление областей улучшения.

Программа также должна включать четкий процесс раскрытия информации, политики по устранению инцидентов и процедуры для соблюдения четырехдневного срока раскрытия информации, установленного правилами SEC и CISA.

Управление и подотчетность

Поскольку новые законы определяют обязанности членов совета директоров, организациям следует

Обучение персонала

Организации должны обучать своих сотрудников передовым методам кибербезопасности, а также тому, как выявлять потенциальные киберугрозы и реагировать на них. Это включает в себя управление инцидентами и их обязанности, когда речь идет о раскрытии информации в соответствии с Правилом кибербезопасности SEC и Директивой CISA.

Взаимодействие со сторонними поставщиками

Организации должны тесно сотрудничать со своими сторонними поставщиками, чтобы обеспечить соблюдение Правил кибербезопасности SEC и Директивы CISA, а также других правил, изложенных в Меморандуме Белого дома и Руководстве NIST. К безопасности цепочки поставок следует относиться серьезно. Это может включать проверку договоров с поставщиками и требование к поставщикам предоставлять регулярные отчеты о своих методах и средствах обеспечения кибербезопасности.

В целом организациям следует применять упреждающий подход к кибербезопасности и расставлять приоритеты в своих усилиях по защите от потенциальных угроз. Разработав комплексную программу кибербезопасности и внедрив передовой опыт, организации могут свести к минимуму риски и обеспечить соответствие правилам кибербезопасности SEC и директиве CISA.

Руководство SEC по кибербезопасности: готовьтесь к худшему, планируйте лучшее

Руководство по кибернадзору и раскрытию информации доступно — или будет доступно — от SEC для публичных компаний и CISA для федеральных агентств. Хотя многие из новых правил все еще находятся на стадии предложений, все организации, несомненно, могут рассчитывать на то, что в ближайшем будущем они возьмут на себя большую ответственность за безопасность данных. Это может даже означать начало дополнительных требований к публичным компаниям, поскольку это связано с текущими правилами для SOC2 и ISO27001.

Организации должны начать готовиться к соблюдению более строгих требований кибербезопасности. Им следует учитывать свою политику раскрытия информации в рамках подготовки к наихудшим сценариям и в то же время активно укреплять свои стратегии и политику управления рисками. Самый простой способ добиться этого? Через данные и автоматизацию.

Используйте данные для соответствия правилу кибербезопасности SEC и директиве CISA

Организации могут использовать данные и автоматизацию для удовлетворения многочисленных требований безопасности, включая управление рисками и политиками. Использование упреждающего подхода к поиску пробелов в кибербезопасности демонстрирует приоритетность кибербезопасности как стратегической функции и в конечном итоге укрепляет доверие заинтересованных сторон. Важно отметить, что это также снижает потребность в управлении инцидентами и раскрытии информации в соответствии с правилом кибербезопасности SEC и директивой CISA…» ***(Utilizing SEC Cybersecurity Rule and CISA Directive | anecdotes // Techstrong Group Inc.***

(https://securityboulevard.com/2023/05/utilizing-sec-cybersecurity-rule-and-cisa-directive-anecdotes/). 28.05.2023).

***

Країни ЄС та Великобританія

«Европейская комиссия предлагает потратить более 1 миллиарда евро на операционные центры кибербезопасности на фоне давних опасений, что киберугрозы в отношении членов континентального альянса останутся незамеченными, опасения, которые стали еще более насущными в связи с вторжением России в Украину.

В конце прошлого месяца комиссия представила предложение о создании европейского «Киберщита», опирающегося на сеть национальных SOC и трансграничных SOC, которые представляют собой консорциум как минимум из трех национальных центров.

Законопроект Закона о киберсолидарности, также создаст Механизм чрезвычайных ситуаций в области кибербезопасности, позволяющий правительствам использовать меры реагирования частного сектора на инциденты во время чрезвычайных ситуаций.

Еще до попытки России завоевать Украину в феврале 2022 года европейские официальные лица сетовали на плохой обмен информацией между национальными столицами об инцидентах в области кибербезопасности, отметив в стратегии кибербезопасности на 2020 год, что «не существует оперативного механизма» для координации между странами-членами и институтами Европейского Союза в случае « крупномасштабные трансграничные киберинциденты или кризис».

С тех пор это упущение стало еще более очевидным для чиновников Европейской комиссии, отслеживающих сообщения о подозрительных инцидентах с безопасностью критически важной инфраструктуры, произошедших после российского вторжения.

В ноябре комиссия инициировала первый этап создания трансграничных операционных центров безопасности, выявив заинтересованность в развертывании и управлении платформой для трансграничных SOC.

«Сегодня между началом распространения вредоносного ПО и моментом его обнаружения проходит в среднем 190 дней», — заявил комиссар ЕС по внутреннему рынку Тьерри Бретон. сказал в середине апреля. «Мы хотим резко сократить это время, до нескольких часов». ***(Akshaya Asokan. European Commission Proposes Network of Cross-Border SOCs // Information Security Media Group, Corp. (https://www.databreachtoday.com/european-commission-proposes-network-cross-border-socs-a-21998). 05.05.2023).***

***

«Во вторник в Бухаресте был официально открыт Европейский центр компетенции в области кибербезопасности (ECCC), первая европейская

организация, базирующаяся в Румынии, которая обеспечивает функционирование общеевропейского киберзащиты.

ЕССС стал «реальностью» почти два года назад, и правление уже какое-то время «достаточно активно, проводя встречи сначала онлайн из-за пандемии, а затем лично», – исполняющий обязанности исполнительного директора ЕССС Мигель Гонсалес-Санчо. сказал.

Нанимать персонал можно было только после того, как у нас был «домик». Он добавил, что в настоящее время в штате 14 сотрудников, но их число будет неуклонно расти, пока в следующем году их не станет 40.

Штаб-квартира ЕССС расположена в здании Политехнического университета Бухареста. Премьер-министр Николае Чукэ признал, что штаб-квартира центра еще не полностью готова, но румынские власти хотели символически открыть ее в День Европы.

По этой же причине пресса не имела доступа ко всему Центру, а только к площади, устроенной для выступлений официальных лиц.

Европейский центр компетенции в области кибербезопасности (ECCC) обеспечит функционирование общеевропейского киберзащиты, заявил Роберто Виола, генеральный директор Департамента сетей связи, контента и технологий Европейской комиссии (DG CNECT).

Представитель ЕС сказал, что Европа становится все более оцифрованной, и есть много преимуществ, но также и рисков.

«Риск состоит в том, что противники демократии будут атаковать европейскую демократию, основы Европы и образ жизни граждан. Вот почему главная цель Европы — оставаться сильными в этой области кибербезопасности», — сказал Виола.

Он добавил: «У Центра есть очень важная задача — укрепить компетенцию в области кибербезопасности по всей Европе, а также начать работать в полную силу».

В этих обстоятельствах предложение Комиссии состояло в том, чтобы создать сеть сотрудничества между центрами, обеспечивающую защитный щит, который бы обеспечивал «непрерывный мониторинг окружающей среды для выявления этих слабых мест, чтобы мы могли в любое время идентифицировать атаку и отразить ее, если это происходит, чтобы защитить наши активы и граждан», — сказал он, добавив, что Центр в Бухаресте будет нести ответственность за приобретение, эксплуатацию и объединение в сеть этих отдельных операционных центров».

Он пояснил, что в центре также будут задействованы группы быстрого технического вмешательства.

Группы быстрого технического реагирования смогут вмешиваться в любую точку Европы, обнаруживать и защищать во время кибератаки, анализировать ее, а затем на основе полученных данных «улучшать наши системы, понимать, что было сделано, где были допущены ошибки и как обстоят дела». можно улучшить в будущем».

Европейский центр компетенции в области кибербезопасности (ECCC) стремится повысить потенциал и конкурентоспособность Европы в области кибербезопасности, работая вместе с Сетью национальных координационных центров (NCC) для создания сильного сообщества кибербезопасности.

ECCC разработает и реализует совместно с государствами-членами, промышленностью и сообществом технологий кибербезопасности общую программу развития технологий и их широкого внедрения в областях, представляющих общественный интерес, и в сферах бизнеса, особенно МСП». ***(Catalina Mihai. Cybersecurity Competence Centre in Bucharest to provide Europe-wide Cyber Shield // EURACTIV MEDIA NETWORK BV. (https://www.euractiv.com/section/politics/news/cybersecurity-competence-centre-in-bucharest-to-provide-europe-wide-cyber-shield/). 10.05.2023).***

***

«Недавно вступил в силу новый Регламент ЕС о цифровой операционной устойчивости финансового сектора (DORA). DORA устанавливает требования кибербезопасности для систем информационно-коммуникационных технологий (ИКТ), поддерживающих бизнес-процессы финансовых организаций, и представляет собой изменение парадигмы для сектора ИКТ. Критически важные сторонние поставщики ИКТ-услуг, которые предоставляют услуги регулируемым финансовым организациям, также будут напрямую регулироваться в соответствии с DORA и подлежат регулирующему надзору со стороны регулирующего органа, который будет создан в соответствии с DORA (так называемый «Ведущий контролер»).

Важно отметить, что DORA также предусматривает повышенную ответственность для отдельных членов органов управления и предусматривает, что они могут быть оштрафованы в соответствии с DORA, а также быть индивидуально названы в публичных решениях регулятора в случае, если компетентный орган установит, что несоблюдение финансовой организацией относилась к физическому лицу.

Кроме того, Директива ЕС о цифровой операционной устойчивости для финансового сектора (Директива DORA вступила в силу), которая вносит поправки в некоторые существующие требования кибербезопасности в рамках существующего регулирования финансовых услуг, таких как Директива о платежных услугах 2 (PSD2), Директива MiFID II и Директива о платежеспособности II.

Ключевые выводы DORA заключаются в следующем:

Сфера применения : DORA — это отраслевой регламент ЕС, направленный на гармонизацию требований кибербезопасности для систем и услуг ИКТ, используемых рядом организаций в сфере финансовых услуг, таких как кредитные, платежные учреждения и учреждения электронных денег, центральные контрагенты (ЦКА), управляющие альтернативными инвестиционными фондами (AIFM), агентства кредитного рейтинга и поставщики услуг краудфандинга и крипто-активов (финансовые организации).

Из-за использования ИКТ и растущей зависимости от поставщиков услуг ИКТ DORA также применяется к сторонним поставщикам услуг ИКТ, которые предоставляют «цифровые услуги и услуги передачи данных» финансовым организациям с использованием систем ИКТ — эти услуги имеют широкое определение и могут включать облачные вычисления, вычисления, программное

обеспечение, анализ данных, центр обработки данных и дополнительные услуги. Компетентные органы в соответствии с DORA будут осуществлять прямой регулирующий надзор за сторонними поставщиками услуг ИКТ (в том числе за пределами ЕС), которые сами не участвуют в регулируемой деятельности, но считаются «критически важными» для регулируемых финансовых организаций.

Ключевые обязательства по DORA:

Для финансовых организаций:

Внедрение системы управления рисками в области ИКТ: это включает разработку и внедрение внутренних киберполитик (например, в отношении аварийного восстановления, непрерывности бизнеса, контроля доступа, реагирования на инциденты и т. д.) и процедур; внедрение мер безопасности ИТ для защиты данных и активов ИКТ; и обязательное кибер-обучение для персонала.

Внедрение усиленных мер по управлению инцидентами: сюда входят меры по адекватному обнаружению, регистрации и классификации инцидентов и надлежащему информированию о них.

Внедрение мер в отношении управления рисками третьих лиц в области ИКТ: DORA вводит ряд новых мер в отношении финансовых организаций для управления рисками, связанными с такими сторонними поставщиками услуг ИКТ. Это включает в себя: (i) принятие стратегии в отношении рисков третьих лиц в сфере ИКТ, в которой риски и взаимозависимости от определенных поставщиков услуг обозначены и оценены; (ii) наличия надлежащих договорных отношений и выполнения минимальных условий, как того требует DORA, со сторонними поставщиками услуг ИКТ, в частности, когда поставщик поддерживает критически важную или важную функцию организации; и (iii) проведение комплексной проверки в соответствии с требованиями DORA до привлечения поставщика услуг.

Для критически важных сторонних поставщиков услуг ИКТ:

Чтобы еще больше минимизировать риск, DORA вводит специальную структуру надзора за критически важными сторонними поставщиками ИКТ-услуг, которая включает в себя назначение специального органа («Главный контролер»), который будет нести ответственность за оценку ИТ-безопасности и физической безопасности поставщика критически важных ИКТ-услуг, политики, СОП, управления, переносимости данных и механизмов функциональной совместимости, а также использует ли он национальные и международные стандарты, применимые к его ИКТ-услугам. На основе этой оценки ведущий контролер разработает индивидуальный план надзора для каждого поставщика критически важных услуг ИКТ, который он будет использовать в качестве основы для нормативного надзора;

В рамках своих регулятивных правоприменительных полномочий Главный надзиратель должен иметь далеко идущие полномочия по расследованию и может налагать периодические штрафные платежи в размере до 1% от среднего дневного мирового оборота поставщика ИКТ в предыдущем финансовом году. Главный надзиратель также может решить опубликовать сведения о поставщике услуг ИКТ, его нарушении и любых лицах, которых он считает ответственными за нарушение.

Кроме того, DORA имеет экстерриториальный охват в том смысле, что поставщики услуг, обозначенные в качестве критически важных сторонних поставщиков ИКТ-услуг в соответствии с DORA и учрежденные за пределами ЕС,

но предоставляющие услуги финансовым организациям в ЕС, должны будут создать дочернюю компанию в ЕС. в течение 12 месяцев после их назначения, чтобы обеспечить эффективное правоприменение компетентными органами ЕС в соответствии с DORA. Кроме того, DORA вводит меры, позволяющие Ведущим наблюдателям также осуществлять свои надзорные полномочия за пределами территории ЕС с согласия стороннего поставщика ИКТ и соответствующих органов в третьей стране.

Санкции: DORA делегирует государствам-членам ЕС определение всех правил, касающихся административных штрафов и мер по исправлению положения, применимых к нарушениям, при условии, что они являются эффективными, пропорциональными и оказывающими сдерживающее воздействие; и они также могут принять решение о наложении уголовных наказаний за нарушение DORA. DORA не устанавливает каких-либо минимальных или максимальных сумм штрафов — это остается на усмотрение государств-членов.

Следующие шаги. DORA официально вступила в силу 17 января 2023 г. и будет полностью применяться с 17 января 2025 г. Из-за сложного характера требований DORA предприятиям следует рассмотреть вопрос о том, входят ли они в сферу действия DORA либо в качестве финансового учреждения, либо в качестве стороннему поставщику ИКТ-услуг, а также изучить требования, изложенные в DORA, в частности, в отношении управления рисками третьих лиц в области ИКТ; и разработать стратегии минимизации рисков в соответствии с DORA и другими европейскими и международными законами о кибербезопасности». ***(William RM Long, Lauren Cuyvers and João D Quartilho. New EU Cyber Law for the Financial Services Industry with Significant Impact on ICT Service Providers // Sidley Austin LLP (https://datamatters.sidley.com/2023/05/08/new-eu-cyber-law-for-the-financial-services-industry-with-significant-impact-on-ict-service-providers/#page=1). 08.05.2023).***

***

«…ENISA, регулирующий орган ЕС в области кибербезопасности, разрабатывает новые, более строгие требования, чтобы гарантировать, что никакое иностранное правительство не может вмешиваться в данные ЕС, согласно проекту предложения, с которым ознакомился Bloomberg.

На практике это означало бы, что поставщики облачных услуг США, такие как Amazon.com Inc., Microsoft Corp. and Alphabet Inc. должна была найти способ гарантировать, что американское правительство не сможет получить доступ к европейским облачным данным, чтобы пройти квалификацию. Облачные компании, не входящие в ЕС, должны будут либо управлять юридическим лицом ЕС отдельно от материнской компании, либо стать частью совместного предприятия с европейской облачной компанией.

Представитель ENISA заявил, что не может комментировать частный документ и что предложение должно быть подписано представителями стран ЕС. Представитель добавил, что самый высокий уровень сертификации предназначен для применения только к небольшому набору случаев, требующих дополнительной безопасности, таких как критически важные инфраструктурные приложения.

Представитель Amazon AWS отказался комментировать проект предложения. Представители Microsoft и Alphabet не сразу ответили на запрос о комментариях.

Более высокий стандарт может использоваться для отбора компаний, которые будут конкурировать за контракты на хранение конфиденциальных правительственных данных. Проект предложения, о котором впервые сообщила Euractiv, будет добровольным и все еще может быть изменен.

ENISA предлагает двухуровневую классификацию кибербезопасности «высокого» уровня. Большинство американских облачных провайдеров уже могут соответствовать предложенному стандарту «EL3», который требует определенного уровня прозрачности данных. Самый высокий уровень — сертификация EL4 — потребует, чтобы данные хранились в ЕС и не подвергались вмешательству иностранного правительства.

Американские компании были обеспокоены тем, что ENISA включит какие-то правила владения облачными данными в ЕС — аналогичные тем, которые уже действуют во Франции — для достижения высшей сертификации. Предложение ENISA будет проще для американских компаний. По словам двух человек, знакомых с деталями, предложение Oracle Sovereign Cloud, например, скорее всего, соответствует предлагаемым требованиям EL4». ***(Jillian Deutsch, Alberto Nardelli. EU Eyes Cyber Plan Aimed at Keeping Cloud Data in Europe // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2023-05-11/eu-eyes-cybersecurity-plan-aimed-at-keeping-cloud-data-in-europe). 11.05.2023).***

***

«Британское правительство сообщило, что кибер-навыки Великобритании, безопасность цепочки поставок и осведомленность предприятий о кибератаках были главными темами повестки дня на втором заседании Национального консультативного совета по кибербезопасности (NCAB). Встреча состоялась в апреле на CyberUK, флагманской правительственной конференции по кибербезопасности в Белфасте, под сопредседательством заместителя премьер-министра и канцлера герцогства Ланкастер Оливера Даудена и ИТ-директора Lloyds Banking Group UK Шэрон Барбер.

NCAB — это форум для более инклюзивного и заинтересованного национального диалога по кибербезопасности, объединяющий лидеров британских научных кругов, промышленности и третьего сектора. Правительство подало заявки на участие в NCAB в мае прошлого года, первое заседание которого состоялось в Лондоне в ноябре. На своем втором заседании правление обсудило достижения Великобритании с момента запуска Национальной киберстратегии и то, как она может повлиять на подход правительства к программам-вымогателям, которые остаются серьезной угрозой национальной безопасности.

В состав NCAB входят высокопоставленные представители таких организаций, как Совет по кибербезопасности Великобритании, Tech UK, Google Cloud, ASOS, Vodafone и Microsoft.

NCAB нацелен на набор сотрудников в области кибербезопасности, стандартизированную безопасность поставщиков, киберустойчивость

Согласно сообщению правительства Великобритании, NCAB обсудил прогресс по трем приоритетным направлениям, движимый рабочими группами NCAB по кибер-навыкам и разнообразию, управлению рисками и кризисами, а также цепочкам поставок, состоящим из членов NCAB и правительства. Это были:

Развивайте кибер-навыки во всей экономике, внедряя более совершенные методы найма, такие как стандартизированные спецификации работы, и изучая, как ускорить развитие талантов начального уровня.

Укрепляйте безопасность цепочек поставок, область, остро нуждающуюся в межотраслевом улучшении, и повышайте эффективность процесса обеспечения качества с помощью стандартизированных анкет для поставщиков.

Повышайте осведомленность предприятий о рисках, связанных с кибератаками, чтобы активизировать действия по обеспечению киберустойчивости.

NCAB заявил, что ожидает объявить о прогрессе и действиях в этих областях на следующем заседании, запланированном на октябрь 2023 года.

Сотрудничество правительства и бизнеса — ключ к борьбе с общими киберугрозами в Великобритании

По словам Барбера, второе заседание NCAB продемонстрировало ценность сотрудничества между государством и бизнесом. «Совместная работа по борьбе с общими угрозами, с которыми мы сталкиваемся, помогает сделать Великобританию безопасным местом для инвестиций и ведения бизнеса. Совет директоров призывает предприятия участвовать в одной из многих блестящих инициатив, реализуемых в отрасли, направленных на укрепление нашей национальной киберэкосистемы и повышение киберустойчивости Великобритании».

По словам министра безопасности Великобритании Тома Тугендхата,. партнерство в области кибербезопасности между правительством и промышленностью должно пойти дальше, чем раньше, чтобы помочь обеспечить безопасность Великобритании и противостоять новым киберугрозам Тугендхат выступил на открытии второго дня конференции CyberUK в апреле, заявив, что, хотя недавние партнерские отношения между правительством и промышленностью были эффективными в борьбе с разнообразными киберрисками, требуется дополнительная работа, чтобы идти в ногу с меняющимся ландшафтом угроз.

Тугендхат выделил три конкретных области, в которых необходимо уделить особое внимание созданию всесторонней экосистемы кибербезопасности, основанной на передовом образовании, опыте, технологиях и кибервозможностях Великобритании. Это профилактика, усиленная защита и новые технологии». ***(Michael Hill. UK cyber skills, supply chain security, ransomware top of National Cyber Advisory Board agenda // IDG Communications, Inc. (https://www.csoonline.com/article/3696693/uk-cyber-skills-supply-chain-security-ransomware-top-of-national-cyber-advisory-board-agenda.html). 16.05.2023).***

***

«Редко когда объявление о работе вызывало такую негативную реакцию. Недавний шаг Министерства финансов Великобритании по найму главы отдела кибербезопасности с зарплатой от 50 500 до 57 500 фунтов стерлингов

вызвал недоверие и насмешки. Менее ясно, привлекло ли это ряд лучших кандидатов.

Правительство высмеивали в социальных сетях за то, что оно предлагало то, что воспринималось как сравнительно низкий уровень вознаграждения за такую важную роль, и основные СМИ также вступили в бой. Metro раскритиковала «мизерную зарплату», а LBC говорила о «зарплатном шторме».

Ни Минфин, ни Кабинет министров не ответили на TechInformed запрос о комментариях. Но многие представители индустрии кибербезопасности были рады поделиться своим мнением об оплате и последствиях недостаточного вознаграждения профессионалов, занимающих ключевые должности с высокими ставками.

«Невероятно, чтобы правительство Великобритании могло эффективно выполнить это требование с такой зарплатой», — говорит Чарли Райман, директор по подбору персонала компании Trident Search, специализирующейся на подборе персонала в области кибербезопасности.

«Мы видим, что сотрудники младшего уровня с 1-2 годами опыта получают предложения выше 60 000 фунтов стерлингов, поэтому просить руководителя киберпространства со всей вытекающей из этого ответственностью принять этот уровень просто нереально», — добавляет он.

По словам Раймана, эта история вызвала большой интерес, потому что, учитывая темпы изменений в отрасли и уровень киберугроз, с которыми сталкиваются компании, на руководящие должности требуются опытные высокоэффективные специалисты, обладающие навыками предотвращения, смягчения последствий и устранения разрушительных киберугроз. -атаки.

Чтобы представить это в перспективе, уточняет он, эквивалентные должности в частном секторе рекламируются с зарплатой в 150 тысяч фунтов стерлингов и выше.

Публичный против частного

Однако существует разница в оплате труда в государственном и частном секторах. Сэм Хамид, соучредитель и управляющий директор SPG Resourcing, консультационной компании с офисами в Лидсе и Ньюкасле, говорит, что, как правило, государственный сектор платит примерно на 30% меньше текущей рыночной ставки для технологических ролей, и кибербезопасность может прийти с премией к остальной части сектора.

«Например, зарплата инженеров по безопасности и архитекторов в государственном секторе варьируется от 68 000 до 72 000 фунтов стерлингов, тогда как аналогичная должность в крупной частной компании легко потребует шестизначную сумму», — говорит Хамид.

«Хотя это правда, что государственный сектор предлагает лучшие льготы, они вряд ли придутся по вкусу тем, кто в начале своей карьеры имеет высокий потенциальный доход».

Однако организации государственного сектора должны предоставлять государственные услуги, богатые данными, а это означает, что им необходимо нанимать, обучать и удерживать ИТ-специалистов, обладающих навыками и личными качествами, чтобы это произошло.

Достижение этих амбициозных целей означает оплату труда, соответствующую требуемому высокому набору навыков. Без этих специальных навыков организации государственного сектора остаются уязвимыми для все более изощренных потенциальных атак и более решительных участников угроз.

В прошлом году кибератака на NHS стала еще одним досадным напоминанием об ущербе, который может быть нанесен государственному сектору. Атака отключила услуги, которыми пользовалась горячая линия медицинских консультаций NHS 111, в результате чего медицинские работники вынуждены полагаться на ручку и бумагу для координации услуг.

Саша Гизе, главный специалист по ИТ-безопасности и управлению услугами SolarWinds, говорит: «Несмотря на то, что в таких сложных атаках задействовано множество вещей, я считаю, что можно сделать больше с точки зрения публичного и частного секторальное сотрудничество, когда речь идет о предотвращении атак — правительство Великобритании просто не может позволить себе рисковать из-за нехватки навыков. Платить достаточно за нужные навыки очень важно».

Универсальный разрыв в оплате труда

Разрыв в оплате труда в государственном и частном секторах отнюдь не уникален для Великобритании.

В отчете Rand за 2021 год « Сравнение кибербезопасности и ИТ-персонала в государственном и частном секторах» указана средняя заработная плата аналитиков по информационной безопасности в государственном секторе США в диапазоне от 80 до 90 тысяч долларов по сравнению с частным сектором США, где средняя заработная плата за тот же навык комплект был в диапазоне 110-120 тысяч долларов.

В другом отчете Axios указано, что в 2022 году средняя годовая зарплата в киберсфере в частном секторе США составляла 100 тысяч долларов, что на 14% больше, чем в среднем в государственном секторе.

В целом, отмечает Райман, заработная плата в Великобритании, как правило, намного ниже, чем в США, где компании платят в среднем на 30% больше. Однако в странах Европы, Ближнего Востока и Африки заметной разницы нет.

Также наблюдалось замедление роста заработной платы в сфере кибербезопасности, которое Гай Голан, генеральный директор фирмы Performanta, специализирующейся на кибербезопасности, объясняет достижением пределов оплаты труда.

«Теперь у вас есть молодые работники начального уровня, получающие, например, базовую зарплату в размере 5000 фунтов стерлингов в месяц. Для сравнения: это больше, чем зарабатывает врач в начале своей карьеры. Я предполагаю, что зарплаты могут остаться такими же, с вероятностью, что они могут даже немного снизиться».

Выше зарплата, выше защита?

В то время как информацию о зарплате довольно легко отследить, гораздо сложнее найти данные о связи между инвестициями в персонал по кибербезопасности и надежностью защиты организации.

«Публикуется много статистических данных о том, сколько тратится на кибербезопасность, и много публикуется о росте числа кибератак и во сколько они обходятся организациям, подвергшимся атаке, но не столько о взаимосвязи между

расходами на кибербезопасность. и его влияние на успешную защиту организаций», — говорит Энди Уильямс, соучредитель Transatlantic Cybersecurity Business Network.

«Это связано с тем, что организации, которые больше всего тратят на кибербезопасность, также, как правило, подвергаются наибольшему количеству атак, причем со стороны самых изощренных злоумышленников, потому что у них есть наиболее ценные информационные активы для защиты, такие как финансовые службы или правительство».

Европейская сеть по кибербезопасности, базирующаяся в Нидерландах организация, которая занимается обучением и обменом информацией о киберугрозах, в сентябре присоединилась к финансируемой ЕС инициативе по обучению экспертов по кибербезопасности для лучшей защиты электросетей.

Управляющий директор Анйос Нейк говорит, что, хотя инвестирование капитала в найм персонала может показаться очевидным решением, это не обязательно серебряная пуля, которую хотели бы организации.

Прием на работу — это только одна часть устранения пробела в навыках. Чтобы сделать это правильно, утверждает Найк, сначала вам нужно знать, каков дефицит навыков в вашей организации.

Он начинается с оценки рисков, чтобы понять риски, от которых вам необходимо защитить свою организацию, и определить меры и средства контроля, необходимые для снижения рисков.

Отсюда вы можете получить то, что требуется с точки зрения ролей, обязанностей и процессов, а также необходимых знаний и навыков в области безопасности для различных управленческих и операционных ролей.

Сравнение этого с вашим фактическим штатным расписанием даст вам полную картину того, что должно произойти, чтобы заполнить пробел в качестве предварительного условия для повышения устойчивости.

Требуемые действия могут включать, например, аутсорсинг наборов навыков, которые вы не сможете поддерживать в своей организации, преобразование безопасности из ответственности персонала в линейную ответственность, наем персонала для полностью новых ролей в юриспруденции/закупках и многое другое.

«Если вы нанимаете технический персонал, не обеспечивая правильную организационную среду и полномочия, и если вы не можете привнести нужные знания и навыки, вы можете создать новый риск и снизить устойчивость вашей организации», — говорит Нейк.

Подрядчики

Существуют некоторые расхождения во мнениях относительно того, конкурентоспособны ли цены на контракты с правительством и государственным сектором Великобритании (а не на оплачиваемые должности с полной занятостью).

Райман говорит, что, вопреки распространенному мнению, государственные контракты довольно конкурентоспособны и могут быть прибыльными для квалифицированных специалистов, выбирающих этот путь. Борьба заключается в том, чтобы найти подходящих людей для этих возможностей.

Напротив, Голан придерживается мнения, что такие контракты часто не имеют конкурентоспособных цен, и основными проблемами являются ограничения по дневным ставкам и продолжительности контрактов.

«Это вынуждает государственный сектор участвовать в долгосрочных проектах, включающих работу по контракту, что противоречит цели быстрого и оперативного взаимодействия. Если использовать аналогию, это похоже на покупку автомобиля, что является крупным вложением, только для того, чтобы один раз проехать из пункта А в пункт Б».

Еще одна новая тенденция, которую заметил Голан, заключается в том, что техническим ресурсам начального уровня поручается решать серьезные проблемы с высокими ставками, «при этом компании придерживаются мнения, что если клиент плохо платит, им будут предоставлены младшие ресурсы. Как и следовало ожидать, результат может быть катастрофическим».

Как ни крути, недоплата — это путь к неприятностям». ***(Rob Gray. Are public sector cyber security salaries enough to attract best-in-class talent? // powered by IResearch Services (https://techinformed.com/public-sector-cyber-security-roles-underpaid/). 15.05.2023).***

***

Австралія та Нова Зеландія

«…Мало того, что правительство Австралии сосредоточено на том, чтобы к 2030 году позиционировать Австралию как мирового лидера в области кибербезопасности, оно (наконец-то) продвинулось вперед с долгожданной реформой закона о конфиденциальности, с изменениями максимальных наказаний и правоприменительных полномочий, внесенными в декабре 2022 года, и дальнейшими событиями, касающимися более полный обзор адекватности австралийских законов о конфиденциальности ожидается к концу 2023 года. Совсем недавно австралийский регулятор конфиденциальности (OAIC) начал расследование ряда крупных кибер-взломов, которые затронули личную информацию миллионов австралийцев.

Дополнительное финансирование инициатив по обеспечению конфиденциальности и кибербезопасности

Факт повышенного риска кибербезопасности и нарушения конфиденциальности в Австралии был по существу подтвержден на этой неделе, когда федеральное правительство объявило в бюджете на 2023/24 год, что OAIC получит более 60 миллионов долларов в течение следующих нескольких лет для финансирования усиления правоприменительной деятельности.

В частности, на 2023/24 финансовый год было выделено дополнительно 17,8 млн долларов и 45 млн долларов на четыре года, чтобы усилить соблюдение OAIC законов Австралии о конфиденциальности. Другое финансирование конфиденциальности данных и кибербезопасности в бюджете на 2023–2024 гг. включает:

23,4 миллиона долларов на помощь малому бизнесу в смягчении последствий кибератак посредством обучения, проводимого Советом организаций малого бизнеса Австралии;

86,5 млн долларов на создание Национального центра по борьбе с мошенничеством, который поможет ASIC бороться с мошенническими веб-сайтами;

26,9 млн долларов на повышение эффективности и защиты цифровых удостоверений личности; и

88,8 млн долларов США в течение 2 лет для поддержки права потребителей на данные в банковском, энергетическом и небанковском кредитных секторах, а также для повышения уровня кибербезопасности.

Укрепление следственной и правоприменительной группы OAIC

Это выделение существенного дополнительного финансирования произошло после очевидных структурных изменений в OAIC, которые предполагают усиление его внутренних следственных и правоохранительных групп. 2 мая 2023 года генеральный прокурор Австралии достопочтенный. Марк Дрейфус KC, член парламента, объявил, что правительство Австралии немедленно начнет поиск нового уполномоченного по вопросам конфиденциальности для наблюдения за соблюдением Закона о конфиденциальности 1988 года (Cth) (Закон). В настоящее время Ангелина Фальк выступает как в качестве комиссара по информации, так и в качестве комиссара по конфиденциальности, но останется только прежней. Заявление генерального прокурора последовало за наймом OAIC Пенни Сноуден, бывшего главного юрисконсульта федеральной полиции Австралии, примерно в феврале 2023 года в качестве помощника комиссара по разрешению споров, а также объявлением о вакансиях в юридических и следственных органах примерно в апреле 2023 года для заполнения недавно созданного отдела крупных расследований, который была создана для борьбы с недавним всплеском крупных кибератак в Австралии.

Предыдущие разработки согласуются с возрастающим риском правоприменения

Упомянутые выше события согласуются с заявленным правительством Австралии намерением усилить соблюдение законов Австралии о конфиденциальности и кибербезопасности Австралии в целом. Они также основаны на нескольких важных событиях в области конфиденциальности и киберпространства в Австралии за последние 6 месяцев:

Ускоренное внесение изменений в Закон в декабре 2022 года, когда Федеральный парламент Австралии принял Закон 2022 года о внесении поправок в законодательство о конфиденциальности (принудительные и другие меры) (Cth). Эти изменения включали:

увеличивается до максимальных штрафов для компаний за серьезное или неоднократное вмешательство в частную жизнь, равных 50 миллионам долларов США или трехкратной стоимости полученной выгоды в зависимости от того, что больше; и

расширены регулирующие полномочия OAIC и Австралийского управления по коммуникациям и средствам массовой информации, которые включают сбор информации и обмен информацией с другими правоохранительными органами.

Более полный пересмотр Закона с дальнейшими реформами ожидается в конце 2023 года после публикации отчета о пересмотре Закона о конфиденциальности в феврале 2023 года и периода консультаций, завершившихся в конце марта 2023 года.

Объявление первого министра кибербезопасности Австралии достопочтенного. Клэр О'Нил, член парламента в феврале 2023 года по разработке Австралийской стратегии кибербезопасности на 2023-2030 годы, которая устанавливает амбициозное стремление Австралии стать к концу этого десятилетия самой кибербезопасной страной в мире.

OAIC начала масштабные расследования некоторых из крупнейших кибератак в истории Австралии на Medibank, Optus и, как было объявлено на этой неделе, Latitude Financial Services. Примечательно, что расследование Latitude является первым совместным расследованием OAIC с иностранным регулирующим органом, являющимся Офис комиссара по вопросам конфиденциальности Новой Зеландии.

Решение OAIC назвать Неделю осведомленности о конфиденциальности в этом году «Назад к основам». Нет никаких сомнений в том, что недавние кибератаки в Австралии привлекли внимание к безопасности личной информации и методам обработки данных предприятий в Австралии, и, в частности, явные неспособности некоторых предприятий уничтожить или деидентифицировать личную информацию, которая не требуется дольше. Может ли внимание OAIC напомнить предприятиям о том, что нужно правильно понимать основы, быть признаком того, что строгое соблюдение австралийских законов о конфиденциальности (в дополнение к крупным расследованиям, которые уже ведутся) не за горами?

Следующие шаги

Кажется почти уверенным, что OAIC продолжит наращивать свою следственную и правоприменительную деятельность в отношении законов Австралии о конфиденциальности в ближайшем будущем. Помимо риска расследования и судебного преследования, мы ожидаем повышенный риск использования OAIC полномочий по сбору информации.

Очень важно, чтобы организации, ведущие бизнес в Австралии, были готовы к тому, что OAIC постучится. Организации должны пересмотреть свои существующие методы обработки данных и безопасности, чтобы убедиться, что они действительно соответствуют «базам». Такая документация, как политика конфиденциальности, уведомления о сборе данных, политика хранения и хранения данных, а также планы реагирования на кибер-инциденты, должны быть пересмотрены и обновлены в той мере, в какой они устарели или не соответствуют законам Австралии». ***(Hamish Fraser, Julie Cheeseman. Privacy breaches & cyber security in Australia - heightened enforcement risk // Bird & Bird (https://www.twobirds.com/en/insights/2023/australia/privacy-breaches-and-cyber-security-in-australia-heightened-enforcement-risk). 11.05.2023).***

***

Індія

«По данным Государственного министерства электроники и информационных технологий Индии, рост цифровизации привел к увеличению числа кибератак и попыток проникновения: только в 2022 году в стране произошло около 14 тысяч инцидентов кибербезопасности.

Чтобы реализовать цели цифровизации и перехода к безбумажной экономике, мы должны улучшить наши процедуры и инфраструктуру кибербезопасности до такой степени, чтобы жители Индии чувствовали себя уверенно в отношении своей личной информации. Индийским учреждениям и предприятиям крайне важно внедрить передовой опыт в области кибербезопасности здравоохранения, чтобы обеспечить будущее.

Устранение пробелов в навыках

Недавнее исследование рынка показало, что сектор кибербезопасности в настоящее время сталкивается с серьезной нехваткой навыков, при этом спрос на услуги кибербезопасности постоянно растет. Одной из возможных причин этого дефицита может быть отсутствие учебной программы в программах колледжей, что препятствует входу в этот сектор новых перспектив.

Чтобы восполнить этот пробел, необходимо принять меры по модернизации системы образования и обеспечить, чтобы профессионалам предоставлялись регулярные возможности для повышения квалификации.

Особое внимание должно быть уделено нескольким критическим областям, таким как управление сетевой безопасностью, управление виртуальными машинами и другим соответствующим навыкам, которые в настоящее время востребованы в отрасли. Возможности повышения квалификации также помогут расширить кадровый резерв в этом секторе и охватить более широкую аудиторию потенциальных клиентов, ищущих прибыльную карьеру.

Кибербезопасность для цифровизации

Защита и безопасность данных пациентов должны стать одним из главных приоритетов индустрии кибербезопасности в 2023 году, поскольку это один из типов информации, на которую чаще всего нацеливаются киберпреступники.

Программа-вымогатель — одна из наиболее часто используемых ворами тактик для проникновения в систему. После эпидемии количество атак программ-вымогателей резко увеличилось, увеличившись на 105% в 2021 году. Но сектор должен быть готов к другим инструментам и методам атак, которые могут использовать хакеры.

Эти атаки могут принимать форму BEC, фишинга или DDoS, когда злоумышленник может отключить сервер жертвы. Поэтому крайне важно, чтобы предприятия информировали своих работников и были готовы к любым новым опасностям.

Преимущество аутсорсинга

Небольшие организации сталкиваются со значительными препятствиями, когда речь идет о реализации мер кибербезопасности, в первую очередь из-за нехватки ресурсов. Программы кибербезопасности требуют постоянного обслуживания и обновления, что требует команды знающих людей для поддержания работы систем на оптимальном уровне.

Для многих компаний выделять столько денег одному отделу нецелесообразно. Для решения этой проблемы необходимы конкретные административные действия, чтобы помочь этим организациям найти первоклассные службы кибербезопасности.

Аутсорсинг кибербезопасности является выгодным решением, поскольку он значительно более доступен и позволяет компаниям объединять ресурсы для оплаты услуг. Недавние инвестиции правительства в размере более 600 крор в развитие национальной инфраструктуры кибербезопасности — это шаг в правильном направлении, поскольку сектору требуется поддержка для поддержки его операций и расширения его горизонтов. Такие инициативы, как Ayushman Bharat Yojana, также внесли значительный вклад в продвижение цифровых технологий в сфере здравоохранения.

Хотя индустрия кибербезопасности добилась значительного прогресса за короткий период, предстоит еще много работы для достижения конечной цели оцифровки отрасли здравоохранения, и кибербезопасность является важнейшим компонентом этих усилий. Крайне важно завоевать доверие потребителей и завоевать доверие, а надежная и безопасная сеть кибербезопасности служит свидетельством высококвалифицированной рабочей силы и дает потребителям уверенность в том, что их информация всегда защищена». ***(Future of healthcare cybersecurity: Key strategies for 2023 and beyond // Udayavani (https://www.udayavani.com/english-news/future-of-healthcare-cybersecurity-key-strategies-for-2023-and-beyond). 28.05.2023).***

***

Інші країни

«Совет по кибербезопасности ОАЭ призвал государственный и частный секторы проявлять максимальную осторожность в отношении любых кибератак, которые могут быть нацелены на национальную цифровую инфраструктуру и активы.

Совет потребовал от государственных и частных организаций активировать систему реагирования на кибер-аварийные ситуации в сотрудничестве с компетентными органами, чтобы обмениваться данными для упреждающего предотвращения возможных злонамеренных атак.

Совет подчеркнул важность противодействия различным кибератакам со стороны жизненно важных секторов, в дополнение к активизации систем защиты и политики кибербезопасности, а также повышению осведомленности властей о любых подозрительных электронных действиях, которые могут нанести вред их системам.

ОАЭ перенимают лучшие стандарты и практики безопасной цифровой трансформации и защиты национальной цифровой инфраструктуры и пространства». ***(UAE cybersecurity council warns public, private entities of cyber attacks // Galadari Printing and Publishing LLC. (https://www.khaleejtimes.com/uae/uae-cybersecurity-council-warns-public-private-entities-of-cyber-attacks). 06.05.2023).***

***

«Средние специальные учебные заведения Турции будут готовить специалистов в сфере кибербезопасности.

С данной целью будут созданы техучилища по кибербезопасности при четырех высших учебных заведениях: Анкарском университете, Эгейском университете, Техническом университете Гебзе и Стамбульском техническом университете.

Активную поддержку проекту оказывает Управление цифровой трансформации при Администрации президента Турции. Техучилища будут расположены на территории технопарков.

Молодежь будут обучать здесь технологиям информационной безопасности, сетевой безопасности, анализу данных, а также базовым шагам по обеспечению кибербезопасности. Учебный процесс предполагает лабораторные и проектные работы.

Поступающие должны пройти предварительно год подготовки на английском языке.

Учащимся будут предоставлены стипендии и поддержка при трудоустройстве в передовых компаниях». ***(Selma Kasap, Elmira Ekberova. Техучилища Турции будут готовить специалистов в сфере кибербезопасности // Anadolu Ajansı (https://www.aa.com.tr/ru/наука-и-технология/техучилища-турции-будут-готовить-специалистов-в-сфере-кибербезопасности/2898481) 16.05.2023).***

***

«В Молдове принят Закон о кибернетической безопасности, который разработан при содействии ЕС в рамках проекта «Быстрая помощь в области кибербезопасности Молдовы». Он вступит в силу с 1 января 2025 г. и призван укрепить кибербезопасность организаций государственного сектора и субъектов критической инфраструктуры страны.

Как передает «ИНФОТАГ», в распространенном Делегацией ЕС пресс-релизе отмечается, что закон разработан при поддержке экспертов Академии электронного управления Эстонии (eGA). Они помогли министерству экономического развития и цифровизации определить сферу ответственности в управлении кибербезопасностью, разработать основные требования кибербезопасности, механизм управления киберинцидентами и мониторинга, а также платформы для обмена информацией.

«Утверждение закона стало для Молдовы важным шагом в укреплении ее устойчивости к гибридным угрозам и создании учреждений в соответствии с нормами ЕС. Мы рады видеть результаты этого проекта», - заявил Посол ЕС в РМ Янис Мажейкс.

В соответствии с законом, компетентный орган республики назначает на основании различных критериев учреждения и поставщиков услуг, от которых будут требовать достижения необходимого уровня кибербезопасности.

«Безопасность, в том числе кибернетическая, - важная цель в повестке Молдовы. Это обусловлено уязвимой геополитической позицией республики, расположенной между Евросоюзом и Россией», - отметил вице-премьер, министр экономики и цифровизации Думитру Алайба». ***(МОЛДОВА УСИЛИТ***

КИБЕРБЕЗОПАСНОСТЬ ПРИ СОДЕЙСТВИИ ЕВРОСОЮЗА // Infotag (https://www.infotag.md/m9_populis/307354/). 12.05.2023).

***

«В настоящее время предпринимаются усилия по формированию в Шри-Ланке Управления кибербезопасности в этом году, сообщило вчера Министерство технологий.

Государственный министр Канака Херат, выступая на конференции по кибербезопасности в Коломбо, поделился обновленной информацией, отметив важность кибербезопасности для правительства.

Он сообщил, что Закон о кибербезопасности был переведен и будет представлен в парламент после утверждения Генеральным прокурором. Принятие Закона проложит путь к созданию Управления.

Государственный министр заверил, что с принятием Закона о кибербезопасности, направленного на устранение риска неправомерного использования цифровых систем в Шри-Ланке, средства массовой информации не будут подвергаться цензуре.

Закон о кибербезопасности направлен на защиту частной жизни граждан от суровых последствий цифровизации, а также данных отдельных учреждений в государственном и частном секторах.

«Закон о кибербезопасности должен защищать индивидуальные и организационные данные в государственном и коммерческом секторах, а также выполнять такие действия, как безопасность веб-сайтов. Без этого цензуры в соцсетях не будет. Пользователи социальных сетей иногда также интересуются этим», — сказал Герат.

«Мы сможем защитить нашу страну от кибератак, а также личных рисков и трудностей, если этот закон будет реализован. В нашей стране в результате определенной активности в социальных сетях погибли дети», — подчеркнул он.

Согласно последнему рейтингу Национального индекса кибербезопасности (NCSI), Шри-Ланка поднялась на 69-е место в 2021 году с 98-го места в 2020 году из 160 стран». ***(Sri Lanka to get Cyber Security Authority this year // Wijeya Newspapers Ltd. (https://www.dailymirror.lk/business/Sri-Lanka-to-getCyber-Security-Authority-this-year/215-259739). 24.05.2023).***

***

«Стратегическое видение обеспечения кибербезопасности Молдовы сегодня обсуждалось на общественных консультациях, проведенных в контексте разработки Стратегии национальной безопасности. Эксперты в секторе кибербезопасности, представители гражданского общества и государственных учреждений, а также академической и частной среды рассказали о немедленных и долгосрочных мерах по повышению киберустойчивости Молдовы, которые сообщил.

Присутствовавший на мероприятии премьер-министр Дорин Речан заявил, что после развязывания Россией войны против Украины Молдова стала объектом гибридных угроз и нападений. Для противодействия им власти сосредоточатся на

консолидации мер кибербезопасности, защите граждан и обеспечении надлежащей работы критической инфраструктуры.

«Кибербезопасность становится все более важной с расширением цифровой повестки дня правительства. Поэтому необходимо, чтобы мы продвигали культуру кибербезопасности во всем обществе, а также активно включались в сотрудничество с зарубежными партнерами в сфере кибербезопасности», — сказал премьер-министр Дорин Речан.

Посол США в Молдове Кент Логсдон подчеркнул, что США и дальше будут поддерживать Молдову в обеспечении кибербезопасности. Он отметил, что эта сфера имеет решающее значение, учитывая, что Молдова продвигается вперед в процессе интеграции в Европейский Союз.

Участники общественных консультаций также обсудили международное партнерство в сфере кибербезопасности и меры, принимаемые Кабмином для усиления реагирования на вызовы в информационном пространстве. Они также проанализировали точку зрения частного сектора на кибербезопасность и способы улучшения обмена информацией между государственным и частным секторами в области кибербезопасности». ***(Strategic vision on ensuring cyber security publicly consulted at Moldova's government // "I.P. MOLDPRES A.I.S." (https://www.moldpres.md/en/news/2023/05/25/23004234). 25.05.2023).***

***

«…Индустрия кибербезопасности в Южной Африке все еще находится в зачаточном состоянии. Тем не менее, есть несколько игроков с многолетним опытом работы в этой области, которые помогают предприятиям и госпредприятиям отражать кибератаки на протяжении всего времени, пока страна подключена к глобальному онлайн-сообществу.

Слишком маленький, слишком поздно

Кибербезопасность исторически была необдуманной покупкой для бизнеса — до тех пор, пока не произойдет взлом. К тому времени может быть уже слишком поздно — компания может быть заблокирована в своих собственных системах, а данные обо всех, с кем она ведет дела и принимает платежи, могут быть украдены.

Важно заранее защитить бизнес от кибератак, потому что любое действие, совершаемое в цифровом пространстве, делает бизнес уязвимым для потенциальных хакеров.

Киберриски изменились, как и услуги и продукты, предлагаемые компаниями, занимающимися кибербезопасностью и соблюдением нормативных требований. Десять лет назад периодическое тестирование на проникновение считалось достаточным средством защиты от атак. Теперь цифровую безопасность компании необходимо постоянно оценивать, контролировать и защищать.

Это также относится к компаниям всех размеров — от глобальных компаний до небольших предприятий. На траектории уровень угроз от вирусов до вредоносных программ и программ-вымогателей был экспоненциальным.

Повышение квалификации, повышение квалификации

Эта быстрая эволюция поставила перед компаниями, занимающимися кибербезопасностью, задачу повысить собственный уровень знаний и методов

управления инцидентами, и наиболее успешными оказались те, кто работал в качестве партнеров, а не просто поставщиков услуг.

Кибербезопасность по-прежнему строится на доверии, но сейчас предприятия ищут партнеров, которые могли бы работать вместе с ними, а не за них. Формирование такого рода партнерских отношений расширяет возможности обеих сторон — компании знают, что их партнер по кибербезопасности заинтересован в их цифровой безопасности, и партнер должен помочь бизнесу: информировать персонал о возникающих угрозах, предупреждать ИТ-отделы о потенциальных слабых местах безопасности и помогать им. активно управлять своей цифровой безопасностью.

За последние два десятилетия Magix построила свою репутацию на основе доверия и партнерства, предлагая свои услуги ведущим финансовым компаниям и государственным предприятиям.

Инновации стали ключом к нашему успеху. Десятилетия доверия с партнерами позволили Magix стать лучшим бизнесом и лучшим партнером. Это дало нам уверенность и пространство для инноваций до такой степени, что мы предоставляем наши услуги на основе потребностей наших клиентов и зрелости их текущих методов кибербезопасности.

Предупрежден - значит вооружен

Pretect от Magix — одна из таких инноваций: настраиваемое партнерство в области кибербезопасности, которое помогает компаниям любого размера активно управлять своей цифровой безопасностью.

После оценки цифрового следа бизнеса решение Pretect адаптируется к потребностям клиента. Он предоставляет бизнесу оперативную онлайн-панель, которая отслеживает угрозы и дает предложения по устранению — и все это по цене, которая соответствует потребностям и размеру бизнеса.

После развертывания Pretect отслеживает уязвимости организации. Посредством регулярных ежемесячных и специальных сеансов обратной связи Magix предупреждает заинтересованных лиц, занимающихся цифровой безопасностью, об угрозах и обсуждает стратегии эффективного устранения. Ваши данные — ваш самый важный актив, и единственная задача партнера по кибербезопасности — работать с вами над их защитой.

Угрозы безопасности стали одной из величайших жизненных определенностей. Таким образом, в мире, где жизнь проживается в цифровом формате, доверительные партнерские отношения в области кибербезопасности никогда не были так важны». ***(Kevin Wotshela. Cybersecurity Requires Partnerships, Not Products // TFS MEDIA (https://techfinancials.co.za/2023/05/24/cybersecurity-requires-partnerships-not-products/). 24.05.2023).***

***

Кіберстрахування

«Глобальные страховщики стремятся выяснить, как избежать покрытия спонсируемых государством кибератак и катастрофических взломов,

поскольку крупные убытки и сокращение расходов некоторых известных компаний пугают рынок.

Чабб Лтд. изучает более высокие цены и страховые отчисления для широко распространенных кибер-событий. Beazley Plc разрабатывает новый продукт военного страхования, выходящий за рамки стандартной киберполитики, для покрытия хакерских атак между государствами. Другие страховщики корректируют свою политику, чтобы исключить акты кибертерроризма.

Атаки программ-вымогателей в 2022 году увеличились на 87% по сравнению с предыдущим годом. К 2025 году глобальные киберпремии превысят 23 миллиарда долларов, заявила перестраховочная компания Swiss Re AG. По его словам, менее 20% предприятий имеют ограничения политики, превышающие средний спрос на программы-вымогатели.

По словам брокеров и страховщиков, пока ведущие операторы решают, как двигаться дальше, корпоративным клиентам приходится иметь дело с хаотичным киберрынком и противоречивыми условиями контрактов.

«На данный момент не существует ничего, что удовлетворяло бы клиентов, страховщиков и брокеров при работе с системными рисками», — сказал Грег Эскинс, руководитель направления киберпродуктов в Marsh & McLennan, имея в виду катастрофические кибератаки.

«С одной стороны, у вас есть большое количество страховщиков, которые говорят, что кибервойна не поддается количественной оценке и не подлежит страхованию. С другой стороны, у вас есть участники рынка, которые ищут решение для этого», — сказал он.

Lloyd's of London, крупнейший мировой страховой рынок, попросил всех перевозчиков, торгующих через его платформу, прекратить покрывать хакерские атаки, поддерживаемые государством. Но многие страховщики, в том числе опасающиеся негативной реакции со стороны клиентов из США, придумывают другие способы управления рисками.

«Рынок, скорее всего, отстанет от одного или двух подходов через 12 или 24 месяца», — сказал Крис Сторер, глава центра кибербезопасности Munich Re.

Компания Lloyd's потрясла рынок в прошлом году, когда впервые предложила исключить кибервойну.

Большинство крупных страховых компаний, в том числе с большим присутствием в США, продают часть покрытия через рынок Ллойда. В то время как некоторые перевозчики поспешили следовать указаниям Ллойда, вступившим в силу в прошлом месяце, другие придерживаются иного подхода.

«Нет единообразия» в полисах киберстрахования, говорит Элизабет Гири, президент страховых решений в Liberty Mutual Group. «Они сильно различаются для каждого из различных покрытий».

Lloyd's заявил, что поддерживаемые государством кибератаки, в результате которых цифровые активы держателя полиса наносят «серьезный ущерб», не будут покрываться. Но этот термин открыт для интерпретации.

По словам Колина Дейли, исполнительного вице-президента брокерской компании CAC Specialty, страхователь теперь может столкнуться с пятью или шестью различными видами исключений из войны в рамках одного стандартного

полиса. Киберпокрытие обычно распределяется между несколькими страховщиками.

Согласно январскому обновлению страховой компании, Бизли сократил покрытие кибератак, затрагивающих критически важную инфраструктуру, которые теперь включают атаки на фондовые биржи и мобильные сети. Бизли также установил 50-процентное ограничение покрытия для облачных сбоев продолжительностью более 72 часов и атак вредоносного ПО на компании с доходом менее 100 миллионов долларов.

«Мы берем на себя множество системных рисков. Есть всего несколько вещей, которые слишком велики», — сказал Пол Бантик, руководитель отдела глобальных киберрисков в Bezley.

Бизли также разрабатывает новый продукт киберстрахования, который должен быть запущен к 1 июля, для покрытия атак, запрещенных исключением войны Ллойда, сказал Бантик. Он добавил, что более 20 других страховых компаний выразили заинтересованность.

Страховщики действуют с новой срочностью после того, как апелляционный суд Нью-Джерси постановил 1 мая, что подразделение Chubb находится на крючке из-за убытков Merck & Co. в размере 1,4 миллиарда долларов в результате предположительно инициированного Россией взлома вредоносного ПО. Суд заявил, что исключение Чаббом войны в политике 2017 года с Merck запрещает возмещение ущерба только от физической войны, а не от кибератак.

«Теперь, когда дело Merck раскрыто, любой страховщик, решивший не обновлять свой военный язык, подвергается существенному риску», — сказал Сторер.

До сих пор усилия страховщиков не привели к последовательному подходу.

«Во многих случаях попытки страховщиков внести ясность фактически привели к еще большей двусмысленности и неопределенности из-за большого разнообразия интерпретаций этих новых и новаторских положений», — сказал Эскинс.

Он также выразил сомнения в необходимости новой отдельной политики кибервойны. «Каждый новый или развивающийся риск не требует совершенно нового продукта», — сказал Эскинс.

Отказ клиента

Компании, которые часто становятся объектами кибератак, в том числе финансовые, медицинские и коммунальные компании, обеспокоены тем, что мандат Ллойда дает страховщикам слишком большую свободу действий, чтобы отказать в покрытии атак, поддерживаемых государством, особенно когда неясно, насколько сильно иностранное правительство был вовлечен.

В некоторых случаях корпоративные клиенты отдавали предпочтение страховщикам, особенно тем, которые работают на рынке США, которые занимали более мягкую позицию в отношении кибервойн и системных рисков.

К сожалению, некоторые страхователи выбирают победителей и проигравших, поскольку страховщики пытаются прояснить пункты, которые никогда не предназначались для покрытия кибервойны или взлома, поддерживаемого государством, сказал Сторер из Munich Re.

Но корпоративные страхователи сбиты с толку меняющимся ландшафтом кибербезопасности, и некоторые скептически относятся к тому, что их политика окупится в случае крупной атаки.

«Многие клиенты чувствуют себя избитыми», — сказал Майкл Гамильтон, глава фирмы по кибербезопасности Critical Insight.

Марк Лэнс, вице-президент GuidePoint Security, сказал, что многие компании сказали ему, что решили отказаться от киберстрахования, решив вместо этого потратить деньги на внутренний контроль безопасности. «Мы слышали это от некоторых крупных государственных компаний, а также от некоторых частных компаний», — добавил он.

Некоторые страховщики, реагируя на сопротивление клиентов и конкурентный рынок, корректируют свою киберполитику, чтобы побудить бизнес остаться.

Бантик говорит, что в этом году Бизли задает страхователям меньше вопросов, чтобы обеспечить более быстрое андеррайтинг. По словам Гири, Liberty Mutual увеличивает средний лимит кибер-покрытия до 10 миллионов долларов с 5 миллионов долларов.

Между тем, премии по основным киберполисам в марте упали на 15% по сравнению с тем же периодом прошлого года, сказал Кристиан Хоффман, глобальный кибер-лидер Aon Plc.

Но любые изменения на рынке, дружественном к покупателю, также могут затруднить соблюдение ограничений Ллойда в отношении кибервойны, и многие страховщики изо всех сил пытаются найти правильный баланс.

Allianz SE «не выбрала направление» в отношении того, как исключить кибервойны, заявила Треса Стивенс, глава компании по кибербезопасности в Северной Америке.

«Вы не хотите оказаться в ситуации, когда вы идете на попятную, потому что у вас есть портфель застрахованных, которые полагаются на вас, чтобы принять правильное решение», — сказала она.

Один из приоритетов для страховщиков — убедиться, что они не попали в ловушку, когда кибератака затрагивает бизнес и его цифровых поставщиков одновременно. Если оператор страхует компанию, а также ее облачных провайдеров, подрядчиков по кибербезопасности и клиентов, все они могут подать страховые иски, когда широкомасштабная атака поразит одну из сетей компании…» ***(Daphne Zhang. Cyber Insurance Market in Turmoil Over State-Backed Attacks // Bloomberg Industry Group, Inc. (https://news.bloomberglaw.com/insurance/cyber-insurance-market-in-turmoil-over-state-backed-attacks). 22.05.2023).***

***

«Глобальний ринок кіберстрахування зафіксував значне зростання в 2020 і 2021 роках, головним чином завдяки значному підвищенню премій. Збільшення частоти та серйозності кібератак у поєднанні з глобальним переходом до віддаленої роботи внаслідок пандемії змусили страховиків підвищити ціни.

На цьому тлі прогнозується зростання глобального ринку кіберстрахування з 16,7 мільярдів доларів прямих премій (DWP) у 2022 році до 33,4 мільярдів доларів у 2027 році. Про це свідчать експерти GlobalData, провідної компанії з обробки даних та аналітики.

Останній звіт GlobalData «Тематична розвідка: кіберстрахування 2023» показує, що навіть із зменшенням попиту (через швидке зростання цін на премії) глобальний DWP на ринку значно зріс у 2021 (66,5%) та 2022 (42,7%).

Бенджамін Хаттон, страховий аналітик GlobalData, коментує:

«Оскільки премії поступово зменшуються в другій половині 2023 року та після неї, а економічні умови стають менш обтяжливими для компаній, попит на кіберстрахування має зростати в майбутньому».

За його словами, вищий рівень кібербезпеки, менша схильність вимагати викуп, виключення війни та більш конкурентоспроможний страховий ландшафт – усе це об'єднається, щоб утримувати кришку від цін у майбутньому. Очікується, що це поступово сприятиме більшому використанню політики як в особистому, так і в комерційному просторі, що призведе до стабільно високих темпів зростання ринку у найближчі роки.

Глобальні кіберризики для бізнесу продовжують зростати після пандемії, і багато малих і середніх підприємств визнають, що їхні кіберризики з того часу зросли. Згідно з дослідженням страхування малого та середнього бізнесу у Великій Британії GlobalData за 2022 рік, майже 50% середніх підприємств заявили, що їхній кіберризик певною мірою зріс після початку COVID-19…» ***(Герман Богапов. Експерти фіксують значне зростання кіберстрахування // HiTech.Expert (https://expert.com.ua/160843-eksperty-fiksuyut-znachne-zrostannya-kiberstrahuvannya.html). 22.05.2023).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Россия давно гордится тем, что имеет «вторую по величине армию» в мире и «лучших» в мире хакеров с большим количеством взломов против США, Европы и Украины. Однако за последние несколько недель, похоже, репутация России была оценена слишком высоко, поскольку она сталкивалась с одним катастрофическим взломом за другим со стороны антипутинских или проукраинских хакерских групп.

Сергей Моргачев, разыскиваемый Федеральным бюро расследований США (ФБР) за участие в хакерских атаках на лиц, причастных к президентским выборам в США в 2016 году, сам подвергся взлому. Моргачев, который является сотрудником российской военной разведки и имеет звание подполковника, считается вдохновителем «Fancy Bear», известного как Advanced Persistent Threat (APT) 28.

Документы, просочившиеся в сеть, показывают, что Могачув был взломан, скорее всего, в марте проукраинской хакерской группировкой Cyber Resistance. Среди захваченных документов были копии паспорта Могачува, техпаспорта автомобиля, водительских прав, личные фотографии, юридические документы,

трудовые рапорты и другие материалы. В ходе взлома была информация об использовании им Cobalt Strike, любимого инструмента киберпреступников для удаленного доступа и управления зараженными компьютерными системами.

Не успев просто пристыдить одного из лучших хакеров России, обыграв его в его же игре, проукраинские хакеры отправились за покупками, используя аккаунт опального российского подполковника на AliExpress, чтобы заказать широкий ассортимент товаров, включая секс игрушки, памятные вещи ФБР и принадлежности для гей-прайда. Согласно первоначальным сообщениям, материалы были успешно отправлены Могарчеву до того, как он узнал о взломе.

В статье, опубликованной Coindesk, говорится, что «986 финансовых кошельков, контролируемых Управлением внешней военной разведки (ГРУ), Службой внешней разведки (СВР) и Федеральной службой безопасности (ФСБ), были обвинены во взломе компанией Chainalysis, которая тесно сотрудничает с Правительство США.

Сообщается, что дружинники «сожгли» несколько кошельков, а это означает, что они были навсегда утеряны и не могли быть восстановлены российскими спецслужбами, которые использовали эти счета. Некоторые источники новостей указали, что по крайней мере часть денег была отправлена проукраинским благотворительным организациям.

По мере того, как месяц продолжал ухудшаться для кибер-эго России, видеоконференция «Российско-иранское сотрудничество в меняющемся мире», организованная российским Институтом Содружества Независимых Государств, была шокирована, когда Служба безопасности Украины (СБУ) объявила о своем присутствии. на мероприятии в самом конце мероприятия.

Используя имя известного российского академика, вирусное видео показывает, как якобы «академик» начинает благодарить участников, прежде чем объявить, что он на самом деле является офицером Службы безопасности Украины. Он продолжил, что все эти которые участвовали в мероприятии, включая переводчиков и фасилитаторов, столкнутся с международными санкциями за их присутствие на мероприятии в качестве соучастников военных преступлений в рамках усилий по ведению незаконной войны против Украины…» ***(Jason Jay Smart. OPINION: Russia Getting Beaten by Hackers // BIZNESGRUPP TOV (https://www.kyivpost.com/opinion/16528). 03.05.2023).***

***

«…Иран периодически упоминает свои кибервозможности в контексте угроз Израилю, показывая, что Тегеран имеет в своем распоряжении различные средства для проведения своих операций. С этой целью в недавней статье в новостном издании Tasnim, выступающем за режим, подчеркивается, что кибер-способности Ирана атаковать израильские веб-сайты являются «частью кибервойны».

Однако Израиль не единственная страна, ставшая жертвой киберинцидентов. Кибератаки исходят из многих стран и совершаются злоумышленниками. В ОАЭ правительственный совет по кибербезопасности подтвердил свои успехи в защите и противодействии злонамеренным кибератакам.

Согласно статье в Al-Ain, атаки не были нацелены на инфраструктуру, национальные цифровые активы и стратегические секторы. В отчете добавлено, что национальная оперативная группа смогла активно реагировать, в том числе на «кибертеррористические организации». Подробности нападавших не уточняются.

Согласно статье в Khaleej Times, базирующейся в ОАЭ, «Мохаммед Хамад Аль Кувейти, глава отдела кибербезопасности правительства ОАЭ, сказал, что Совет по кибербезопасности ОАЭ сотрудничает со своими партнерами в предотвращении более 50 000 кибератак каждый день против стратегических национальных секторов».

Кувейт выступил с комментариями на Oracle CloudWorld Tour в Абу-Даби 2023. В отчете отмечается, что он добавил, что «банковский, финансовый, медицинский, нефтегазовый секторы являются наиболее целевыми, и что всем атакам активно и эффективно противостоит цифровая сфера, чтобы защитить страну».

В статье на веб-сайте бизнеса и финансов Zawya также отмечается, что Совет по кибербезопасности «подчеркивал важность противодействия различным кибератакам со стороны жизненно важных секторов, в дополнение к активизации систем защиты и политик кибербезопасности и повышению осведомленности властей о любых подозрительных электронных действиях, которые могут повредить их системы. ОАЭ перенимают лучшие стандарты и практики безопасной цифровой трансформации и защиты национальной цифровой инфраструктуры и пространства».

В феврале в статье Tech Monitor отмечалось, что «количество кибератак со стороны Ирана на цели в Израиле удвоилось за последний год», цитируя главу израильского Национального кибердиректора Габи Портного, который, согласно отчету, сказал, что «другие страны в регионе также ощутили на себе последствия атак со стороны иранских киберпреступников и призвали к более широкому обмену данными между правительствами».

В статье Tasnim проблема была сформулирована в контексте послания Ирана «сионистскому режиму» о том, что Израиль «никогда не должен чувствовать себя в безопасности». Это может быть хвастовство или отражение недавних и предстоящих операций.

В этом контексте важно отметить, что Иран недавно нормализовал отношения с Саудовской Аравией.

Киберфронт может быть более простым способом для Ирана похвастаться атаками, которые можно как бы правдоподобно отрицать. Страна может заявить, что она осуществила «кибератаку», фактически ничего не сделав. Например, в июне 2019 года США заявили, что предприняли «кибератаки» на Иран в отместку за то, что Иран сбил разведывательный беспилотник Global Hawk стоимостью 200 миллионов долларов в Оманском заливе.

Заявления о «кибератаках» — это способ для страны заявить, что она «атаковала» или приняла ответные меры без необходимости предоставления доказательств, которые могут привести к реальному конфликту. Страны могут участвовать в массовых «кибервойнах», в которых никто не пострадал и не

пострадал, а общественность может даже не знать о том, что «война» имела место или, возможно, ее не было?

В связи с этим Иран утверждает, что он все больше осваивает кибернетические возможности, что это важный аспект его современной войны. Он также заявил, что «оккупационный режим Израиля переживает новую войну, отличную от предыдущих войн».

В отчете Tasnim подробно описано, чем именно кибервойна отличается от классической войны: «Технологическая и радиоэлектронная война смогла превзойти многие военные возможности, а компьютерные устройства и клавиатуры стали новейшим фронтом израильской войны и нанесли наибольшие потери наиболее жизненно важным и стратегические институты этого режима».

Эти заявления появились после недавних сообщений о потенциальном сотрудничестве между Ираном и Россией в области хакерских атак, а также сообщения о том, что кибергруппа Anonymous Sudan провела кибератаки в День Кудса.

Al-Monitor отметил в то время, что кибератаки были нацелены на банки в Израиле, а CTech заявила, что они нацелены на Почту Израиля и ирригационные системы.

В прошлом году The Jerusalem Post сообщила о 70-процентном росте враждебной кибератаки. В другом отчете, основанном на данных Microsoft, также отмечается, что около четверти иранских кибератак нацелены на Израиль. Иран также нацелен на США и другие страны.

Иранские СМИ утверждают, что «анонимной хакерской группе и ряду других неизвестных имен удалось атаковать израильский режим и большую часть его критически важных инфраструктур за счет использования брешей в безопасности программ и систем израильских электронных баз данных».

Затем он цитирует другие арабские СМИ, утверждая, что количество попыток взлома увеличилось: «Палестинское сопротивление и другие иностранные группы сосредоточили свои усилия на нанесении ударов по всем точкам присутствия израильских оккупантов на оккупированной палестинской территории». ***(SETH J. FRANTZMAN. Does Iran see cyberwar as a way to avoid real war? – analysis // Jpost Inc. (https://www.jpost.com/middle-east/iran-news/article-742295). 07.05.2023).***

***

«Пентагон працює над тим, щоб перетворити свої мережі та процеси на архітектуру «нульової довіри», які автоматизують перевірку того, що хакери не отримують доступу до секретних даних, повідомляє Defense One. Мета проєкту – встановити «нульовий рівень довіри» вже до 2027 року.

Сьогодні автоматизація допомагає виявляти та реагувати на кіберзагрози швидше та ефективніше, ніж здатна людина. Вона також може допомогти керувати складними мережами та системами, які потребують великої кількості ресурсів та часу.

«Ми повинні бути здатними швидко адаптуватися до мінливої обстановки», — сказав журналістам генерал-лейтенант Марія Барретт. «Ми повинні бути здатними швидко ухвалювати рішення і діяти».

Барретт зазначила, що Кіберкомандування армії використовує автоматизацію для управління своєю мережею Joint Regional Security Stacks (JRSS), яка об'єднує дані із різних джерел для забезпечення безпеки. Автоматизація допомагає морпіхам швидше отримувати інформацію та приймати рішення на полі бою.

Проте автоматизація — не значить, що треба відмовитися від людського чинника. Військові служби наголошують, що автоматизація має бути прозорою та контрольованою людиною.

Барретт також зазначила, що автоматизація потребує навчання та культурних змін у військових організаціях. «Ми повинні навчати наших людей тому, як використовувати автоматизацію та як довіряти їй», — сказала вона.

Автоматизація також потребує співробітництва між військовими службами та Пентагоном для створення єдиних стандартів та практик.

Зрештою автоматизація допоможе Пентагону і військовим службам підвищити свою кіберстійкість та ефективність в умовах кіберзагроз, що постійно змінюються…» ***(У Пентагоні побоюються хакерів із Росії та Китаю: що вигадали військові // Фокус (https://focus.ua/uk/digital/564089-u-pentagoni-poboyuyutsya-hakeriv-iz-rosiyi-ta-kitayu-sho-vigadali-vijskovi). 03.05.2023).***

***

«Напередодні саміту Ради Європи, який розпочнеться у вівторок, спостерігався сплеск спроб кібератак проти ісландської інфраструктури…

CERT-IS, ісландська команда з кібербезпеки, повідомила про незвично велику кількість комп'ютерних атак на ісландські компанії та установи напередодні саміту Ради Європи, який відбудеться в Рейк'явіку у вівторок і в середу.

Метою цих атак не обов'язково є крадіжка даних або руйнування системи, а скоріше здійснення величезного тиску на системи, що призводить до тимчасового колапсу, заявив Гугмундур Арнар Сігмундссон, директор CERT-IS.

Гудмундур припустив, що ці напади, ймовірно, здійснюють групи, які симпатизують Росії, і їхня головна мета – посіяти хаос.

«Це типова картина, яку спостерігають під час подібних міжнародних зустрічей. Перед початком заходу роблять спроби зламати системи, а як тільки зустрічі починаються, атаки посилюються», – пояснив він.

Ісландія, яка головує в Комітеті міністрів Ради Європи, організовує саміт глав держав та урядів, який збере 46 держав-членів 16-17 травня в Рейк'явіку.

Це 4-й саміт Ради Європи з моменту її створення у 1949 році.

Саміт буде присвячений основним цінностям Ради Європи та підтримці України через конкретні заходи, спрямовані на досягнення справедливості для жертв російської агресії.

Президент Володимир Зеленський у вівторок, 16 травня, виступить на сесії відкриття саміту Ради Європи». ***(Напередодні саміту Ради Європи зафіксували серію кібератак проти інфраструктури Ісландії // Європейська правда (https://www.eurointegration.com.ua/news/2023/05/16/7161764/). 16.05.2023).***

***

«Серія скоординованих кібератак, спрямованих на те, щоб поставити під загрозу шанси скандинавської країни на вступ до НАТО, завдала шкоди її найбільшим компаніям.

З лютого таємнича хакерська група, що іменує себе Anonymous Sudan, атакувала десятки шведських аеропортів, лікарень і банків за допомогою розподілених атак типу «відмова в обслуговуванні», нібито у відповідь на спалення Корану перед посольством Туреччини в Стокгольмі на початку цього року.

Так звані DDoS-атаки, які переводять веб-сайти та служби в автономний режим, перевантажуючи їх інтернет-трафіком, порушили онлайн-програми Національної громадської телекомпанії Швеції і вивели з ладу веб-сайти Scandinavian Airlines, державної енергетичної компанії Vattenfall і оборонної фірми Saab AB. Про це пише Bloomberg.

Група, що стоїть за цією кампанією, стверджує, що складається з хактивістів зі східноафриканської країни, метою яких є переслідування «всіх, хто виступає проти ісламу».

Але більш уважне вивчення записів Anonymous Sudan у соціальних мережах - і даних про атаки - показує, що група не є ні суданською, ні ісламістською, говорить Маттіас Волен, який керував розслідуванням злому для Truesec, однієї з найбільших шведських фірм з кібербезпеки.

За його словами, Anonymous Sudan має ознаки того, що є добре організованим підрозділом росіян, які розбираються в шведській політиці та соціальних проблемах. «Їхня очевидна мотивація полягає в тому, щоб організувати атаки, спрямовані на посилення напруженості у відносинах із мусульманською меншиною країни і чинення тиску на Туреччину, щоб вона твердо відкинула заявку Швеції на вступ до НАТО. Якби їм це вдалося, це могло б зробити Швецію більш вразливою для майбутніх нападів», - зазначив Волен.

За словами Волена, загальнодоступна інформація в Telegram-каналі групи містила підказки про її справжнє походження. Так, у розділі біографії Anonymous Sudan у якості основної мови вказано російську, а місцезнаходження - Росія. Група також приєдналася до проросійської політичної хакерської групи Killnet, яка націлена на організації та країни, які виступають проти війни в Україні. Крім того, офіційний акаунт, що належить хакерському колективу Anonymous, заперечує будь-який зв'язок з групою.

Ще одна підказка полягає в тому, що Anonymous Sudan, здається, добре фінансується. За даними іншої шведської компанії з кібербезпеки Baffin Bay Networks, замість того, щоб використовувати мережі заражених комп'ютерів для дешевих атак - як зазвичай проводять атаки хактивісти - група орендувала 61 сервер у Німеччині у підрозділу IBM Corp. SoftLayer. Через два тижні після початку атак Anonymous Sudan компанія Baffin Bay заявила, що працювала з IBM над відключенням серверів.

«IBM співпрацює з галузевими партнерами і правоохоронними органами для виявлення і припинення зловмисного використання платформи IBM Cloud, як це сталося в даному випадку. Ми цінуємо співпрацю Baffin Bay Networks в цьому питанні», - йдеться в заяві IBM.

Професор міжнародних відносин в Норвезькому інституті оборонних досліджень Катажина Зіск зазначає, що знання хакерами релігійних і політичних точок тертя в Швеції, а також схожість атак з іншими російськими операціями впливу, наштовхують до висновку, що група контролювалася або управлялася російськими спецслужбами.

Сама група Anonymous Sudan заперечує твердження про те, що працює від імені Росії. «Ми не маємо ніякого відношення до Росії. Ми допомагаємо їм, тому що вони допомагали нам раніше, і це спосіб відплатити», - написала група в Telegram після того, як Truesec опублікувала звіт.

Зазначається, що атаки Anonymous Sudan демонструють, що російські хакери знаходять нові способи втручання в політичні процеси демократичних супротивників РФ. Вони стають усе більш активними в просуванні геополітичних інтересів Росії.

Всього за кілька місяців Anonymous Sudan став однією з найактивніших груп хактивістів в інтернеті й засобом просування різних інтересів Росії. Хоча угруповання здійснювало напади на різні країни, в тому числі на Данію, Францію, Німеччину, Індію та Ізраїль, експерти вважають, що її головна мета - підірвати підтримку розширення НАТО, спрямовану на посилення захисту Північної Європи від російської агресії.

За словами Волена, російська хакерська атака "вміло використовувала" політичні уразливості, а саме потребу Швеції в прихильності Туреччини і боротьбу країни з асиміляцією тисяч мусульманських біженців, щоб зробити шлях її в НАТО більш складним…» ***(Олександр Топчій. Російські хакери націлилися на Швецію, видаючи себе за ісламістів – Bloomberg // UNIAN.NET (https://www.unian.ua/techno/communications/rosiyski-hakeri-nacililisya-na-shveciyu-vidayuchi-sebe-za-islamistiv-bloomberg-12256656.html?_gl=1*k48tb*_ga*MTM5NjQ5Mjg2NC4xNjYyMDI1NDg3*_ga_TECJ2YKWSJ*MTY4NDY3OTYwMy4yLjEuMTY4NDY3OTcyOS40LjAuMA..*_ga_DENC12J6P3*MTY4NDY3OTYwMy4yLjEuMTY4NDY3OTcxMS4yMi4wLjA.*_ga_238PLP1PQZ*MTY4NDY3OTYwNS4yLjEuMTY4NDY3OTcxMS4yMi4wLjA.*_ga_P6EEJX21DY*MTY4NDY3OTYwNS4yLjEuMTY4NDY3OTcxMS4yMi4wLjA.). 15.05.2023).***

***

«Киберконфликт имеет множество форм. Первый – это регулярный государственный шпионаж с целью получения информации. Например, как задокументировано в отчете Центра стратегических и международных исследований (CSIS), в 2013 году китайские хакеры украли конструкции американского оружия и нацелились на гражданские и военные морские операции в Южно-Китайском море. В том же году, как показал Эдвард Сноуден, Соединенные Штаты вели кибершпионаж против китайских целей. Атака SolarWinds в 2020 году, совершенная подразделением российской военной разведки, проникла в министерства финансов и внутренней безопасности США, а также в ряд частных организаций.

Второй — шпионаж в пользу промышленных технологий, осуществляемый как частными, так и государственными субъектами, а также их комбинациями. В качестве одного из многих примеров, еще в 2011 году ФБР сообщило о 11 миллионах

долларов убытков американских предприятий китайским торговым компаниям. В 2021 году российские и китайские спецслужбы нацелились на Европейское агентство по лекарственным средствам и украли документы, касающиеся вакцин и лекарств от COVID-19. В 2022 году фирма по кибербезопасности Cyberreason сообщила о «массовом взломе коммерческой тайны китайцами» компанией Winnti APT Group, «которая специализируется на кибершпионаже и краже интеллектуальной собственности и, как считается, работает в интересах китайского государства».

Третий — атаки программ-вымогателей с целью получения прибыли, что является основным сектором роста для кибермира. Только в 2021 году Colonial Pipeline стала объектом атаки программы-вымогателя со стороны российской хакерской группы DarkSide, а крупнейшая в мире мясоперерабатывающая компания JBS стала жертвой атаки программы-вымогателя со стороны российской группы REvil.

Колониальный трубопровод — крупнейший нефтепровод нефтепереработки в Соединенных Штатах, протянувшийся от Техаса до Нью-Йорка и транспортирующий 3 миллиона баррелей топлива каждый день. Атака DarkSide заключалась в самом обычном взломе пароля — несмотря на то, что Colonial Pipeline инвестировала 200 миллионов долларов в ИТ-системы, включая кибербезопасность, — и привела к острой нехватке газа на юго-востоке США. Генеральный директор Colonial Pipeline принял решение заплатить выкуп в размере 5 миллионов долларов США / 75 биткойнов, а затем уведомить власти. Позже министерству юстиции США удалось вернуть не менее 2,3 миллиона долларов (60 биткойнов) в криптовалюте.

Атака REvil на JBS привела к хакерской атаке, которая привела к остановке операций в США, Канаде и Австралии. JBS быстро выплатила хакерам выкуп в размере 11 миллионов долларов в биткойнах, чтобы восстановить операции. Его значение отражено в том факте, что JBS обеспечивает пятую часть всей говядины и свинины, потребляемой в Соединенных Штатах. Все эти взломы осложняются тем, что правительство США мало контактирует с частными лицами, подвергшимися атаке, а российское правительство, среди прочего, получает прибыль и предоставляет прикрытие хакерам, которые соглашаются не атаковать его.

Четвертый — саботаж государства в отношении промышленных предприятий, коммунальных служб и банков. Яркими примерами являются американо-израильская атака Stuxnet на Иран и российская атака на Украину. 17 июня 2010 года иранцы начали сообщать о машине, которая снова и снова перезагружалась, чтобы саботировать центрифуги (важнейшие системы промышленного контроля, являющиеся неотъемлемой частью очистки радиоактивного урана). Этот «Stuxnet» был первым случаем киберсаботажа (использование цифрового кода, разработанного для уничтожения чего-то физического) и, как тогда считалось, был частью длительной американской кампании кибероперации против иранской ядерной программы, известной как Олимпийские игры. который начался во время президентства Джорджа Буша-младшего и продолжился при Бараке Обаме.

За последние несколько лет Украина пережила множество кибератак со стороны России, которые нанесли ущерб украинским СМИ, финансам, транспорту,

военным, политикам, электроэнергетике и энергетике. Эти атаки были рассчитаны и проведены в попытке саботировать и контролировать Украину.

Пятая — киберполитические кампании, направленные на то, чтобы повлиять или подорвать политические процессы или поддержать сепаратистские движения. Они прямо нацелены на «политическую независимость» и «территориальную целостность» и, таким образом, приводят в действие мощные нормы против агрессии и в пользу ответных мер самообороны. В 2016 году, в известном случае, было обнаружено, что Россия повлияла на выборы в США в 2016 году через Facebook. Основными последствиями были хакерские атаки на 39 баз данных избирателей штатов, предвыборный штаб Клинтон, Национальный комитет Демократической партии и Комитет по кампании Демократической партии в Конгрессе. Политически дискредитирующая информация была опубликована и распространена в качестве пропаганды в социальных сетях, а избирательные участки в некоторых регионах были остановлены из-за фальсификации в день выборов. ФБР стало известно об этих российских зарубежных кибератаках за несколько месяцев до выборов, но оно не смогло остановить и предотвратить массовые атаки, исходящие от множества разных хакеров.

В начале 2018 года Министерство юстиции США обвинило двенадцать российских разведчиков во взломе, хотя Кремль отрицал свою причастность. Эти атаки продолжались». ***(Michael W. Doyle. 5 types of cyberattacks target everything from food to pipelines to democracy // Freethink Media, Inc. (https://bigthink.com/the-present/5-types-cyberattacks/). 19.05.2023).***

***

«Официальные лица США считают, что китайские хакеры все еще могут иметь доступ к конфиденциальным компьютерным сетям США, на которые они нацелились в последние месяцы, поскольку высокопоставленный американский кибер-чиновник сказал CNN, что он обеспокоен «размахом и масштабом» деятельности.

Недавно раскрытая хакерская кампания, поддерживаемая китайским правительством, нацеленная на ключевые секторы США, такие как морские и транспортные сети, «неприемлема», поскольку хакеры искали доступ к сетям, которые могли бы позволить им нарушить работу критически важных служб в будущем, заявил директор Агентства национальной безопасности по кибербезопасности. Роб Джойс сказал в интервью в четверг.

Официальные лица США все еще пытаются проверить, были ли китайские хакеры изгнаны из сетей, которые они взломали в течение многомесячной кампании, сказал Джойс, добавив, что АНБ расследует хакерские усилия Китая с прошлого года.

Китайские хакеры нацелились на неназванную организацию на тихоокеанской территории США в Guam в рамках вероятных усилий по разработке возможностей, которые могут нарушить «критическую коммуникационную инфраструктуру» между США и Азией в случае кризиса, заявила Microsoft, раскрывая активность в среду.

Предполагаемое нападение на критически важную инфраструктуру на Guam усиливает сохраняющиеся опасения США в отношении того, что Китай может использовать свои кибервозможности в ожидании будущего конфликта с США в Тихом океане.

Хакеры пытались внедриться во многие организации, не имеющие очевидной разведывательной ценности, и «подготовить» себя в компьютерных сетях США для потенциальных будущих операций, сказал Джойс CNN.

США и их союзники немедленно усилили выводы Microsoft в среду и призвали операторов инфраструктуры проверить свои сети на наличие компрометации. Китайское правительство отвергло обвинения и, в свою очередь, обвинило США в проведении хакерских операций в Китае.

Это новый фронт напряженности в киберпространстве, который годами пронизывал отношения США и Китая. Это следует за возмущением в США по поводу китайского воздушного шара-шпиона, сбитого Пентагоном в феврале.

По словам официальных лиц США и частных экспертов, Россия тоже давно пытается закрепиться в критически важной инфраструктуре США. Но Джойс, проработавший в АНБ более двух десятилетий и работавший над наступательными кибероперациями, сказал, что недавно обнаруженная китайская деятельность привлекла его внимание.

«Я думаю, что разница здесь в том, насколько дерзкой она является по размаху и масштабу», — сказал Джойс CNN. «Поэтому нам нужно дать всем возможность защищаться от него».

Опасения по поводу Тайваня

По словам Джойса, АНБ — крупное американское агентство электронного шпионажа с зарубежной миссией — использовало свои разведывательные возможности для изучения инструментов китайских хакеров и проверки конфиденциальной инфраструктуры США, на которую они нацелились. По данным Microsoft, помимо морских и транспортных организаций, хакеры преследовали правительственные учреждения США, а также производственные и строительные фирмы.

«Мы считаем, что это предвзятое отношение к критически важной инфраструктуре — в более широком смысле, чем просто [потенциальное] прерывание связи», — сказал Джойс CNN, добавив: «Мы согласны с оценкой Microsoft».

Нападение на Гуам вызывает особую озабоченность, поскольку он играет ключевую роль в военных усилиях США по противодействию и сдерживанию территориальных амбиций Китая в Тихом океане. Корпус морской пехоты США в январе выбрал Гуам в качестве места для открытия своей первой за 70 лет новой базы, на которой, по официальным данным, могут разместиться 5000 морских пехотинцев.

Республиканский член палаты представителей Майк Галлахер из Висконсина заявил CNN в четверг, что «военная мобильность США в Индо-Тихоокеанском регионе абсолютно необходима для нашей безопасности», выразив при этом обеспокоенность по поводу новой предполагаемой китайской хакерской операции.

Официальные лица США обеспокоены тем, что китайские хакеры создали плацдармы в критически важной инфраструктуре Тайваня, которые Пекин может использовать для отключения ключевых услуг, таких как электричество, в случае китайского вторжения на Тайвань, заявил журналистам в марте высокопоставленный представитель министерства обороны США.

«Практически нет никаких сомнений в том, что, если США будут непосредственно вовлечены в конфликт с Китаем из-за Тайваня, Китай будет стремиться использовать свои кибервозможности, чтобы сделать вооруженные силы США менее эффективными в бою», — сказал Джамиль Н. Джаффер, основатель и исполнительный директор Института национальной безопасности юридического факультета Университета Джорджа Мейсона.

«Учитывая это, доступ к критически важной инфраструктуре, которую Китай развивает на Гуаме и в других местах, представляет собой важный и растущий риск для способности США эффективно реагировать в случае конфликта с Китаем», — сказал Джаффер CNN.

Тайваньские эксперты по кибербезопасности увидели в отчете Microsoft знакомого врага и тут же начали проверять свои системы на наличие признаков компрометации.

«Мы видели подобные методы и атаки на Тайване, — сказал Сун-тинг Цай, генеральный директор тайваньской компании по кибербезопасности TeamT5. Цай сказал, что его аналитики все еще проводят расследование, но не смогли сопоставить хакеров, упомянутых Microsoft, с известной китайской хакерской группой.

Более длинная игра, в которую некоторые китайские хакеры играют на Тайване, заключается в том, чтобы «проникать в целевые сети [и] среды, делать все возможное, чтобы стать невидимыми, оставаться в критически важных системах, а затем вносить сбои, когда им это нужно», — сказал Цай CNN». ***(Sean Lyngaas. US officials believe Chinese hackers may still have access to key US computer networks // Cable News Network (https://edition.cnn.com/2023/05/26/politics/us-chinese-hackers-rob-joyce). 26.05.2023).***

***

«Агентства кибербезопасности из Канады, США, Австралии, Новой Зеландии и Великобритании, известные как Five Eyes, опубликовали предупреждение о кибератаке, спонсируемой Китаем.

«Это предупреждение предназначено для ИТ-специалистов и руководителей уполномоченных организаций», — говорится в заявлении Канадского центра кибербезопасности.

В совместном бюллетене на 24 страницах говорится, что некоторые программные и аппаратные компоненты, такие как маршрутизаторы, могут быть затронуты.

В бюллетене утверждается, что компании частного сектора выявили спонсируемую Китаем хакерскую группу, известную как Volt Typhoon, которая нацелена на критически важную инфраструктуру США. Тактика включает в себя стирание своего следа и использование встроенных инструментов для достижения своих целей.

Китайское правительство отвергло обвинения и заявило, что хакером был США, сообщает Reuters.

Microsoft также выпустила заявление с рекомендациями, включая смену паролей и использование многофакторной аутентификации для защиты сетевых систем.

Схема атаки Volt Typhoon от Microsoft от 24 мая 2023 г. Фото предоставлено Microsoft / www.microsoft.com

Профессор международных отношений и политологии Университета Торонто Аурел Браун заявил, что участие «Пяти глаз» означает широкомасштабную атаку, не направленную на конкретные киберинфраструктуры.

«Это важно, особенно для Соединенных Штатов, потому что они не хотят, чтобы это рассматривалось просто как своего рода двусторонний спор», — сказал Браун.

Браун, который также является сотрудником Центра Дэвиса в Гарвардском университете, сказал, что реакция Китая на то, что США являются хакером в этом случае, известна в психологии как проекция. Это дипломатическая тактика, используемая со времен Советского Союза.

«Должны ли мы что-то с этим делать? Мы должны были сделать это вчера», — сказал он.

Кроме того, он сказал, что Канада и США должны применять тактику, применяемую Эстонией, которая создала «своего рода группы кибер-спецназа, которые могут действовать… и они разработали огромное количество навыков защиты от кибератак».

Браун сказал, что Канада должна защищать важные активы, такие как электрическая сеть, которая уязвима.

«Мы должны иметь возможность также нанести им киберущерб», — сказал он.

Заместитель декана непрерывного профессионального обучения в колледже Хамбер Фрэнсис Симс сказал, что нет ничего бесплатного, и люди должны быть осторожны, предоставляя свои данные в Интернете.

Симс, который также является профессором кибербезопасности, сказал, что каждые 39 секунд происходит кибератака, и около 98 процентов из них основаны на социальной инженерии, которая «эффективно заставляет кого-то делать то, что он не должен делать, когда речь идет о кибербезопасности.»

По его словам, причины атаки, подобной той, о которой сообщила Five Eyes, включают слежку, срыв и получение денежной выгоды.

И Браун, и Симс предупредили об использовании китайских технологий, включая такие платформы, как TikTok.

«Несколько лет назад в Китае правительство приняло закон, согласно которому в случае возникновения какой-либо угрозы национальной безопасности или предполагаемой угрозы правительство может изъять документы любой китайской компании в любое время», — сказал Симс». ***(Antonio Peláez Barceló. Canada needs better protection against cyberattacks, experts say // Humber News (https://humbernews.ca/2023/05/canada-needs-better-protection-against-cyberattacks-experts-say/). 25.05.2023).***

***

«…Киберсилы теперь являются неотъемлемой частью ударного потенциала страны в военное время. Соединенные Штаты даже сейчас планируют кибератаки военного времени против Китая, если они понадобятся. По данным на 2018 год, у американцев есть около 240 000 сотрудников оборонных ведомств и подрядчиков, которые вносят свой вклад в киберзащиту и кибератаки, причем, вероятно, до одной трети доступно для поддержки последних.

В случае войны эти кибератаки США могут быть выдержаны во всем диапазоне военных возможностей Китая. Цель состоит в том, чтобы добиться так называемого «доминирования в принятии решений». Это «распад» китайских систем и системы принятия решений, «таким образом, поражение их наступательных возможностей» — если мы можем интерпретировать высказывания бывшего командующего Индо-Тихоокеанским командованием США адмирала Филипа Дэвидсона как ссылку на Китай.

Австралия гораздо более осторожно относится к киберпреступлениям, чем США, но оба союзника идут в ногу. Канберра находится в процессе утроения численности своих наступательных кибервойск в рамках проекта Redspice, о котором было объявлено в прошлом году.

В случае войны он может атаковать объекты военного командования и управления в любой точке Китая. Более легкие цели могут включать критически важную национальную инфраструктуру, такую как энергосистема, поддерживающая военные действия.

Киберсила Австралии останется небольшой по сравнению с США. Но он также может призвать частные отечественные или иностранные корпорации к разработке пакетов атак против Китая, как это делают США.

Австралия стремится к наступательным возможностям мирового класса в киберпространстве. Союзники AUKUS тесно координируют свои действия в кибероперациях, и эта область деятельности является основным направлением деятельности новой группировки.

В 2020 году Соединенное Королевство создало новую организацию — Национальные киберсилы, занимающиеся наступательными ударными операциями.

В рамках этого альянса «кибер-тройки» с США и Великобританией киберсилы Австралии, вероятно, останутся самым мощным ударным потенциалом страны против Китая на десятилетия вперед.

Конечно, кибератаки не гарантируют успеха. Но вызвать сбои в значительных масштабах можно с помощью целенаправленных усилий на всех этапах наступательных кибероперациий, особенно в координации с нашими союзниками.

Наиболее важным этапом является первый: обеспечение актуальной информации о системах другой стороны. Усилия, приложенные к киберразведке против вооруженных сил Китая, на самом деле являются основой кибернаступательных групп, даже если разведчики не считаются играющими «наступательную» роль.

Китай отлично разбирается в киберпреступлениях. Но, вопреки распространенному мнению, кибербезопасность не является сильной стороной Китая, и это делает его особенно уязвимым для атак в военное время. Международный институт стратегических исследований подсчитал, что у Китая есть определенные фундаментальные недостатки, на преодоление которых уйдет много лет, в том числе в сфере кибербезопасности, образовании и политике.

Китайские лидеры считают, что они значительно отстают от США и их союзников с точки зрения военных кибервозможностей. Это, вероятно, ограничит их выбор в отношении начала войны за Тайвань.

Австралии не нужно стесняться этой наступательной способности против Китая по политическим мотивам, потому что Китай планирует сделать то же самое против нас в случае войны.

Китай уже ведет кибершпионаж в отношении Австралии и других стран в рамках подготовки к крупному кризису. Он почти наверняка разрабатывает возможности для вывода из строя военных систем и инфраструктуры противника, если это необходимо.

Министр обороны Ричард Марлес недавно повторил давнее мнение о том, что чем больше у нас наступательных возможностей, например, за счет подводных лодок, тем больше страна может внести свой вклад в союзническое сдерживание потенциальных агрессоров.

Австралийские политические лидеры должны уделить первоочередное внимание способности вооруженных сил атаковать цели в Китае в крупном масштабе в маловероятном случае войны. И лидеры должны обеспечить, чтобы кибер-силы имели больше высококвалифицированных людей, посвященных этой задаче, и более мощную отечественную кибер-индустрию.

Для того чтобы военные и политические лидеры более уверенно шли по этому пути, Силам обороны Австралии также необходимо будет провести переоценку военного баланса сил в Азиатско-Тихоокеанском регионе с учетом киберпревосходства США и их союзников над Китаем.

Это также может позволить австралийцам чувствовать себя более уверенно в отношении возможных китайских военных угроз. Выбор, который китайские лидеры могут сделать, спровоцировав кризис, будет определяться их мнением о том, что их вооруженные силы не так конкурентоспособны в этом аспекте военной мощи США и их союзников». ***(Greg Austin. Deterring China isn't all about submarines. Australia's 'cyber offence' might be its most potent weapon // The Conversation Media Group Ltd***

(https://theconversation.com/deterring-china-isnt-all-about-submarines-australias-cyber-offence-might-be-its-most-potent-weapon-204749). 04.05.2023).

***

Кіберзахист закладів охорони здоров'я

«Министерство здравоохранения и социальных служб США (HHS) продолжает играть центральную роль, помогая организациям здравоохранения защищаться от угроз кибербезопасности, выпуская сводки по кибербезопасности и новую структуру кибербезопасности за последние 60 дней.

6 апреля 2023 г. HHS предупредила медицинские организации об угрозе кибербезопасности для электронных медицинских карт (EMR/EHR). Этот последний брифинг об угрозах является одним из первых, выпущенных для организаций здравоохранения в рамках новой системы кибербезопасности HHS (и следует за предыдущим брифингом «Тенденции эксфильтрации данных в здравоохранении»).

В дополнение к конкретным брифингам по ключевым областям киберриска HHS представила новую структуру через Администрацию агентства по стратегической готовности и реагированию (ASPR) для оказания помощи организациям здравоохранения в реагировании на киберугрозы. Это новое руководство — «Руководство по внедрению кибербезопасности» — является продуктом государственно-частного партнерства, призванного улучшить управление киберрисками в эпоху роста числа кибератак в сфере здравоохранения.

Руководство содержит ряд добровольных передовых практик, помогающих организациям здравоохранения устранять риски кибербезопасности для таких элементов, как данные пациентов, интеллектуальная собственность, производство медицинского оборудования и исследования. Эти методы охватывают идентификацию и управление рисками, контроль доступа и мониторинг цепочки поставок, а также корпоративное управление программами управления киберрисками. В руководстве подчеркивается важность того, чтобы советы директоров рассматривали кибербезопасность как проблему управления рисками в масштабах всего предприятия, а не просто как проблему ИТ.

С помощью этого руководства HHS стремится помочь государственным и частным организациям здравоохранения привести свои программы информационной безопасности в соответствие с концепцией кибербезопасности, разработанной Национальным институтом стандартов и технологий (NIST). NIST недавно выпустил предлагаемое обновление для этой структуры в январе вместе с новой структурой для искусственного интеллекта (ИИ)...

ASPR разработал руководство совместно с рабочей группой по кибербезопасности Координационного совета сектора здравоохранения (в которую входят медицинские компании, больницы и отраслевые группы) при участии NIST и других федеральных агентств. Этот проект следует за объявлением Белого дома о Национальной стратегии кибербезопасности ранее в марте, призывающим к сотрудничеству частного и государственного секторов против киберугроз критической инфраструктуре.

Сектор здравоохранения является особенно важной мишенью для субъектов киберугроз и подобные рекомендации могут помочь организациям устранить бреши в своей защите». ***(Natasha G. Kohne, Michelle A. Reed, Joseph Hold. HHS Unveils New Cybersecurity Guide // Akin Gump Strauss Hauer & Feld LLP (https://www.akingump.com/en/insights/blogs/ag-data-dive/hhs-unveils-new-cybersecurity-guide). 10.05.2023).***

***

«Во время пандемии Covid-19 в начале 2021 года компьютеры ирландской системы здравоохранения были взломаны хакерами, которые получили доступ к файлам пациентов и разместили сотни таких файлов в Интернете. В результате сеть пришлось отключить.

Реверберации были широко распространены, поскольку встречи были отменены, самые конфиденциальные данные людей были украдены, и даже такие процедуры, как компьютерная томография, были остановлены. Атака стала одним из крупнейших взломов поставщика медицинских услуг в мире.

Имейте в виду разрыв

«В настоящее время существует серьезный пробел в возможностях кибербезопасности здравоохранения», — сказал Христос Ксенакис, профессор цифровых систем Пирейского университета в Греции. «Больницы должны работать должным образом и защищать наши данные».

С мая 2021 года по июнь 2022 года агентство ЕС по кибербезопасности — ENISA — обнаружило в государствах-членах в общей сложности 623 инцидента с программами-вымогателями, аналогичными инциденту в Ирландии. Здравоохранение было пятым наиболее целевым сектором этих атак.

Это, в свою очередь, привело к увеличению инвестиций и технологическому развитию отрасли. Ученые, медицинские работники и правительства все чаще принимают меры для предотвращения сценариев, подобных ирландскому.

Ответ заключается не только в лучшем программном обеспечении. Кибербезопасность чаще всего связана с людьми и изменением их поведения.

К такому выводу пришла Сабина Магалини, профессор хирургии Католического университета Святого Сердца в Риме, Италия.

Она координировала финансируемый ЕС проект PANACEA по улучшению кибербезопасности больниц. Инициатива длилась 38 месяцев до февраля 2022 года.

Человеческие ошибки

«Человеческая ошибка — один из основных рисков кибербезопасности для больниц, — сказал Магалини. «Риск лежит на людях, что логично. Больница — это не атомная электростанция, и ее нельзя закрыть таким же образом».

Больницы, как правило, оживленные места. Персоналу необходимо выполнять медицинские обязанности и одновременно работать на различных компьютерных системах.

Исследования во время PANACEA показали, что в течение одного дня медсестрам часто приходилось входить в компьютерные системы более 80 раз.

Это отнимает много времени и приводит к сокращению пути, в том числе к тому, что один и тот же пароль используется группой людей или пароли записываются на листе бумаги рядом с компьютером.

В целом исследование показало, что персонал больницы плохо соблюдал меры предосторожности в области кибербезопасности и в процессе оставлял лазейку, которую могли использовать злоумышленники.

«Нам необходимо улучшить взаимодействие между медицинскими работниками и компьютерами, — сказал Магалини. «Как врач или медсестра, вы одновременно лечите пациента и пользуетесь компьютером. Это беспокойно.

Меры безопасности

PANACEA придумала, как облегчить сотрудникам больниц соблюдение мер предосторожности в области кибербезопасности. Одним из примеров является программное обеспечение, обеспечивающее более безопасную систему входа в систему.

«Программное обеспечение позволяет распознавать лица медицинских работников, — сказал Магалини. «Это позволит избежать проблем, которые мы наблюдаем сегодня с паролями».

Проект также экспериментировал с низкотехнологичными альтернативами. Исследователи расклеили наклейки и плакаты в участвующих больницах, чтобы подтолкнуть медицинских работников к выполнению основных процедур кибербезопасности.

По словам Магалини, образование также должно сыграть свою роль, в том числе для врачей.

«Обучение кибербезопасности должно быть включено в их программы ординатуры», — сказала она.

Упрощенный обмен

Другой проект, финансируемый ЕС, CUREX, способствовал обмену медицинской информацией между больницами. Ксенакис из Пирейского университета координировал проект, который длился 40 месяцев до марта 2022 года.

«Данные о здоровье — это самые конфиденциальные данные», — сказал он. «Хакеры платят больше за данные о здоровье, чем за информацию о кредитных картах».

При отправке информации о пациенте в другое медицинское учреждение больница может не знать о мерах кибербезопасности получателя.

CUREX обратился к этой неопределенности.

В рамках проекта разработано программное обеспечение, которое может помочь обнаружить любые уязвимости в системе безопасности сторонней организации. Система упрощает для медицинских учреждений обмен информацией в соответствии с правилами защиты данных ЕС.

— Все дело в оценке риска, — сказал Ксенакис. «А для этого вам нужно знать, насколько безопасна другая организация».

Последующая работа

Европейские исследователи и организации по кибербезопасности вкладывают средства в ответы на эти вопросы.

В продолжение PANACEA и CUREX ЕС софинансирует закупки средств кибербезопасности для больниц, покрывая 50% стоимости новых мер.

Так что даже несмотря на то, что атаки на европейские больницы продолжаются регулярно, эксперты видят повод для оптимизма в отношении будущего.

«Европейские поставщики кибербезопасности быстро становятся более зрелыми, — сказал Ксенакис. «В свою очередь, больницы осознают необходимость покупать новые инструменты и повышать уровень их безопасности». ***(Tom Cassauwers. The race to make hospitals cybersecure // European Commission (https://ec.europa.eu/research-and-innovation/en/horizon-magazine/race-make-hospitals-cybersecure). 24.05.2023).***

***

Захист персональних даних та соціальні мережі

«Amazon, Google, Microsoft и другие поставщики облачных услуг, не входящие в Европейский Союз, желающие получить метку кибербезопасности ЕС для обработки конфиденциальных данных, могут сделать это только через совместное предприятие с компанией из ЕС, согласно проекту документа ЕС, с которым ознакомился Reuters.

В документе говорится, что американские технологические гиганты и другие лица, участвующие в совместном предприятии, могут иметь только миноритарный пакет акций, а сотрудники, имеющие доступ к данным ЕС, должны будут пройти специальную проверку и должны находиться в блоке из 27 стран.

В документе добавлено, что облачная служба должна управляться и поддерживаться из ЕС, а все данные клиентов облачной службы должны храниться и обрабатываться в ЕС, а законы ЕС имеют приоритет над законами других стран в отношении поставщика облачных услуг.

Последний проект предложения от агентства по кибербезопасности ЕС ENISA касается схемы сертификации ЕС (EUCS), которая будет ручаться за кибербезопасность облачных сервисов и определять, как правительства и компании в блоке выбирают поставщика для своего бизнеса.

Хотя новые положения подчеркивают озабоченность ЕС по поводу вмешательства со стороны государств, не входящих в ЕС, они, вероятно, вызовут критику со стороны американских технологических гигантов, обеспокоенных тем, что их не пускают на европейский рынок.

Big Tech надеется, что рынок государственных облачных услуг будет стимулировать рост в ближайшие годы, в то время как потенциальный бум ИИ после вирусного успеха OpenAI ChatGPT также может повысить спрос на облачные услуги.

«Сертифицированные облачные сервисы управляются только компаниями, базирующимися в ЕС, при этом ни одна организация из-за пределов ЕС не имеет эффективного контроля над CSP (поставщиком облачных услуг), чтобы снизить риск

вмешательства властей, не входящих в ЕС, подрывающих правила, нормы и ценности ЕС.», — говорится в документе.

«Предприятия, чей зарегистрированный головной офис или штаб-квартира не зарегистрированы в эмигрирующем государстве ЕС, не должны, прямо или косвенно, единолично или совместно, иметь положительный или отрицательный эффективный контроль над CSP, подающей заявку на сертификацию облачной службы», — говорится в сообщении.

В документе говорится, что более жесткие правила будут применяться к персональным и неличным данным особой важности, нарушение которых может оказать негативное влияние на общественный порядок, общественную безопасность, жизнь или здоровье людей или защиту интеллектуальной собственности.

По словам источника в отрасли, последний проект может привести к фрагментации единого рынка ЕС, поскольку каждая страна имеет полное право вводить требования, когда сочтет это целесообразным.

Торговая палата США ранее заявляла, что план ставит американские компании в неравное положение.

ЕС заявляет, что эти шаги необходимы для защиты прав блока на данные и конфиденциальности.

Страны ЕС рассмотрят проект в конце этого месяца, после чего Европейская комиссия примет окончательную схему». ***(Foo Yun Chee. EU proposes tougher cyber security labelling rules for Amazon, Google, Microsoft // nextmedia Pty Ltd. (https://www.itnews.com.au/news/eu-proposes-tougher-cyber-security-labelling-rules-for-amazon-google-microsoft-594192). 10.05.2023).***

***

«Расследование крупной утечки данных о состоянии здоровья в Европе показывает, как трудно расследовать крупное дело с участием многих тысяч жертв, а также то, на что способен хакер, чтобы вымогать деньги.

После кибератаки на лечебный психотерапевтический центр в Хельсинки в 2020 году преступник пригрозил разместить в Интернете конфиденциальные записи пациентов, если клиника Вастаамо не заплатит 40 биткойнов, что на тот момент эквивалентно примерно 400 000 евро. Когда клиника не заплатила, хакер вынудил отдельных пациентов заплатить с помощью запугивающих электронных писем.

«Это жестокое преступление, — сказал Паси Вайнио, окружной прокурор Финляндии, курирующий это дело.

Группы здравоохранения по всему миру подвергаются нападениям со стороны киберпреступников, а некоторые злоумышленники используют личную информацию о пациентах. Хакеры разместили обнаженные фотографии больных раком в Интернете после февральской кибератаки на сеть здравоохранения Lehigh Valley Health Network в Аллентауне, штат Пенсильвания.

В деле Вастаамо одна жертва сказала, что хакер дал ей 24 часа, чтобы заплатить около 200 евро в биткойнах, иначе ее записи о лечении будут опубликованы. Тийна Парикка, тренер по развитию лидерства, которая живет за пределами Хельсинки, рассказала, что у нее были приступы паники, она две недели не ходила на работу и позвонила на горячую линию после попытки вымогательства.

«Как будто кто-то пришел ко мне домой и угрожал мне ножом», — сказала она.

Спустя два с половиной года после кибератаки финские правоохранительные органы находятся на завершающей стадии уголовного расследования.

В феврале полиция Франции арестовала подозреваемого по делу Вастаамо и экстрадировала его в Финляндию. Марко Лепонен, старший инспектор Национального бюро расследований Финляндии, заявил, что подозреваемый отрицает свою причастность к преступлению. Следователи должны закончить сбор доказательств в этом месяце и предъявить обвинения к октябрю, когда истекает срок давности.

По словам следователей, это дело станет проверкой правовой системы Финляндии из-за большого количества полицейских отчетов и количества жертв. По словам финских официальных лиц, пятнадцать прокуроров изучат технические доказательства и заявления примерно 24 000 пациентов, чьи данные были раскрыты, а некоторые из них были опубликованы в Интернете. Всего пострадало 33 000 пациентов.

По словам г-на Лепонена, следователи говорят, что, по их мнению, все жертвы из Финляндии, но получение данных от поставщиков технологий, базирующихся в других регионах, требует много времени. Он отказался назвать страны, заявив лишь, что власти одних ответили через две-три недели, а власти других - два года.

«Двигаться шаг за шагом и следить за тем, что сделал подозреваемый, это очень, очень медленно», — сказал он.

По словам г-на Вайнио, прокуроры будут тратить около 10 минут на изучение каждого отчета, чтобы решить, использовать ли его в суде. По словам г-на Вайнио, логистика судебного разбирательства будет сложной, поскольку финское законодательство требует, чтобы в судах присутствовали все потерпевшие, которые хотят присутствовать. Кроме того, жертвам утечки медицинских данных гарантируется анонимность, которая может быть скомпрометирована, если появятся тысячи людей, сказал он.

«Наша правовая система не предназначена для такого рода дел», — сказал он.

Между тем г-жа Парикка заявила, что не платила хакеру и не знает, были ли ее личные данные размещены в Интернете. В качестве меры предосторожности она теперь использует услуги по замораживанию кредитов, чтобы заблокировать кредиты, взятые на ее имя. «Я не думаю, что кто-то может заверить меня, что [безопасность] какой-либо базы данных надежна», — сказала она.

Она потребовала компенсацию в размере около 11 000 евро за ущерб, причиненный ей кибератакой. Эта цифра была рассчитана на основе правительственных рекомендаций, которые рекомендуют от 1 500 до 5 000 евро за нарушение конфиденциальности, в результате которого данные были переданы очень большому количеству людей, и от 500 до 2 000 евро. для меньшего распространения.

Деньги, однако, не компенсируют весь ущерб жертвам, сказал г-н Вайнио. По его словам, по крайней мере некоторые личные данные пациентов останутся в сети, потому что финские следователи не могут удалить все случаи распространения вредоносной информации в Интернете. «Он будет там бесконечно». ***(Catherine***

Stupp. Breach of Mental-Health Records Challenges Nation's Court System // Dow Jones & Company, Inc. (https://www.wsj.com/articles/breach-of-mental-health-records-challenges-nations-court-system-4a7d42cf). 11.05.2023).

***

«Киберпреступники, атаковавшие американскую компанию спутникового телевидения Dish в начале этого года, похитили конфиденциальные данные сотрудников, сообщила компания.

В уведомлении об утечке данных, поданном компанией в Генеральную прокуратуру штата Мэн, отмечается, что примерно 300 000 человек пострадали в результате атаки программы-вымогателя.

Веб-сайты и приложения компании были отключены, ее колл-центры недоступны, а удаленные сотрудники лишены доступа к внутренним системам. Инцидент также затронул клиентов, поскольку вход в некоторые приложения канала Dish TV был невозможен.

Тысячи сотрудников

В то время информации о взломе было мало, но документы показывают, что злоумышленники украли личную информацию 296 851 человека. Диш говорит, что записи принадлежали сотрудникам (в компании работает около 16 000 человек), членам семей сотрудников и «ограниченному числу» других лиц.

Несмотря на регистрацию, мы до сих пор точно не знаем, какие данные украли хакеры. В заявлении говорится, что хакеры получили доступ к номерам водительских прав и «другим формам» идентификации, а представитель компании Эдвард Витеча отказался поделиться более подробной информацией со СМИ по этому вопросу.

Компания заявила, что «получила подтверждение того, что извлеченные данные были удалены», предполагая, что злоумышленники не будут передавать их в темную сеть. Это также свидетельствует о том, что компания пришла к соглашению с злоумышленниками и, скорее всего, заплатила выкуп.

Сообщается, что за атакой стоит группа Black Basta, и на ее сайте утечки данные Dish еще не опубликованы, что подтверждает идею о том, что сделка была заключена.

Dish, однако, не захотела прямо сказать, заплатила она требование о выкупе или нет, но и не оспаривала требование, говорится в публикации». ***(Sead Fadilpašić. Dish ransomware attack stole details from thousands of employees // Future US, Inc. (https://www.techradar.com/news/dish-ransomware-attack-stole-details-from-thousands-of-employees). 20.05.2023).***

***

«Поскольку миллионы людей используют чат-боты на основе ИИ, такие как ChatGPT, риски кибербезопасности, связанные с генеративными моделями ИИ, стали серьезной проблемой как для частных лиц, так и для компаний.

Хотя эти генеративные модели AL предназначены для облегчения общения и предоставления полезных ответов, эксперты выразили обеспокоенность тем, что они создают большие риски взлома и утечки данных, которые могут поставить под угрозу личную информацию.

Отчет Palo Alto Networks Unit 42 недавно показал, что мошенничество, связанное с ChatGPT, растет, и, несмотря на то, что OpenAI (создатель ChatGPT) предоставляет пользователям бесплатную версию ChatGPT, мошенники ведут жертв на мошеннические веб-сайты, утверждая, что им нужно платить за эти услуги.

«Они могут собрать и украсть информацию, которую вы предоставляете. Другими словами, предоставление чего-либо чувствительного или конфиденциального может подвергнуть вас опасности. Ответами чат-бота также можно манипулировать, чтобы дать вам неправильные ответы или вводящую в заблуждение информацию», — заявили исследователи из Palo Alto Networks Unit 42.

В отчете отмечается увеличение на 910% ежемесячных регистраций доменов, связанных с ChatGPT, в период с ноября 2022 года по апрель 2023 года.

ИИ давно стал частью индустрии кибербезопасности. Однако генеративный ИИ и ChatGPT оказывают глубокое влияние на будущее.

Нилеш Крипалани, генеральный директор ИТ-услуг и консалтинговой компании Clover Infotech, сказал: «ChatGPT может повлиять на ландшафт кибербезопасности за счет разработки более сложных методов социальной инженерии или фишинговых атак. Такие атаки используются, чтобы заставить людей разглашать конфиденциальную информацию или предпринимать действия, которые могут поставить под угрозу их безопасность».

Он предупредил, что благодаря способности генерировать убедительный и естественно звучащий язык «языковые модели ИИ, такие как ChatGPT, потенциально могут использоваться для создания более убедительных и эффективных методов социальной инженерии и фишинговых атак».

В марте OpenAI признал, что платежная информация некоторых пользователей могла быть раскрыта, когда ChatGPT отключился из-за ошибки.

Компания, поддерживаемая Microsoft, отключила ChatGPT из-за ошибки в библиотеке с открытым исходным кодом, которая позволяла некоторым пользователям видеть заголовки из истории чата другого активного пользователя.

OpenAI обнаружил, что ошибка могла вызвать непреднамеренную видимость «информации, связанной с платежами, у 1,2% подписчиков ChatGPT Plus, которые были активны в течение определенного девятичасового окна».

Затем OpenAI запустила программу вознаграждения за обнаружение ошибок для ChatGPT и других продуктов, предложив до 20 000 долларов исследователям в области безопасности, чтобы помочь компании отличить добросовестный взлом от злонамеренных атак, поскольку она столкнулась с нарушением безопасности.

В дополнение к рискам кибербезопасности также важно понимать, что ChatGPT может спровоцировать неправомерное использование личных данных людей.

В ходе необычного инцидента ChatGPT ложно назвал невиновного и уважаемого профессора права в США в списке ученых-правоведов, которые в прошлом подвергали студентов сексуальным домогательствам в рамках исследовательского исследования.

Джонатан Терли, заведующий кафедрой права общественных интересов Шапиро в Университете Джорджа Вашингтона, был потрясен, когда узнал, что ChatGPT назвал его в рамках исследовательского проекта ученых-юристов, которые подвергали кого-то сексуальным домогательствам.

«Программа сразу сообщила, что меня обвинили в сексуальных домогательствах в статье Washington Post 2018 года после того, как я нащупал студентов юридического факультета во время поездки на Аляску», — сказал Терли. На самом деле он никогда не возил студентов на Аляску, и The Post никогда не публиковала подобную статью.

Терли сказал, что его «никто никогда не обвинял в сексуальных домогательствах или нападениях».

Председатель Федеральной торговой комиссии США (FTC) Лина Хан предупредила, что современные технологии искусственного интеллекта, такие как ChatGPT, могут использоваться для «ускорения» мошенничества.

«ИИ представляет собой целый набор возможностей, но также представляет целый ряд рисков», — сказал Хан представителям Палаты представителей в прошлом месяце.

«Я думаю, мы уже видели, как его можно использовать для ускорения мошенничества и жульничества. Мы обращаем внимание участников рынка на то, что случаи, когда инструменты ИИ эффективно разрабатываются для обмана людей, могут поставить их на крючок для действий FTC», — заявила она.

Ряд известных исследователей ИИ, в том числе генеральный директор Twitter Илон Маск и Стив Возняк, соучредитель Apple, подписали открытое письмо, призывающее лаборатории ИИ по всему миру остановить разработку крупномасштабных систем ИИ, сославшись на опасения по поводу «серьезные риски для общества и человечества», которые, как утверждается, представляет это программное обеспечение.

Более того, Meta (ранее Facebook) обнаружила создателей вредоносных программ, которые пользуются интересом публики к ChatGPT и используют этот интерес для побуждения пользователей к загрузке вредоносных приложений и расширений браузера.

Компания заявила, что обнаружила около 10 семейств вредоносных программ, выдающих себя за ChatGPT, и аналогичные инструменты для взлома учетных записей в Интернете.

Meta также обнаружила и заблокировала более 1000 таких уникальных вредоносных URL-адресов в своих приложениях». ***(ChatGPT's arrival raises personal data theft, hacking risks many times over // The Statesman Limited***

(https://www.thestatesman.com/technology/chatgpts-arrival-raises-personal-data-theft-hacking-risks-many-times-over-1503178980.html). 07.05.2023).

***

«…Одно из опасений, связанных с технологиями искусственного интеллекта, такими как ChatGPT, заключается в том, что преступники и другие злоумышленники будут делать с этой силой.

Это то, что Европол, правоохранительный орган Европейского Союза, изучил в своем недавнем отчете в ChatGPT под названием «Влияние моделей большого языка на правоохранительные органы».

В отчете говорится, что ChatGPT, построенный на основе технологии большой языковой модели OpenAI GPT3.5, может «значительно облегчить злоумышленникам понимание и последующее совершение различных видов преступлений».

Это связано с тем, что, хотя информация, на которой обучается ChatGPT, уже находится в свободном доступе в Интернете, технология может предоставить пошаговые инструкции по любым темам, если пользователь задает правильные контекстные вопросы.

Вот типы преступлений, о которых предупреждает Европол, чат-боты или LLM потенциально могут помочь преступникам.

Мошенничество, выдача себя за другое лицо и социальная инженерия

ChatGPT и другие чат-боты, такие как Bard от Google, поразили пользователей своей способностью писать по-человечески на любую тему, основываясь на подсказках пользователя.

Они могут подражать стилям письма знаменитостей и изучать стиль письма на основе введенного текста, прежде чем создавать новые записи в этом изученном стиле. Это открывает систему для потенциального использования преступниками, которые хотят выдать себя за кого-то или за стиль письма организации, что, возможно, может быть использовано в фишинговом мошенничестве.

Европол также предупреждает, что ChatGPT может использоваться для придания легитимности различным видам онлайн-мошенничества, например, путем создания массы поддельного контента в социальных сетях для продвижения мошеннических инвестиционных предложений.

Одним из верных признаков потенциального мошенничества при общении по электронной почте или в социальных сетях являются очевидные орфографические или грамматические ошибки, допущенные преступниками при написании контента.

Имея в своих руках мощь LLM, даже преступники, плохо владеющие английским языком, смогут создавать контент, который больше не имеет этих красных флажков.

Эта технология также созрела для использования теми, кто хочет создавать и распространять пропаганду и дезинформацию, поскольку она способна создавать аргументы и повествования с большой скоростью.

Киберпреступность для новичков

ChatGPT не только хорошо пишет слова, но и владеет рядом языков программирования. По мнению Европола, это может повлиять на киберпреступность.

«С текущей версией ChatGPT уже можно создавать базовые инструменты для различных вредоносных целей», — предупреждает отчет.

Это были бы базовые инструменты для создания фишинговых страниц, например, но они позволяют преступникам, практически не имеющим знаний в области кодирования, создавать вещи, которые они не могли создать раньше.

Неизбежные улучшения в возможностях LLM означают, что эксплуатация со стороны преступников «обеспечивает мрачные перспективы» в ближайшие годы.

Тот факт, что последняя версия преобразователя OpenAI, GPT-4, лучше понимает контекст кода и исправляет ошибки, означает, что «это бесценный ресурс» для преступников с небольшими техническими знаниями.

Европол предупреждает, что с улучшением технологии ИИ она может стать намного более продвинутой, «и, как следствие, опасной».

Дипфейки уже имеют последствия в реальном мире

Варианты использования ChatGPT, о которых предупреждает Европол, — это лишь одна из областей ИИ, которую могут использовать преступники.

Уже были случаи, когда дипфейки ИИ использовались для мошенничества и причинения вреда людям. В одном случае женщина сказала, что ей было всего 18 лет, когда она обнаружила свои порнографические фотографии, циркулирующие в Интернете, несмотря на то, что никогда не делала и не делилась этими изображениями.

Ее лицо было добавлено в цифровом виде к изображениям тела другого человека. Она сказала Euronews Next, что это «пожизненное заключение». Отчет Deeptrace Labs за 2019 год показал, что 96% дипфейкового онлайн-контента является порнографией без согласия.

В другом случае ИИ использовался для имитации звука чьего-то голоса, чтобы обмануть члена его семьи, используя технику дипфейка.

Европол завершил свой отчет, заявив, что для правоохранительных органов важно «оставаться в авангарде этих событий», а также предвидеть и предотвращать преступное использование ИИ». ***(Luke Hurst. Europol is worried criminals may exploit the powers of ChatGPT. Here's why // euronews.com (https://www.euronews.com/next/2023/05/08/europol-is-worried-criminals-may-exploit-the-powers-of-chatgpt-heres-how). 09.05.2023).***

***

«Администрация Джо Байдена бросает вызов тысячам хакеров, чтобы узнать, смогут ли они взломать системы искусственного интеллекта (ИИ), такие как ChatGPT. Это часть серии новых действий, направленных на продвижение «ответственных» инноваций в области искусственного интеллекта (ИИ), которые защищают права и безопасность американцев.

На прошлой неделе Белый дом объявил, что ведущие разработчики ИИ в США, включая Google, Microsoft, OpenAI, Nvidia и Anthropic, в августе примут участие в публичном тестировании своих систем ИИ на Defcon 31. Это одна из крупнейших в мире конференций по кибербезопасности. проводится ежегодно в Лас-Вегасе.

В то же время вице-президент США Камала Харрис встретилась с руководителями технологических фирм OpenAI, Microsoft, Alphabet и Anthropic, чтобы обсудить критические риски и возможности ИИ, особенно те, которые касаются кибербезопасности, биозащиты и безопасности.

«Эти независимые учения предоставят исследователям и общественности критически важную информацию о влиянии этих моделей и позволят компаниям и разработчикам ИИ предпринять шаги для устранения проблем, обнаруженных в этих моделях», — говорится в брифинге Белого дома.

«Тестирование моделей ИИ независимо от правительства или компаний, которые их разработали, является важным компонентом их эффективной оценки».

Сервис больших языковых моделей (LLM) OpenAI ChatGPT приобрел популярность в прошлом году как образовательный инструмент, который может ускорить написание задач и даже научить людей программировать. Однако есть много опасений, что технология предвзята и дает ответы, поскольку она рассматривает интернет-контент с конца 1990-х годов до 2021 года.

Хотя администрация президента Байдена признает, что «ИИ — одна из самых мощных технологий нашего времени», она также хочет убедиться, что любые возможные риски снижены.

Поэтому правительство США возлагает «основную ответственность» на технологические фирмы, чтобы убедиться, что их продукты безопасны, прежде чем они будут развернуты.

В феврале президент США подписал указ, предписывающий федеральным агентствам «искоренить предвзятость» при разработке любых используемых систем. Приказ должен был обеспечить защиту граждан от компьютерной алгоритмической дискриминации.

Это произошло после того, как многочисленные примеры показали, что использование ИИ в судах, академических кругах и торговле может привести к тому, что компьютеры будут принимать дискриминационные решения. Это произошло из-за того, что в них были введены исторические данные, которые показали явное предубеждение против определенных классов общества.

Но объявление также свидетельствует о четком признании со стороны правительства США того, что компании, занимающиеся искусственным интеллектом, действительно обладают большой потенциальной ценностью.

Наряду с объявлениями о рисках Белый дом также изложил планы по созданию семи новых национальных научно-исследовательских институтов ИИ при поддержке правительства в размере 140 миллионов долларов (111 миллионов фунтов стерлингов).

Идея состоит в том, чтобы продвигать прорывы с использованием ИИ в таких областях, как климат, сельское хозяйство, энергетика, здравоохранение, образование и кибербезопасность.

«Импульс ИИ сейчас огромен, и он уже прошел точку, когда его можно запретить. Разумный подход заключается в том, чтобы узнать как можно больше о технологиях искусственного интеллекта, чтобы ими можно было управлять», — сказал The Standard Крис Ховард, глава глобального отдела исследований аналитической компании Gartner.

«Образование ведет к лучшему регулированию. Регулирование ведет к лучшим стандартам. Стандарты делают инновации практичными и полезными».

Он говорит, что подход правительства США к работе с ИИ является результатом прецедента, установленного Microsoft в 2018 году, когда технический гигант предпринял необычный шаг, попросив законодателей разработать законы, регулирующие распознавание лиц.

«Мой опыт работы с этими технологическими компаниями показывает, что они приветствуют участие правительства на ранних этапах внедрения», — добавил Ховард.

«Открытый диалог лучше, чем найти что-то в будущем, и вы не построили это взаимодействие. Вот тогда и случаются плохие вещи. Понимание такой технологии, как ИИ, с разных точек зрения смягчит рефлекторные реакции». ***(Mary-Ann Russon. US challenges hackers to break ChatGPT and other AI models // Standard (https://www.standard.co.uk/tech/us-hackers-chatgpt-google-anthropic-openai-microsoft-b1079820.html). 10.05.2023).***

***

«В марте Агентство Европейского Союза по кибербезопасности (ENISA) опубликовало отчет «Кибербезопасность ИИ и стандартизация», в котором подробно описаны существующие, планируемые и рассматриваемые стандарты, относящиеся к кибербезопасности искусственного интеллекта (ИИ). В отчете выявляется несколько пробелов в существующих подходах к защите цифровой инфраструктуры и приводятся практические рекомендации по их устранению, включая принятие технических стандартов, которые будут применяться при создании инфраструктуры кибербезопасности при развертывании искусственного интеллекта.

В отчете указывается несколько проблемных областей в существующих технических стандартах, связанных с кибербезопасностью и искусственным интеллектом. Особое внимание уделяется стандартам, связанным с традиционными сферами парадигмы безопасности конфиденциальности, целостности и доступности (CIA), а также стандартам, направленным на дополнение предложений, включенных в проект Закона об искусственном интеллекте Европейского Союза (ЕС). Выявленные пробелы CIA состоят из данных и методологий ИИ, включая прослеживаемость данных и компонентов ИИ на протяжении их жизненного цикла, непонимание свойств, присущих машинному обучению (МО) в таких областях, как метрики и тестирование, а также неспособность стандартов, которые должны быть адаптированы к новым технологиям. В отчете также отмечается, что в проекте Закона об ИИ есть пробелы в отношении пересечения кибербезопасности и тестирования систем ИИ.

Разработка стандартизированного подхода к кибербезопасности ИИ

В отчете обсуждается важность стандартизации в отношении кибербезопасности ИИ с акцентом на машинное обучение как на движущую силу технологий ИИ. Он начинается с описания особенностей машинного обучения и отмечает, что системы ИИ иногда делают неверные прогнозы. Далее в отчете

обсуждается важность «объяснимости» в системах ИИ, чтобы решения, принимаемые алгоритмами, могли быть понятны людям.

Ключевой темой отчета является то, что в нем описывается взаимосвязь между ИИ и кибербезопасностью, определяя три аспекта отношений между ИИ и кибербезопасностью: кибербезопасность ИИ, ИИ, используемый для поддержки кибербезопасности, и злонамеренное использование ИИ.

Сначала в отчете основное внимание уделяется первому измерению, кибербезопасности ИИ, и обсуждаются как «узкая», так и «широкая» интерпретации этой концепции. «Узкий» относится к CIA компонентов ИИ, связанных данных и процессов, а «широкий» относится к характеристикам надежности ИИ, таким как объяснимость, надежность, точность и прозрачность.

Затем в отчете обсуждается работа различных организаций по стандартизации, таких как CEN-CENELEC, ETSI и ISO-IEC, по разработке стандартов и руководств, связанных с ИИ и кибербезопасностью. В нем отмечается, что многие из этих организаций работают над стандартами, которые охватывают как узкую, так и широкую интерпретацию кибербезопасности, при этом оценивая степень, в которой существующие стандарты решают проблемы кибербезопасности, и выявляя основные пробелы.

Далее в отчете рассматривается роль кибербезопасности в проекте Закона об ИИ и выявляются пробелы в стандартизации, которые необходимо устранить. Он также ссылается на несколько соответствующих стандартов ISO/IEC и описывает требования к различным аспектам ИИ, таким как качество данных, управление рисками и прозрачность.

Отчет завершается рекомендациями для организаций, организаций, разрабатывающих стандарты, и тех, кто готовится к реализации проекта Закона об искусственном интеллекте. Рекомендации:

Используйте стандартизированную и согласованную терминологию ИИ для кибербезопасности, включая характеристики надежности и таксономию различных типов атак, характерных для систем ИИ.

Разработать конкретное/техническое руководство о том, как существующие стандарты, связанные с кибербезопасностью программного обеспечения, следует применять к ИИ.

Неотъемлемые черты ML должны быть отражены в стандартах.

Обеспечить установление связей между техническими комитетами по кибербезопасности и техническими комитетами по ИИ, чтобы стандарты ИИ в отношении характеристик надежности и качества данных учитывали потенциальные проблемы кибербезопасности.

Идентификация рисков кибербезопасности и определение соответствующих требований безопасности должны основываться на системном анализе и, при необходимости, на отраслевых стандартах.

Поощрять исследования и разработки в областях, где стандартизация ограничена технологическим развитием

Поддерживать разработку стандартов для инструментов и компетенций субъектов, осуществляющих оценку соответствия.

Обеспечить согласованность между проектом Закона об искусственном интеллекте и другими законодательными инициативами в области кибербезопасности, в частности Регламентом (ЕС) 2019/881 (Закон о кибербезопасности) и предложением COM (2022) 454 о регламенте горизонтальных требований к кибербезопасности для продуктов с цифровыми элементами (Закон о кибербезопасности). Закон об устойчивости).

Основные выводы

В отчете ENISA обсуждается важность стандартизации в отношении кибербезопасности ИИ.

В частности, он охватывает:

Степень, в которой стандарты общего назначения могут быть адаптированы к ИИ

Необходимость уточнения терминов и концепций ИИ

Важность руководства о том, как стандарты, связанные с кибербезопасностью, следует применять к ИИ

Необходимость дальнейших исследований и разработок для устранения пробелов в знаниях и технологиях

Важность прослеживаемости и происхождения данных и компонентов ИИ

Необходимость в стандартах, отражающих неотъемлемые черты машинного обучения

Необходимость единого подхода к надежности и важность разработки руководств и стандартов для поддержки кибербезопасности в системах ИИ.

Необходимость нормативной согласованности между проектом Закона об искусственном интеллекте и другим законодательством о кибербезопасности…» ***(Bennett Borden, Christopher Cullen, Coran Darling and Samantha Tyner-Monroe. ENISA identifies gaps in approaches to the cybersecurity of AI // DLA Piper (https://www.technologyslegaledge.com/2023/05/enisa-identifies-gaps-in-approaches-to-the-cybersecurity-of-ai/#page=1). 09.05.2023).***

***

«Хотя искусственный интеллект (ИИ) не нов, Google Bard, Microsoft Bing, ChatGPT и подобные продукты сделали технологию доступной и понятной для среднего потребителя. Однако опасения по поводу конфиденциальности и безопасности привели к призывам приостановить разработку ИИ и проявить интерес к жесткому регулированию. Хотя эти риски необходимо устранять, нельзя упускать из виду общие преимущества искусственного интеллекта, машинного обучения и больших языковых моделей для кибербезопасности и национальной безопасности. Вместо этого директивным органам следует подумать о том, как Соединенные Штаты могут в полной мере использовать технологии в этих областях. Существует три прямых применения указанных технологий на индивидуальном, системном и национальном уровне.

Во-первых, ИИ может принести пользу киберзащитникам. В 2022 году на выявление и пресечение утечки данных ушло около 277 дней, при этом для выявления некоторых причин утечек требовалось более 300 дней. Интересно, что средняя экономия составляет 1,12 миллиона долларов, если нарушения устраняются

в течение 200 дней или меньше, а организации, использующие ИИ и автоматизацию, экономят в среднем 3 миллиона долларов. Скорость и финансовая экономия важны, но некоторые исследования показывают, что показатели обнаружения увеличиваются. Технология искусственного интеллекта может служить ключевым аспектом более эффективного и своевременного обнаружения угроз, автоматизируя задачи, которые в противном случае пришлось бы выполнять аналитику-человеку, синтезируя более крупные и сложные наборы данных и потенциально лучше предоставляя менее квалифицированным практикам.

Недавно появились специальные продукты для кибербезопасности, использующие большие языковые модели, чтобы помочь защитникам, и теперь автоматическая оценка угроз стала реальностью. Тем временем разрабатываются другие усовершенствования, которые могут позволить анализировать потенциальные вредоносные программы за считанные секунды. У использования ИИ в кибербезопасности есть недостатки, в том числе качество доступных данных для обучения, но, как и в большинстве аспектов безопасности, нельзя полностью полагаться ни на одно решение. ИИ — не единственное решение кибербезопасности, но он может сыграть свою роль.

Во-вторых, ИИ может принести пользу традиционным системам, необходимым для национальной безопасности. На недавних слушаниях в Сенатском комитете по вооруженным силам обсуждалось, как ИИ и машинное обучение могут улучшить операции Министерства обороны. Примечательно, что был подчеркнут тот факт, что Соединенные Штаты имеют «основные системы вооружений на триллионы долларов, которые крайне уязвимы для кибератак». К сожалению, киберуязвимости систем вооружения не являются чем-то новым. Тестирование показало, что системы можно взять под контроль с помощью относительно простых инструментов и методов и в значительной степени работать незаметно.

Однако идея о том, что с этими угрозами невозможно справиться без ИИ и преимуществ, которые он дает, набирает обороты. Одно из самых ярких приложений — обнаружение аномалий и помощь в определении того, что представляет собой кибератака. Даже если бы наши системы вооружения были одинаково продвинуты с точки зрения безопасности, ИИ принес бы пользу, но ИИ становится критически важным, когда это не так. Не говоря уже о том, что эта технология также предлагает военным оперативное преимущество, как показала Army Vantage.

В-третьих, ИИ может улучшить национальную безопасность. Эта технология выходит далеко за пределы Соединенных Штатов, и наши противники стремятся максимально использовать ее и ее возможности. Как отмечается в Ежегодной оценке угроз разведывательного сообщества, «Китай быстро расширяет и совершенствует свой искусственный интеллект (ИИ) и возможности анализа больших данных…», и Китай прямо заявил о своем желании стать основным центром инноваций в области ИИ к 2030 году. Добавьте к этому тот факт, что Китай занимается массовым сбором данных и не ограничен верховенством закона, и у них есть неотъемлемое преимущество. Китай, безусловно, не собирается соблюдать паузу в развитии ИИ или уважать лучшие практики, разработанные Соединенными Штатами или их союзниками.

Это не означает, что Соединенные Штаты должны продвигать ИИ без каких-либо барьеров, но неспособность рассматривать его как стратегический приоритет и бороться за то, чтобы оставаться впереди, создает серьезные риски для нации. Это также означает, что и правительство, и частный сектор должны обеспечить максимальную безопасность ИИ, потому что наши противники будут стремиться использовать любые уязвимости. Полезны недавние инвестиции, объявленные Белым домом, наряду с текущей работой Национального института стандартов и технологий (NIST) в рамках их концепции управления рисками ИИ, основанной на его киберструктурах и конфиденциальности принципах. Точно так же планы хакеров публично оценить системы генеративного ИИ на DEF CON 2023 являются положительными и напоминают прошлые примеры, такие как «Взлом Пентагона», когда правительство взаимодействовало с хакерами для обнаружения уязвимостей.

В то время как отрицательные и тревожные аспекты ИИ привлекли большое внимание, нельзя игнорировать его положительные и важные применения, особенно в свете того, что Конгресс, Белый дом и регулирующие органы прокладывают путь вперед. Неспособность признать преимущества ИИ в области кибербезопасности и национальной безопасности рискует оставить нас позади наших противников или упустить киберуязвимость». ***(Brandon Pugh. AI's key role in cybersecurity and national security // Microsoft (https://www.msn.com/en-us/news/other/ai-s-key-role-in-cybersecurity-and-national-security/ar-AA1b9dqn). 14.05.2023).***

***

«В сегодняшнюю цифровую эпоху обеспечение безопасности технологий на основе ИИ, таких как ChatGPT, имеет первостепенное значение. Чтобы усилить защиту и защититься от потенциальных уязвимостей, несколько брендов в области кибербезопасности специализируются на повышении безопасности систем чат-ботов с искусственным интеллектом. Эти бренды предлагают ряд продуктов и услуг, направленных на различные аспекты кибербезопасности, от обнаружения и предотвращения угроз до защиты данных и сетевой безопасности. Используя свой опыт, эти бренды способствуют повышению безопасности ChatGPT, защите взаимодействия с пользователем и снижению потенциальных рисков. Вот пять известных брендов кибербезопасности, которые преуспели в повышении безопасности ChatGPT и аналогичных систем, управляемых искусственным интеллектом.

Palo Alto Networks — ведущая компания в области кибербезопасности, которая предлагает ряд продуктов и услуг для сетевой безопасности, включая обнаружение и предотвращение угроз на основе ИИ. Их опыт в области искусственного интеллекта и машинного обучения может помочь выявить и устранить потенциальные уязвимости в системах ChatGPT.

CrowdStrike — компания, занимающаяся кибербезопасностью, известная своей передовой платформой для защиты конечных точек. Они специализируются на обнаружении и реагировании на сложные угрозы, в том числе нацеленные на системы искусственного интеллекта. Их решения могут помочь защитить инфраструктуру и конечные точки, используемые ChatGPT, обеспечив защиту от потенциальных кибератак.

Symantec, в настоящее время часть Broadcom, является известным брендом в области кибербезопасности, предлагающим широкий спектр продуктов и услуг. Их опыт включает анализ угроз, безопасность конечных точек, защиту данных и облачную безопасность. Решения Symantec могут помочь защитить ChatGPT от различных угроз безопасности и обеспечить конфиденциальность взаимодействия пользователей.

Noventiq — ведущий мировой поставщик решений и услуг в области цифровой трансформации и кибербезопасности со штаб-квартирой и листингом в Лондоне. Компания обеспечивает, упрощает и ускоряет цифровую трансформацию для бизнеса своих клиентов, связывая более 75 000 организаций из всех секторов с сотнями лучших в своем классе поставщиков ИТ, включая AWS, Google, Microsoft, Adobe, Oracle, VMWare и многих других. наряду с собственными услугами и решениями. Предложения Noventiq помогают защитить ChatGPT от различных угроз безопасности, гарантируя конфиденциальность взаимодействия с пользователем.

Fortinet — глобальная компания в области кибербезопасности, которая обеспечивает сетевую безопасность, защиту конечных точек и решения для анализа угроз на основе ИИ. Их технологии могут помочь защитить инфраструктуру, поддерживающую ChatGPT, обеспечив надежную защиту от киберугроз и поддерживая целостность системы». ***(Defending the Virtual Assistants: 5 Cybersecurity Brands Safeguarding ChatGPT's Security // Bennett, Coleman & Company Limited (https://www.timesnownews.com/technology-science/defending-the-virtual-assistants-5-cybersecurity-brands-safeguarding-chatgpts-security-article-100254051). 15.05.2023).***

***

«Как мы знаем, с момента запуска chatGPT он покорил мир. Это интеллектуальное творение OpenAI. Это творческий инструмент, полезный почти во всех областях. Говорим ли мы о средствах массовой информации, здравоохранении, технических отделах или любом финансовом учреждении, везде и в каждой области чат доказывает свою эффективность.

Если говорить о кибербезопасности, то генеративный ИИ также трансформирует кибербезопасность. Киберпреступники используют ИИ для проведения изощренных и оригинальных крупномасштабных атак. По словам Кристофера Альберга, генерального директора платформы анализа угроз, защитники также используют ту же технологию для защиты критически важной инфраструктуры, государственных учреждений и бизнес-сетей.

Более того, генеративный ИИ позволил киберпреступникам автоматизировать атаки, сканировать поверхности атак и создавать контент, который резонирует с различными географическими демографическими данными и регионами.

С другой стороны, это также позволяет злоумышленникам нацеливаться на более широкий круг потенциальных жертв в разных странах. Более того, они внедрили технологию для создания убедительных фишинговых писем. Кроме того, сгенерированный ИИ текст позволяет злоумышленникам создавать персонализированные электронные письма и текстовые сообщения для обмана целей.

Альберг заявляет: «Я думаю, вам не нужно мыслить очень творчески, чтобы понять, что, чувак, это может помочь киберпреступникам стать авторами, что является проблемой».

Машинное обучение и искусственный интеллект для специалистов по кибербезопасности появились сравнительно недавно. Обнаружение и реагирование на конечных точках (EDR), когда ML/AI использует поведенческую аналитику для выявления аномальных действий, было одним из самых популярных вариантов использования.

Более того, он может выявлять выбросы, используя заведомо хорошее поведение, после чего он может убивать процессы, блокировать учетные записи, запускать оповещения и делать другие вещи.

Потенциал ИИ в кибербезопасности

AI использует Splunk, который работает со своим языком, языком обработки поиска (SPL), который помогает понять мощь chatGPT. ChatGPT уже изучил SPL и может превратить подсказку младшего аналитика в запрос всего за несколько секунд.

Тем не менее, chatGPT может написать предупреждение об атаках методом перебора против Active Directory. Он может создать предупреждение и объяснить логику запроса.

С другой стороны, наиболее убедительным вариантом использования chatGPT является автоматизация повседневных задач для чрезмерно расширенной ИТ-команды. Active Directory содержит почти сотни и тысячи учетных записей. Эти учетные записи имеют привилегированные разрешения; бизнес может быть не в состоянии расставить приоритеты для его реализации.

Теперь можно делегировать создание этих сценариев в chatGPT, который может разработать логику для распознавания и отключения учетных записей, которые не были активны в течение последних 90 дней.

В то время как младшие инженеры могут помочь старшим инженерам высвободить больше времени для более сложной работы. Предположим, они пишут и планируют этот сценарий в дополнение к изучению того, как работает логика.

ChatGPT можно использовать для пурпурной команды или совместной работы красной и синей команд для проверки и улучшения состояния безопасности организации, если кто-то ищет множитель силы в динамичных упражнениях.

Он может создавать базовые модели сценариев, которые может использовать пентестер, или устранять неполадки в сценариях, которые могут работать неправильно.

Преимуществ много, но есть и ограничения.

ИИ полезен для ускорения или введения альтернативных путей для любого подробного анализа. Если говорить о кибербезопасности, то она играет жизненно важную роль в автоматизации задач и порождает новые идеи.

Тем не менее, есть определенные ограничения для этой полезности. Мы не можем запрограммировать инструмент ИИ, чтобы он функционировал как человек. Его можно использовать для анализа данных и получения результатов на основе фактов, которые любой может ввести.

Кроме того, одним из наиболее значительных преимуществ ИИ является автоматизация повседневных задач, позволяющая людям сосредоточиться на более творческой или трудоемкой работе.

ИИ — это эффективный инструмент, используемый инженерами по кибербезопасности или системными администраторами. Например, он может переписать инструмент парсинга даркнета, сократив время выполнения с дней до часов.

Увы, если есть какие-то недостатки у ИИ, влияющего на принятие решений людьми, всякий раз, когда он использует слово «автоматизация», возникает ощутимый страх, что технология будет развиваться и сделает людей устаревшими в их карьере.

Кроме того, злоумышленники используют инструменты для создания более убедительных и успешных фишинговых писем». ***(Senoria Khursheed. ChatGPT Is About To Revolutionize CyberSecurity // TechJuice (https://www.techjuice.pk/chatgpt-is-about-to-revolutionize-cybersecurity/). 15.05.2023).***

***

«Поскольку многие предприятия не решаются разрешить сотрудникам кибербезопасности использовать инструменты ИИ в своей работе, опасаясь, что эта область не регулируется и все еще недостаточно развита, ключевые мыслители из различных отраслей недавно написали открытое письмо с требованием прекратить эксперименты с ИИ, более продвинутые, чем ChatGPT-4.

Некоторые даже говорят, что буквы недостаточно, и общество не готово справиться с разветвлениями ИИ.

К сожалению, ящик Пандоры уже открыт, и те, кто делают вид, что мы можем обратить вспять любое из этих нововведений, заблуждаются…

Хакеры, использующие ChatGPT, стали быстрее и изощреннее, чем раньше, и аналитики по кибербезопасности, не имеющие доступа к аналогичным инструментам, могут очень быстро оказаться в вооружении и перехитрить этих злоумышленников с помощью ИИ.

Они используют ChatGPT для создания кода для фишинговых писем, вредоносного ПО, инструментов шифрования и даже для создания торговых площадок в даркнете.

Возможности хакеров по использованию ИИ безграничны, и в результате многие аналитики также прибегают к несанкционированному использованию систем ИИ только для того, чтобы выполнить свою работу.

По данным HelpNet Security, 96% специалистов по безопасности знают, что кто-то использует неавторизованные инструменты в их организации, а 80% признались, что сами используют запрещенные инструменты.

Это доказывает, что ИИ уже широко используется в индустрии кибербезопасности, в основном из-за необходимости.

Участники опроса даже сказали, что «они выберут неавторизованные инструменты из-за лучшего пользовательского интерфейса (47%), более специализированных возможностей (46%) и более эффективной работы (44%)».

Фатальные недостатки, которыми можно воспользоваться

Корпорации спотыкаются, пытаясь понять управление ИИ, но пока они это делают, их сотрудники явно игнорируют правила и, возможно, ставят под угрозу деятельность компании.

Согласно исследованию Cyberhaven, в котором приняли участие 1,6 миллиона сотрудников, 3,1% из них вводят конфиденциальную информацию о компании в ChatGPT. Хотя это число кажется небольшим, 11% вопросов пользователей содержат личную информацию.

Это могут быть имена, номера социального страхования, внутренние файлы компании и другая конфиденциальная информация.

ChatGPT учится на каждом разговоре со своими пользователями и может извергать информацию о пользователе, если ее правильно исследовать.

Это фатальный недостаток для корпоративного использования, учитывая, как хакеры могут манипулировать системой, чтобы получить ранее скрытую информацию.

Что еще более важно, ИИ также будет знать механизмы безопасности, которые компания использует при установке на корпоративный сервер.

Вооружившись этой информацией, злоумышленник может успешно получить и распространить конфиденциальную информацию.

Мы не можем остановить инновации

Будь то облако или Интернет, интеграция новых технологий всегда вызывала споры и сомнения.

Но остановить инновации невозможно, когда преступники получили доступ к передовым инструментам, которые практически делают всю работу за них.

Чтобы правильно решить эту проблему, связанную с безопасностью нашего общества, компании должны применять предыдущие правила управления к ИИ

Повторное использование проверенных временем процедур позволит компаниям догнать злоумышленников и устранить дисбаланс сил.

Упрощенное регулирование среди специалистов по кибербезопасности позволит компаниям контролировать, какие инструменты используют сотрудники, когда они их используют и какая информация вводится.

Контракты между поставщиками технологий и организациями также распространены при использовании корпоративного облака и могут применяться к туманной сфере ИИ.

Мы можем создать только безопасную, контролируемую среду

Мы прошли точку невозврата, и критическое принятие — наше единственное решение жить в мире, управляемом ИИ.

Повышение уровня инноваций, повышение общедоступности и простота использования дали киберпреступникам преимущество, которое трудно повернуть вспять.

Чтобы изменить ситуацию, компании должны внедрить искусственный интеллект в безопасной контролируемой среде.

Передовые технологии почти не поддаются контролю, и аналитики по кибербезопасности должны научиться ответственно их использовать.

Обучение сотрудников и разработка корпоративных инструментов укрепят процедуры кибербезопасности до тех пор, пока такой гигант отрасли, как Microsoft, не будет использовать недавно анонсированный инструмент анализа безопасности Security Copilot для преобразования отрасли.

Тем временем компании должны перестать прятать голову в песок, надеясь, что реальность изменится.

Вещи станут более антиутопическими, если организации будут продолжать игнорировать безудержные проблемы вместо того, чтобы иметь дело с неудобным миром, который мы создали». ***(Rodrigo Loureiro. AI has been dubbed a 'nuclear' threat to cybersecurity. But it can be also used for defence // euronews (https://www.euronews.com/2023/05/04/ai-has-been-dubbed-a-nuclear-threat-to-cybersecurity-but-it-can-also-be-used-for-defence). 04.05.2023).***

***

«После успеха ChatGPT от OpenAI, Bing Chat от Microsoft и Google Bard исследователи создали новую модель ИИ с гораздо более мрачным уклоном.

В то время как большие языковые модели (LLM), лежащие в основе ChatGPT и Google Bard, обучались на данных из открытой сети, DarkBERT обучался исключительно на данных из даркнета. Да, вы правильно прочитали, эта новая модель ИИ была обучена на данных хакеров, киберпреступников и других мошенников.

Группа южнокорейских исследователей опубликовала документ (PDF), в котором подробно описывается, как они создали DarkBERT, используя данные из сети Tor, которая часто используется для доступа к даркнету. Просматривая темную сеть и затем фильтруя необработанные данные, они смогли создать базу данных темной сети, которую они использовали для обучения DarkBERT.

Удивительно, но DarkBERT уже удалось превзойти другие большие языковые модели, несмотря на то, что он обучался на данных из очень неожиданного места.

Хотя DarkBERT — это новая модель ИИ, на самом деле она основана на архитектуре RoBERTa, которая представляет собой подход к ИИ, разработанный еще в 2019 году исследователями Facebook, согласно нашему дочернему сайту Tom’s Hardware.

В исследовательском документе, подробно описывающем внутреннюю работу RoBERTa, Meta AI объясняет, что это «надежно оптимизированный метод предварительной подготовки систем обработки естественного языка (NLP)», который улучшает BERT (представления двунаправленного кодировщика от трансформеров), который был выпущен Google назад. в 2018 году. Поскольку поисковый гигант сделал BERT открытым исходным кодом, исследователи Facebook смогли улучшить его производительность в ходе повторного исследования.

Благодаря оптимизированному методу Facebook был выпущен RoBERTa, который смог дать самые современные результаты в тесте НЛП General Language Understanding Evaluation (GLUE).

Однако теперь южнокорейские исследователи DarkBERT показали, что RoBERTa может делать даже больше, поскольку он был недостаточно обучен, когда он был первоначально выпущен. Подавая данные RoBERTa из даркнета в течение

почти 16 дней по двум наборам данных (один необработанный, а другой предварительно обработанный), исследователи смогли создать DarkBERT.

К счастью, у исследователей нет планов выпускать DarkBERT для широкой публики., они принимают запросы в академических целях. Тем не менее, по словам Дексерто. Тем не менее, DarkBERT, скорее всего, предоставит правоохранительным органам и исследователям гораздо лучшее понимание даркнета в целом.

Как обезопасить себя при использовании чат-ботов с искусственным интеллектом

Как и в случае с любым другим программным обеспечением или онлайн-сервисом, вы должны быть осторожны при использовании чат-ботов с искусственным интеллектом, поскольку вы можете заразиться вредоносным ПО от поддельных приложений ChatGPT или даже раскрыть конфиденциальные данные, как это недавно сделали сотрудники Samsung.

Вот почему вы хотите убедиться, что вы действительно переходите на правильный веб-сайт при использовании этих популярных чат-ботов с искусственным интеллектом. Если вы ищете приложение ChatGPT, Bing Chat или Google Bard, вы его еще не найдете, поскольку OpenAI, Microsoft и Google еще не выпустили официальные приложения для своих чат-ботов с искусственным интеллектом.

Точно так же вы не хотите нажимать на какие-либо ссылки в подозрительных электронных письмах, в которых утверждается, что вы перейдете к чат-боту с искусственным интеллектом или которые помогут вам получить доступ сразу. Мошенники хорошо осведомлены о текущем увлечении чат-ботами с использованием ИИ и прямо сейчас используют его в своих атаках. В то же время следует избегать рекламы чат-ботов с искусственным интеллектом, поскольку киберпреступники часто злоупотребляют Google Ads и другими рекламными сервисами, чтобы направлять ничего не подозревающих пользователей на фишинговые сайты.

Для дополнительной защиты при экспериментировании с чат-ботами с искусственным интеллектом вы должны использовать лучшее антивирусное программное обеспечение на своем ПК, лучшее антивирусное программное обеспечение для Mac на своем Mac и одно из лучших антивирусных приложений для Android на своем смартфоне. Таким образом, если ссылка на чат-бота с искусственным интеллектом действительно ведет к вредоносному ПО, ваш антивирус сначала обнаружит его, прежде чем ваши устройства смогут заразиться.

DarkBERT может представлять будущее моделей ИИ, которые обучаются в одной конкретной области, чтобы сделать их более специализированными. Учитывая его популярность до сих пор, мы не удивимся, если увидим аналогичные модели ИИ, разработанные таким образом в будущем». ***(Anthony Spadafora. New DarkBert AI was trained using dark web data from hackers and cybercriminals // Future US, Inc. (https://www.tomsguide.com/news/new-darkbert-ai-was-trained-using-dark-web-data-from-hackers-and-cybercriminals). 17.05.2023).***

***

«Департамент науки, инноваций и технологий (DSIT) опубликовал руководство для местных органов власти по защите от киберугроз в подключенных местах и инициативах «умных городов».

В нем говорится, что альфа-версия сборника безопасных подключенных мест является ответом на взаимосвязанные системы умных мест, которые делают их привлекательными мишенями для враждебных субъектов.

Руководство было создано в сотрудничестве с группой местных властей — Брэдфорд, Вестминстер, Дорсет, Мертир-Тидвил, Перт и Кинросс, а также Южно-Лондонским партнерством — и предоставляет практическую поддержку для обеспечения кибербезопасности при использовании таких решений, как автоматизированный трафик и системы обращения с отходами и интеллектуальный мониторинг окружающей среды.

Он охватывает несколько ключевых проблем кибербезопасности, с которыми местные органы власти сталкиваются при развертывании технологий, включая управление кибербезопасностью, управление рисками, закупки и безопасность цепочки поставок, а также рекомендации по проведению анализа угроз.

Он также включает блок-схему для понимания того, какие из его ресурсов могут быть наиболее полезными для организации, и ссылки на Принципы кибербезопасности подключенных мест, опубликованные Национальным центром кибербезопасности (NCSC) в 2021 году.

Расширение опыта

Министр по вопросам кибербезопасности, искусственного интеллекта и интеллектуальной собственности виконт Камроуз сказал: «Подключенные места предлагают огромные преимущества для всей страны не только за счет улучшения государственных услуг для наших сообществ, но и благодаря новым инновациям, которые откроют более высокооплачиваемые рабочие места и поднимут нашу экономику.

«Мы уже являемся мировыми лидерами в области кибербезопасности, о чем свидетельствуют такие новаторские меры, как Режим безопасности продуктов. Жизненно важно, чтобы этот опыт был перенесен на развитие наших подключенных мест.

«Этот сборник поможет сделать именно это — предложить практическую и доступную поддержку местным органам власти, поскольку мы совместно работаем над созданием безопасных и устойчивых подключенных мест по всей Великобритании».

Плейбук будет подвергаться тестированию и итерации». ***(Mark Say. DSIT publishes guide for cyber security in smart cities // Informed Communications Ltd. (https://www.ukauthority.com/articles/dsit-publishes-guide-for-cyber-security-in-smart-cities/). 17.05.2023).***

***

«…Согласно NIST, пять функций Cybersecurity Framework: «Идентификация, защита, обнаружение, реагирование, восстановление». Как ИИ может быть полезным для специалиста по безопасности в любой из этих областей?

Прозрачность и объяснимость

Мне приходилось отстаивать определенные решения, принятые на основе информации, полученной от технологических инструментов, перед моими руководителями на разных этапах моей карьеры. Один из вопросов, который всегда задают, звучит так: «Почему вы были достаточно уверены в том, чтобы принять решение XYZ?»

В подобных случаях вам нужно пройтись по тому, как вы перешли от интеллекта к пониманию и действию, чтобы они могли прийти к тому же выводу, что и вы, с учетом тех же входных данных. Одной из проблем со многими моделями и решениями ИИ является отсутствие прозрачности в отношении того, как была разработана модель. Это также включает в себя то, как были объединены наборы данных, загруженные в модель.

Справедливость

Системы ИИ настолько проницательны, насколько проницательны данные, используемые для обучения этих моделей. В них можно непреднамеренно и непреднамеренно закодировать предвзятость. Это может привести к неправильному анализу и, в конечном счете, к неправильным решениям с серьезными последствиями. В частности, если определенные тенденции уязвимости не будут выбраны, организация может подвергнуться крупной атаке.

Ключом к решению проблемы предвзятости является слово «репрезентативная выборка». Согласно Investopedia, «репрезентативная выборка — это подмножество населения, которое стремится точно отразить характеристики большей группы».

Например, компания может ежедневно сталкиваться с миллионом киберугроз. Эти угрозы могут включать в себя SQL-инъекции, управление и контроль, фишинговые атаки, программы-вымогатели и так далее. Если модель ИИ обучена реагировать на эти угрозы, данные, используемые для такого обучения, должны быть репрезентативными для всей популяции в той степени, в которой каждая угроза составляет популяцию.

Безопасность

Что происходит, когда вашим самым слабым звеном становится привратник, роль которого состоит в том, чтобы охранять главный вход в дом от внешних злоумышленников? Скажем, они оставляют ворота открытыми и засыпают или просто вступают в сговор с преступниками. Вот что происходит, когда технология ИИ, используемая для киберзащиты, не управляется правилами кибергигиены, такими как регулярные обновления, безопасность на этапе проектирования и тестирование.

Несколько лет назад я проводил тестирование на проникновение для клиента. Моя команда и я испробовали все обычные методы и подходы, чтобы найти уязвимость в сети, но не нашли ни одной. В конце концов, мы обнаружили уязвимость в решении для обеспечения безопасности, используемом внутренней командой безопасности для защиты организации. Мы воспользовались этим, и это было нашим продвижением по горизонтали внутри организации, пока мы не добрались до контроллера домена.

Заключение

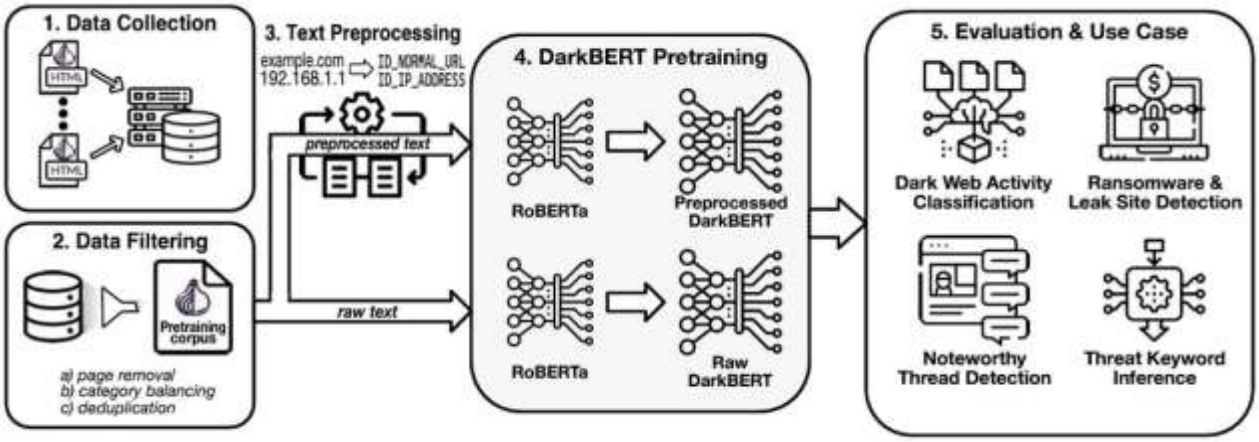
Риски искусственного интеллекта действительно все еще возникают — как и в случае с любой технологией, которую мы считали «новой» в последнее десятилетие, от больших данных и облачных вычислений до квантовых вычислений и многого другого. Использование технологии требует принятия риска. Поэтому важно, когда мы используем возможности и преимущества ИИ, чтобы мы использовали конкретные, динамичные рамки для управления рисками ИИ». ***(Fene Osakwe. The Risks And Rewards Of Artificial Intelligence In Cybersecurity // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/05/22/the-risks-and-rewards-of-artificial-intelligence-in-cybersecurity/?sh=63846d5296db). 22.05.2023).***

***

«Исследователи из Корейского передового института науки и технологий (KAIST) и организации по анализу данных S2W представили DarkBERT, беспрецедентную языковую модель, специально обученную на данных, извлеченных из даркнета.

DarkBERT стремится расширить возможности профессионалов в области кибербезопасности, снабдив их передовым инструментом для выявления и обозначения потенциальных угроз, скрывающихся в глубинах Интернета.

Эта уникальная система искусственного интеллекта использует язык, используемый в темной веб-среде, что позволяет ей улучшить возможности понимания инструментов искусственного интеллекта. DarkBERT может стать бесценным активом для специалистов по кибербезопасности и правоохранительных органов.



Чтобы обеспечить оптимальную адаптацию к языку, распространенному в даркнете, исследовательская группа провела тщательный процесс. Они тщательно просканировали сеть Tor, создав обширную базу данных для DarkBERT.

Команда внедрила методы дедупликации, фильтрации данных и тщательной предварительной обработки для решения этических проблем, связанных с контентом темной сети, который часто содержит конфиденциальную информацию.

В процессе обучения DarkBERT подвергался воздействию двух разных наборов данных в течение 16 дней. Предварительно обработанные данные подверглись тщательной очистке с внесением исправлений для защиты личности

организаций-жертв, сведений об утечке данных, угрожающих заявлений и незаконных изображений.

Примечательно, что значительная часть набора данных, насчитывающая более тысячи страниц, была отнесена к категории развлечений для взрослых.

Эта важная разработка прокладывает путь к дальнейшему изучению и совершенствованию систем искусственного интеллекта, обученных даркнету, предлагая многообещающие возможности для усиления цифровой защиты от киберугроз. Понимая методологию этих злоумышленников, мы можем обезопасить себя даже в самых темных местах в Интернете.

Хотя DarkBERT представляет собой новаторское достижение, выпуск этой модели ИИ для широкой публики в настоящее время не ожидается из-за потенциальных рисков, связанных с материалами даркнета. Однако академические учреждения могут запросить доступ к DarkBERT в исследовательских целях». ***(Emre Çitak. Cybersecurity experts develop a dark web-trained AI // SOFTONIC INTERNATIONAL S.A. (https://www.ghacks.net/2023/05/27/dark-web-trained-ai-darkbert/?amp). 27.05.2023).***

***

«Искусственный интеллект (ИИ) стал неотъемлемой частью современной жизни, оказывая влияние на различные отрасли и отрасли. От здравоохранения до финансов ИИ меняет наш образ жизни и работы. Однако по мере того, как ИИ продолжает развиваться, он также вызывает опасения по поводу безопасности и конфиденциальности. В результате пересечение правил ИИ и кибербезопасности стало критически важной областью внимания как для правительств, предприятий, так и для частных лиц.

Одной из основных проблем на этом перекрестке является отсутствие стандартизированных правил разработки и развертывания ИИ. Хотя некоторые страны начали внедрять политику в отношении ИИ, до сих пор нет глобального консенсуса в отношении того, как эффективно регулировать ИИ. Это отсутствие единообразия может привести к несоответствиям в том, как разрабатываются и развертываются системы ИИ, потенциально создавая уязвимости, которыми могут воспользоваться киберпреступники.

Более того, технологии ИИ могут использоваться как в оборонительных, так и в наступательных целях в сфере кибербезопасности. С одной стороны, ИИ может помочь организациям более эффективно обнаруживать киберугрозы и реагировать на них. Например, алгоритмы машинного обучения могут анализировать огромные объемы данных для выявления закономерностей и аномалий, которые могут указывать на кибератаку. Автоматизируя этот процесс, организации могут быстрее и эффективнее реагировать на угрозы, уменьшая потенциальный ущерб, причиняемый кибератаками.

С другой стороны, киберпреступники также могут использовать искусственный интеллект для проведения более изощренных атак. Например, вредоносное ПО на основе ИИ может адаптироваться и развиваться, чтобы обойти меры безопасности, что усложняет защиту организаций от этих угроз. Кроме того, ИИ можно использовать для автоматизации атак социальной инженерии, таких как

фишинг, путем обработки естественного языка для создания более убедительных и персонализированных сообщений, которые с большей вероятностью могут ввести жертв в заблуждение.

Учитывая эти проблемы, важно, чтобы правительства и организации сотрудничали в разработке комплексных правил ИИ, которые решают проблемы кибербезопасности. Один из подходов к достижению этого — установление международных стандартов и лучших практик для разработки и развертывания ИИ. Создавая общую основу для регулирования ИИ, страны могут работать вместе, чтобы гарантировать, что технологии ИИ разрабатываются и используются ответственно, сводя к минимуму потенциальные риски, связанные с их использованием.

Еще одна возможность заключается в содействии государственно-частному партнерству для решения проблем, связанных с искусственным интеллектом и кибербезопасностью. Сотрудничая с отраслевыми экспертами, правительства могут получить ценную информацию о новейших технологиях искусственного интеллекта и их потенциальном влиянии на безопасность. Это сотрудничество может помочь в разработке более эффективных правил ИИ и стратегий кибербезопасности, гарантируя, что как государственный, так и частный сектор лучше подготовлены к борьбе с возникающими угрозами.

Кроме того, организации должны уделять первоочередное внимание инвестициям в образование и обучение в области искусственного интеллекта и кибербезопасности. Предоставляя сотрудникам необходимые навыки и знания, организации могут лучше защищаться от кибератак с использованием ИИ и обеспечивать ответственное использование технологий ИИ. Сюда входит не только техническое обучение, но и обучение этическим соображениям, связанным с ИИ и его потенциальным влиянием на общество.

В заключение, пересечение правил ИИ и кибербезопасности создает как проблемы, так и возможности для правительств, предприятий и отдельных лиц. Работая вместе над разработкой комплексных правил ИИ, устанавливая международные стандарты и инвестируя в образование и обучение, мы можем использовать потенциал ИИ, сводя к минимуму риски, связанные с его использованием. Поскольку ИИ продолжает формировать наш мир, крайне важно, чтобы мы оставались бдительными и активными в решении проблем кибербезопасности, которые он представляет, обеспечивая более безопасное будущее для всех». ***(Marcin Frąckiewicz. The Intersection of AI Regulations and Cybersecurity // TS2 Space Sp. z o.o. (https://ts2.space/en/the-intersection-of-ai-regulations-and-cybersecurity/). 22.05.2023).***

***

Кіберзлочинність та кібертероризм

«…Особым типом атаки на системы, которая создает значительные угрозы, является атака по времени кэширования (CTA). Атаки на кэш-память — это атаки на систему безопасности, которые используют временные

характеристики кэш-памяти в компьютерных системах. Кэши — это небольшие высокоскоростные компоненты памяти, в которых хранятся часто используемые данные, что снижает задержку доступа к памяти и повышает общую производительность системы. Основная идея атак тайминга кэша заключается в том, что злоумышленник тщательно контролирует доступ к собственной памяти, чтобы вызвать определенное поведение кэша.

В настоящее время методы, используемые для обнаружения атак с синхронизацией кэша, в значительной степени зависят от эвристики и экспертных знаний. Эта зависимость от ручного ввода может привести к нестабильности и неспособности адаптироваться к новым методам атаки. Для преодоления этой проблемы недавно было предложено решение под названием MACTA (Multi-Agent Cache Timing Attack). MACTA использует подход мультиагентного обучения с подкреплением (MARL), который использует обучение на основе популяции для обучения как злоумышленников, так и детекторов. Используя MARL, MACTA стремится преодолеть ограничения традиционных методов обнаружения и повысить общую эффективность обнаружения атак с синхронизацией кэша.

Для разработки и оценки MACTA была создана реалистичная смоделированная среда под названием MA-AUTOCAT, которая позволяет обучать и оценивать злоумышленников и детекторов кэш-тайминга контролируемым и воспроизводимым образом. Используя MA-AUTOCAT, исследователи могут изучать и анализировать работу MACTA в различных условиях.

Результаты показали, что MACTA является эффективным решением, не требующим ручного вмешательства специалистов по безопасности. Детекторы MACTA демонстрируют высокий уровень обобщения, достигая уровня обнаружения 97,8% против эвристической атаки, которая не была обнаружена во время обучения. Кроме того, MACTA снижает пропускную способность атаки злоумышленников на основе обучения с подкреплением (RL) в среднем на 20%. Это снижение пропускной способности атаки подчеркивает эффективность MACTA в предотвращении атак с синхронизацией кэша. Против невидимого детектора SOTA средний уровень уклонения злоумышленников MACTA достигает 99%. Это указывает на то, что злоумышленники MACTA обладают высокой способностью уклоняться от обнаружения и представляют серьезную проблему для существующих механизмов обнаружения.

В заключение MACTA предлагает новый подход к снижению угрозы атак с синхронизацией кеша. Используя MARL и обучение на основе популяции, MACTA повышает адаптивность и эффективность обнаружения атак с синхронизацией кэша. Таким образом, это кажется очень многообещающим для устранения уязвимостей безопасности». ***(Tanya Malhotra. Meet MACTA: An Open-Sourced Multi-Agent Reinforcement Learning Approach for Cache Timing Attacks and Detection // Marktechpost Media Inc. (https://www.marktechpost.com/2023/05/06/meet-macta-an-open-sourced-multi-agent-reinforcement-learning-approach-for-cache-timing-attacks-and-detection/). 06.05.2023).***

***

«…глобальные кибератаки выросли на 7% уже в первом квартале 2023 года. «Еженедельные кибератаки во всем мире увеличились на 7% в первом квартале 2023 года по сравнению с тем же периодом прошлого года, при этом каждая фирма сталкивается в среднем с 1248 атаками в неделю. Цифры взяты из. последнего исследовательского отчета Check Point, в котором также говорится, что сектор образования и исследований подвергся наибольшему количеству атак, увеличившись в среднем до 2507 на организацию в неделю (увеличение на 15% по сравнению с первым кварталом 2022 года) Отчет Check Point также показывает, что в первом квартале 2023 года каждая 31 организация в мире еженедельно подвергалась атакам программ-вымогателей»…

Кроме того, основные статистические данные о вредоносных программах за 2023 год усугубляют проблемы с кибербезопасностью. По оценкам, каждый день обнаруживается 560 000 новых вредоносных программ, и в настоящее время циркулирует более 1 миллиарда вредоносных программ. Это означает, что каждую минуту четыре компании становятся жертвами атак программ-вымогателей…

В довершение всего к более тревожной статистике, согласно общедоступному трекеру утечки данных, созданному британским новостным сайтом The Independent, на сегодняшний день почти 340 миллионов человек пострадали от публично заявленных утечек или утечек данных в 2023 году…

В прошлом году глобальные подключения 5G увеличились на 76% в 2022 году до 1,05 млрд; Проникновение 5G в Северной Америке достигло 32%. Ожидается, что к 2023 году глобальные подключения 5G достигнут 1,9 млрд. Для кибербезопасности это означает меньшую задержку и более быстрые атаки со стороны злоумышленников…

Расширяются как кибератаки, так и уязвимости. В новом отчете State of Cyber Assets Report (SCAR), выпущенном компанией по управлению киберактивами JupiterOne, проанализировано более 291 миллиона активов, результатов и политик для определения текущего состояния корпоративных облачных активов. В отчете показано, что количество активов, которыми управляют организации, в среднем увеличилось на 133% по сравнению с прошлым годом, со 165 000 в 2022 году до 393 419 в 2023 году. Количество уязвимостей в системе безопасности выросло непропорционально, подскочив на 589%. Согласно отчету, данные являются наиболее уязвимым типом активов, на которые приходится почти 60% всех обнаружений безопасности.

«В отчете также освещены проблемы, с которыми сталкиваются группы безопасности, и показано, что в среднем группа безопасности отвечает за 393 419 активов и атрибутов, 830 639 потенциальных угроз безопасности и 55 473 политики. Это привело к усталости от безопасности и нехватке персонала во многих организациях…

В то время как многие отрасли промышленности, в том числе финансы, образование и розничная торговля, стали объектами кибератак, отрасль здравоохранения по-прежнему находится под прицелом хакеров-преступников. Это имеет смысл, поскольку многим учреждениям здравоохранения по-прежнему не хватает необходимых инвестиций и опыта в области кибербезопасности, поскольку их финансирование идет на медицинское оборудование и операции. Преступные

хакеры склонны хвататься за низко висящие плоды. В случае со здравоохранением риски ответственности делают программы-вымогатели логическим средством вымогательства.

«Согласно отчету IBM «Стоимость утечки данных за 2022 год», отрасль здравоохранения по-прежнему остается самой дорогой отраслью для взлома — в среднем 10,1 миллиона долларов — двенадцатый год подряд. Компания Fortified Health обнаружила, что 78 % утечек данных в 2022 г. были связаны с хакерскими атаками и ИТ-инцидентами, что на 45 % больше, чем в 2018 г. На несанкционированный доступ — вторую основную причину — приходилось 38 % инцидентов в 2018 г., а сейчас на его долю приходится только 16 %.. Другими отмеченными причинами были кража, потеря и ненадлежащее удаление данных».

«Злоумышленники часто нацеливаются на организации здравоохранения, потому что взломы и инциденты имеют большое значение. Поскольку здравоохранение является жизненно важной услугой, организации с большей вероятностью будут платить выкуп, чтобы обеспечить непрерывный уход, когда сбои в работе могут иметь разрушительные последствия. Кроме того, организации здравоохранения обладают ценными данными, такими как личная и финансовая информация. Злоумышленники часто могут перепродавать записи по высоким ценам в даркнете…»

Фишинг по-прежнему является одним из предпочтительных методов, используемых преступными хакерами. Почему, потому что это легко сделать и успешно, особенно сейчас, когда многие атаки автоматизируются.

Новое исследование показывает, что до половины всех вложений электронной почты в формате HTML являются вредоносными. «Этот уровень распространенности вредоносного HTML удвоился по сравнению с тем, что было в прошлом году, и, по-видимому, не является результатом кампаний массовых атак, которые рассылают одно и то же вложение большому количеству людей».

«Barracuda использовала свою телеметрию для проведения анализа в мае 2022 года и обнаружила, что 21% HTML-вложений, отсканированных ее продуктами в этом месяце, были вредоносными. Это был, безусловно, самый высокий показатель отношения числа вредоносных файлов к количеству очищенных файлов, отправляемых по электронной почте, но с тех пор он постепенно ухудшался, достигнув 45,7%, а в марте этого года вероятность того, что оно вредоносное, составляет один из двух…»

Новые технологии в сочетании с возможностью оплаты в криптовалютах, которые трудно отследить, ускорили атаки программ-вымогателей в последние годы. Тенденция сохраняется, требования выкупа, сроки восстановления, выплаты и судебные иски о нарушениях растут.

«В 2022 году мы наблюдали увеличение средних требований о выкупе, средних выплат выкупа и среднего времени восстановления в большинстве отраслей», — пишут авторы отчета. «Затишье с программами-вымогателями, которое ознаменовало начало года, закончилось. Группы вымогателей возобновили атаки, и организации должны удвоить свои усилия, чтобы защитить себя от растущих атак».

Управление цифровыми активами и данными Baker Hostetlet проанализировало более 1160 инцидентов с 2022 года. Хотя многие организации повысили безопасность и устойчивость, данные показывают, что субъекты угроз продолжают адаптироваться и находить точки опоры в сети с помощью уклончивого вредоносного ПО, социальной инженерии, «многофакторной аутентификации». бомбардировки» и вброс учетных данных».

Среднее время восстановления после программ-вымогателей выросло почти во всех секторах, «и в большинстве случаев значительно». В 2021 году среднее время восстановления для всех секторов составило чуть более недели. В прошлом году в секторах розничной торговли, ресторанов и гостиничного бизнеса среднее время восстановления увеличилось с 7,8 дней в 2021 году до 14,9 дней в 2022 году, или на 91%.

В здравоохранении продолжительность восстановления увеличилась на 69%, затем последовал рост на 54% в энергетическом и технологическом секторах и на 46% в сегментах государственной промышленности. Это увеличение отразило всплеск требований о выкупе в 6 из 8 отраслей, при этом средняя выплата составила 600 688 долларов…»

Одна из самых больших уязвимостей для кибератак была в цепочке поставок. Это было подчеркнуто нарушениями Colonial Pipeline и Solar Winds и многими другими. Защитить любой бизнес или организацию от множества кибератак — сложная задача, но когда они являются частью цепочки поставок с другими сторонами или поставщиками, это становится еще более сложной задачей. Реальность такова, что 9 из 10 компаний недавно обнаружили риски безопасности цепочки поставок программного обеспечения.

«Опрос, проведенный компанией Reversing Labs, посвященный рискам в цепочке поставок программного обеспечения, показал, что почти 90 % технических специалистов обнаружили значительные риски в своей цепочке поставок программного обеспечения за последний год. Более 70% заявили, что существующие решения для обеспечения безопасности приложений не обеспечивают необходимой защиты. Для исследования были опрошены более 300 глобальных руководителей, специалистов по технологиям и безопасности всех уровней, непосредственно отвечающих за программное обеспечение в корпоративных компаниях».

«Почти все респонденты (98%) признали, что проблемы с цепочкой поставок программного обеспечения представляют значительный риск для бизнеса, ссылаясь на проблемы, выходящие за рамки кода с уязвимостями, раскрытием секретов, подделкой и неправильной настройкой сертификатов. Интересно, что более половины технических специалистов (55%) назвали утечку секретов через исходный код серьезным бизнес-риском, за которым следуют вредоносный код (52%) и подозрительный код (46%)…»

А данные, опубликованные в отчете Black Kite о среде программ-вымогателей за 2023 год, показывают, что число жертв программ-вымогателей, о которых было объявлено в марте 2023 года, почти вдвое больше, чем в апреле 2022 года, и в 1,6 раза выше, чем в пиковый месяц 2022 года. Другие ключевые выводы с 1 апреля 2022 года по 31 марта, 2023, включают:

Основными целевыми отраслями были производство (19,5%), профессиональные, научные и технические услуги (15,3%) и образовательные услуги (6,1%).

Соединенные Штаты были главной страной-жертвой, на которую приходилось 43% организаций-жертв, за ними следуют Великобритания (5,7%) и Германия (4,4%).

Группы вымогателей, как правило, нацелены на компании с годовым доходом от 50 до 60 миллионов долларов, при этом сторонние поставщики часто становятся жертвами вымогательства информации о клиентах.

В первые группы программ-вымогателей за анализируемый период вошли Lockbit (29%), AlphaVM (BlackCat) (8,6%) и Black Basta (7,2%).

Поскольку раскрытие информации о взломе может повлиять на репутацию компании и цены акций, это часто связано с нежеланием сообщать о вторжении общественности. Новые законы, требующие раскрытия информации, особенно в банковском и финансовом сообществе, уже приняты и должны помочь подавить эту тенденцию, но, по-видимому, она еще не укоренилась.

«Новое исследование, опубликованное кибербезопасности сегодня поставщиком Bitdefender, опросило более 400 ИТ-специалистов и специалистов по безопасности, которые работают в компаниях с 1000 и более сотрудников. Bitdefender обнаружил, что 42% опрошенных ИТ-специалистов и специалистов по безопасности получили указание сохранять конфиденциальность нарушений, то есть скрывать их, когда о них следовало сообщать.»

«Возможно, еще более шокирует то, что 29,9% респондентов признались, что на самом деле сохраняли конфиденциальность нарушения, а не сообщали о нем. Это исследование подчеркивает, что вызывающее тревогу количество организаций готовы игнорировать свои обязательства сообщать об утечках данных регулирующим органам и клиентам, пытаясь избежать юридических и финансовых санкций…»

Хотя угрозы более изощренны и эффективны, существуют некоторые основные меры кибергигиены, которые может предпринять любая компания или частное лицо, чтобы стать менее мишенью. Они включают:

Многофакторная проверка подлинности (MFA): MFA помогает ограничить возможность несанкционированного доступа. Обеспечение «постоянной» многофакторной идентификации с помощью дополнительных физических элементов управления или временных вторичных кодов усложняет жизнь киберпреступникам.

Управление идентификацией и доступом: Управление идентификацией и доступом («IAM») гарантирует, что только нужные люди и должности в вашей организации могут получить доступ к инструментам, которые им необходимы для выполнения их работы. С помощью приложений единого входа ваша организация может управлять приложениями сотрудников, не заставляя их входить в каждое приложение в качестве администратора.

Надежное управление паролями: есть практические средства, чтобы избавиться от этой вредной привычки использовать простые пароли для взлома. Не используйте пароли по умолчанию на своих устройствах, а при создании паролей

усложняйте их. Подумайте о том, чтобы сделать их длинными или использовать фразы с буквами, цифрами и символами.

Защитные инструменты: для лучшей защиты также рассмотрите возможность использования брандмауэров, а также установки антивирусного программного обеспечения и программного обеспечения для обнаружения вторжений на ваши устройства.

Обновление и резервное копирование: обязательно своевременно обновляйте и исправляйте свою сеть и поддерживайте надежную программу резервного копирования, которая сегментирует и шифрует конфиденциальные данные.

Наконец, у вас должен быть план реагирования на инциденты. Любой человек в растущей и сложной кибер-вселенной может стать жертвой, а злоумышленники всегда имеют асимметричное преимущество.

Это всего лишь небольшой снимок некоторых тенденций и статистических данных, которые появятся в киберэкосистеме в 2023 году. Как никогда важно быть бдительными и осведомленными о киберугрозах, поскольку на горизонте киберугроз есть о чем беспокоиться». ***(Chuck Brooks. Cybersecurity Trends & Statistics; More Sophisticated And Persistent Threats So Far In 2023 // Forbes (https://www.forbes.com/sites/chuckbrooks/2023/05/05/cybersecurity-trends--statistics-more-sophisticated-and-persistent-threats-so-far-in-2023/?sh=4f38601a7cb6). 05.05.2023).***

***

«Около половины ракетной программы Северной Кореи финансируется за счет кибератак и кражи криптовалюты, заявил во вторник представитель Белого дома.

Федеральное правительство США прилагает широкие усилия, чтобы понять, почему «такая страна, как [Северная Корея], настолько изобретательна в этом пространстве», — заявила Энн Нойбергер, заместитель советника по национальной безопасности по кибербезопасности и новым технологиям, на мероприятии, организованном некоммерческой организацией Special. Проект конкурентных исследований.

Спецслужбы США работают над выявлением северокорейских оперативников, а министерство финансов отслеживает украденную криптовалюту, сказал Нойбергер, добавив, что администрация Байдена «тратит много времени и усилий» на решение этой проблемы.

Эта оценка предполагает, что хакерские атаки и киберпреступность являются ключом к выживанию северокорейского режима. Комментарии Нойбергера прозвучали на фоне возросшей обеспокоенности международного сообщества ракетной и ядерной программой Пхеньяна. CNN сообщал, что новая межконтинентальная баллистическая ракета, которую Северная Корея испытала в апреле, может позволить режиму быстрее наносить ядерные удары большой дальности Ранее.

В прошлом месяце министерство юстиции обвинило северокорейца в сложной схеме отмывания денег, в рамках которой сотрудники американских криптовалютных компаний помогали финансировать северокорейский режим.

На публичном мероприятии в июле прошлого года Нойбергер сказал, что северокорейцы «используют кибернетику, чтобы получить, по нашим оценкам, до трети своих средств для финансирования своей ракетной программы». Представитель Нойбергер сообщил CNN в среду, что обновленная цифра, которую она привела на этой неделе, является точной. Это говорит о том, что в последующие месяцы важность этой проблемы, во всяком случае, только возросла.

Согласно сообщениям ООН и частных компаний, за последние несколько лет северокорейские хакеры украли миллиарды долларов у банков и компаний, занимающихся криптовалютой, что стало ключевым источником дохода для режима. Официальные лица США давно подозревали, что по крайней мере часть этих денег идет на разработку оружия Пхеньяном, но редко публично подробно говорили об этом.

Недавнее расследование CNN выявило безудержные усилия северокорейских хакеров по краже криптовалюты и ее отмыванию в наличные деньги, которые могли бы помочь финансировать оружейные программы диктатора Ким Чен Ына. Другое расследование CNN выявило одного криптовалютного предпринимателя, который сказал, что его фирма невольно отправила северокорейскому ИТ-специалисту десятки тысяч долларов.

Такая северокорейская киберактивность является частью регулярных разведывательных продуктов, представляемых высокопоставленным чиновникам США, иногда включая президента Джо Байдена, как ранее сообщил высокопоставленный чиновник США CNN». ***(Sean Lyngaas. Half of North Korean missile program funded by cyberattacks and crypto theft, White House says // Cable News Network (https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/). 10.05.2023).***

***

«Неизвестные хакеры попытались проникнуть в Dragos, одну из ведущих фирм в области промышленной кибербезопасности, которая работает с государственными учреждениями и коммунальными службами по всему миру, в рамках безуспешной кампании, нацеленной на руководителей компании и членов их семей, сообщила фирма в среду.

«Мы уверены, что наши многоуровневые средства контроля безопасности помешали злоумышленнику выполнить то, что мы считаем его основной целью — запустить программу-вымогатель», — написала компания в сообщении в блоге, в котором говорится, что попытки вымогательства начались в понедельник и что никакие корпоративные системы или продукты не были взломан.

Однако хакерская группа получила доступ к личному адресу электронной почты нового сотрудника отдела продаж до того, как этот человек начал работать в компании. По словам Драгоса, хакеры начали красть общие данные из программы совместной работы Microsoft SharePoint, а также 25 аналитических отчетов и систем поддержки клиентов после входа в учетную запись электронной почты нового сотрудника. Компания отметила, что в одном из этих разведывательных отчетов был IP-адрес клиента. Неясно, когда хакеры взломали адрес электронной почты нового сотрудника.

«Хотя внешняя фирма по реагированию на инциденты и аналитики Dragos считают, что событие локализовано, расследование продолжается. Данные, которые были утеряны и, вероятно, будут обнародованы, потому что мы решили не платить за вымогательство, вызывают сожаление», — сказал Драгош.

Хакеры попытались проникнуть в несколько других частей инфраструктуры Dragos, таких как служба поддержки ИТ, финансовые и маркетинговые системы. Кроме того, злоумышленники пытались получить доступ к системе распознавания сотрудников и «лидерам продаж», говорится в отчете. По словам компании, хакеры не смогли получить доступ к этим системам из-за правил управления доступом на основе ролей.

По словам Dragos, когда он не ответил на требования о вымогательстве, хакеры начали атаковать руководителей, членов их семей и других лиц, связанных с компанией. Одно из сообщений гласило: «Им нет дела до вас или вашей организации. Будьте как сотни компаний, которые обращаются с нами должным образом».

После того, как Dragos по-прежнему не вмешивался, преступники связались с несколькими известными контактами Dragos, «чтобы получить ответ», пишет компания. «Наше решение состояло в том, что лучшим ответом было не связываться с преступниками», — сказал Dragos.

Скриншот канала Telegram, опубликованный в Твиттере vx-underground, онлайн-репозиторием вредоносных программ, похоже, является субъектом, который нацелился на Dragos, хотя это не было подтверждено. Канал, похоже, был создан в среду после сообщения в блоге Dragos.

Владелец канала заявил, что инцидент не был атакой программы-вымогателя. Преступные хакеры назвали Dragos «преступной организацией», которая «вместо того, чтобы достичь решения», заплатив за вымогательство, компания «пытается серьезно преуменьшить значение инцидента».

Подозреваемые хакеры также заявили, что инцидент не был атакой программы-вымогателя, и заявили, что у них есть доступ к более чем 130 гигабайтам данных, украденных из сетей Dragos. До сих пор не было никаких доказательств того, что утверждение верно.

Публичный ответ Dragos на нападение и прозрачность компании вызвали одобрение экспертов. Брейн Харрелл, бывший помощник секретаря DHS, сказал, что «хотя это не повлияло на клиентов, это яркий пример того, как изолировать, смягчать последствия, восстанавливать и раскрывать информацию».

«Часто компании замолкают, кружат вокруг фургонов и отказываются отвечать, когда сталкиваются с проблемой безопасности», — сказал он. «Поскольку противники из числа национальных государств нацелены на сообщества поставщиков, обслуживающих критически важную инфраструктуру, эта модель прозрачности является одной из моделей, которым могут подражать другие, сталкиваясь с проблемой». ***(Christian Vasquez. Hackers attempt to extort Dragos and its executives in suspected ransomware attempt // CyberScoop (https://cyberscoop.com/dragos-cyberattack-ransomware/). 10.05.2023).***

***

«В новом отчете поставщика услуг по защите от кражи и фильтрации содержимого DNS DNSFilter Inc отмечается значительный всплеск трафика на вредоносные сайты, содержащие угрозы, за шесть месяцев до марта.

Отчет State of Internet Security Q1 '23 показал, что с октября по март трафик на сайты с угрозами увеличился на 61%, но рост трафика был намного выше, когда речь шла о сайтах, идентифицированных как предлагающие злонамеренный фишинг, вредоносное ПО, крипто-мошенничество и трафик ботнета, который подскочил на 282%.

Отражая аналогичный вывод из недавнего отчета Cofense Inc., DNSFilter обнаружил, что трафик только на фишинговые сайты за тот же период вырос на 464%. В отчете говорится, что рост фишинга указывает на то, что фишинг по-прежнему является успешной тактикой для хакеров и что компаниям необходимо делать больше для информирования своих сотрудников об этих атаках.

Возможно, неудивительно, что фишинговые и мошеннические атаки чаще всего были направлены на финансовые услуги, за которыми следуют розничная торговля, дистрибуция и производство. В финансовом секторе почти 83% кликов по доменным угрозам были связаны с фишингом и обманом, а компании, занимающиеся программным обеспечением, оборудованием и технологиями, показали 39% кликов.

Около 61% доменных угроз, направленных на здравоохранение и медицинские организации, также были кликнуты. В отчете отмечается, что сотрудники здравоохранения и медицинского сектора в два раза чаще нажимают на фишинговые ссылки, чем сотрудники других секторов.

В отчете также указано, что 78% угроз были обнаружены на уровне DNS, что указывает на необходимость того, чтобы группы информационных технологий в разных отраслях сосредоточили внимание на своих корпоративных сетях.

«Организации должны работать безопасно, не опасаясь стать жертвами фишинга, программ-вымогателей или других атак на основе DNS», — отмечается в отчете. «Эти компании должны знать, что они защищены, обнаруживая и блокируя угрозы, а также устанавливая и применяя политики в отношении контента с мониторингом в реальном времени».

DNSFilter уже упоминался в новостях в марте, когда он объявил о новом совместном решении с Banyan Security для упрощения корпоративной безопасности с нулевым доверием. Решение сочетает передовые технологии обнаружения угроз и фильтрации контента DNSFilter с платформой удаленного доступа Banyan Security, чтобы обеспечить наименее привилегированный доступ к приложениям и службам в гибридных и мультиоблачных инфраструктурах». ***(Duncan Riley. Traffic to malicious sites surges through March // SiliconANGLE Media Inc. (https://siliconangle.com/2023/05/11/traffic-malicious-sites-surges-through-march/). 11.05.2023).***

***

«У GlobalLogic розповіли 24 Каналу, що сім з десяти малих підприємств не готові захищатися від цифрових шахраїв, а досвідчені хакери можуть проникнути в систему організації всього за 12 годин. Однак інтеграція систем

кібербезпеки на ранніх стадіях розробки програмного забезпечення може підвищити безпеку персональних даних і знизити потенційні втрати від злому.

Інженери GlobalLogic вважають, що для боротьби зі зростаючими загрозами кібератак необхідно впроваджувати комплексні програмні рішення.

На галузь кібербезпеки чекають чималі виклики

У 2023 році головним викликом для фахівців з кібербезпеки стане використання штучного інтелекту для автоматизації хакерських атак і пошуку нових способів злому. Мобільні пристрої, SaaS-застосунки та сервери, що зберігають великі обсяги персональних даних, можуть стати вразливими до нових вірусів.

Українські інженери вже впроваджують нові розробки для зміцнення глобальної кібербезпеки. Вони створюють новітні системи захисту, своєчасно оновлюють програмне забезпечення, оцінюють ризики та стійкість окремих систем.

Інженери GlobalLogic розробили та впровадили програми цифрової безпеки у низці сфер, зокрема:

охорона здоров'я,
освіта,
електронні платежі,
медіа,
мобільні застосунки.

Вони також захищають домівки користувачів – від систем відеоспостереження до домашніх роутерів.

Наприклад, українські інженери допомогли розробити домашній роутер для компанії з інформаційної та мережевої безпеки, який попереджає користувачів про кіберзагрози. Це обладнання використовують близько 500 операторів зв'язку та понад 1 000 підприємств в ЄС, захищаючи 23 мільйони абонентів тільки в Європі.

Захист розумних будинків

Українські інженери також зробили значний внесок у підвищення безпеки «розумних» будинків, розробивши програмне забезпечення для приватних будинків та багатоповерхових комплексів. Крім того, вони створили безпечні мобільні платіжні додатки та провели аудит і тестування на проникнення для виробників медичного обладнання.

Невід'ємною частиною кібербезпеки бізнесу залишаються регулярні системні аудити. Наприклад, інженери перевірили стійкість навчальної програми для провідного виробника газованих напоїв, виявивши 24 вразливості, 17 з яких були критичними. Це спонукало замовника збільшити фінансування кібербезпеки та провести повторне тестування системи після усунення вразливостей.

На практиці українські інженери роблять значний внесок у глобальну кібербезпеку захищаючи мільйони людей від кіберзагроз, розробляючи інноваційні та безпечні програмні рішення, які захищають приватних осіб, підприємства та організації. Їх робота має вирішальне значення у боротьбі з кіберзлочинністю та постійному розвитку безпечних систем у технологічному ландшафті, що постійно змінюється». ***(Михайло Года. Українські інженери захищають 23 мільйони європейців від кіберзагроз // ПрАТ «Телерадіокомпанія «Люкс»***

(https://24tv.ua/tech/23-milyoni-yevropeytsiv-zahishheni-vid-kiberzagroz-zavdyaki-ukrayinskim_n2308579). 07.09.2023).

***

«Характер кибератак быстро меняется. Генеративный ИИ, облачная сложность и геополитическая напряженность являются одними из новейших видов оружия и помощников в арсеналах злоумышленников. Три четверти (74%) лиц, принимающих решения в области безопасности, говорят, что конфиденциальные данные их организаций были «потенциально скомпрометированы или взломаны только за последние 12 месяцев». Это отрезвляющий базовый уровень кибербезопасности для любого директора по информационной безопасности.

Злоумышленники быстро используют генеративный ИИ в качестве оружия, находят новые способы скомпрометировать сложность облака и используют геополитическую напряженность для запуска более изощренных атак, прежде чем станет лучше, будет только хуже.

В отчете Forrester «Главные угрозы кибербезопасности в 2023 году» (требуется клиентский доступ) содержится строгое предупреждение о главных угрозах кибербезопасности в этом году, а также рекомендации для директоров по информационной безопасности и их команд по противодействию им. Применяя генеративный ИИ в качестве оружия и используя ChatGPT, злоумышленники оттачивают свои вымогательства и социальной инженерии. методы

Два фронта глобальной угрозы

Директора по информационной безопасности вынуждены бороться с давно укоренившимися угрозами и в то же время обнаруживают, что не готовы противостоять новым. Программа-вымогатель и социальная инженерия посредством компрометации деловой электронной почты (BEC) — это давние угрозы, на защите от которых директора по информационной безопасности годами концентрировались. Тем не менее, несмотря на то, что специалисты по безопасности вложили миллионы долларов в укрепление своих технических стеков, конечных точек и систем управления идентификацией для борьбы с программами-вымогателями, количество нарушений продолжает расти.

Во-первых, поскольку они ищут новые способы увеличить размер и скорость выплат программ-вымогателей, злоумышленники делают цепочки поставок, поставщиков медицинских услуг и больницы главными целями. Любая цель, которая предоставляет срочные услуги и не может позволить себе долгое время не работать, является источником более крупных выплат программ-вымогателей, поскольку этим предприятиям необходимо немедленно вернуться в онлайн.

Прогнозы Forrester и результаты опросов также показывают, почему по мере появления новых угроз все больший процент взломов остается незарегистрированным. Директора по информационной безопасности и предприятия не захотят признавать, что они были не готовы. Двенадцать процентов специалистов по безопасности и управлению рисками говорят, что за последние 12 месяцев у них было от шести до более 25 взломов. Нарушения, представленные в этом отчете, связаны с BEC, атаками с использованием социальной инженерии и программами-

вымогателями. Появляются новые, более смертоносные стратегии атак, направленные на разрушение защиты на основе ИИ.

Устаревшие системы на основе периметра, не предназначенные для обновления на основе ИИ, являются наиболее уязвимыми. С грядущей новой волной кибератак, которые стремятся извлечь выгоду из самых слабых звеньев любого данного бизнеса, включая сложные облачные конфигурации, разрыв между зарегистрированными и фактическими нарушениями будет увеличиваться.

В 7 из 10 организаций, опрошенных Forrester, в прошлом году произошло как минимум одно нарушение. Двенадцать процентов подверглись шести или более атакам, в которых использовались давние технические приемы. Источник: Главные угрозы кибербезопасности Forrester в 2023 г.

Взгляд Forrester на главные угрозы кибербезопасности в этом году

В связи с новой волной угроз Forrester ожидает новых смертоносных атак, поскольку злоумышленники расширяют свой опыт в области искусственного интеллекта, чтобы побеждать новейшее поколение средств защиты от кибербезопасности. VentureBeat узнала, что это уже происходит, поскольку незащищенные пробелы между конечными точками и защитой личности являются слабым звеном, на которое обращают внимание злоумышленники.

Президент CrowdStrike Майкл Сентонас сказал VentureBeat в недавнем интервью, что необходимость устранения пробелов между защитой конечных точек и защитой личных данных является «одной из самых больших проблем, с которыми люди хотят справиться сегодня. Сессия хакерского разоблачения, которую Джордж и я провели на RSA [2023], должна была показать некоторые проблемы с идентификацией и сложностью, а также почему мы связали конечную точку с идентификацией [и] с данными, к которым пользователь обращается. Это критическая проблема. И если вы можете решить это, это сложно, но если вы можете, вы решаете большую часть киберпроблемы организации».

Появляются реальные угрозы развертыванию ИИ

Используя генеративный ИИ, ChatGPT и поддерживающие их большие языковые модели, злоумышленники могут масштабировать атаки с невозможными ранее уровнями скорости и сложности. Forrester прогнозирует, что варианты использования будут продолжать расти, ограничиваясь только творческим подходом злоумышленников.

Одним из первых вариантов использования является метод отравления данных, вызывающий дрейф алгоритмов, что снижает эффективность обнаружения средств защиты электронной почты или потенциальный доход от по электронной торговле механизмов рекомендаций. То, что когда-то было нишевой темой, теперь стало одной из самых насущных угроз, которую нужно предвидеть и противостоять. Forrester отмечает, что, хотя многие организации не сталкиваются с непосредственным риском этой угрозы, важно понимать, какие поставщики средств безопасности могут защитить от атак на модели и алгоритмы ИИ. Forrester рекомендует в отчете, что «если вам нужно защитить развертывание ИИ в вашей фирме, рассмотрите таких поставщиков, как HiddenLayer, CalypsoAI и Robust Intelligence».

Сложность облачных вычислений растет

Облачные сервисы используют 94 % предприятий, а 75 % считают, что безопасность является главной задачей. Целых две трети компаний имеют облачную инфраструктуру. В прошлом году Gartner подсчитала, что переход на облачные технологии повлияет на корпоративные расходы на ИТ в этом году на сумму более 1,3 трлн долларов и почти на 1,8 трлн долларов в 2025 году. По сравнению с 41 % в 2022 году, к 2025 году 51% ИТ-расходов будет перемещен в общедоступное облако. А на облачные технологии будет приходиться 65,9% расходов на прикладное ПО в 2025 году по сравнению с 57,7% в 2022 году.

Эти прогнозы доказывают, что все более сложная природа облачных вычислений и инфраструктуры хранения данных создает значительные риски для безопасности. Forrester отмечает, что небезопасные конфигурации инфраструктуры IaaS, атаки без вредоносного ПО и повышение привилегий, а также дрейф конфигурации — это лишь некоторые из множества поверхностей угроз, о которых директорам по информационной безопасности и их командам необходимо знать и защищать.

В отчете рекомендуется, чтобы предприятия создавали отказоустойчивое и надежное управление облаком и использовали инструменты безопасности, такие как собственные возможности безопасности платформ IaaS, управление состоянием безопасности в облаке и управление состоянием безопасности SaaS, для обнаружения и устранения угроз и попыток взлома.

Форрестер приводит вторжение России в Украину и ее безжалостные кибератаки на украинскую инфраструктуру как примеры геополитических кибератак с непосредственными глобальными последствиями. Forrester сообщает, что субъекты национального государства будут продолжать использовать кибератаки на частные компании в геополитических целях, таких как шпионаж, рычаги давления на переговорах, контроль над ресурсами и кража интеллектуальной собственности, чтобы получить технологическое превосходство.

Форрестер указывает на продолжающуюся дипломатическую и торговую напряженность между Китаем и США как на горячую точку, которая может усилить атаки на предприятия. В отчете говорится, что в конце 2022 года США ограничили экспорт китайских полупроводниковых микросхем и импорт коммуникационного оборудования. Китай ввел санкции против американских оборонных подрядчиков в начале 2023 года. Россия сталкивается с европейскими торговыми запретами и экспортным контролем. Эти конфликты могут затронуть частные компании. Северная Корея, крадущая 741 миллион долларов в криптовалюте из Японии, является еще одним примером того, как геополитические угрозы могут быстро дестабилизировать финансовое положение всей страны.

Программы-вымогатели продолжают атаковать организации

По данным Forrester, программы-вымогатели остаются главной киберугрозой, и злоумышленники требуют двойного вымогательства для предотвращения раскрытия данных. Злоумышленники также требуют выкуп от клиентов взломанных предприятий, чтобы сохранить конфиденциальность своих данных, что еще больше подрывает репутацию и доверие предприятия.

Forrester наблюдает атаки программ-вымогателей, нацеленных на критически важную инфраструктуру и цепочки поставок, где задержки могут стоить миллионы долларов. Злоумышленники знают, что если они смогут нарушить цепочку поставок, их требования о более высоких выплатах программ-вымогателей будут быстро удовлетворены предприятиями, которые не могут позволить себе простоять в течение длительного времени.

Больше всего беспокоит вывод Forrester о том, что в период с 2016 по 2021 год количество атак программ-вымогателей на больницы удвоилось, подвергая опасности жизни людей. Программы-вымогатели — это обычная тактика, которую Северная Корея использует для финансирования своих программ шпионажа и разработки ракет.

В ответ более 30 стран сформировали Инициативу по борьбе с программами-вымогателями (CRI) в октябре 2021 года для борьбы с глобальными программами-вымогателями. Австралия возглавляет Международную по борьбе с целевую группу программами-вымогателями (ICRTF) для борьбы с программами-вымогателями в рамках стратегии CRI. Forrester рекомендует предприятиям также «уделять одинаковое внимание защите от программ-вымогателей и подписываться на внешних поставщиков услуг по анализу угроз, таких как CrowdStrike или Mandiant».

В отчете также напоминается группам безопасности и управления рисками в компаниях с критической инфраструктурой, что они должны быть готовы сообщать о кибер-инцидентах в течение 72 часов и выплачивать выкуп в течение 24 часов в CISA в соответствии с Законом об отчетах о кибер-инцидентах для критически важной инфраструктуры от 2022 года.

Социальная инженерия BEC лидирует среди программ-вымогателей по страховым случаям

ФБР Центр жалоб на преступления сообщил, что в 2021 году компаниям был нанесен ущерб в размере 2,4 миллиарда долларов в результате социальной инженерии BEC. Мошеннические требования о переводе средств в результате атак BEC превысили все типы требований в 2022 году, обогнав атаки программ-вымогателей. Атаки социальной инженерии BEC используют человеческий фактор. Они используют фишинг, например, для кражи учетных данных и неправомерного использования учетных записей.

Forrester отмечает, что кампании социальной инженерии BEC переходят в новую фазу, стремясь объединить несколько каналов связи, чтобы убедить жертв действовать. Некоторые кампании включают процесс CAPTCHA для повышения их легитимности. В отчете сообщается, что недостаточно принять проверку подлинности сообщений на основе домена, отчетность и соответствие (DMARC) для проверки подлинности электронной почты. Предприятиям следует использовать подход к изменению поведения, основанный на данных, чтобы измерять прогресс, и корректировать курс с помощью дополнительного обучения и технологий, чтобы снизить риск успеха атак с использованием социальной инженерии.

Службы безопасности должны быть готовы

Последний отчет Forrester об угрозах кибербезопасности — это серьезное предупреждение организациям по всему миру, чтобы они готовились к эпохе новых стратегий атак. Злоумышленники продолжают совершенствовать свое мастерство,

включая новые тактики для использования генеративного ИИ в качестве оружия, использования сложности облака и использования геополитической напряженности для проведения более изощренных атак.

В то время как предприятия продолжают финансировать бюджеты на кибербезопасность для сдерживания атак социальной инженерии BEC и программ-вымогателей, им также необходимо начать планировать, как прогнозировать, выявлять и реагировать на угрозы для их моделей и алгоритмов ИИ и данных, которые они используют. Чтобы улучшить аналитику угроз, группы безопасности должны объединить эти разнообразные усилия, чтобы остановить кибератаки следующего поколения». ***(Louis Columbus. Forrester predicts 2023's top cybersecurity threats: From generative AI to geopolitical tensions // VentureBeat (https://venturebeat.com/security/forrester-predicts-2023-top-cybersecurity-threats-generative-ai-geopolitical-tensions/). 22.05.2023).***

***

«Любой, кто работает в сфере ИТ-безопасности, скажет вам, что он участвует в гонке вооружений. Цифровизация мировой экономики за последние два десятилетия привела к тому, что самые распространенные кибератаки стали для преступных организаций лучшим средством получения прибыли. Следовательно, как отделы ИТ-безопасности, так и киберпреступные картели стремились подорвать усилия друг друга в постоянном тет-а-тет взломе и патчах.

Новое независимое исследование, проведенное по заказу Sophos, показывает, что преимущество в этой гонке неумолимо переходит к киберпреступникам. В ходе опроса 3000 бизнес-лидеров, отвечающих за кибербезопасность своих организаций в 14 странах, более 94% респондентов сообщили, что за последний год они подверглись той или иной форме кибератаки. Между тем ошеломляющие 93% организаций заявили, что считают выполнение основных задач по обеспечению безопасности «сложным». Еще хуже процент респондентов, ставших жертвами кибератак за последние 12 месяцев. В то время как программы-вымогатели были излюбленным инструментом подрывной деятельности киберпреступников, 27% организаций подверглись фишинговым атакам, а 26% и 24% подверглись краже данных и кибервымогательству соответственно.

Часто причиной этих разрушительных нарушений был так называемый активный противник, субъект угрозы, способный адаптировать свои методы, тактику и процедуры в режиме реального времени в ответ на защитные действия ИТ-отделов и их партнеров. 23% организаций заявили, что их атаки были предприняты этими типами хакеров, хотя кажется, что они больше заинтересованы в предлагаемых более крупных и привлекательных целях — для компаний стоимостью 10 миллионов долларов или меньше количество зарегистрированных активных атак злоумышленников снизилось. всего до 11%.

Время отклика

Пока что все так удручающе — настроение усугубляется общим чувством усталости среди респондентов, отражающих кибератаки. Согласно опросу, около 93% компаний сочли выполнение основных оперативных задач в области кибербезопасности «сложным», при этом среднее время обнаружения, источника и

устранения угроз составляет в среднем до 15 часов для фирм со штатом от 3001 до 5000 человек. Более того, около 55 % респондентов заявили, что отражение кибератак негативно влияет на работу их ИТ-команд над другими проектами.

Как должны реагировать организации? Одним из очевидных шагов было бы уменьшение поверхности атаки, которую могут подкупить хакеры. Сокращая базовое количество возможностей, которые киберпреступники могут использовать для взлома систем вашей компании, ИТ-отделы кибербезопасности могут более эффективно сосредоточить свои усилия. Адаптивная защита также важна, не в последнюю очередь в борьбе с активными противниками, которые по умолчанию принимают ту же атакующую позицию.

Респонденты соглашаются. Три четверти опрошенных заявили, что планируют добавить инструменты Endpoint Detection and Response (EDR) и/или Extended Detection and Response (XDR) в течение года. Между тем, 44% обдумывали инвестиции в услуги управляемого обнаружения и реагирования (MDR). Sophos может помочь во всех трех случаях. Его решения EDR, сети, брандмауэра, облака и электронной почты помогают автоматически блокировать 99,98% угроз, а встроенная проверка работоспособности учетной записи выявляет области, в которых существующие корпоративные средства защиты отсутствуют.

Только сопоставив адаптивные способности со следующим поколением киберпреступников, фирмы могут надеяться защитить себя от растущей волны киберпреступности. Используя инструменты Sophos, использующие данные телеметрии из огромной сети корпоративных клиентов и средства контроля кибербезопасности третьих сторон, компании могут делать это и многое другое, тем самым защищая себя и свою клиентскую базу от авантюристических киберпреступных картелей». ***(Cybersecurity in 2023 is a two-speed system // New Statesman Media Group Ltd. (https://techmonitor.ai/partner-content/cybersecurity-in-2023-two-speed-system). 22.05.2023).***

***

«ФБР, Агентство кибербезопасности и безопасности инфраструктуры (CISA) и Австралийский центр кибербезопасности (ACSC) предупреждают малые предприятия об использовании программного обеспечения для удаленного доступа, такого как протокол удаленного рабочего стола (RDP), из-за эскалации угроз, исходящих от банды вымогателей BianLian.

Кибербанда, свирепствующая с 2022 года, успешно взламывает системы Windows, используя учетные данные RDP. После получения личных данных они вымогают деньги, угрожая опубликовать информацию.

Согласно бюллетеню агентства #StopRansomware, ограничение использования программного обеспечения для удаленного доступа является наиболее эффективным способом предотвращения вымогательства. Но есть ряд других практических мер, которые может предпринять бизнес, о которых мы расскажем в этой статье.

Если вы используете протокол удаленного рабочего стола Microsoft (RDP), возможно, пришло время подумать о переходе на альтернативу.

Это связано с тем, что, согласно релизу совместного совета по кибербезопасности (SCA), компьютерное программное обеспечение

эксплуатируется BianLian — бандой киберпреступников и разработчиком программ-вымогателей, которые уже почти год нацелены на предприятия и организации критической инфраструктуры.

Согласно заявлению, недавно разосланному агентствами, кибербанда использовала RPD как точку входа в Windows Systems. Затем, получив доступ, они развертывают вредоносное программное обеспечение для кражи дополнительных учетных данных или эксфильтрации конфиденциальных данных с целью вымогательства у жертвы.

Известно, что помимо использования учетных данных RPD злоумышленники также используют тактику фишинга для получения конфиденциальной информации от работников.

Группа вымогателей BianLian была впервые обнаружена в июне 2022 года. С момента своего возникновения банда перечислила на своем портале вымогательства в общей сложности 118 организаций, 71% из которых являются американскими компаниями.

Банда также перешла от вымогательства у жертв путем шифрования их файлов к угрозам обнародования украденных данных. По мере того, как стратегии BianLian становятся все более безжалостными, угрозы, которые она представляет для американского бизнеса, никогда не были такими серьезными.

Итак, каковы наилучшие способы избежать этой тактики, согласно последнему отчету органов безопасности?

Как компаниям защититься от BianLian?

Неудивительно, что лучший способ избежать преследования со стороны BianLian — ограничить использование программного обеспечения для удаленного рабочего стола, такого как RDP.

Если вы не можете прекратить использование программного обеспечения, совет по кибербезопасности рекомендует проводить аудит инструментов удаленного доступа и следить за ненормальным использованием этих программ, просматривая журналы.

Закрытие неиспользуемых портов RDP, принудительная блокировка учетной записи после определенного количества попыток входа и применение многофакторной аутентификации (MFA) с защитой от фишинга — вот некоторые другие советы, которые агентства по кибербезопасности предложили в своем выпуске.

Помимо аудита вашего программного обеспечения для удаленного рабочего стола, они также советуют ограничить использование PowerShell и обновить Windows PowerShell до последней версии.

Согласно руководству, поддержание надлежащей гигиены паролей — это еще один способ предотвратить угрозы. Это включает в себя создание кодов доступа длиной 15 символов и более, их хранение в признанных в отрасли менеджерах паролей и отключение подсказок для пароля». ***(Isobel O'Sullivan. FBI Issues Stark Warning on Remote Desktop Ransomware // Tech.co (https://tech.co/news/fbi-warning-limit-remote-desktop-software). 18.05.2023).***

***

«Согласно новым данным Sophos, компаниям необходимо свыкнуться с мыслью о том, что злоумышленники будут пробираться сквозь их защиту. Но они все еще могут бросить им вызов, как только они пробьют ворота.

Некоторые из самых опасных уязвимостей, с которыми сталкиваются компании сегодня, — это те, которые в любом другом мире остались бы совершенно незамеченными. Эти уязвимости, известные как LOLBins — отсылка к бинарным файлам «жить за счет земли», а не к практике маниакального смеха над мусорными баками, — это исполняемые файлы, встречающиеся естественным образом в операционных системах; ошибки в коде, допущенные давным-давно, которые остаются незамеченными разработчиками, но охотно разыскиваются среднестатистическим киберпреступником.

Затем, конечно же, появляется множество других уязвимостей, которые предоставляют злоумышленникам окно во внутреннюю работу вашей корпорации. Согласно новому отчету Sophos Active Adversary Report for Business Leaders, анализу 152 расследований реагирования на инциденты (IR) в 31 стране уязвимости ProxyShell и Log4Shell вырисовывались особенно крупными. Скомпрометированные учетные данные также являются источником особого беспокойства, объясняет Джон Шир, местный технический директор фирмы по кибербезопасности.

«Сегодняшние злоумышленники не взламывают систему, а входят в систему, — говорит Шиер. «Реальность такова, что среда угроз выросла по объему и сложности до такой степени, что защитникам не осталось заметных пробелов, которые можно было бы использовать. Для большинства организаций дни работы в одиночку давно позади».

Эпидемия программ-вымогателей

Между тем программы-вымогатели остановили свой экспоненциальный рост в качестве метода атаки. Тем не менее, это остается чумой. Две трети фирм, исследованных командой Sophos IR, обнаружили, что эта форма цифрового захвата заложников была сочтена угрозой, что неудивительно, учитывая, что программы-вымогатели фигурировали почти в трех четвертях их расследований за последние три года. Время пребывания атакующего также уменьшается. Данные Sophos показывают, что для всех типов атак злоумышленники проводят в системах компании в среднем десять дней по сравнению с 15 днями в предыдущем году. Это не зависит от размера компании.

Существуют решения — услуги, которые могут помочь компаниям сформулировать глубокую защиту, чтобы лучше защитить себя от атак. «Организации, которые успешно внедрили многоуровневую защиту с постоянным мониторингом, получают лучшие результаты с точки зрения серьезности атак», — говорит Шиер. Причина проста: улучшенная защита, в свою очередь, означает, что злоумышленники ускоряют свои атаки, становятся более заметными для отделов ИТ-безопасности и сталкиваются с ними на гораздо более раннем этапе, чем в противном случае. И наоборот, добавляет Шиер, «те, у кого не будет упреждающего мониторинга, пострадают от самых серьезных последствий».

Короче говоря, поэтому предприятия не должны падать духом. В то время как среда угроз постоянно развивается, Sophos по-прежнему готова пресечь оппортунистические авантюры киберпреступников, предлагая такие услуги, как

облачная центральная консоль управления и доступ к Sophos X-Ops, своему междоменному подразделению анализа угроз. «Это действительно все, везде и сразу», — говорит Шиер о текущей среде угроз. «Однако для предприятий доступны инструменты и услуги, которые могут частично облегчить оборонительную нагрузку, позволяя им сосредоточиться на своих основных бизнес-приоритетах». ***(The key to good corporate cybersecurity is defence in depth // New Statesman Media Group Ltd. (https://techmonitor.ai/partner-content/key-to-good-corporate-cybersecurity-defence-in-depth). 22.05.2023).***

***

«Последний отчет Microsoft Cyber Signals показывает, как киберпреступники используют операционные технологии (OT) в качестве шлюзов в сеть организации.

Это происходит в то время, когда соединения IoT в регионе растут, и GSMA прогнозирует, что к 2025 году в регионе MENA ожидается 1,1 миллиарда подключений IoT. Именно этот рост OT и IoT дал киберпреступникам больше возможностей взломать сеть организации.

Отчет Microsoft Cyber Signals — это регулярный краткий обзор киберугроз, в котором освещаются тенденции в области безопасности и информация, собранная из 65 триллионов ежедневных сигналов безопасности Microsoft и 8500 экспертов по безопасности. Последнее издание показало, что конвергентные системы ИТ, Интернета вещей (IoT) и OT представляют более широкий риск для критической инфраструктуры.

Для ИТ-директоров на Ближнем Востоке и в Африке (MEA) последствия возможного нарушения безопасности имеют первостепенное значение во все более сложной среде угроз. Об этом свидетельствует рост расходов на кибербезопасность на Ближнем Востоке и в Северной Африке (БВСА) на 11,2% к 2022 году.

Растущие темпы цифровой трансформации в африканском регионе способствуют появлению новых векторов атак и возможностей для киберпреступников. Для нигерийских ИТ-директоров последствия возможного нарушения безопасности являются их главной заботой, поскольку они стремятся ориентироваться во все более сложной среде угроз и нормативно-правовой базы.

Об этом говорится в исследовании «Тенденции корпоративной безопасности в Нигерии», проведенном IDC по заказу Microsoft. Нигерийские организации осознают важность разработки упреждающего подхода к безопасности. Опрос IDC показал, что 72% организаций в Нигерии увеличили бюджеты на безопасность на 10% и более за последние несколько лет.

Рост цифровой трансформации в регионе позволил организациям управлять своими зданиями, аварийными системами и контролем доступа с помощью интеллектуальных устройств, подключенных к сети. Кроме того, мы наблюдаем увеличение количества устройств IoT на рабочем месте, чтобы лучше обеспечить гибридную работу, такую как интеллектуальные конференц-залы с микрофонами и камерами.

Поскольку ландшафт угроз продолжает расширяться и становиться все более сложным, организациям необходимо переосмыслить свой подход к киберрискам,

чтобы оставаться на шаг впереди потенциальных злоумышленников. Cyber Signals обнаружила, что в настоящее время в Интернете открыто более 1 миллиона подключенных устройств, на которых работает Boa, устаревшее и неподдерживаемое программное обеспечение, которое все еще широко используется в устройствах IoT и комплектах для разработки программного обеспечения…» ***(Justus Adejumoh. IT Teams Face Cyber Security Challenges By New OT Threat // Independent Newspapers Limited (https://independent.ng/it-teams-face-cyber-security-challenges-by-new-ot-threat/).*** 18.05.2023).

***

«Согласно специальному отчету RSM по индексу бизнеса среднего бизнеса США (MMBI) по кибербезопасности, представленному RSM, кибербезопасность по-прежнему представляет риск для предприятий среднего бизнеса, поскольку среда угроз развивается в условиях продолжающейся геополитической напряженности, экономической неопределенности и сохраняющихся последствий пандемии COVID-19. RSM US LLP («RSM») в партнерстве с Торговой палатой США.

Опрос RSM MMBI показывает, что хотя риски взломов остаются повышенными, количество зарегистрированных взломов несколько снижается второй год подряд. Двадцать процентов руководителей среднего звена сообщили, что их компания столкнулась с утечкой данных в прошлом году, что представляет собой небольшое снижение по сравнению с 22 процентами год назад. Несмотря на снижение количества зарегистрированных утечек, их количество по-прежнему в два раза выше, чем семь лет назад. Количество руководителей небольших компаний среднего размера (доход от $10 млн до менее чем $50 млн), сообщивших об утечке, соответствовало прошлогодним данным (12%), в то время как более крупные организации (годовой доход от $50 млн до $1 млрд) сообщили об утечке. снижение нарушений (с 30% в 2022 году до 28% в этом году).

Результаты опроса MMBI показывают, что предприятия среднего бизнеса предпринимают активные шаги для смягчения угроз кибербезопасности, о чем свидетельствуют 68% респондентов, которые заявили, что в настоящее время они используют полис киберстрахования для защиты от интернет-рисков. Это больше, чем 61% в прошлогоднем отчете. Более пристальный взгляд на данные показывает, что количество небольших компаний среднего размера, имеющих киберстрахование, увеличилось до 67% с 65% в 2022 году, в то время как более крупные компании, сообщившие о наличии полиса, значительно подскочили до 70% в этом году с 57% в 2022 году.

В отчете подробно описаны актуальные аналитические данные о кибербезопасности среднего рынка и тенденции конфиденциальности данных, а также тактики, которые организации могут использовать для усиления программ безопасности и конфиденциальности.

Атаки программ-вымогателей и угрозы захвата бизнеса растут, тактика манипулирования сотрудниками вызывает ключевую озабоченность

Как и в предыдущие годы, программы-вымогатели остаются основной угрозой кибербезопасности для среднего рынка, а атаки приводят к нескольким уровням

вредных последствий. По данным MMBI за этот год, 35% руководителей среднего звена заявили, что они столкнулись с атакой или спросом программ-вымогателей, по сравнению с 23% в прошлом году. Крупные компании среднего размера сообщили о значительном увеличении количества атак с 54% в этом году по сравнению с 29% в прошлогоднем отчете, в то время как в небольших организациях количество инцидентов немного снизилось до 13% с 16% в прошлом году.

Угрозы захвата бизнеса — одна из самых устойчивых и широко распространенных кибератак на компании среднего размера. Сообщаемая частота попыток поглощения бизнеса значительно увеличилась в данных этого года: 58% руководителей среднего бизнеса указали, что сторонние лица пытались манипулировать сотрудниками, притворяясь доверенными третьими лицами или руководителями компании, по сравнению с 45% в прошлом году. Руководители небольших компаний среднего размера сообщили о небольшом увеличении количества атак до 53% в этом году с 51% в 2022 году, в то время как более крупные компании указали на резкий скачок числа инцидентов до 63% с 40%.

Опрошенные руководители также сообщили, что 48% попыток манипулировать сотрудниками были успешными за последний год, что значительно больше, чем 27% по данным 2022 года. Крупные организации среднего размера продемонстрировали наибольший рост, сообщив о 68% успешности атак по сравнению с 38% только в прошлом году. Небольшие компании среднего размера сообщили о небольшом росте в этом году, до 21% с 15%.

Компании серьезно относятся к киберугрозам и продолжают реагировать на них

Большинство компаний среднего размера понимают ценность обучения как средства защиты от атак с захватом бизнеса, при этом 89% руководителей сообщили, что их организация проводит обучение по крайней мере для некоторых сотрудников тому, как обнаруживать, идентифицировать и предотвращать попытки получения несанкционированного доступа, что соответствует прошлогоднему отчету. данные. Крупные компании среднего размера предлагают обучение большему количеству сотрудников: 97% обучают некоторых или всех сотрудников по сравнению с 81% более мелких компаний.

Кроме того, доверие к стратегиям кибербезопасности остается очень высоким на среднем рынке. Второй год подряд 96% респондентов были уверены в своих текущих мерах по защите данных, что соответствует прошлогоднему рекорду. RSM приписывает некоторую высокую степень уверенности расширению внедрения облачных технологий, а также очевидному изменению стратегии, направленной на инвестирование большего количества ресурсов в области кибербезопасности. Число руководителей, которые сообщили о специальной функции, ориентированной на безопасность и конфиденциальность, значительно увеличилось до 77% в этом году по сравнению с 60% в прошлогоднем опросе.

Многие компании среднего размера также изменили структуру своей отчетности за последний год. В опросе этого года 40% руководителей сообщили, что человек, наиболее ответственный за безопасность данных и конфиденциальность, подчиняется непосредственно генеральному директору, что больше, чем 25% в прошлом году. Это число немного снизилось в небольших компаниях среднего

размера (с 38% в 2022 г. до 33% в 2023 г.), но значительно выросло в более крупных организациях (с 16% до 43%).

Только 57% опрошенных руководителей заявили, что знакомы с требованиями Общего регламента ЕС по защите данных (GDPR). Это указывает на плато с 58% в 2022 году, несмотря на повышенную осведомленность и правоприменительную деятельность. Как и в прошлые годы, респонденты из крупных организаций были лучше знакомы с требованиями GDPR, чем респонденты из небольших организаций — 84% против 28%.

С распространением законов и нормативных актов о конфиденциальности в Соединенных Штатах большинство компаний среднего бизнеса понимают, что в ближайшем будущем им, вероятно, придется соблюдать обязательства по соблюдению. Среди респондентов опроса RSM, знакомых с требованиями GDPR, 90% заявили, что их организациям, вероятно, придется соблюдать требования конфиденциальности, аналогичные GDPR, на федеральном уровне или уровне штата в США в течение следующих двух лет. Девяносто шесть процентов руководителей, знакомых с GDPR, заявили, что подготовка к новым законам и правилам о конфиденциальности является приоритетной задачей, как и в прошлом году.

Данные опроса, которые используются для расчета этого индекса, были получены от 406 респондентов в период с 9 по 30 января 2023 года.

Об индексе среднего бизнеса США RSM

RSM US LLP и Торговая палата США объединились, чтобы представить RSM Индекс бизнеса среднего рынка США (MMBI). Он основан на исследовании фирм среднего размера, проведенном Harris Poll, которое началось в первом квартале 2015 года. Опрос проводится четыре раза в год, в первый месяц каждого квартала: январь, апрель, июль и октябрь. Группа опроса состоит примерно из 1500 руководителей среднего рынка и предназначена для точного отражения условий на среднем рынке.

Созданный в сотрудничестве с Moody's Analytics, MMBI основан на подмножестве вопросов в опросе, в котором респондентам предлагается сообщить об изменении различных показателей. Респондентам задают в общей сложности 20 вопросов по образцу других качественных бизнес-опросов, например, от Института управления поставками и Национальной федерации независимых предприятий.

20 вопросов касаются изменений в различных показателях их бизнеса, таких как доходы, прибыль, капитальные затраты, найм, вознаграждение работникам, уплаченные цены, полученные цены и товарно-материальные запасы. Есть также вопросы, касающиеся экономики и перспектив, а также доступности кредитов и заимствований. По 10 вопросам респондентов просят сообщить об изменении по сравнению с предыдущим кварталом; для остальных 10 их просят указать вероятное направление этих же индикаторов на шесть месяцев вперед.

Ответы на каждый вопрос представлены в виде индексов распространения. MMBI — это составной индекс, рассчитываемый как равная взвешенная сумма диффузионных индексов для 10 вопросов опроса плюс 100, чтобы MMBI не стал отрицательным. Показатель выше 100 для MMBI указывает на то, что средний рынок в целом расширяется; ниже 100 указывает на то, что он в целом сокращается. Расстояние от 100 указывает на силу расширения или сжатия». ***(RSM US Cybersecurity Special Report Highlights Volatile Threat Environment as More Middle***

Market Firms Report // RSM US LLP (https://rsmus.com/newsroom/2023/rsm-us-cybersecurity-special-report-highlights-volatile-threat-environment-as-more-middle-market-firms-report-having-cyber-insurance.html). 25.05.2023).

***

Діяльність хакерів та хакерські угруповування

«Термин «китайский хакер» стал общепринятым в поп-культуре, но, похоже, у азиатской нации есть аналогичный термин для США: «Империя хакеров». Это имя фигурирует в новом китайском отчете, в котором ЦРУ обвиняется в использовании кибератак против Китая и других стран.

Согласно The Reg, расследование под названием «Матрица», проведенное Национальным центром реагирования на компьютерные вирусы Китая и местной фирмой по кибербезопасности 360 Total Security, было опубликовано в отчете под названием Empire of Hacking: The US Central Intelligence Agency — Part I.

В отчете утверждается, что следователи, изучающие ряд кибератак в Китае, захватили и извлекли большое количество троянов, функциональных плагинов и образцов атакующих платформ, предположительно тесно связанных с ЦРУ, что выявило «империю хакеров», находящуюся под контролем США пишет South China Morning Post.

«Это кибероружие прошло строгий, стандартизированный и профессиональный контроль разработки программного обеспечения, которому ЦРУ однозначно следует при разработке оружия для кибератак», — говорится в отчете.

Но многие выводы основаны на старой информации, полученной из серии утечек ЦРУ от Wikileaks в 2017 году под кодовым названием Vault7. В нем содержались подробности о глобальной тайной хакерской программе агентства, используемом вредоносном ПО и десятках эксплойтов нулевого дня в отношении широкого спектра продуктов американских и европейских компаний, включая телефоны Apple и Android, Windows и смарт-телевизоры, которые были взломаны, чтобы их микрофоны можно было использовать в качестве подслушивающих устройств.

«В настоящее время они охватили почти все активы Интернета и IoT по всему миру, что позволяет контролировать иностранные сети и красть важные конфиденциальные данные в любое время», — говорится в отчете. «Цели этих атак включают критически важную информационную инфраструктуру, аэрокосмическую промышленность, исследовательские институты, нефтяную и нефтехимическую промышленность, крупные интернет-компании и правительственные учреждения в различных странах. Эти атаки можно проследить до 2011 года и они продолжаются до сих пор».

В отчете также упоминается история попыток ЦРУ подорвать социалистические режимы, а также разработка Соединенными Штатами протокола TOR, против которого неоднократно выступал Китай из-за его использования теми, кто не согласен с правящей Коммунистической партией страны.

«США должны серьезно отнестись к опасениям международного сообщества и отреагировать на них, а также прекратить использование кибероружия для осуществления шпионажа и кибератак по всему миру», — заявил официальный представитель министерства иностранных дел Мао Нин…» ***(Rob Thubron. China calls the US an "Empire of Hacking," citing 2017 Wikileaks files // TechSpot, Inc. (https://www.techspot.com/news/98594-china-calls-us-empire-hacking-citing-2017-wikileaks.html). 07.05.2023).***

***

«Подобно Вергилию, проводящему Данте через недра средневекового ада эпохи Возрождения, Скотт Дж. Шапиро ведет читателей книги Fancy Bear Goes Phishing: The Dark History of the Information Age in Five Extraordinary Hacks через современную: дикую сферу киберхакинга. Подземный мир книги может быть даже более ужасным, чем у Данте, — по крайней мере, там читатель может почувствовать безопасность поэтического контроля великого писателя. Техно-мучения Fancy Bear хаотичны, часто непостижимы, а когда они незаконны, часто за пределами досягаемости возмездия. Но читатели, которые дочитают книгу до конца — это не всегда будет легко, — уйдут с более глубоким пониманием нашей тревожной цифровой среды.

Во введении к Fancy Bear Шапиро пишет: «Эти пять историй, каждая из которых содержит элементы человеческого интереса, также иллюстрируют мое сообщение именно потому, что они показывают, что самые интересные вопросы, поставленные нашим бурным новым [кибер]миром, имеют мало или вообще ничего общего с с технологией как таковой.... Хакерство касается людей, и моя цель — подойти к этому как таковому». В этой книге Шапиро предстает как интеллигентный ученый-репортер, посвятивший себя тому, чтобы помочь своим читателям понять различные формы кибер-уловок… Fancy Bear иногда кажется скорее примером кибербеспредела, чем его исследованием. Но, читатель, оставайтесь с Fancy Bear до конца. Это, несмотря на ее недостатки, мудрая книга.

«Пять экстраординарных хаков», упомянутых в Fancy Bear, подзаголовке составляют его структуру. Существует история хакерства, от ботаника Роберта Морриса-младшего, который мог бы изобрести это искусство в 1988 году, вплоть до группы Fancy Bear, также известной как APT 28, связанной с российским правительством, которая вмешалась в Президентская гонка в США 2016 года. Есть также рассказы о пестрых методах (тех, что используются сейчас и которые еще только появятся) кибервойны. Книга, несмотря на обещание автора исследовать человеческий фактор, в основном рассказывается через тщательное изучение кибертехнологий. И это, по крайней мере для меня, было проблематично.

Шапиро обсуждает различные инструменты, используемые хакерами: черви, вирусы, вормы (гибриды червей и вирусов), распределенные атаки типа «отказ в обслуживании» (DDoS). его ресурсы — доступная пропускная способность, сетевые подключения, память, место для хранения или его центральные процессоры. Чтобы исчерпать эти ресурсы, злоумышленники обычно используют «ботнет», набор ботов». Он также освещает фишинг (отсюда и название книги) и многое другое.

Автор дает определения downcode («технический компьютерный код»), upcode («инструкции, которые мы выбираем») и метакод («фундаментальные принципы, управляющие всеми формами вычислений») и тщательно исследует их моральные последствия. Он исследует различия между кодом и данными (код: «набор инструкций»; данные: «противоположный коду») и то, как «один из основных методов, используемых хакерами, заключается в манипулировании неоднозначностями между кодом и данными.» Шапиро разъясняет значение компьютерных операционных систем, таких как UNIX (построенная в 1971 году, она содержала «огромное количество дыр в безопасности»), Linux и Windows. Он считает их «красивыми» (каждому свое), потому что «операционная система играет роль волшебника, охранника и управляющего бэк-офисом, выступая посредником между программным обеспечением и оборудованием».

Рассмотрение в книге природы и приемов кибервойны особенно интригует. Шапиро считает, что полномасштабная кибервойна вряд ли произойдет, по крайней мере, в ближайшем будущем: «Одна из причин, по которой мы не видели крупномасштабной кибератаки на Соединенные Штаты, заключается в том, что нет никого, кто мог бы ее осуществить. Но даже если бы это было технически возможно, это было бы не в интересах злоумышленников. Любой такой удар был бы катастрофой для агрессора». Кроме того, «[b]поскольку слабые государства, как правило, не совершают разрушительных атак на сильные, нам не следует ожидать киберармагеддона в ближайшее время». Чувствовать себя лучше? Не так быстро. Следствием этого, как утверждает Шапиро, является то, что «... хотя кибероружие редко бывает достаточно мощным, чтобы выиграть военное столкновение или удержать территорию, оно является отличным инструментом сопротивления. Они используются слабыми государствами для беспокойства, клеветы, воровства и саботажа — и, что наиболее важно, тайно и отрицательным образом».

Я предполагаю, что я тот читатель, на которого рассчитана книга, — неученый, интересующийся наукой и техникой. Но у меня были проблемы, иногда большие, с запутанными погружениями Шапиро в технологии. Это иронично и загадочно, потому что он хороший писатель. Так что, возможно, это просто природа Fancy Bear темы. В любом случае, поскольку вы уже ознакомились с некоторыми краткими примерами набегов автора на разъяснение технологии, я упомяну только еще один краткий пример, подтверждающий мою точку зрения.

«Эвристика, — пишет автор, — играет существенную роль в том, что психологи называют теориями двойственного процесса мышления и выбора. Согласно теориям двойного процесса, наша когнитивная жизнь состоит из двух систем ментального кодирования. Первая, которую [психолог Дэниел] Канеман называет Системой 1, — это быстрая система. Он автоматически и быстро дает ответы на множество вопросов, обычно касающихся убеждений, которые необходимо сформировать, и действий, которые необходимо выполнить немедленно. Эвристика, принадлежащая Системе 1, работает посредством замещения». Эвристика, благослови их; но я все еще не в курсе.

Шапиро, директор Центра права и философии Йельского университета и университетской лаборатории кибербезопасности, также является профессором права и философии в Йельской школе права. Но вот за что я его очень уважаю: он

рассудительный. Он предлагает свои «три Р», методы, которые в некоторой степени препятствуют киберпреступности: «пути к киберпреступности, платежи за киберпреступность и штрафы за уязвимое программное обеспечение». И он дополняет эти три пункта несколькими важными предостережениями: «[Они] не являются серебряными пулями, которые решат нашу проблему кибер-незащищенности, но они более эффективны, чем постоянное «заплати и молись», которое до сих пор характеризовало нашу цифровую жизнь».

«Кибербезопасность — это не преимущественно технологическая проблема, требующая преимущественно инженерного решения. Это человеческая проблема, которая требует понимания человеческого поведения», — продолжает он, заключая, что «не существует такой вещи, как «решение» «проблемы» кибербезопасности».

Шапиро с оптимизмом полагает, что вполне возможно, что кибер-отчаянные (преступные хакеры кажутся почти всегда мужчинами — я бы хотел, чтобы автор обсудил это явление более подробно, чем он) могут с правильными стратегиями и учителями стать «белыми шляпами», цифровыми добрыми самаритянами. Я не такой оптимистичный, но я предвзято отношусь к этому вопросу.

Став жертвой программы-вымогателя несколько лет назад и потеряв все свои файлы, когда отказался платить, я испытываю глубокую, свирепую ненависть к «черным шляпам» хакеров и подозреваю, что они не поддаются исправлению. Но, полагаю, это не имеет отношения к моему подведению итогов: Шапиро — надежный эскорт для множества людей, измученных современным кибер-лабиринтом». ***(Howard Schneider. The Human Problem of Cyberwar // The Progressive Inc. (https://progressive.org/latest/human-problem-cyberwar-schneider-220523/). 22.05.2023).***

***

Вірусне та інше шкідливе програмне забезпечення

«Согласно новым данным, недавно обнаруженное семейство вредоносных программ для мобильных устройств находилось в магазине Google Play и собирало счета для сотен тысяч людей.

Исследователи кибербезопасности из «Лаборатории Касперского» недавно обнаружили Fleckpe, который, по их словам, был интегрирован как минимум в 11 приложений для Android, которые в совокупности были загружены примерно 620 000 раз.

Приложения в основном представляют собой редакторы изображений, обои, приложения для красоты и тому подобное.

Когда жертва устанавливает приложение, вредоносное ПО незаметно инициирует либо разовую, либо ежемесячную подписку на определенные платные услуги. Эти премиальные услуги могут либо принадлежать третьей стороне, при этом операторы вредоносного ПО получают долю, либо они могут принадлежать самим злоумышленникам, что позволяет им получать полную сумму.

Как бы то ни было, злоумышленники заработали приличную сумму, так как исследователи обнаружили, что вредоносное ПО активно как минимум с 2022 года,

хотя точная сумма неизвестна. Большинство жертв находятся в Таиланде, Малайзии, Индонезии, Сингапуре и Польше, а меньший процент разбросан по всему миру.

«Все приложения были удалены с рынка к моменту публикации нашего отчета, но злоумышленники могли развернуть другие, еще не обнаруженные приложения, поэтому реальное количество установок может быть выше», — сказал Касперский…

Вредоносное ПО этого типа не потребует выкупа и не уничтожит данные на конечной точке, но может украсть личную информацию и, безусловно, приведет к более высоким расходам со стороны оператора связи. Чтобы предотвратить такие инциденты, рекомендуется проверять отзывы и рейтинги в магазине приложений, прежде чем что-либо загружать». ***(Sead Fadilpašić. This wallet-draining Google Play malware has been installed over half a million times - these are the apps to watch out for // Future US, Inc. (https://www.techradar.com/news/this-google-play-malware-has-been-installed-over-half-a-million-times-so-remove-now). 05.05.2023).***

***

«…С марта 2023 года исследователи безопасности Meta (открывается в новой вкладке) обнаружили 10 новых семейств вредоносных программ или компьютерных программ со злым умыслом, использующих ChatGPT и связанные темы для нападения на пользователей Интернета.

Всего за несколько месяцев с момента запуска ChatGPT мошенники создали горы поддельных расширений для браузеров, мобильных приложений и других программ, предлагающих инструменты ChatGPT. Некоторые мошеннические программы на самом деле имеют полуфункциональные возможности чат-бота, которые существуют вместе с основным вредоносным ПО, чтобы дольше избегать обнаружения.

Многие мошеннические чат-боты имитируют предложения Google и TikTok, поскольку эти продукты появляются в новостях. В ответ на жесткие меры некоторые мошенники обращаются к более мелким сервисам, таким как Buy Me a Coffee, для размещения и доставки вредоносных программ.

Мошенники продвигают загрузку продуктов с помощью убедительной рекламы, ориентированной на уязвимых пользователей в Facebook и Instagram, а также в электронной почте и на других интернет-платформах. Как только пользователи загружают эти поддельные программы с целевых страниц, подобных приведенной ниже, мошенники могут получить доступ к самым личным данным жертв и даже к банковским счетам.

Meta предупреждает, что устройства пользователей могут быть заражены вредоносным ПО, если они проявляют следующие признаки:

Меньшее время автономной работы устройства.

Подозрительные действия в аккаунте, которые пользователи не санкционировали, включая финансовые расходы.

Более низкая скорость устройства или неожиданное зависание.

В вашем браузере часто появляются подозрительные всплывающие окна.

Странные панели инструментов, значки или вкладки, которые вы не устанавливали.

Meta заблокировала (откроется в новой вкладке) более 1000 уникальных мошеннических веб-адресов на тему ChatGPT со своих платформ социальных сетей и поделилась ими с другими технологическими компаниями, чтобы принять меры в отношении их собственности.

Meta также внедряет новую поддержку удаления вредоносных программ для предприятий, пострадавших от подделок ChatGPT и других видов мошенничества. Новый инструмент поддержки компании помогает пользователям идентифицировать и удалять вредоносное ПО, в том числе с помощью сторонних антивирусных инструментов.

Meta повышает требования к авторизации для конфиденциальных действий учетной записи Meta Business, таких как доступ к кредитной линии или смена бизнес-администраторов. Теперь компаниям потребуется использовать двухфакторную аутентификацию, проверку электронной почты или одобрение коллег для выполнения действий, которые могут иметь значительные финансовые или корпоративные последствия.

Чтобы мошенники не добавляли себя в качестве бизнес-администраторов Facebook или Instagram, предприятия теперь могут создавать ограничения, позволяющие администраторам получать доступ к своим мета-бизнес-менеджерам только из доверенных, выбранных доменов и более эффективно проверять доступ людей.

Наконец, вскоре Meta представит учетные записи Meta Work, которые, наконец, отделят личные профили администраторов в Facebook и Instagram от процесса входа в Business Manager. Хакеры часто начинают со взлома личных учетных записей ключевых сотрудников бизнеса, чтобы получить доступ к их более прибыльным корпоративным логинам. Этот шаг может смягчить один из наиболее распространенных векторов угроз для взлома корпоративных учетных записей Facebook и Instagram». ***(Ben Demers. Meta Warns of ChatGPT Scams On Facebook and Instagram // Future US, Inc. (https://www.kiplinger.com/personal-finance/meta-warns-of-chatgpt-scams-on-facebook-and-instagram). 06.05.2023).***

***

«Новая версия уже активного вредоносного ПО теперь переключается на 1Password — на наш взгляд, лучший менеджер паролей для семей — и KeePass.

ViperSoftX — это похититель информации, который уже преследовал криптовалютные кошельки, но теперь он атакует больше из них, в дополнение к нескольким веб-браузерам — не только Google Chrome — и менеджерам паролей.

Он также имеет более сильное шифрование кода и лучше избегает обнаружения антивирусными инструментами.

ViperSoftX может установить вредоносное расширение Chrome VenomSoftX, но, по словам исследователей безопасности Trend Micro (открывается в новой вкладке), теперь оно также может заражать Microsoft Edge, Mozilla Firefox, Opera и Brave.

Вредоносная программа была впервые обнаружена в 2020 году при краже криптовалюты с помощью RAT (троян удаленного доступа) на основе JavaScript. Однако к 2022 году Avast (открывается в новой вкладке) обнаружил, что его

возможности значительно расширились, и поставщик кибербезопасности заявил, что он остановил около 100 000 атак на своих клиентов со стороны вредоносного ПО на протяжении большей части прошлого года. Большинство жертв находились в США, Италии, Бразилии и Индии.

Однако похоже, что теперь ViperSoftX расширила свое глобальное присутствие, и Trend Micro обнаружила дополнительную заметную активность в Австралии, Японии, Тайване, Малайзии и Франции. Предприятия и потребители также становятся мишенью. Аналитики выяснили, что вредоносное ПО часто прячется в программных кряках и активаторах.

Trend Micros обнаружила, что в дополнение к атакам на многие другие криптокошельки последняя версия ViperSoftX ищет файлы, связанные с 1Password и KeePass, и пытается украсть данные, связанные с их расширениями браузера.

Эксплойт, отслеживаемый как CVE-2023-24055, позволяет экспортировать сохраненные пароли в обычный текстовый файл, но Trend Micro теперь обнаружила доказательства того, что он используется ViperSoftX.

Тем не менее, он сообщил BleepingComputer (открывается в новой вкладке), что может украсть хранилища пользователей на более поздних этапах атаки, как только вредоносное ПО захватит и извлечет данные из системы жертвы и отправит их злоумышленнику.

Что еще более тревожно, новый ViperSoftX использует неопубликованную загрузку DLL, чтобы ошибочно распознать его как доверенный процесс и, таким образом, остаться незамеченным программным обеспечением безопасности. Он также проверяет, присутствуют ли в системе инструменты мониторинга, такие как VMWare или Process Monitor, и антивирусное программное обеспечение, такое как Защитник Windows и ESET, прежде чем он начнет свои процессы.

Он также использует отображение байтов, метод шифрования своего кода таким образом, что его намного сложнее расшифровать, не имея для этого правильной карты». ***(Lewis Maddison. This vicious new malware version is now targeting password managers // Future US, Inc. (https://www.techradar.com/news/this-vicious-new-malware-version-is-now-targeting-password-managers). 02.05.2023).***

***

«Группа американских специалистов по кибербезопасности обнаружила вредоносное ПО в ходе трехмесячного развертывания в Латвии, исследуя цифровую инфраструктуру на наличие уязвимостей.

Так называемая охотничья операция, проведенная Кибернациональной миссией, стала второй подобной операцией в бывшем советском государстве. Это завершилось «недавно», сообщило Киберкомандование США 10 мая.

«Во время поисков в Латвии кибергруппы обнаружили вредоносное ПО, проанализировали его и получили более полное представление о [тактике, методах и процедурах] противника», — говорится в заявлении командования. C4ISRNET поинтересовался вредоносной программой и ее потенциальной атрибуцией.

Силы миссии работали вместе с CERT.LV, основной латвийской группой реагирования на кибер-экстренные ситуации, и канадскими военными. Канада возглавляет миссию усиления НАТО в европейской стране с 2017 года.

«Вместе с нашими надежными союзниками, США и Канадой, мы можем сдерживать участников киберугроз и укреплять нашу взаимную устойчивость», — Байба Кашкина, генеральный менеджер CERT.LV. заявила «Это может произойти только посредством реальных оборонительных кибероперацій и сотрудничества. Проведенные оборонительные кибероперации позволили нам сделать нашу государственную инфраструктуру более сложной мишенью для злоумышленников».

CNMF развертывал почти четыре десятка раз в 22 странах, включая Украину перед вторжением России и Албанию после иранских кибератак, чтобы укрепить разбросанные сети и вернуться с идеями, которые можно применить в США.

США считают Китай и Россию своими наиболее значительными киберугрозами. Иран и Северная Корея также входят в список, но в меньшей степени.

Кашкина назвала Латвию излюбленной мишенью «российских хактивистов и хакерских групп, поддерживающих российское государство». Латвийское правительство обвинило российские компании в фишинге и распределенных атаках типа «отказ в обслуживании».

Поисковые операции — это оборонительные действия, предпринятые по приглашению иностранного правительства. Они являются частью стратегии постоянного взаимодействия CYBERCOM, средством постоянного контакта с противниками, обеспечивая при этом упреждающие, а не ответные действия…» ***(Colin Demarest. US cyber team unearths malware during 'hunt-forward' mission in Latvia // Defense News (https://www.defensenews.com/cyber/2023/05/10/us-cyber-team-unearths-malware-during-hunt-forward-mission-in-latvia/). 10.05.2023).***

***

«Команда реагування на комп'ютерні надзвичайні ситуації (CERT-UA) повідомила, що група хакерів, відома як UAC-0006, відповідальна за розповсюдження електронних листів через скомпрометовані акаунти. Листи містять ZIP-архів, який після завантаження запускає виконуваний файл, що встановлює шкідливе програмне забезпечення SmokeLoader.

Що відомо про нову загрозу

Ця кампанія кібератак розпочалася у квітні 2023 року і є фінансово мотивованою. Група UAC-0006 має історію фінансово вмотивованих кібератак, які були здійснені з 2013 по липень 2021 року. Хакери мають на меті скомпрометувати комп'ютери бухгалтерів, які використовуються для підтримки фінансової діяльності, наприклад, для доступу до систем дистанційного банківського обслуговування.

Отримавши доступ, вони викрадають автентифікаційні дані:

логіни,

паролі,

ключі/сертифікати.

Далі вони здійснюють несанкціоновані платежі за допомогою бота HVNC безпосередньо зі скомпрометованого комп'ютера.

Як захиститися від таких атак?

Щоб мінімізувати шкоду від цих атак, рекомендується тимчасово заблокувати запуск wscript.exe (Windows Script Host) на комп'ютері. Це пов'язано з тим, що група

UAC-0006 зазвичай використовує завантажувачі JavaScript. Блокування запуску wscript.exe тимчасово знижує шанси стати жертвою цього типу атаки.

Використання шахрайських електронних листів з підробленими рахунками та платіжними вимогами є відносно новою тактикою для цієї групи, і цілком ймовірно, що вони продовжуватимуть розвивати свою тактику, щоб уникнути викриття. Вкрай важливо, щоб фізичні та юридичні особи не втрачали пильності та вживали заходів для захисту від подібних атак». ***(Михайло Года. Держспецзв'язку попередила про новий комп'ютерний вірус від хакерів UAC-0006 // ПрАТ «Телерадіокомпанія «Люкс» (https://24tv.ua/tech/osterigaytesya-novogo-kompyuternogo-virusu-derzhspetszvyazku_n2309786). 09.05.2023).***

***

«Компания SentinelOne, занимающаяся кибербезопасностью, сегодня сообщила о новом вирусе для Mac, который при открытии на вашем Mac дает хакерам доступ к вашему компьютеру. Вирус под названием «Geacon» представляет собой версию вируса Cobalt Strike, который некоторое время использовался против пользователей Windows.

Теперь эта новая версия вируса может быть имплантирована на компьютеры пользователей Mac, позволяя хакерам проникнуть в систему с так называемым троянским конем — безобидным на первый взгляд файлом, который в конечном итоге позволяет хакерам получить доступ к вашей машине.

Что оно делает?

Нацеленный на macOS Mavericks и выше, вирус способен проникать в машины с чипами Intel или Apple. Это требует, чтобы вы предоставили ему доступ к вашей камере, микрофону и привилегиям администратора, поэтому очень важно следить за всем, что вы устанавливаете из Интернета.

Оказавшись на вашем Mac, он отправляет «маяки» злоумышленникам, которые загрузили вирус и разослали его ничего не подозревающим жертвам. Sentinel One говорит, что эти маяки имеют «множество функций для таких задач, как сетевая связь, шифрование, дешифрование, загрузка дополнительных полезных данных и эксфильтрация данных».

По сути, хакер может получить доступ к вашим данным, местоположению и материалам, отправленным через ваше соединение для передачи данных.

Подобные вирусы на самом деле легко доступны хакерам для загрузки на Github — этот можно загрузить от создателя по имени «z3ratu1». К счастью, защититься от подобных вирусов достаточно просто.

Первое, что нужно сделать, это просто быть особенно осторожным при загрузке программного обеспечения на свой лучший Mac. Убедитесь, что вы точно знаете, откуда берутся ваши приложения и программное обеспечение, и загружайте их только из надежных источников.

Кроме того, убедитесь, что у вас установлено антивирусное или защитное программное обеспечение, чтобы убедиться, что вы не подвержены атакам. Есть программное обеспечение SentinelOne, а также такие опции, как Avast или другие лучшие антивирусные программы для Mac. Позаботьтесь о безопасности в Интернете — компьютеры Mac уже не так защищены от вирусов, как раньше».

(Tammy Rogers. macOS is being targeted by 'Cobalt Strike' that opens your machine up to hackers // Future US, Inc. (https://www.imore.com/mac/macos/macos-is-being-targeted-by-cobalt-strike-that-opens-your-machine-up-to-hackers). 17.05.2023).

***

«Исследователи кибербезопасности обнаружили новое вредоносное вредоносное ПО, предназначенное для нарушения работы систем жизнеобеспечения или другой важной инфраструктуры.

Специалисты Mandiant назвали вредоносное ПО CosmicEnergy и считают, что оно очень похоже на обнаруженный ранее Sandworm. Sandworm — это печально известное вредоносное ПО, спонсируемое российским государством, которое в 2016 году снова было нацелено на украинские энергосистемы.

Важное различие между CosmicEnergy и Sandworm заключается в том, что предыдущий не был обнаружен после инцидента с безопасностью, но немного в результате поиска рисков. Кто-то из России загрузил вредоносное ПО на VirusTotal полтора года назад, и именно там его обнаружили исследователи Mandiant.

Разработано для коучинга

Судя по всему, вредоносное ПО было разработано компанией «Ростелеком-Фото вольтаик», подразделением кибербезопасности «Ростелекома» — общероссийского оператора связи.

Предварительный вывод заключается в том, что вредоносное ПО было разработано для обучения, скорее всего, для обучения ИТ-отдела простым методам поведения в случае точного нападения на сеть. Исследователи заявили, что один такой коучинг снова был проведен в сотрудничестве с Министерством энергетики России в 2021 году.

«Подрядчик мог бы разработать его как программное обеспечение для симуляции отключения электроэнергии, организованное Ростелеком-Фото вольтаик», — заявляют исследователи. совершенно другой субъект — как с нашего разрешения, так и без него — повторно использовал код, связанный с киберпространством, для разработки этой вредоносной программы».

Тем не менее, учитывая функциональные возможности CosmicEnergy, исследователи не могут исключить вероятность того, что вредоносное ПО вполне может быть использовано для точной атаки.

В любом случае, вредоносное ПО не было замечено в дикой природе, сообщили исследователи TechCrunch. Кроме того, они сообщили изданию, что вредоносному ПО «не хватает возможностей обнаружения», а это означает, что субъекты риска должны сначала провести разведку скомпрометированного сообщества на наличие таких проблем, как IP-адреса и учетные данные, прежде чем иметь возможность организовать атаку.

«Изобретение новейших вредоносных программ OT [операционных технологий] представляет мгновенный риск для затронутых организаций, поскольку такие открытия происходят нечасто, и поскольку вредоносное ПО в основном использует небезопасные варианты конструкции сред OT, которые вряд ли можно быстро исправить в любое время, — заключили исследователи». ***(This dangerous Russian-linked malware could shut down power grids – Mobilemall // Mobile Mall***

Pakistan (https://mobilemall.com.pk/blog/this-dangerous-russian-linked-malware-could-shut-down-power-grids/). 26.05.2023).

***

«Компанія ESET повідомляє про виявлення поширеного шкідливого програмного забезпечення AceCryptor для шифрування. Ця загроза поширюється у всьому світі з 2016 року, при цьому багато зловмисників активно використовують її для розповсюдження власних шкідливих програм.

Протягом 2021 та 2022 років телеметрія ESET зафіксувала понад 240 тисяч випадків виявлення цього шкідливого програмного забезпечення, що становить понад 10 тисяч щомісяця. Ймовірно, загроза продається в даркнеті або на підпільних форумах. Багато зловмисників використовують цей шифрувальник для уникнення виявлення рішеннями з безпеки. Зокрема загроза AceCryptor застосовувала численні способи обходу виявлення протягом багатьох років.

Для кіберзлочинців уникнення виявлення шкідливих програм є складним завданням. Шифрувальники — це перший рівень захисту від виявлення для загроз під час поширення. Незважаючи на те, що зловмисники можуть створювати та підтримувати власні шифрувальники, на це часто потрібен час та технічні можливості постійно вдосконалювати загрозу. Про це каже Якуб Калоч, дослідник ESET:

«Саме тому шифрувальники як послуга користуються попитом».

Серед сімейств шкідливих програм, які використовували AceCryptor, одним з найпоширеніших є RedLine Stealer. Ця загроза застосовується для викрадення облікових даних банківської картки та іншої конфіденційної інформації, завантаження файлів і навіть крадіжки криптовалюти. RedLine Stealer вперше виявлено на початку 2022 року, відтоді зловмисники почали використовувати AceCryptor та продовжують це робити.

«Таким чином можливість виявлення AceCryptor допомагає нам не тільки фіксувати нові загрози, але й відстежувати дії кіберзлочинців», — пояснює Калоч.

Через використання різними кіберзлочинцями шкідливе програмне забезпечення, запаковане AceCryptor, поширюється різними способами. Відповідно до даних телеметрії ESET, ці загрози розповсюджувалися переважно через шкідливі інсталятори піратського програмного забезпечення або спам-листи із небезпечними вкладеннями. Ще один спосіб інфікування — інші загрози, які завантажували нове шкідливе програмне забезпечення, запаковане AceCryptor.

Оскільки шкідливе програмне забезпечення використовують багато кіберзлочинців, жертвою може стати будь-який користувач. Через різноманітність таких шкідливих програм важко оцінити небезпеку наслідків для жертви. Наприклад, жертва могла відкрити небезпечне вкладення електронної пошти, а потім завантажилися додаткові загрози.

Незважаючи на те, що віднесення AceCryptor до конкретної групи кіберзлочинців наразі неможливе, дослідники ESET припускають, що AceCryptor продовжуватиме широко використовуватися. Більш ретельне відстеження допоможе виявити нові сімейства шкідливого програмного забезпечення з використанням цього шифрувальника.

У зв’язку з небезпекою атак спеціалісти ESET рекомендують дотримуватися основних правил кібербезпеки, зокрема не відкривати невідомі листи та документи, використовувати складні паролі та двофакторну автентифікацію, вчасно оновлювати програмне забезпечення, а також забезпечити надійний захист домашніх пристроїв та корпоративної мережі». ***(Герман Богапов. Нова загроза атакує щомісяця 10 тисяч пристроїв // HiTech.Expert (https://expert.com.ua/161174-nova-zagroza-atakuye-schomisyacya-10-tysyach-prystroiv.html). 25.05.2023).***

***

Програми-вимагачі

«Атака программы-вымогателя со стороны плодовитой группы под названием Royal вызвала перебои в работе многих систем Далласа за последние три дня.

Веб-сайты оставались недоступными, и службы экстренного реагирования продолжали полагаться на планы экстренного резервного копирования на выходные. Городские власти заявили, что на звонки 911 и 311 все еще отвечают, и они не верят в утечку информации жителей и продавцов.

«Был достигнут значительный прогресс, но процесс восстановления продолжается», — заявили официальные лица Далласа в пятничном пресс-релизе.

Нарушение произошло всего через несколько месяцев после того, как Royal нацелился на Центральный оценочный округ Далласа, вынудив их заплатить 170 000 долларов.

Поскольку городские эксперты по кибербезопасности борются за восстановление услуг, этот эпизод заставил другие города Техаса обратить внимание на собственные усилия по обеспечению безопасности.

«Кибербезопасность — это работа в режиме 24/7/365, которая включает в себя адаптацию того, что мы узнаем из ситуаций других, для усиления нашей собственной защиты», — сказал Сэм Брэдфорд, директор по информационным технологиям в Мескит.

Эксперты описывают Royal как изощренную «банду», которая примерно в двух третях случаев получает доступ к сетям жертв с помощью фишинга. Они говорят, что это одна из многих «оппортунистических» групп, которые шифруют данные и угрожают публично опубликовать их, если не будет выплачен выкуп.

Даллас впервые сообщил в среду, что он подвергся возможной атаке программы-вымогателя, затронувшей 311 и муниципальные суды, а также значительно затруднившей работу полиции и пожарных. На следующий день городские власти заявили, что отдел информационных и технологических служб Далласа «изолировал проблему» и постепенно восстанавливал обслуживание, отдавая приоритет «отделам общественной безопасности и работе с жителями».

Городские власти повторили в выпуске новостей в пятницу вечером, что поставщики ИТС и кибербезопасности продолжают работать «непрерывно, чтобы быстро изолировать вирус и постепенно восстанавливать обслуживание». Сроки, когда системы будут восстановлены, пока неясны.

Представитель города Даллас в пятницу не ответил на вопросы о том, как произошло нападение и предъявлял ли Роял какие-либо требования, заявив, что персонал «посвящен операциям» и недоступен для интервью.

Неясно, будет ли город платить Royal, но эксперты говорят, что это неразумно, так как злоумышленники могут вернуться и не расшифровать все данные.

«Если вы заплатите выкуп одной группе или одной банде, другие могут вернуться через пару месяцев», — сказала Джесс Парнелл, вице-президент по операциям безопасности компании Centripetal Networks из Вирджинии, занимающейся кибербезопасностью.

Агентство кибербезопасности и инфраструктуры сообщает, что фишинг, обычно через фальшивую гиперссылку или вредоносное ПО, замаскированное под вложение, является наиболее распространенным способом, которым люди, использующие Royal, получают доступ к сетям. По словам Парнелла, другие методы включают использование протокола удаленного рабочего стола, украденные учетные данные и получение доступа к учетным записям электронной почты пользователей.

Ожидается, что Билл Зелински, директор по информационным технологиям Далласа, в понедельник проинформирует комитет общественной безопасности городского совета по этому вопросу. Согласно служебной записке, направленной в пятницу членам комитета, официальные лица включили брифинг в повестку дня как для публичного обсуждения, так и для закрытого заседания.

Пока публика ждет подробностей, города Северного Техаса используют Даллас в качестве урока.

Брайс Картер, директор по информационной безопасности Арлингтона, сказал, что для городов важно знать, «что влияет на тех, кто рядом с нами», чтобы знать, на чем сосредоточить свою собственную защиту.

Он сказал, что в последние годы Арлингтон выделил больше ресурсов на кибербезопасность, чтобы помочь ограничить масштабы и радиус поражения онлайн-атак, которые, по его словам, стали более изощренными с появлением новых технологий.

«Единственный способ, которым мы все можем быть устойчивыми, — это работать и сотрудничать вместе как коллективная сила», — сказал Картер. «Если мы не можем этого сделать, значит, мы все работаем изолированно, а это значит, что мы выбрасываем слишком много энергии».

Картер сказал, что местные органы власти по всей стране начинают понимать, что инвестиции в кибербезопасность необходимы для предоставления услуг гражданам.

«Это действительно беспрецедентный риск, когда речь идет о местных органах власти, и может быть трудно иметь некоторую устойчивость, потому что бюджеты, как правило, ограничены», — сказал Картер. «Это не то, с чем 20 лет назад нам когда-либо приходилось иметь дело».

Представитель Denton Стюарт Бердсай подтвердил это мнение, добавив, что официальные лица внимательно следят за окружающей средой в свете теракта в Далласе.

Он сказал, что в Denton есть процессы для защиты от кибератак, но он также полагается на сотрудников, которые усердно используют электронную почту и технологии для предотвращения эксплойтов.

«Как только мы узнаем официальную причину [в Далласе], мы сможем сосредоточить свое внимание на этих областях, если они также будут в нашей среде», — сказал Бердсай.

Представитель Irving Эйприл Рейлинг заявила, что город сотрудничает с поставщиком, чтобы постоянно отслеживать и реагировать на угрозы кибербезопасности. В свете атаки в Далласе поставщик повысил уровень своей осведомленности и бдительности, «чтобы обеспечить максимальную защиту цифровых активов», — сказал Рейлинг.

Брэдфорд, ИТ-директор Mesquite, сказал, что официальные лица напоминают персоналу о необходимости сохранять бдительность после того, как системы Далласа были скомпрометированы.

«Мы надеемся, что Даллас сможет обнаружить основную причину атаки, удалить ее из своих систем на 100% и вернуться к нормальной работе ради своих граждан и сотрудников», — сказал Брэдфорд». ***(Kelli Smith and Zaeem Shaikh. As Dallas ransomware attack stretches into day 3, other Texas cities boost cybersecurity // The Dallas Morning News (https://www.dallasnews.com/news/2023/05/05/as-dallas-ransomware-attack-stretches-into-day-3-other-texas-cities-boost-cybersecurity/). 05.05.2023).***

***

«…Исследователи кибербезопасности из компании Kroll, занимающейся консультированием по рискам и финансам, недавно обнаружили разновидность программы-вымогателя, известную как Cactus.

Помимо обычной операции — шифрования файлов и оставления после себя записки с требованием выкупа — у вредоносной программы также есть уникальный способ избежать обнаружения антивирусными программами и решениями для защиты конечных точек.

…программа-вымогатель имеет три основных режима исполнения, один из которых — шифрование. После развертывания полезной нагрузки злоумышленники предоставят вредоносному ПО уникальный ключ AES, известный только им. Этот ключ используется для расшифровки файла конфигурации программы-вымогателя и открытого ключа RSA, необходимого для шифрования всего остального на целевой конечной точке. Ключ представляет собой строку HEX, жестко закодированную в двоичном коде шифровальщика.

Декодируя строку HEX, злоумышленники получают зашифрованные данные, которые они могут прочитать, если у них есть ключ AES.

«CACTUS, по сути, шифрует себя, что затрудняет его обнаружение и помогает обойти антивирусы и инструменты мониторинга сети», — сказала Bleeping Computer Лори Яконо, заместитель управляющего директора по киберрискам в Kroll.

Что еще делает Cactus интересным, так это то, что он имеет несколько режимов шифрования, включая быстрый режим. Если операторы решат запустить оба режима

один за другим, файлы будут зашифрованы дважды и получат два расширения файлов.

Об операции программы-вымогателя Cactus известно очень мало. Мы не знаем, подвергаются ли в настоящее время нападениям какие-либо предприятия или ведутся переговоры о выплате. Хотя это не подтверждено, в некоторых сообщениях утверждается, что группа запрашивает «миллионы», требуя выплаты. Мы также не знаем, насколько успешной была группа в прошлом.

Как обычно, лучший способ защититься от программ-вымогателей — регулярно обновлять программное и аппаратное обеспечение, настраивать решения для кибербезопасности и обучать персонал опасностям фишинга и атак социальной инженерии». ***(Sead Fadilpašić. This devious new ransomware encrypts itself to avoid your antivirus // Future US, Inc. (https://www.techradar.com/news/this-devious-new-ransomware-encrypts-itself-to-avoid-your-antivirus). 09.05.2023).***

***

«В эпоху эскалации атак программ-вымогателей хорошие политики и процедуры резервного копирования стали необходимы. Только в 2022 году во всем мире было обнаружено 236,1 миллиона атак программ-вымогателей. Киберпреступники используют вредоносное ПО, криптографию и проникновение в сеть, чтобы блокировать компании от их данных, атакуя хранилище, шифруя данные и отключая резервное копирование. Распространенность атак программ-вымогателей, когда компании вынуждены предъявлять финансовые ультиматумы, удерживая свои системы и резервные копии в заложниках, заставляет предприятия улучшать свою безопасность и, следовательно, свои протоколы резервного копирования данных.

При правильном резервном копировании и процедурах аварийного восстановления системы, зараженные программами-вымогателями, могут быть восстановлены довольно быстро, что препятствует действиям злоумышленников. Однако хакеры научились удалять или уничтожать резервные копии одновременно с шифрованием и блокировкой производственных файлов. Если их цели могут восстановить свои системы из резервных копий, то, очевидно, им не нужно будет платить выкуп.

Политика 3-2-1

Политика резервного копирования 3-2-1 существует уже несколько десятилетий и представляет собой традиционный «золотой стандарт» обеспечения безопасности резервных копий. Это влечет за собой создание трех копий данных с использованием двух разных носителей, при этом по крайней мере одна резервная копия должна быть удалена. Желательно, чтобы резервная копия также была неизменной, то есть никто не мог удалить, изменить или зашифровать резервную копию в течение установленного периода времени.

За последние 20 лет или около того «два разных носителя» обычно означали одну копию на традиционных жестких дисках, а другую копию на ленте. Неизменяемость чаще всего достигалась, буквально беря ленту и помещая ее в картонную коробку, или ломая пластиковый язычок на картридже с лентой, что делало его недоступным для записи. При создании удаленной копии чаще всего

выполнялось копирование файлов резервных копий между двумя корпоративными центрами обработки данных.

Войдите в облако. В последние годы облако стало популярным местом для хранения резервных копий. Его внедрение заставило большинство компаний пересмотреть традиционную политику 3-2-1. Большинство организаций используют гибридный подход. Поскольку пропускная способность облака ограничена, резервные копии сначала направляются на локальное устройство хранения, что обычно быстрее, чем резервное копирование непосредственно в облако. То же самое верно и для восстановления из резервных копий. Восстановление из локальной копии всегда будет быстрее. Однако что, если хакеры уничтожили локальную резервную копию (что весьма вероятно)? Тогда можно было бы обратиться к копии в облаке.

Сегодня большинство поставщиков облачных хранилищ предлагают «неизменяемое» хранилище, что означает, что оно заблокировано и не может быть изменено или удалено. Эта неизменность — именно то, что вам нужно, чтобы хакеры не уничтожили ваши резервные копии. А облако всегда находится «вне площадки», что удовлетворяет одному из важнейших требований политики резервного копирования 3-2-1. Если произойдет пожар, наводнение или что-то еще, что повредит локальную резервную копию, у вас все равно будет облако. Что касается третьего экземпляра, люди больше не видят необходимости в двух разных видах медиа. На сегодняшний день наиболее распространенной процедурой является репликация облачной копии во второе облачное местоположение, предпочтительно находящееся на расстоянии не менее 500 км. Обе облачные копии должны быть неизменяемыми.

Помимо атак программ-вымогателей, есть и другие причины, по которым компании теряют свои первичные данные и вынуждены восстанавливать их из резервных копий. Наиболее распространенной из них является человеческая ошибка — например, кто-то нажимает не ту кнопку и случайно стирает или искажает первичные данные. Но техника тоже может выйти из строя. Если локальное устройство резервного копирования выйдет из строя, у вас останутся облачные копии. Жесткие диски имеют ограниченный срок службы, и большинство из них рано или поздно выйдет из строя. Программное обеспечение, такое как RAID, делает дисковые массивы устойчивыми к отказам дисков, но не устраняет их.

Как правило, поставщики облачных хранилищ предлагают гораздо более высокую надежность данных, чем локальные устройства хранения. Золотой стандарт, принятый Amazon, Google, Microsoft и Wasabi, — это 11 девяток прочности. Если вы посчитаете, 11 девяток долговечности означают, что если пользователь дает вам миллион объектов для хранения, по статистике вы будете терять один объект каждые 659 000 лет. Вот почему вы никогда не услышите о том, что поставщики облачных хранилищ теряют данные клиентов. При наличии двух копий в двух разных облачных дата-центрах шансы потерять данные из-за отказа оборудования практически нулевые. Этот уровень долговечности делает старое требование «двух разных сред» устаревшим.

Помимо повышения надежности, вторая облачная копия значительно повышает доступность данных резервного копирования. Хотя само хранилище

может иметь надежность на 11 девяток, целые центры обработки данных время от времени отключаются из-за сбоев связи. Доступность дата-центра обычно больше похожа на 4 девятки. С двумя отдельными облачными копиями, если один облачный центр обработки данных отключен, вы все равно можете получить доступ к своим резервным копиям во втором облачном центре обработки данных. В случае атаки программы-вымогателя вы можете предположить, что локальная копия будет уничтожена, поэтому вам придется полагаться на восстановление из облака. Если облако по какой-то причине отключено, ваш бизнес будет остановлен до тех пор, пока вы не получите доступ к своим резервным копиям. Вот почему наличие двух облачных копий — хорошая инвестиция.

Важность стратегии резервного копирования «с воздушным зазором»

В целом, в случае атаки организации должны иметь возможность быстро восстанавливать свои данные и сокращать сбои в своих бизнес-операциях. Поставщики программного обеспечения для резервного копирования в настоящее время продвигают новую стратегию, которая заменит старую стратегию 3-2-1. Они называют это стратегией 3-2-1-1-0. Это означает 3 копии, по крайней мере, в 2 местах, из которых 1 копия удалена, 1 копия хранится неизменно и проверена на отсутствие ошибок. Неизменяемую копию часто называют «воздушным зазором», потому что она физически или логически не связана с корпоративной сетью и, следовательно, невидима для всех, кто проник в корпоративную сеть. Эта характеристика «воздушного зазора» достигается за счет того, что репликация облачных копий предоставляется поставщику облачных услуг. Таким образом, пользователь выполняет резервное копирование не в два разных облачных хранилища, а только в одно. Затем поставщик облачных услуг выполняет репликацию полностью невидимым для сети способом.

Такой подход является важной мерой, позволяющей организациям восстанавливать свои данные, не опасаясь заражения или потери. Благодаря стратегии изолированного резервного копирования в сочетании с регулярным мониторингом и тестированием функций резервного копирования предприятия могут продолжать работу даже перед лицом атаки, уменьшая потенциальный ущерб и финансовые потери, которые могут возникнуть в результате нарушения кибербезопасности.

В связи с увеличением частоты и изощренностью кибератак, а также с тем фактом, что поставщики постоянно совершенствуют возможности обеспечения надежности, организации должны проявлять инициативу в отношении своих стратегий безопасности и регулярно проверять свои существующие стратегии на соответствие новым достижениям, чтобы обеспечить постоянную лучшую в своем классе защиту своих данных. Хотя традиционный подход к резервному копированию 3-2-1 остается ключевой тактикой для начала разработки методов защиты от киберугроз, одного этого подхода уже недостаточно для обеспечения передовой защиты от современных киберугроз. Реализация стратегии резервного копирования с воздушным зазором, включающая резервные копии, физически отделенные от первичных и вторичных хранилищ данных, в настоящее время является наиболее эффективным методом, который организации могут использовать для защиты от потери или повреждения данных». ***(David Friend. Why the 3-2-1***

backup strategy is obsolete // Future US, Inc. (https://www.techradar.com/opinion/why-the-3-2-1-backup-strategy-is-obsolete). 22.05.2023).

***

«…Программы-вымогатели представляют собой растущую и неотложную угрозу для организаций в Сингапуре из-за высокого уровня цифрового подключения. Программы-вымогатели могут иметь разрушительные последствия для организаций, поскольку они могут привести к значительной потере данных, сбоям в работе, подверженности юридическим и нормативным рискам, финансовому ущербу и ущербу для репутации. Хотя эта тревожная тенденция, несомненно, вызовет обеспокоенность по поводу подверженности киберстраховщиков рискам, существуют равные возможности для роста, поскольку, вероятно, возрастет интерес и спрос на киберстрахование.

Целевая группа по борьбе с программами-вымогателями

В подтверждение распространенности программ-вымогателей и серьезного воздействия программ-вымогателей была созвана Целевая группа по борьбе с программами-вымогателями («CRTF»), в состав которой вошли высокопоставленные представители различных государственных учреждений, для изучения этой растущей тенденции, разработки политики и предложения рекомендаций по эффективному противодействию этому риску.

CRTF опубликовал отчет 29 ноября 2022 года («Отчет CRTF»), призванный служить планом действий правительства и соответствующих агентств по защите Сингапура от атак программ-вымогателей. В отчете CRTF содержится несколько комментариев и рекомендаций, касающихся киберстраховщиков, и он заслуживает пристального внимания.

Четыре основных направления деятельности, рекомендованные CRTF

CRTF рекомендует правительству сосредоточиться на следующих четырех основных направлениях действий для эффективного противодействия угрозе программ-вымогателей:

(1) Компонент 1: Укрепление защиты объектов с высокой степенью риска

CRTF подчеркивает, что предотвращение успешной атаки программ-вымогателей имеет первостепенное значение, и это потребует от всех организаций повысить свою киберактивность и принять строгие технические меры для повышения кибербезопасности.

В частности, CRTF рекомендует критической информационной инфраструктуре («CII») и малым и средним предприятиям («SME»): уделять должное внимание

a) CRTF признает, что недавно пересмотренный Кодекс практики кибербезопасности («CCOP») предоставляет адекватное руководство для владельцев CII («CIIO») по соответствующим мерам выявления и снижения рисков в настоящее время, и что CCOP будет регулярно обновляться, чтобы он оставался соответствующий.

b) Для малых и средних предприятий, хотя CRTF отмечает, что существуют инициативы, которые помогут малым и средним предприятиям помочь в сравнительном анализе их практики кибербезопасности, CRTF рекомендует

разработать схемы стимулирования и поддержки для повышения осведомленности и повышения степени внедрения этих существующих инициатив.

(2) Компонент 2: разрушить бизнес-модель программ-вымогателей

Распространенность атак программ-вымогателей растет, поскольку они остаются прибыльным предприятием для преступников, а жертвы часто соглашаются на требования выкупа. CRTF предложила правительству переиздать бюллетени, которые отговаривают от выплаты выкупа и подчеркивают связанные с этим риски и последствия.

CRTF также рекомендовал изучить последствия полисов киберстрахования, которые обеспечивают покрытие выплат выкупа, и оценить потенциальные последствия, если такое покрытие будет прекращено. CRTF отметила предварительные данные, свидетельствующие о том, что застрахованные более склонны платить выкупы там, где предоставляется страховое покрытие, что способствует росту индустрии программ-вымогателей.

CRTF отметила проблемы с отслеживанием потока выкупных платежей, учитывая, что они часто выплачиваются в криптовалюте, которая впоследствии переводится в другие криптовалюты или криптовалюты, ориентированные на конфиденциальность. Чтобы обойти эти проблемы, CRTF рекомендует рассмотреть вопрос об обязательном для организаций сообщении о выплатах выкупа. Правительство одновременно улучшит свои возможности отслеживания, потенциально используя опыт поставщиков решений для блокчейна.

(3) Компонент 3: Поддержка восстановления

CRTF подчеркивает, что сотрудничество и помощь организаций-жертв являются ключом к эффективному противодействию программам-вымогателям. Для поощрения такого сотрудничества CRTF рекомендует:

(a) Предоставление ресурсов для помощи в восстановлении после атак программ-вымогателей путем создания единого портала для доступа организаций ко всем ресурсам, связанным с программами-вымогателями, таким как ключи дешифрования и контрольные списки ответов.

(b) Поощрение киберстрахования как практики управления рисками и изучения Правительством методов увеличения покупки киберстрахования, особенно среди СПО и МСП.

(4) Компонент 4: Работа с международными партнерами

Учитывая безграничный характер программ-вымогателей, CRTF подчеркивает, что для устранения угрозы необходимы скоординированные глобальные усилия. Для расширения международного сотрудничества CRTF рекомендует:

a) правительству ускорить трансграничное сотрудничество правоохранительных органов для обмена информацией;

b) продолжение работы с Целевой группой по финансовым мероприятиям в целях борьбы с отмыванием денег и финансированием терроризма; и

(c) Работать с международными партнерами над изучением влияния страховых полисов, покрывающих выплаты выкупа, на индустрию программ-вымогателей.

Что это означает для киберстраховщиков?

Отчет CRTF подтверждает, что киберстрахование является ключевым решением для программ-вымогателей, особенно для управления финансовыми рисками атак программ-вымогателей и повышения устойчивости общества к ним. Рекомендация по увеличению использования киберстрахования — отличная новость для киберстраховщиков, стремящихся расширить свой рынок, особенно среди CIIO и SME — двух категорий организаций, к которым стоит стремиться для роста бизнеса.

CRTF рекомендует создать руководство по киберстрахованию и адаптировать страховые пакеты для CIIO и SME, чтобы упростить процесс обнаружения. Киберстраховщики могут заранее принять это и предложить индивидуальные решения для этих целевых организаций. Киберстраховщики могут также захотеть рассмотреть смягченные требования к информации и стандарты ИТ-безопасности на этапе андеррайтинга для МСП, в частности, применяя подход «больше затрат по сравнению с риском», чтобы не отговаривать эти организации от покупки киберстрахования.

В мае 2023 года Агентство кибербезопасности Сингапура («CSA») запустило «План здравоохранения в области кибербезопасности» для правомочных МСП — схему, предназначенную для оказания финансовой поддержки МСП в привлечении консультантов по кибербезопасности для выполнения ими роли «руководителя» МСП. Офицеры по информационной безопасности», а также проводят «проверки» кибербезопасности и улучшают гигиену кибербезопасности. Соответствующие требованиям МСП могут получить до 70 % поддержки софинансирования, если они зарегистрируются у консультантов по кибербезопасности, привлеченных CSA. Это следует рассматривать как долгожданное событие для киберстраховщиков, нацеленных на рынок МСП. Повышая осведомленность о кибербезопасности и передовой опыт, схема CSA поможет малым и средним предприятиям снизить подверженность киберрискам. Это, в свою очередь, сделает их более привлекательными для киберстраховщиков.

Еще один вопрос, потенциально представляющий интерес для киберстраховщиков, — это рекомендация CRTF изучить вопрос о том, следует ли запретить покрытие платежей программ-вымогателей в Сингапуре. Покрытие выплат выкупа в настоящее время широко доступно в полисах киберстрахования в Сингапуре.

Дебаты о запрете платежей программами-вымогателями набирают обороты во всем мире, но их эффективность сомнительна. Противники утверждают, что, хотя это может закрыть один источник финансирования, это может побудить злоумышленников-вымогателей прибегать к более злонамеренным формам вымогательства, чтобы заставить организации прибегнуть к выплате выкупа для восстановления доступа к своим системам или данным. Это может сделать организации уязвимыми к большим финансовым потерям без защиты страхового покрытия. Две британские страховые ассоциации, представляющие сотни известных страховых компаний, недавно представили объединенному комитету парламента по стратегии национальной безопасности в декабре 2022 года доказательства, призывая правительство Великобритании избегать запрета на платежи программ-

вымогателей, ссылаясь на то, что они могут оказать неблагоприятное воздействие на организации и могут привести к росту неплатежеспособности и безработицы.

CRTF также признает, что без международного согласования страховых полисов, покрывающих выплаты выкупа, любая попытка запретить их на внутреннем рынке может привести только к тому, что организации будут обращаться за таким покрытием к зарубежным поставщикам. Это окажет негативное влияние на бизнес киберстраховщиков. Принимая во внимание вышеизложенное, киберстраховщики в Сингапуре могут захотеть активно взаимодействовать с правительством по этому вопросу». ***(Sumyutha Sivamani. Ransomware Crackdown in Singapore: Impact on Insurers // Clyde & Co LLP (https://www.clydeco.com/en/insights/2023/05/ransomware-crackdown-in-singapore-impact-on-insure). 22.05.2023).***

***

Фішингові атаки

«Злоумышленники все чаще используют Greatness, провайдера фишинга как услуги (PhaaS), для нацеливания на компании по всему миру с аутентичными целевыми страницами, которые на самом деле просто воруют конфиденциальные данные.

Согласно новому отчету Cisco Talos, инструмент, впервые созданный в середине 2022 года, демонстрирует значительный рост числа пользователей, поскольку злоумышленники нацелены на учетные записи Microsoft 365 компаний из США, Канады, Великобритании, Австралии и других стран. Южная Африка.

Злоумышленники атакуют фирмы в сфере производства, здравоохранения, технологий, образования, недвижимости, строительства, финансов и бизнес-услуг, стремясь получить конфиденциальные данные или учетные данные пользователей.

Хуже всего то, что Greatness значительно упрощает процесс настройки фишинговой кампании, существенно снижая порог входа.

Чтобы атаковать фирму, хакерам нужно сделать всего несколько вещей: войти в сервис, используя свой API-ключ; предоставить список целевых адресов электронной почты; создайте содержимое электронной почты (и измените любые другие детали по умолчанию по своему усмотрению).

После этого Greatness занимается рутинной работой по рассылке жертв. Те, кто попадутся на уловку и откроют сопроводительное вложение, получат запутанный код JavaSCript, который соединяется с сервером службы и захватывает вредоносную целевую страницу.

Сама страница частично автоматизирована — она берет журнал целевой компании и фоновое изображение с подлинной страницы входа в Microsoft 365 работодателя и предварительно заполняет правильный адрес электронной почты, делая его более правдоподобным для цели.

Затем целевая страница действует как посредник между пользователем и фактической страницей входа в Microsoft 365, проходя через процесс проверки подлинности и даже запрашивая код MFA, если для учетной записи настроена

многофакторная проверка подлинности. Как только пользователь входит в систему, злоумышленники захватывают файл cookie сеанса через Telegram, обходят MFA и получают доступ.

«Аутентифицированные сеансы обычно истекают через некоторое время, что, возможно, является одной из причин, по которой используется бот телеграммы — он информирует злоумышленника о действительных файлах cookie как можно скорее, чтобы гарантировать, что они могут быстро добраться, если цель интересна», — говорится в отчете Cisco». ***(Sead Fadilpašić. This dangerous phishing attack is targeting Microsoft users everywhere, so be on your guard // Future US, Inc. (https://www.techradar.com/news/this-dangerous-phishing-attack-is-targeting-microsoft-users-everywhere-so-be-on-your-guard). 11.05.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Власти США взломали секретную сеть скомпрометированных компьютеров, которую российские спецслужбы построили и годами использовали для слежки за членами НАТО, сообщило во вторник министерство юстиции.

ФБР удалось разрушить глобальную сеть компьютеров, которые были скомпрометированы «сложной вредоносной программой», известной как «Змея», говорится в заявлении Министерства юстиции. Для этого агентство провело санкционированную судом операцию по отключению Snake на скомпрометированных компьютерах с помощью инструмента, предписывающего вредоносному ПО уничтожить себя.

В течение почти двух десятилетий подразделение Федеральной службы безопасности России (ФСБ) — правопреемника советского КГБ — использовало Snake для нацеливания и кражи конфиденциальных документов из компьютерных систем в десятках стран мира, включая членов НАТО, Министерство юстиции. — сказал Департамент.

«Мы считаем Snake самым совершенным инструментом кибершпионажа в арсенале ФСБ», — говорится в бюллетене Агентства по кибербезопасности и безопасности инфраструктуры (CISA). «Во всем мире ФСБ использовала Snake для сбора конфиденциальной информации от высокоприоритетных целей, таких как правительственные сети, исследовательские центры и журналисты».

CISA подробно описал один конкретный случай, когда агентам ФСБ удалось использовать Snake для «доступа и извлечения конфиденциальных документов по международным отношениям, а также других дипломатических сообщений» через жертву в неуказанной стране НАТО. В бюллетене говорится, что в США ФСБ «преследовала» несколько секторов, включая государственные учреждения, критическое производство, финансовые услуги, образование, средства массовой информации и малый бизнес.

Согласно письменным показаниям ФБР, агентство работало с партнерами из разведки США и иностранными правительствами, чтобы выяснить, как работал Snake. ФСБ использовала Snake для извлечения данных из секретных компьютерных систем, в том числе управляемых правительствами стран НАТО, и передачи данных через скомпрометированные системы в США, прежде чем они были переданы обратно в Россию. Из-за этого жертвам было трудно раскрыть, как сеть была подключена.

В конце концов, благодаря анализу Snake, ФБР разработало способность расшифровывать и расшифровывать сообщения Снейка, сообщило министерство юстиции. Затем ФБР создало инструмент под названием Perseus, который мог связываться со Snake в определенной системе и использовать команды, чтобы заставить вредоносное ПО по существу самоуничтожиться.

«Российские правительственные деятели годами использовали этот инструмент для сбора разведывательных данных», — заявил Роб Джойс, директор по кибербезопасности Агентства национальной безопасности. «Инфраструктура Snake распространилась по всему миру. Технические детали помогут многим организациям найти и отключить вредоносное ПО по всему миру».

Высокопоставленные чиновники Министерства юстиции высоко оценили способность ФБР нейтрализовать сеть ФСБ.

«Министерство юстиции совместно с нашими международными партнерами демонтировало глобальную сеть зараженных вредоносным ПО компьютеров, которые российское правительство использовало в течение почти двух десятилетий для ведения кибершпионажа, в том числе против наших союзников по НАТО», — заявил генеральный прокурор Меррик Гарланд. заявление.

«Мы будем продолжать укреплять нашу коллективную оборону против дестабилизирующих усилий российского режима, направленных на подрыв безопасности Соединенных Штатов и наших союзников», — продолжил он». ***(Jake Epstein. Russian security agents have been using a secret network of corrupted computers to spy on NATO for decades, but the US just busted it open, feds say // Insider Inc. (https://www.businessinsider.com/us-cracked-computer-network-built-russia-fsb-spy-nato-doj-2023-5). 09.05.2023).***

***

«Во вторник чиновники ФБР произвели эффект разорвавшейся бомбы: после долгих лет наблюдения за исключительно незаметным вредоносным ПО, которое одно из самых передовых хакерских подразделений Кремля установило на сотни компьютеров по всему миру, агенты выгрузили полезную нагрузку, которая заставила вредоносное ПО отключиться.

Контрвзлом был нацелен на Snake, название обширного кроссплатформенного вредоносного ПО, которое уже более двух десятилетий используется для шпионажа и саботажа. Snake разработана и управляется Turla, одной из самых сложных APT в мире, сокращенно от продвинутых постоянных угроз, термин для давно работающих хакерских групп, спонсируемых национальными государствами.

Если бы хакерство, спонсируемое государством, было бы бейсболом, то Turla была бы не просто командой Высшей лиги — она была бы постоянным

претендентом на плей-офф. Исследователи из нескольких охранных фирм в основном согласны с тем, что Turla стояла за взломом данных Министерства обороны США в 2008 году, а в последнее время — Министерства иностранных дел Германии и вооруженных сил Франции. Группа также известна тем, что распространяет скрытое вредоносное ПО для Linux и использует спутниковые интернет-каналы для обеспечения скрытности своих операций.

Одним из самых мощных инструментов в арсенале Turla является Snake, своего рода цифровой швейцарский армейский нож, который работает на Windows, macOS и Linux. Написанный на языке программирования C, Snake представляет собой модульную серию компонентов, построенных поверх массивной одноранговой сети, которая тайно связывает один зараженный компьютер с другим. По данным ФБР, на сегодняшний день Snake распространился более чем в 50 странах и заразил компьютеры, принадлежащие правительствам стран-членов НАТО, американскому журналисту, освещавшему Россию, а также секторам, связанным с критической инфраструктурой, связью и образованием.

Краткий список возможностей Snake включает бэкдор, который позволяет Turla устанавливать или удалять вредоносное ПО на зараженных компьютерах, отправлять команды и передавать данные, представляющие интерес для Кремля. Профессионально разработанное программное обеспечение Snake использует несколько уровней пользовательского шифрования для шифрования команд и удаленных данных. По сети P2P зашифрованные команды и данные проходят через цепочку точек перехода, состоящую из других зараженных машин, что затрудняет обнаружение или отслеживание активности.

Происхождение Snake восходит как минимум к 2003 году, когда был создан предшественник под названием «Uroburos», разновидность уробороса, который является древним символом, изображающим змею или дракона, пожирающего собственный хвост. Изображение немецкого философа и теолога Якоба Бёме в низком разрешении, которое показано ниже, в какой-то момент служило ключом к избыточному бэкдору, который Turla установила на некоторые взломанные конечные точки.

Название Uroburos сохранилось в ранних версиях вредоносного ПО, даже после того, как оно было переименовано в Snake — например, в строке «Ur0bUr()sGoTyOu#». В 2014 году строка была заменена на «gLASs D1cK». Другие строки намекают на внутренние шутки, личные интересы разработчиков и насмешки, направленные на исследователей безопасности, которые анализируют или противодействуют их коду.

По словам ФБР, несмотря на браваду разработчиков, Snake является одним из самых сложных вредоносных программ, когда-либо найденных. Модульная конструкция, настраиваемые уровни шифрования и высокое качество кодовой базы сделали обнаружение антивирусным программным обеспечением трудным, если не невозможным. Однако по мере того, как агенты ФБР продолжали следить за Snake, они постепенно обнаруживали некоторые неожиданные слабости. Во-первых, имелся критически важный криптографический ключ с простой длиной всего 128 бит, что делало его уязвимым для факторинговых атак, раскрывающих секретный ключ. Этот слабый ключ использовался при обмене ключами Диффи-Хеллмана, что

позволяло каждой зараженной машине иметь уникальный ключ при обмене данными с другой машиной.

Еще одна ошибка: разработчики Snake забыли очистить готовый код для новой версии артефактов программирования. Этот сбой дал важные новые сведения о том, как работает вредоносное ПО, поскольку оно раскрывало имена функций, строки в открытом тексте и комментарии разработчиков…

В конце концов следователи обнаружили, что индивидуальная структура HTTP, используемая Snake для реализации обслуживания сеанса, позволяла вредоносному ПО обрабатывать несколько HTTP-пакетов как часть одного сеанса, зашифрованного слабым ключом. Открытие позволило исследователям идентифицировать данные, отправленные с одной зараженной Snake машины на другую.

«Уникальная реализация HTTP в Turla работает как своего рода подпись, при этом 8-байтовый компонент метаданных пакета Snake-HTTP увеличивается предсказуемым образом», — написал специальный агент ФБР Тейлор Форри в письме под присягой, поданном в поддержку запроса на утвержденный судом ордер на обыск. «Соответственно, наблюдая всего за двумя или тремя пакетами HTTP, ФБР научилось идентифицировать компьютеры, которые обмениваются данными с помощью Turla Snake-HTTP, и может сделать вывод о том, что имплантаты Snake на двух компьютерах аутентифицировали себя как вредоносное ПО Snake. ”

Используя информацию, полученную за эти годы, агенты ФБР в конечном итоге разработали Perseus, приложение, которое могло определять, когда две машины обмениваются данными друг с другом, используя собственный HTTP Snake. Perseus работает, имитируя начало протокола аутентификации сеанса Snake, чтобы «спровоцировать предполагаемый имплант Snake на другом компьютере, чтобы обеспечить ответ, уникальный для сетевых коммуникаций Snake», — объяснил Форри. Обмен аналогичен отправке одним компьютером «пинга» другому компьютеру для проверки сетевого подключения…

ФБР разработало возможность, используя PERSEUS, выдавать себя за операторов Turla Snake и отдавать команды вредоносному ПО Snake, которые эффективно и навсегда отключают его. Используя коды аутентификации, которые ФБР получило для имплантатов Snake на компьютерах субъектов, ФБР может использовать PERSEUS для выполнения полных протоколов аутентификации Snake и установления сеанса, а также для отправки команд на компьютеры субъектов, которые будет интерпретировать вредоносное ПО Snake на компьютерах субъектов. как законные и исполнить.

В частности, ФБР разработало метод, использующий некоторые встроенные команды Snake, описанные выше, которые при передаче PERSEUS с компьютера, контролируемого ФБР, вредоносному ПО Snake на компьютерах субъектов завершат работу приложения Snake и, в случае Кроме того, навсегда отключить вредоносное ПО Snake, перезаписав жизненно важные компоненты имплантата Snake, не затрагивая никакие законные приложения или файлы на компьютерах субъектов.

ФБР всесторонне протестировало этот метод и подтвердило, что он эффективен при отключении вредоносного ПО Snake и что этот метод не оказывает неблагоприятного воздействия на компьютер, на котором размещено вредоносное

ПО Snake. Действительно, в ходе тестирования ФБР подтвердило, что компьютер, зараженный Snake и вылеченный с помощью PERSEUS, будет продолжать работать в обычном режиме. Примечательно, что команды, передаваемые PERSEUS, отправляются с использованием пользовательских протоколов связи и шифрования, разработанных Turla для вредоносного ПО Snake, и поэтому могут быть интерпретированы и выполнены только имплантатами Snake. Таким образом, компьютер, не скомпрометированный Снейком, не сможет понять команды ПЕРСЕЯ и проигнорирует их.

Окружной судья США Шерил Л. Поллак из Восточного округа Нью-Йорка утвердила ордер на обыск, который дал ФБР добро на отправку команд Perseus на определенный набор IP-адресов, включенных в приложение.

Судебные документы представляют собой интригующий, но в конечном счете неполный отчет о том, как работал контрвзлом против Turla. В совместном бюллетене по кибербезопасности, выпущенном правоохранительными органами всего мира, содержится несколько дополнительных деталей. В справке говорится:

«Все коммуникации Snake состоят из «сеансов Snake», независимо от того, поверх какого легитимного протокола работает Snake. Верхний уровень шифрования Snake, называемый уровнем enc, использует многоэтапный процесс для создания уникального сеансового ключа. Сеансовый ключ формируется посредством комбинации обмена ключами Диффи-Хеллмана, смешанного с предварительным общим ключом (PSK), известным обеим сторонам. Этот PSK хранится в одном из каналов связи, хранится в Очереди.29

Общее создание сеансового ключа требует 12 шагов связи, по шесть в каждом направлении, которые включают обмен псевдослучайными значениями, используемыми в процессе обмена Диффи-Хеллмана, а также пользовательские аспекты метода получения сеансового ключа Snake. Сеансовый ключ используется для шифрования заголовков команд и (внутренних) зашифрованных полезных данных.

Это уровень, на котором произошла критическая ошибка предоставления значения 128 бит вместо 128 байт для вызова DH_generate_parameters в библиотеке OpenSSL. Из-за недостаточной длины ключа возможен взлом части обмена Диффи-Хеллмана. Обратите внимание, что на следующем рисунке переменные «p», «g», «a» и «b» используются в стандартных описаниях Диффи-Хеллмана».

Оплошность Turla — не первый случай, когда хакерская организация, поддерживаемая государством, терпит серьезные неудачи из-за небрежного надзора или отсутствия внимания к деталям. В 2010 году агрессивный компьютерный червь, известный как Stuxnet, заразил тысячи компьютеров и спровоцировал многолетнее расследование. Выяснилось, что это дело рук Агентства национальной безопасности и его коллег из Израиля. Предполагалось, что он незамеченным проникнет на иранский ядерный объект в Натанзе, саботирует урановые центрифуги и тихо исчезнет. Неспособность Stuxnet стать предназначенной для хирургического контроля полезной нагрузкой является напоминанием о том, насколько плохо могут обстоять дела даже для APT национального государства…» ***(Dan Goodin. How one of Vladimir Putin's most prized hacking units got pwned by the FBI // Condé Nast***

(https://arstechnica.com/information-technology/2023/05/how-the-fbi-pwned-turla-a-kremlin-jewel-and-one-of-worlds-most-skilled-apts/). 10.05.2023).

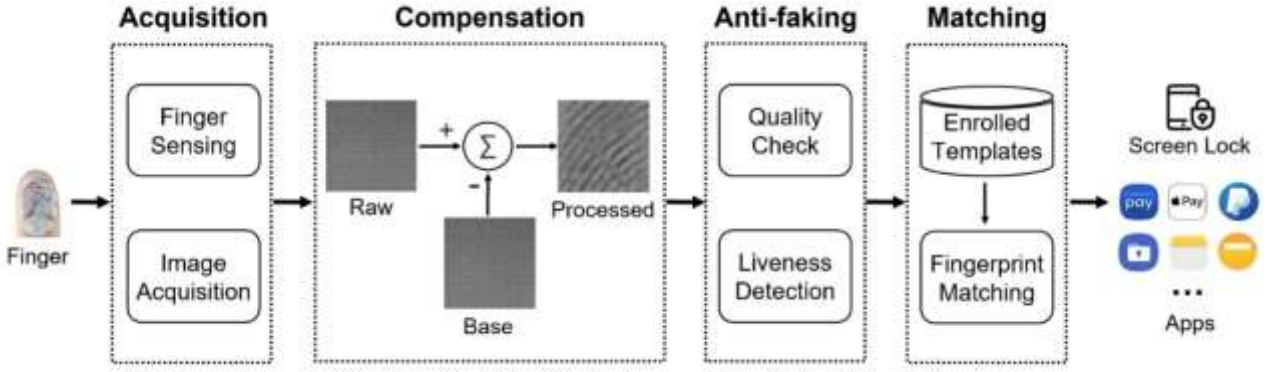
***

«Исследователи разработали недорогую атаку на смартфон, которая взламывает отпечаток пальца аутентификации, используемый для разблокировки экрана и выполнения других конфиденциальных действий на ряде устройств Android всего за 45 минут.

Эта атака, названная ее создателями BrutePrint, требует от злоумышленника физического контроля над устройством, когда оно потеряно, украдено, временно передано или оставлено без присмотра, например, когда владелец спит. Цель: получить возможность выполнять атаку грубой силы, которая пытается подобрать огромное количество отпечатков пальцев, пока не будет найден тот, который разблокирует устройство. Атака использует уязвимости и слабости в SFA устройства (аутентификация по отпечатку пальца смартфона).

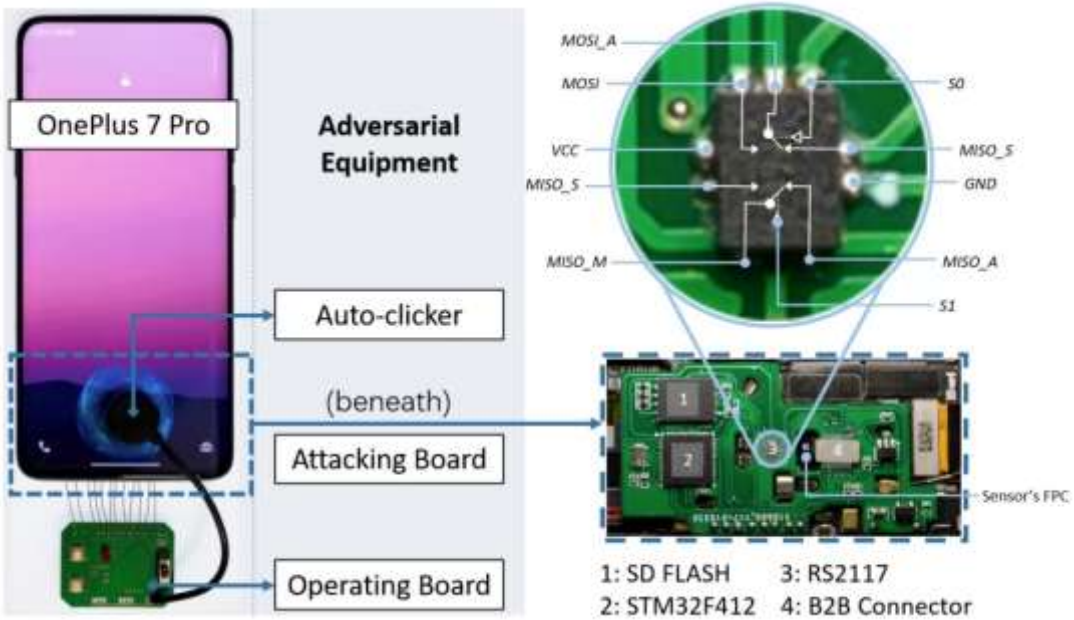
Обзор брутпринта

BrutePrint — это недорогая атака, которая позволяет людям разблокировать устройства, используя различные уязвимости и слабые места в системах аутентификации по отпечаткам пальцев смартфонов. Вот рабочий процесс этих систем, которые обычно обозначаются аббревиатурой SFA.



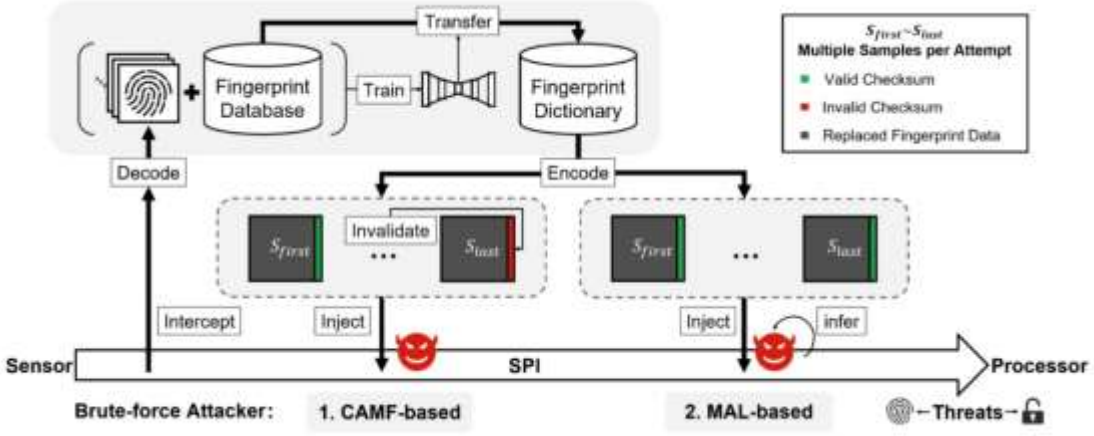
Рабочий процесс системы аутентификации по отпечатку пальца смартфона.

Ядром оборудования, необходимого для BrutePrint, является печатная плата за 15 долларов, которая содержит (1) микроконтроллер STM32F412 от STMicroelectronics, (2) двунаправленный двухканальный аналоговый коммутатор, известный как RS2117, (3) флэш-карту SD с 8 ГБ памяти. память и (4) межплатный разъем, соединяющий материнскую плату телефона с гибкой печатной платой датчика отпечатков пальцев.



Устройство противника, составляющее основу атаки BrutePrint.

Кроме того, для атаки требуется база данных отпечатков пальцев, аналогичная тем, которые используются в исследованиях или просочились в реальных взломах, таких как эти.



Обзор атаки BrutePrint.

Не все смартфоны одинаковы

Подробнее о том, как работает BrutePrint, позже. Во-первых, разбивка того, как поживают различные модели телефонов. Всего исследователи протестировали 10 моделей: Xiaomi Mi 11 Ultra, Vivo X60 Pro, OnePlus 7 Pro, OPPO Reno Ace, Samsung Galaxy S10+, OnePlus 5T, Huawei Mate30 Pro 5G, Huawei P40, Apple iPhone SE, Apple iPhone 7.

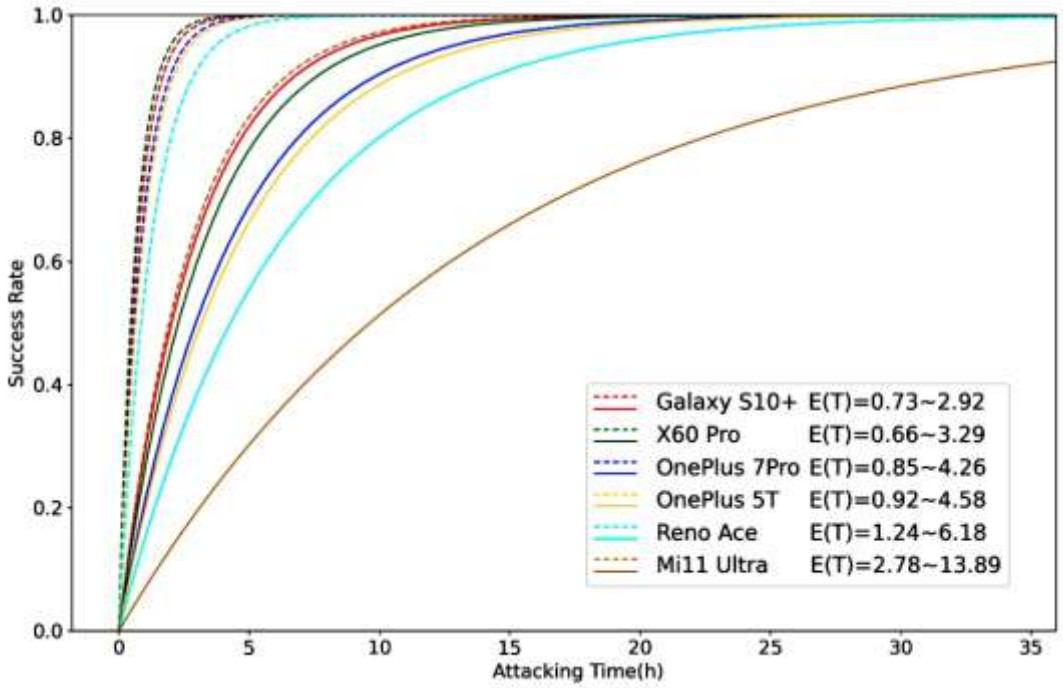
Device				Sensor		Attempt Limit		
Manuf./Model	OS/Ver.	TEE	r_{max}	Manuf.	Type	ScreenLock[1]	Payment[2]	Privacy[3]
Xiaomi Mi 11 Ultra	Android 11	QTEE	5	Goodix	Optical (ultra-thin)*	5×4	5×4	5
Vivo X60 Pro	Android 11	Kinibi	5	Goodix	Optical*	5	∞	5
OnePlus 7 Pro	Android 11	QTEE	5	Goodix	Optical*	5	5	5
OPPO Reno Ace	Android 10	QTEE	5	Goodix	Optical*	5×4	5×4	5×4
Samsung Galaxy S10+	Android 9	Knox	4	Qualcomm	Ultrasonic*	5×10	5	5×10
OnePlus 5T	Android 8	QTEE	5	Goodix	Capacitive	5×4	5×4	5×4
Huawei Mate30 Pro 5G	HarmonyOS 2	TrustedCore	5	Goodix	Optical*	5×4	5×∞	5×∞
Huawei P40	HarmonyOS 2	TrustedCore	5	Novatek	Optical*	5×4	5×∞	5×∞
Apple iPhone SE	iOS 14.5.1	Secure Enclave	5	AuthenTec	Capacitive	5	5	5
Apple iPhone 7	iOS 14.4.1	Secure Enclave	5	AuthenTec	Capacitive	5	5	5

* In-display fingerprint sensors that are incorporated under the screen.
[1] A1: unlock the screen of the devices.
[2] A2: make payments on pre-installed payment apps. Since OnePlus Pay is made exclusive to some countries, we use PayPal instead. For other models, the specific apps are Mi Pay, Vivo Pay, OPPO Pay, Samsung Pay, Huawei Pay, and Apple Pay.
[3] A3: login pre-installed privacy protection apps. Hidden Folders for Xiaomi, Secure Folder for Samsung, File Safe for Vivo, Private Safe for OPPO, LockBox for OnePlus, Safe for Huawei and Notes for Apple.

Список протестированных устройств вместе с различными атрибутами устройств.

Исследователи протестировали каждый из них на наличие уязвимостей, недостатков или восприимчивости к различным методам атак. Изучаемые атрибуты включали количество выборок при множественной выборке, наличие функции устранения ошибок, поддержку горячего подключения, возможность декодирования данных и частоту передачи данных по SPI. Кроме того, исследователи протестировали три атаки: попытка обхода ограничений, захват изображений отпечатков пальцев и перебор отпечатков пальцев…

Наконец, исследователи представили результаты, показывающие время, которое потребовалось различным телефонам для подбора отпечатков пальцев. Поскольку количество времени зависит от разрешенного количества отпечатков, исследователи установили для каждого один отпечаток.



Уровень успеха различных тестируемых устройств: Galaxy S10+ занял наименьшее количество времени (от 0,73 до 2,9 часов), а Mi11 - больше всего (от 2,78 до 13,89 часов).

Хотя особенности различались, в результате BrutePrint может пытаться использовать неограниченное количество отпечатков пальцев для аутентификации на всех восьми протестированных моделях Android. В зависимости от различных факторов, включая структуру аутентификации по отпечаткам пальцев конкретного

телефона и количество отпечатков пальцев, сохраненных для аутентификации, это занимает от 40 минут до 14 часов.

Внедрение BrutePrint на утерянном или украденном устройстве

В отличие от аутентификации по паролю, которая требует прямого совпадения между тем, что вводится, и тем, что хранится в базе данных, аутентификация по отпечатку пальца определяет совпадение с использованием эталонного порога. В результате для успешной атаки грубой силой по отпечаткам пальцев требуется только, чтобы введенное изображение обеспечивало приемлемое приближение к изображению в базе данных отпечатков пальцев. BrutePrint манипулирует коэффициентом ложного принятия (FAR), чтобы увеличить порог, поэтому принимается меньше приблизительных изображений.

BrutePrint действует как противник посередине между датчиком отпечатков пальцев и доверенной средой выполнения и использует уязвимости, позволяющие делать неограниченные предположения.

В атаке BrutePrint злоумышленник снимает заднюю крышку устройства и прикрепляет печатную плату за 15 долларов, на которой база данных отпечатков пальцев загружена во флэш-память. Затем злоумышленник должен преобразовать базу данных в словарь отпечатков пальцев, отформатированный для работы с конкретным датчиком, используемым целевым телефоном. Процесс использует перенос в нейронном стиле при преобразовании базы данных в пригодный для использования словарь. Этот процесс увеличивает шансы на совпадение.

Имея словарь отпечатков пальцев, устройство злоумышленника теперь может вводить каждую запись в целевой телефон. Обычно защита, известная как ограничение попыток, эффективно блокирует телефон после достижения заданного количества неудачных попыток входа в систему. BrutePrint может полностью обойти это ограничение в восьми протестированных моделях Android, а это означает, что устройство злоумышленника может делать бесконечное количество догадок. (На двух iPhone атака может увеличить количество догадок до 15, что в три раза превышает разрешенные пять.)

Обходы являются результатом использования того, что, по словам исследователей, является двумя уязвимостями нулевого дня в системе аутентификации по отпечаткам пальцев практически всех смартфонов. Уязвимости — одна известная как CAMF (сбой отмены после сопоставления) и другая MAL (сопоставление после блокировки) — возникают из-за логических ошибок в структуре аутентификации. Эксплойты CAMF делают недействительной контрольную сумму передаваемых данных отпечатков пальцев, а эксплойты MAL выводят результаты сопоставления с помощью атак по сторонним каналам.

Аутентификация по отпечатку пальца смартфона использует SPI (последовательный периферийный интерфейс) для подключения датчика и процессора устройства. BrutePrint действует как противник посередине, который подключается к этому соединению и получает данные, которые эффективно перехватывают изображения отпечатков пальцев, хранящиеся на целевом устройстве.

Способность BrutePrint успешно перехватывать отпечатки пальцев, хранящиеся на устройствах Android, но не на iPhone, является результатом одного простого различия в конструкции: iOS шифрует данные, а Android — нет…

BrutePrint — это работа Ю Чена из Tencent и Илин Хе из Чжэцзянского университета. Они предложили несколько программных или аппаратных изменений, призванных смягчить атаки. Одним из изменений является предотвращение обхода ограничения попыток путем проверки эксплойтов CAMF. Проверка работает, устанавливая дополнительный лимит на отмену ошибок. Еще одно предлагаемое исправление — предотвращение атак злоумышленника посередине путем шифрования данных, передаваемых между датчиком отпечатков пальцев и процессором устройства. Наконец, исследователи рекомендуют изменения, которые заставят сбор отпечатков пальцев вести себя последовательно, независимо от того, выводятся ли совпадающие результаты…» ***(Dan Goodin. Here's how long it takes new BrutePrint attack to unlock 10 different smartphones // Condé Nast (https://arstechnica.com/information-technology/2023/05/hackers-can-brute-force-fingerprint-authentication-of-android-devices/). 23.05.2023).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Microsoft Exchange ИТ-команды, работающие с серверами (открывается в новой вкладке), очень медленно устанавливают исправления для своих конечных точек, в результате чего тысячи устройств по-прежнему уязвимы для некоторых серьезных уязвимостей.

Об этом говорится в новом отчете CyberNews, в котором утверждается, что более 85 000 серверов по-прежнему подвержены нескольким уязвимостям удаленного выполнения кода (RCE), а именно CVE-2023-21529, CVE-2023-21706 и CVE-2023-21707.

В отчете недостатки описываются как «чрезвычайно опасные» из-за того, что они могут позволить злоумышленникам запускать вредоносный код и компрометировать почтовые ящики людей и сообщения электронной почты, хранящиеся на серверах.

Недостатки были обнаружены в середине февраля 2023 года, и Microsoft быстро выпустила исправление для решения проблемы.

Однако, по их словам, многие ИТ-команды еще не применили эти исправления. На самом деле, согласно данным Shadowserver Foundation, количество уязвимых серверов в феврале составляло 87 000, а это означает, что подавляющее большинство ИТ-команд в основном игнорировали эту угрозу безопасности и просто решили не применять исправление.

Исследователи проанализировали примерно 250 000 подключенных к Интернету серверов Microsoft Exchange и обнаружили, что именно 85 261

подвержены этим уязвимостям RCE (34,33%). Большинство уязвимых серверов находились в Германии — 18 000 из них.

На втором месте США с почти 16 000 серверов, за ними следуют Великобритания (3 734), Франция (2 959) и Россия (2 775). Особый интерес представляли Россия и Китай, поскольку компании в этих странах предпочитали более старые версии MS Exchange 2016, «хотя более новые версии по-прежнему использовались в выпусках 2019 и 2013 годов», — отмечают исследователи.

Влияние «примерно одинаковое», но уязвимости разные.

Хотя трудно определить, кто может использовать эти недостатки и с какой целью, Cybernews подчеркивает, что «похожие уязвимости» были обнаружены в прошлом российскими государственными деятелями. Издание утверждает, что эти недостатки мало чем отличаются от тех, которые ГРУ использовало в 2020 году для участия в крупномасштабных атаках на государственные учреждения, предприятия и организации». ***(Sead Fadilpašić. Thousands of Microsoft servers are at risk from some serious security bugs // Future US, Inc. (https://www.techradar.com/news/thousands-of-microsoft-servers-are-at-risk-from-some-serious-security-bugs). 10.05.2023).***

***

«Тестовий злам супутника проходив у рамках CYSAT, одного з найбільших заходів з кібербезпеки та космічної галузі, що відбувся у Парижі. За словами організаторів CYSAT, метою випробувань було показати космічним інженерам, як мислять хакери і якої шкоди вони можуть завдати супутнику, а також як можна виявити, усунути і, зрештою, запобігти атаці.

Хакерам вдалося успішно продемонстрували ризики, які скомпрометований супутник може становити для всієї космічної екосистеми, адже вони отримали доступ до інтерфейсу керування зондом і змогли маніпулювати його системою, наприклад, збити з пантелику систему обробки зображень, замаскувавши якийсь об'єкт, а також завантажити шкідливий код.

Реальні загрози для космічних апаратів

Віце-президент Thales з кібернетичних рішень П'єр-Ів Жоліве заявив, що зі зростанням кількості військових і цивільних застосувань, які сьогодні залежать від супутникових систем, космічна галузь повинна брати до уваги кібербезпеку на кожному етапі життєвого циклу супутника. Навчання надали можливість підвищити обізнаність про потенційні недоліки і вразливості для підвищення кіберстійкості супутників і космічних програм.

За словами Чарльза Денєра, експерта з кібербезпеки і національної безпеки, застарілі супутники, вразливі для хакерів з ворожих держав, таких як Росія, мають величезні можливості для кібератак. Це стало величезним викликом, оскільки супутникові знімки були бажаним активом у конфліктах, який використовувався обома сторонами для оцінки стратегічних позицій військ.

Як супутники допомагають Україні у війні

Супутники Starlink Ілона Маска забезпечили Україні стабільний інтернет, протидіючи повномасштабному вторгненню Росії в ході якого були виведені з ладу важливі ланки української комунікаційної інфраструктури та критично важливих

послуг. Саме обладнання Starlink дозволило організувати можливість швидкого відновлення важливих вузлів інфраструктури та продовжити боротьбу.

Тим часом Китай оголосив війну угрупованню Starlink, яке налічує близько 3500 супутників на орбіті Землі, і розробляє власний флот супутників, оснащених новою зброєю зі штучним інтелектом, в тому числі лазерами і потужними мікрохвилями, а також здатних нести військове корисне навантаження.

Випробування проведене ЄКА на своєму наносупутнику, підкреслює зростаючу потребу у застосуванні кібербезпекових інструментів у космічній галузі. В умовах зростаючої залежності від супутникових систем для надання критично важливих послуг на Землі важливо враховувати кібербезпеку на кожному етапі життєвого циклу супутника, щоб підвищити кіберстійкість супутників і космічних програм». ***(Михайло Года. Хакери вперше в історії зламали державний космічний супутник // ПрАТ «Телерадіокомпанія "Люкс"» (https://24tv.ua/tech/esa-provela-pershiy-istoriyi-test-zlam-suputnika-realnomu-chasi_n2305721). 02.05.2023).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…AV-TEST, независимая организация, которая оценивает и оценивает антивирусное и антивирусное программное обеспечение, протестировала 18 антивирусных пакетов для Windows 10. Исследование включало тестирование программ на 12 000 образцов вредоносных программ, смешанных с 1,5 миллионами файлов, чтобы определить, какие из них могут отличить вредоносные программы от вредоносных программ и чего-то безвредного. Он также проверил наличие программ-вымогателей, хотя AV-TEST отмечает, что даже положительное обнаружение не может предотвратить развитие атаки.

Были протестированы 18 пакетов безопасности: AhnLab, Avast, AVG, Avira, Bitdefender, ESET, F-Secure, G DATA, K7 Computing, Kaspersky, Malwarebytes, McAfee, Microsoft Defender, Microworld, Norton, PC Matic, Protected. сети и Trend Micro.

AV-TEST присвоил в общей сложности 6 баллов в каждой из трех категорий тестов: защита, производительность и удобство использования.

Хорошей новостью для тех, кто его использует, является то, что Microsoft Defender получил высшие баллы 6 в категориях защиты и удобства использования, но 5/6, за которые он был оценен по производительности, был худшим из всех протестированных программ.

«Самая высокая системная нагрузка в тесте была создана антивирусной программой «Защитник Windows» для потребителей. Поскольку системная нагрузка значительно выше, чем у других продуктов, Defender потерял целый балл, таким образом получив 5 из 6 баллов», — пишет AV. -TECT.

Не было подробно объяснено, насколько сильно Защитник загружает системы и насколько плохо он работает с другими антивирусными программами.

В другом месте 14 из 18 пакетов были удостоены рейтинга лучших продуктов, набрав 17,5 или выше. Microsoft Defender, ESET, Microworld и ПК набрали 17 баллов, но AV-TEST подчеркнул, что они по-прежнему обеспечивают очень надежный уровень безопасности, просто допустили несколько незначительных ошибок.

Наихудшая оценка в категории из всех, 3,0, была дана PC Matic в разделе удобства использования, что принесло ему самый низкий общий балл (15). AV-TEST обнаружил, что PC Matic выявил более двух десятков ложных срабатываний и заблокированных приложений.

Шести продуктам удалось получить высший балл 18: Avast, Avira, Bitdefender, G DATA, Kaspersky и Trend Micro». ***(Rob Thubron. Examination of 18 antivirus programs shows Microsoft Defender has the highest system load // TechSpot, Inc. (https://www.techspot.com/news/98634-examination-18-antivirus-programs-shows-microsoft-defender-has.html). 10.05.2023).***

***

«Компания Cloudflare, занимающаяся интернет-решениями, сегодня представила Cloudflare One для искусственного интеллекта, свой новейший набор элементов управления безопасностью с нулевым доверием. Эти инструменты позволяют предприятиям безопасно и надежно использовать новейшие генеративные инструменты искусственного интеллекта, защищая при этом интеллектуальную собственность и данные клиентов. Компания считает, что функции пакета предложат организациям простые, быстрые и безопасные средства внедрения генеративного ИИ без ущерба для производительности или безопасности.

«Cloudflare One предоставляет командам любого размера возможность использовать лучшие инструменты, доступные в Интернете, без проблем с управлением или проблем с производительностью. Кроме того, это позволяет организациям проверять и анализировать инструменты искусственного интеллекта, которые начали использовать члены их команды», — сказал VentureBeat Сэм Ри, вице-президент по продукту в Cloudflare. «Команды безопасности могут затем ограничить использование только утвержденными инструментами и, в рамках тех, которые утверждены, контролировать и блокировать, как данные передаются этим инструментам, используя политики, построенные вокруг конфиденциальных и уникальных данных [их организации]».

Cloudflare One для ИИ предоставляет предприятиям комплексную безопасность ИИ с помощью таких функций, как прозрачность и измерение использования инструментов ИИ, предотвращение потери данных и управление интеграцией.

Cloudflare Gateway позволяет организациям отслеживать количество сотрудников, экспериментирующих с сервисами ИИ. Это обеспечивает контекст для составления бюджета и планов корпоративного лицензирования. Сервисные токены также предоставляют администраторам четкий журнал запросов API и контроль над определенными сервисами, которые могут получать доступ к данным обучения ИИ.

Cloudflare Tunnel обеспечивает зашифрованное только исходящее соединение с сетью Cloudflare, а служба предотвращения потери данных (DLP) предлагает

защиту, позволяющую закрыть человеческий пробел в том, как сотрудники обмениваются данными.

«Искусственный интеллект сулит невероятные перспективы, но без надлежащих ограждений он может создавать значительные бизнес-риски. Продукты Cloudflare с нулевым доверием первыми обеспечивают защиту для инструментов ИИ, поэтому предприятия могут воспользоваться возможностью, которую открывает ИИ, обеспечивая при этом обмен только теми данными, которые они хотят предоставить», — сказал Мэтью Принс, соучредитель и генеральный директор Cloudflare. письменное заявление.

Организации все чаще внедряют генеративные технологии искусственного интеллекта для повышения производительности и инноваций. Но технология также представляет значительные риски для безопасности. Например, крупные компании запретили популярные приложения для генеративного ИИ-чата из-за утечки конфиденциальных данных. В недавнем опросе, проведенном KPMG в США, 81% руководителей США выразили озабоченность по поводу кибербезопасности в отношении генеративного ИИ, а 78% выразили обеспокоенность по поводу конфиденциальности данных.

По словам Реи из Cloudflare, клиенты выражают повышенную озабоченность по поводу входных данных для генеративных инструментов искусственного интеллекта, опасаясь, что отдельные пользователи могут непреднамеренно загрузить конфиденциальные данные. Организации также выразили опасения по поводу обучения этих моделей, что создает риск предоставления чрезмерно широкого доступа к наборам данных, которые не должны покидать организацию. Открывая данные для этих моделей, организации могут непреднамеренно поставить под угрозу безопасность своих данных.

«Главная забота директоров по информационной безопасности и ИТ-директоров сервисов искусственного интеллекта — это чрезмерный обмен информацией — риск того, что отдельные пользователи, по понятным причинам взволнованные инструментами, случайно передадут конфиденциальные корпоративные данные этим инструментам», — сказал Риа VentureBeat. «Cloudflare One для ИИ предоставляет этим организациям комплексный фильтр, не замедляя работу пользователей, чтобы гарантировать, что общие данные разрешены, а несанкционированное использование неутвержденных инструментов заблокировано».

Компания утверждает, что Cloudflare One для ИИ предоставляет командам необходимые инструменты для предотвращения таких угроз. Например, путем сканирования данных, которыми обмениваются, Cloudflare One может предотвратить загрузку данных в службу.

Кроме того, Cloudflare One облегчает создание безопасных путей для обмена данными с внешними службами, которые могут регистрировать и фильтровать доступ к этим данным, тем самым снижая риск утечки данных.

«Cloudflare One для ИИ дает компаниям возможность контролировать каждое взаимодействие своих сотрудников с этими инструментами или взаимодействие этих инструментов с их конфиденциальными данными. Клиенты могут начать с каталогизации того, какие инструменты ИИ используют их сотрудники, без особых

усилий, полагаясь на наш предварительно подготовленный анализ», — пояснил Реа. «Всего за несколько кликов они могут заблокировать или контролировать, какие инструменты используют члены их команды».

Компания утверждает, что Cloudflare One для ИИ первым предлагает ограждения вокруг инструментов ИИ, поэтому организации могут извлечь выгоду из ИИ, гарантируя, что они будут делиться только теми данными, которые они хотят раскрыть, не рискуя своей интеллектуальной собственностью и данными клиентов.

Служба DLP Cloudflare сканирует контент, поскольку он оставляет устройства сотрудников для обнаружения потенциально конфиденциальных данных во время загрузки. Администраторы могут использовать предварительно предоставленные шаблоны, такие как номера социального страхования или кредитных карт, или определять термины или выражения для конфиденциальных данных. Когда пользователи пытаются загрузить данные, содержащие один или несколько примеров этого типа, сеть Cloudflare блокирует это действие до того, как данные достигнут места назначения.

«Клиенты могут сообщить Cloudflare типы данных и интеллектуальной собственности, которыми они управляют и [которые] никогда не покинут их организацию, поскольку Cloudflare будет сканировать каждое взаимодействие их корпоративных устройств со службой ИИ в Интернете, чтобы фильтровать и блокировать эти данные. их организации, — объяснила Рея.

Реа сказал, что организации обеспокоены доступом внешних служб ко всем данным, которые они предоставляют, когда модели ИИ необходимо подключиться к обучающим данным. Они хотят, чтобы модель ИИ была единственной службой, предоставляющей доступ к данным.

«Сервисные токены обеспечивают своего рода модель аутентификации для автоматизированных систем так же, как пароли и вторые факторы обеспечивают проверку подлинности для пользователей», — сказал Рея. «Сеть Cloudflare может создавать сервисные токены, которые могут быть предоставлены внешней службе, такой как модель ИИ, а затем действовать как вышибала, проверяя каждый запрос на получение внутренних обучающих данных на предмет наличия этого сервисного токена».

По данным компании, брокер безопасности облачного доступа (CASB) Cloudflare, точка обеспечения безопасности между поставщиком облачных услуг и его клиентами, вскоре сможет сканировать инструменты искусственного интеллекта, используемые предприятиями, и обнаруживать неправильную конфигурацию и неправильное использование. Компания считает, что ее платформенный подход к безопасности позволит компаниям во всем мире использовать улучшения производительности, предлагаемые развивающимися технологиями, новыми инструментами и плагинами, не создавая узких мест. Кроме того, платформенный подход обеспечит соблюдение компаниями последних правил.

«Cloudflare CASB сканирует приложения «программное обеспечение как услуга» (SaaS), в которых организации хранят свои данные и выполняют некоторые из своих наиболее важных бизнес-операций, на предмет возможного неправомерного использования», — сказал Реа. «В рамках Cloudflare One для ИИ мы планируем создать новые интеграции с популярными инструментами ИИ для

автоматического сканирования на предмет неправильного использования или неправильно настроенных значений по умолчанию, чтобы помочь администраторам быть уверенными в том, что отдельные пользователи случайно не открывают двери в свои рабочие места».

Он сказал, что, как и многие организации, Cloudflare ожидает узнать, как пользователи будут применять эти инструменты по мере того, как они становятся все более популярными на предприятии, и готова адаптироваться к вызовам по мере их возникновения.

«Одна область, в которой мы заметили особую озабоченность, — это хранение данных этих инструментов в регионах, где обязательства по суверенитету данных требуют большего контроля», — сказал Реа. «Сеть центров обработки данных Cloudflare в более чем 285 городах по всему миру дает нам уникальное преимущество, помогая клиентам контролировать, где хранятся их данные и как они передаются во внешние места назначения». ***(Victor Dey. Cloudflare unveils Cloudflare One for AI to enable safe use of generative AI tools // VentureBeat (https://venturebeat.com/security/cloudflare-unveils-cloudflare-one-for-ai-to-enable-safe-use-of-generative-ai-tools/). 15.05.2023).***

***