**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

№ 4 (квітень)

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.– №4 (квітень) . – 188 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

«В Україні провели перші командно-штабні навчання зі стійкості критичної інфраструктури Critical Infrastructure Resilience Exercises (CIREX), які розроблені на базі методичних рекомендацій Агентства США з питань кібербезпеки та захисту інфраструктури (CISA).

Про це повідомив заступник голови Державної служби спеціального зв'язку та захисту інформації Олександр Потій, передає Укрінформ з посиланням на прессслужбу відомства.

Зазначається, що Державна служба спеціального зв'язку та захисту інформації України за підтримки проєкту USAID «Кібербезпека критично важливої інфраструктури України» провела перші командно-штабні навчання зі стійкості критичної інфраструктури Critical Infrastructure Resilience Exercises (CIREX), розроблені на базі методичних рекомендацій Агентства США з питань кібербезпеки та захисту інфраструктури (CISA).

«Це перші командно-штабні навчання, які ми проводимо в межах співпраці з CISA та з урахуванням нових рішень уряду, якими затверджено єдину систему заходів із реагування на кіберінциденти та рівні їхньої критичності, що розроблені фахівцями Держспецзв'язку. Далі у планах — опрацювання під час подібних навчань всього спектру викликів, перед якими постають оператори об'єктів критичної інфраструктури», - зазначив він.

Головна ціль CIREX полягала в опрацюванні питань протистояння кіберзагрозам та координації зусиль у відбитті кібератак. Участь у навчанні взяли представники енергетичного сектору, які протягом дня відпрацьовували механізми реагування на кібератаки типу Ransomware (програм-здирників відповідно до чинної таксономії кіберінцидентів)…» ***(Захист енергоб'єктів від кібератак: в Україні провели перші командно-штабні навчання CIREX // Укрінформ (https://www.ukrinform.ua/rubric-technology/3698002-zahist-energobektiv-vid-kiberatak-v-ukraini-proveli-persi-komandnostabni-navcanna-cirex.html). 19.04.2023).***

***

Національна система кібербезпеки

«Україна починає будувати систему захисту критичної інфраструктури від можливих ворожих атак. Її створять відповідно до найкращих світових практик та чинних вимог європейського законодавства. Про це повідомляє Держспецзв'язку України у телеграмі.

Держспецзв'язку та Американська агенція з кібербезпеки та захисту критичної інфраструктури CISA уклали меморандум про співпраці. І вже були проведені навчання відповідно до методики CISA. Саме ця організація має провідний досвід у питаннях захисту об'єктів критичної інфраструктури.

Нині Україна напрацьовує необхідну нормативно-правову базу. Зокрема, створюють переліки об'єктів критичної інфраструктури. Після чого мають

ухвалити постанову про затвердження порядку ведення реєстру критичної інфраструктури.

Зазначається, що поява реєстру стане важливим кроком для координації захисту інфраструктури.

Відповідальними за захист об’єктів критичної інфраструктури будуть оператори. ЗСУ оберігатиме ці об’єкти від ракетних обстрілів, СБУ — проти диверсій, а Держспецзв’язку — проти кібератак.

«Для проходження наступної зими потрібно вже зараз активізувати зусилля для підготовки до загроз та захисту енергетичної інфраструктури.

Реєстр ОКІ та вчасне подання інформації для його наповнення є вкрай важливими для захисту критичної інфраструктури України», — додали у Держспецзв’язку…» ***(Юлія СЕРГЕЄВА. В Україні створять систему захисту критичної інфраструктури // Вечірній Київ (https://vechirniy.kyiv.ua/news/81812/). 23.04.2023).***

***

Кібервійна проти України

«Кабінет Міністрів затвердив Порядок реагування на кіберінциденти та кібератаки.

Про це повідомив заступник голови Державної служби спеціального зв'язку та захисту інформації Олександр Потій, передає Укрінформ із посиланням на Телеграм-канал відомства.

«Порядок затверджує єдиний механізм впровадження суб’єктами забезпечення кібербезпеки операційних процедур реагування на кіберінциденти. Також він визначає чіткі й зрозумілі рівні критичності кіберінцидентів/кібератак та етапи реагування на них», - зазначив очільник Держспецзв'язку.

Затвердження документа дає можливість формувати процеси реагування на кіберінциденти та кібератаки відповідно до завчасно спланованих заходів, а також розвиває підходи, які були закладені в організаційно-технічній моделі кіберзахисту, розробленій у 2021 році.

Потій додав, що Служба впродовж трьох місяців з дня набрання чинності постанови має затвердити методичні рекомендації щодо реагування суб'єктами кібербезпеки на події у кіберпросторі…» ***(Кабмін затвердив порядок реагування на кіберінциденти та кібератаки // Укрінформ (https://www.ukrinform.ua/rubric-technology/3691554-kabmin-zatverdiv-poradok-reaguvanna-na-kiberincidenti-ta-kiberataki.html). 04.04.2023).***

***

«Российские хакеры следят за камерами видеонаблюдения в украинских кафе для сбора информации, заявил во вторник представитель американской разведки.

По словам директора отдела кибербезопасности Агентства национальной безопасности (АНБ) Роба Джойса, при поддержке государства они пытаются выяснить информацию о проходящих колоннах с гуманитарной помощью.

Выступая в аналитическом центре Центра международных и стратегических исследований в Вашингтоне, он сказал, что российские хакеры атаковали украинские информационные системы с самого начала более широкого наступления их страны.

«Атаки на интересы Украины, будь то финансовые, государственные, частные [или] бизнес, происходят постоянно», — сказал Джойс, отметив, что часто они были направлены «просто на срыв» операций.

Чиновник АНБ назвал некоторых российских хакеров «креативными».

«Мы наблюдаем, как российские хакеры подключаются к веб-камерам, чтобы наблюдать за колоннами и поездами, доставляющими помощь», — сказал он.

«Вместо того, чтобы использовать [камеры] в общественном месте, которые доступны в Интернете, они смотрят в камеру наблюдения в кафе и видят дорогу, которую им нужно увидеть».

Российские хакеры также сосредотачивают свои операции на американских оборонных предприятиях и логистических компаниях, чтобы узнать больше о поставках оружия в Украину, продолжил Джойс.

«Они ежедневно подвергаются давлению со стороны россиян», — сказал он.

В марте американское новостное агентство CCN получило отчет, в котором утверждалось, что европейские военные, энергетические и транспортные организации стали мишенью российских хакеров в явной шпионской кампании.

Он оставался незамеченным в течение нескольких месяцев, пока бушевала война на Украине, несмотря на усиленную оборонительную позицию западных правительств». ***('Creative' Russian hackers tapping into CCTV in cafes in Ukraine, says US // euronews.com (https://www.euronews.com/next/2023/04/12/creative-russian-hackers-tapping-into-cctv-in-ukrainian-cafes-says-us?utm_source=flipboard.com&utm_campaign=feeds_next&utm_medium=referral). 12.04.2023).***

***

«По словам экспертов, Украина столкнулась с «беспрецедентным» объемом связанных с Россией кибератак более чем через год после вторжения в страну.

Но новый независимый отчет Европейской инициативы по исследованию киберконфликтов (ECCRI) также предупреждает, что, хотя Киев продемонстрировал замечательную устойчивость перед лицом российских киберугроз, ответ может создать некоторые «тревожные прецеденты».

Почти 40-страничное исследование, подготовленное по заказу Национального центра кибербезопасности (NCSC) и опубликованное одновременно с конференцией CyberUK в Белфасте, появилось на фоне опасений, что угроза, исходящая от связанных с Россией кибергрупп, выходит за пределы Украины, с Великобританией и ее союзниками. также цели.

В исследовании высоко оценивается «невероятная стойкость и решимость», продемонстрированные Украиной в ее защите киберпространства, и указывается, в частности, на успех так называемой ИТ-армии страны — добровольческой сети хакеров, которые с самого начала конфликта ведут кибервойну с Россией.

Но он вызывает обеспокоенность по поводу стирания границы между комбатантами и гражданскими лицами, задавая вопрос, что будет с военнослужащими ИТ-армии после окончания войны, и предупреждая, что она «вышла за рамки нескольких важных кибернорм».

«ИТ-армия добилась большого успеха во многом потому, что они нашли способ геймифицировать ответ на конфликт.

«В своих усилиях по набору IT-армия романтизировала роль добровольцев. Руководство ИТ-армии также предоставило четкие пошаговые инструкции о том, как нацеливаться и добиваться результатов», — говорится в отчете.

В нем отмечается, что «в прошлом странам приходилось иметь дело с гражданскими лицами, которые уезжали и присоединялись к террористическим организациям, радикализировались, а затем возвращались в свои родные страны».

Авторы говорят: «Многие правительства разработали системы для борьбы с этой потенциальной угрозой. Однако с помощью кибероперациий субъект может проводить атаки на расстоянии.

«Привлечь человека в ИТ-армию Украины гораздо проще, чем процессы радикализации, которые мы видели в прошлом, и нет хорошей существующей правовой базы для решения этого вопроса».

В другом месте отчета, основанном на результатах семинара, проведенного ранее в этом году, авторы обнаружили, что в контексте войны становится все труднее проводить различие между киберпреступными группами и политическими активистами.

«Некоторые группы утверждают, что занимаются «хактивизмом», но, похоже, больше заинтересованы в финансовой выгоде, чем в политических заявлениях. Другие преступные группировки даже раскололись из-за политических разногласий», — говорится в отчете.

«Участники также отметили, что цели нескольких преступных групп, похоже, сместились с отказа в доступе к информации для получения финансовой выгоды к краже этой информации для целей государственной разведки. Эти группы сосредоточились на проникновении и сборе информации в качестве своей основной цели».

Указывая на растущую опасность, которую представляют программы-вымогатели, авторы говорят, что правительства, подвергающиеся санкциям, такие как московский режим Владимира Путина, часто будут иметь стимул «дать преступникам расширенное пространство для маневра».

В четверг участники конференции в Белфасте обсудят вопросы кибербезопасности и украинский конфликт.

Пол Чичестер, директор по операциям Национального центра кибербезопасности, сказал: «Мы очень благодарны ECCRI за этот важный и ценный анализ кибераспектов российско-украинского конфликта на сегодняшний день.

«Отчет предлагает ряд полезных идей, не в последнюю очередь о том, чему Украина научила нас о силе устойчивых систем перед лицом устойчивых кибератак.

«Поскольку мы смотрим в будущее во время нашей конференции CyberUK, это своевременный вклад в дискуссию о том, что мы можем извлечь из конфликта, а также об ограничениях нашего нынешнего понимания».

Министр безопасности Том Тугендхат заявил, что правительство оценит выводы доклада и «извлечет уроки», которые он предлагает…» ***(Dominic McGrath. Ukraine's success in cyberwarfare could create 'concerning precedents' – study // INDEPENDENT (https://www.independent.co.uk/news/uk/ukraine-tom-tugendhat-volodymyr-zelensky-national-cyber-security-centre-kyiv-b2323103.html). 20.04.2023).***

***

«Україна стала першою у світі країною, яка протистоїть повноцінній кіберагресії як складовій повномасштабної гібридної війни. Та вже зараз зрозуміло, що навіть після закінчення конвенційної війни хакерські атаки не припиняться. Щоб їм протистояти, потрібно постійно підвищувати рівень кіберзахисту систем, відповідно – попит на фахівців у цій сфері лише зростатиме.

Передусім нові фахівці з кіберзахисту можуть посилити лави основних суб'єктів Національної системи кібербезпеки, серед яких – Держспецзв'язку, Служба безпеки України, Міністерство оборони України, Національний банк, розвідувальні органи.

Потребують кіберфахівців й інші державні органи та установи. Робота в державних органах – це робота на найвищому рівні, адже сьогодні роль України у світовій екосистемі кіберзахисту істотно зросла. Саме в державному секторі у кращих фахівців є можливість представляти країну на міжнародному рівні та відігравати важливу роль у міжнародних процесах.

Це і законодавча робота, і робота над стандартами захисту, перевірка захищеності програмного забезпечення, побудова систем кіберзахисту, а також безпосередньо кіберзахист і дослідження кіберінцидентів у складі команд реагування. Такі команди вже є у нас, в Держспецзв'язку (Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA), в НБУ.

Крім того, відповідно до національної стратегії з кібербезпеки, Україна розвиває мережу галузевих та регіональних центрів або команди реагування. Такі команди спеціалізуються на захисті у своїх галузях та регіонах і обмінюються даними про загрози із CERT-UA.

Наявність глибокої галузевої та регіональної експертизи дає можливість більш ефективно протистояти специфічним загрозам, а координація з головним кіберцентром країни – ефективно забезпечувати кіберзахист всієї країни.

Регіональні команди реагування – це можливість для талановитих людей, які мешкають у регіонах, будувати кар'єру, мати гідну заробітну плату та захищати країну.

Не менше фахівці з кібербезпеки потрібні бізнесу. Перша у світі кібервійна показала, що компаній, які можуть бути не цікавими для хакерів, майже не існує.

Тому кожен на своєму підприємстві повинен створювати відповідні підрозділи, наймати найкращих фахівців чи залучати аутсорсингові компанії. І що більший бізнес чи чутливіша інформація, яка зберігається в інформаційних системах підприємства, що більше людей залежать від роботи компанії, то надійнішим має бути кіберзахист.

Саме тому висококваліфіковані фахівці будуть об'єктом полювання як для хедхантерів зі спеціалізованих організацій, які надають послуги у сфері кібербезпеки та кіберзахисту, так і для HR-підрозділів компаній, які бажають мати потужну inhouse-команду». ***(Герман Богапов. В Україні зросла потреба у фахівцях із кіберзахисту // HiTech.Expert (https://expert.com.ua/159158-v-ukraini-zrosla-potreba-u-fahivcyah-iz-kiberzahystu.html). 21.04.2023).***

***

«Кібератаки Росії на Україну не припинялися. Нова хвиля — це чергове попередження, що кібервійна відбувається і атаки здійснюватимуться з боку росіян. Про це сьогодні, 17 квітня, в ефірі телеканалу FREEДОМ повідомив експерт з кібербезпеки Сергій Денисенко.

Так він прокоментував інформацію видання The Economist, що російські хакери готують нову кампанію проти України. Зокрема, за інформацією ЗМІ, росіяни намагатимуться використовувати шкідливе програмне забезпечення для знищення даних.

«Якщо вони заявляють, що це новий метод кібервійни, тобто знищення інформації, це можна порівняти з фізичним знищенням нашої критичної інфраструктури тими ж ракетами. Цей процес із кожним днем посилюється, але ми даємо відповідну відсіч. І таких небажаних, критичних інцидентів у нас поки що немає, сподіваюся, і не буде», — сказав Денисенко.

The Economist також уточнює, що торік Росія розширила свої кібероперації в Польщі та Східній Європі, і цьогоріч атаки тривають. Напередодні стало відомо, що компанія Rheinmetall (виробник танків Leopard) у Німеччині стала жертвою кібератаки. Прокуратура Кельна ініціювала відповідне провадження у цій справі.

«Наші зарубіжні партнери повинні були очікувати кібератак. Основне завдання цих кібератак — повне припинення роботи того чи іншого підприємства. Грубо кажучи, з темпами технологічного процесу більшість підприємств комп'ютеризувалася, все роблять машини, і, якщо впливати на комп'ютери, які керують процесом, можна зупинити саме виробництво, включно з вимкненням електрики, телекомунікаційних зв'язків. Тобто можна повністю загасити те чи інше підприємство», — прокоментував експерт із кібербезпеки». ***(Російські хакери готують нову кампанію проти України — коментар експерта з кібербезпеки // UATV (https://uatv.ua/uk/rosijski-hakery-gotuyut-novu-kampaniyu-proty-ukrayiny-komentar-eksperta-z-kiberbezpeky/). 17.04.2023).***

***

«США відправили до України спеціалістів, які допомагають боротися з російськими кібератаками. Про це заявив генерал-майора армії США Вільям Хартман - повідомляє Reuters.

Генерал-майор армії США Вільям Хартман проінформував, що впродовж останніх трьох років Національне управління кібербезпеки США (CNMF) провело 47 таких оборонних операцій у 20 країнах.

CNMF направило 43 фахівців в Україну, яка бореться з російськими кібернападами під час війни, яку Росія називає «спеціальною операцією».

«Це групи захисту, які ми надсилаємо, і вони полюють на спільних супротивників, знаходять інструменти та можливості», - додав американський генерал…» ***(В Україні американські хакери допомагають боротися з кібератаками // бізнес/медіа бюро ekonomika+ (https://delo.ua/politics/v-ukrayini-z-kiberatakami-dopomagayut-borotisya-amerikanski-xakeri-415885/). 25.04.2023).***

***

Світові тенденції в галузі кібербезпеки

«…В новом исследовании, опубликованном кибербезопасности поставщиком Bitdefender, сегодня было опрошено более 400 специалистов в области ИТ и 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.

Исследование проводится менее чем через год после того, как FTC осудила бывшего CSO Uber Джозефа Салливана за попытку скрыть взлом Uber в 2016 году. Дело показало, что ложь об утечке данных является серьезным уголовным преступлением во многих юрисдикциях.

Так почему же так много технологических лидеров оказывают давление на своих сотрудников, чтобы они скрывали утечку данных? Ответ заключается в том, что ландшафт киберугроз становится все более требовательным: 52% организаций столкнулись с утечкой данных за последние 12 месяцев.

Пять угроз, о которых респонденты сообщили, что их больше всего беспокоят, — это уязвимости программного обеспечения и нулевые дни (53,9%),

фишинг и социальная инженерия (52,2%), атаки на цепочку поставок (49%), программы-вымогатели (48,5%) и внутренние угрозы (36,5%). %).

«Во всем мире организации [испытывают] огромное давление, чтобы бороться с развивающимися угрозами, такими как программы-вымогатели, уязвимости нулевого дня и шпионаж, борясь со сложностями, связанными с расширением охвата безопасности в разных средах, и с постоянной нехваткой навыков», — сказал Андрей Флореску, заместитель генерального директора и старший вице-президент по продуктам группы бизнес-решений Bitdefender.

Хотя трудно гарантировать, что организация ответственно отнесется к киберинцидентам, проактивные руководители безопасности могут попытаться уменьшить вероятность обмана, снизив нагрузку на отделы безопасности людей.

Это включает в себя инвестиции в решения по предотвращению угроз, их обнаружению и реагированию, которые позволяют пользователям быстрее реагировать и разрешать инциденты безопасности, чтобы меньше влиять на организацию и меньше подвергаться юридическим и финансовым рискам.

«Результаты этого опроса более чем когда-либо демонстрируют важность многоуровневой безопасности, которая обеспечивает расширенное предотвращение угроз, обнаружение и реагирование на них в рамках всего бизнеса, одновременно повышая эффективность, что позволяет группам безопасности делать больше с меньшими затратами», — сказал Флореску». ***(Tim Keary. A third of organizations admit to covering up data breaches // VentureBeat (https://venturebeat.com/security/a-third-of-organizations-admit-to-covering-up-data-breaches/). 05.04.2023).***

***

«По данным DigitalOcean, для малых и средних предприятий (и стартапов в частности) взломы могут иметь разрушительные последствия...

Исследователи обнаружили:

Кибербезопасность вызывает все большую озабоченность у малого бизнеса. 54% респондентов говорят, что сейчас они больше обеспокоены кибербезопасностью, чем год назад.

В 80% стартапов и малых и средних предприятий один или несколько сотрудников занимаются вопросами безопасности. 38% опрошенных предприятий заявили, что в их обязанности не входит ни одного сотрудника, занимающегося безопасностью, а в 42% всего один сотрудник занимается безопасностью.

Конфиденциальность данных является главной проблемой для стартапов, но 57% респондентов не имеют сотрудников, занимающихся конфиденциальностью данных. Исследование показало, что 74% предприятий говорят, что конфиденциальность данных является главной заботой их бизнеса, но в большинстве из них нет сотрудников, занимающихся конфиденциальностью данных.

Нехватка времени, чтобы сосредоточиться на безопасности и идти в ногу с изменяющимися угрозами, является самой большой проблемой для бизнеса». ***(Lack of security employees makes SMBs sitting ducks for cyber attacks // Help Net Security (https://www.helpnetsecurity.com/2023/04/04/smbs-security-posture/). 04.04.2023).***

***

«…по мере развития бизнеса расширяются и потенциальные угрозы. Бизнес-лидеры должны ориентироваться во все более сложном и постоянно меняющемся мире императивов кибербезопасности, которые требуют инновационных подходов для снижения этих новых рисков.

Исследование будущего кибербезопасности, проведенное компанией Deloitte Global за 2023 год, показало, что 70 процентов респондентов высшего звена сообщили, что вопросы кибербезопасности фигурируют в повестке дня их совета директоров на регулярной основе, ежемесячно или ежеквартально. Учитывая, что искусственный интеллект (ИИ) и когнитивные вычисления входят в число пяти основных приоритетов цифровой трансформации лидеров, предприятия изучают новые варианты использования этих технологий в системах кибербезопасности, используя инструменты для сдерживания и реагирования по мере роста угроз.

Эти новые технологии стимулируют цифровую трансформацию и, в свою очередь, требуют новых навыков и новаторского мышления от современной рабочей силы.

Однако тот же опрос показывает, что эти организации с высоким уровнем зрелости значительно чаще называют нехватку квалифицированных специалистов по кибербезопасности главной проблемой. Эта нехватка кибер-талантов означает не просто отсутствие кандидатов. Скорее, отрасль испытывает дефицит в поиске нужных профессионалов — тех, кто может помочь организациям полностью раскрыть потенциал ИИ и других передовых методов кибербезопасности.

Применение этих новых технологий требует человеческого мышления с тонким пониманием процессов принятия решений. В результате для поиска нужных талантов потребуется рассмотреть более широкий круг кандидатов, в том числе с нетрадиционным технологическим опытом.

Помимо традиционного

Кандидаты с нетехническим образованием могут предоставить все необходимое для быстрой реализации творческих решений в условиях высокой нагрузки. Менеджеры по найму должны выходить за рамки технических знаний кандидата, оценивая реальный опыт и передаваемые навыки, чтобы определить, обладают ли они устойчивостью, чтобы добиться успеха в быстро меняющейся киберэкосистеме и оставаться адаптивными и гибкими в условиях кризиса.

Кроме того, компаниям необходимо подумать о том, как создать гибкие, хорошо оснащенные команды, обладающие обширным и глубоким опытом, необходимым для соответствия меняющимся потребностям сегодняшнего дня. Для некоторых это может означать выход за рамки традиционных границ, открытие ролей в новых регионах за пределами «традиционных» технологических центров, где это возможно.

Это также может означать создание и внедрение программ «обучения для найма», которые формируют сильный технический опыт кандидата. Новые инструменты, такие как дополненная реальность (AR) и виртуальная реальность (VR), могут обучать кандидатов с нетрадиционным опытом, обеспечивая соответствующий опыт в контролируемой среде, которая при этом позволяет полностью погрузиться в критические рабочие функции.

Сотрудничество с академическими кругами для включения программирования в учебные программы — еще один способ помочь следующему поколению сотрудников приобрести многогранные технические знания, дополняющие нематериальную ценность, которую различные кандидаты могут принести командам.

Разносторонне квалифицированная команда с глубоко укоренившимися, обширными знаниями и опытом будет лучше подготовлена для навигации, внедрения и эксплуатации решений в масштабе. Компании должны диверсифицировать кадровый резерв, поскольку они определяют приоритеты цифровой трансформации и используют искусственный интеллект и другие передовые киберстратегии для усиления операций и достижения долгосрочного успеха.

Этот момент времени предоставляет бизнес-лидерам уникальную точку перегиба, чтобы изменить устаревшие подходы к найму, а также приветствовать и взращивать таланты нового поколения с более широким набором навыков и более разнообразным мышлением — тех, кто может выдержать шторм, продолжая защищать предприятие». ***(Linda Walsh. Cybersecurity hiring: Drive transformation through new talent pipelines // Red Hat, Inc. (https://enterprisersproject.com/article/2023/4/cybersecurity-new-talent-pipelines). 06.04.2023).***

***

«На рынок кибербезопасности вливаются миллиарды долларов, а риски кибератак хорошо задокументированы. Но ИТ-руководителям по-прежнему необходимо привести веские аргументы, чтобы выделить необходимую часть бюджета своих организаций для инвестиций в кибербезопасность.

«Кибербезопасность рассматривается как вспомогательный компонент ИТ, — говорит InformationWeek Ларри Уайтсайд-младший, директор по информационным технологиям компании RegScale, занимающейся разработкой программного обеспечения GRC в режиме реального времени. «Однако средства контроля, связанные с кибербезопасностью, напрямую влияют не только на ИТ-состояние организации, но также на ее состояние риска, соответствие требованиям и, возможно, ее финансовое положение, поскольку сбой в любой из упомянутых областей может иметь разрушительные последствия для организации».

Демонстрация того, как кибербезопасность влияет на конечный результат, может помочь ИТ-руководителям привести убедительные аргументы высшему руководству, но нарисовать такую картину не всегда легко. «Расходы на кибербезопасность могут быть особенно сложными, потому что они — в общем и целом — скорее превентивные, чем противодействующие. Это другой разговор, чем, скажем, программное обеспечение для повышения производительности, где вы, возможно, сможете более быстро измерить ценность», — говорит Дэвид Вайсонг, ИТ-директор консалтинговой компании по энергетике Energy Solutions.

Уайтсайд, Вайсонг и трое других руководителей высшего звена делятся своим мнением о том, как кибербезопасность может оказать заметное влияние на доходы компании.

Поддержка соответствия

Компании, работающие во многих отраслях, должны инвестировать в кибербезопасность, чтобы соответствовать нормативным требованиям. Невыполнение этого требования может привести к большим штрафам и потере бизнеса. Energy Solutions работает в строго регулируемой отрасли со сложными требованиями соответствия; большинство его клиентов - коммунальные предприятия. «В ходе бесед с нынешними клиентами и обсуждений (и предложений) с потенциальными клиентами мы поняли, что укрепление нашей системы безопасности с помощью наглядных процессов безопасности будет не только благоразумным для постоянной защиты от угроз, но и разумным для нашего бизнеса», — делится Вайсонг.

По словам Вейсонга, компания Energy Solutions прошла сертификацию SOC 2 Type 2 в качестве основы для своей стратегии модернизации безопасности.

«Чтобы получить конкурентное преимущество, мы заняли позицию превышения минимальных требований безопасности, которые предъявляют многие коммунальные предприятия», — уточняет он. «Окупаемость инвестиций для преодоления этих минимальных порогов — минимальных порогов, которые продолжают расти — очевидна».

Повышение операционной эффективности

В качестве ИТ-директора страховой организации World Insurance Associates Майкл Корриган руководил компанией, инвестируя в антивирусы нового поколения, средства обнаружения и реагирования конечных точек, улучшенную ИТ-гигиену и управляемые решения для поиска угроз. «Улучшенные средства контроля кибербезопасности могут повысить эффективность работы, а также эффективность расследования и сдерживания, что увеличивает конечный доход», — говорит он.

Реагирование на инцидент

Чем быстрее компания сможет восстановиться после инцидента кибербезопасности, тем дешевле это будет. минуту. Согласно исследованию компании Pingdom, занимающейся мониторингом производительности и доступности веб-сайтов, средняя стоимость простоя составляет 9000 долларов. Более крупные компании могут потерять миллионы доходов всего за несколько часов простоя.

«Хотя никто не застрахован от взлома, инвестиции в программу кибербезопасности могут уменьшить воздействие события, и компании, у которых есть инструменты и программы для реагирования на инциденты, в конечном итоге работают хорошо», — говорит Дуг Барбин, директор по развитию и управляющий директор компании Schellman, занимающейся аттестацией соответствия ИТ.

Сохранение доверия

Брайан Уиллетт уже семь лет является директором по информационным технологиям компании Lexmark International, занимающейся решениями для обработки изображений. Он курирует глобальную кибербезопасность, конфиденциальность данных и управление более чем 140 сайтами по всему миру. «Я руководил крупнейшей инвестицией Lexmark в ИТ-безопасность более чем за десятилетие. Это включало: безопасность по дизайну, нулевое доверие и

безопасность цепочки поставок — охватывая 10 000 мировых поставщиков», — сказал он InformationWeek.

Эти инвестиции сыграли решающую роль в укреплении доверия клиентов компании. «Поскольку нормативные и договорные требования к защите данных продолжают расти, клиенты все чаще ищут партнеров, которые одинаково уважают защиту данных», — говорит Уиллетт. Ущерб репутации и вытекающее из этого недоверие могут привести к упущенной выгоде, когда клиенты решат искать конкурентов, которые демонстрируют способность защищать свои ценные данные.

Управление страховыми премиями

В связи с продолжающейся эскалацией кибератак становится все труднее получить страховое покрытие, а страховые взносы становятся все дороже. с 2020 по 2021 год прямые письменные премии за киберпокрытие увеличились. Согласно отчету Национальной ассоциации уполномоченных по страхованию, на 75,3%. Тенденция роста премиальных цен, вероятно, продолжится.

По словам Корригана, хотя кибератаки — это вопрос «когда, а не если», упреждающий подход к кибербезопасности может сделать взносы по страхованию кибербезопасности более управляемыми.

Новое дело

Кибербезопасность может сохранить доход за счет сокращения затрат, связанных с предотвратимыми атаками, нормативными штрафами и ростом страховых взносов. Он также может активно увеличивать доход за счет удержания и привлечения новых клиентов. «Наш новый стек кибербезопасности и инициативы по соблюдению требований привели не только к продлению существующих контрактов с клиентами, но и позволили нам надежно заключить новые клиентские контракты», — сказал Вейсонг.

Привлечение топ-менеджеров на борт

Установление адекватного бюджета на кибербезопасность и осуществление правильных инвестиций — это усилия, в которых участвует весь высший менеджмент предприятия. Первый шаг — убедиться, что все заинтересованные стороны понимают риски. «Инвестиции в кибербезопасность не должны осуществляться бессистемно. Стратегические инвестиции, соответствующие риску, окажут большее влияние», — говорит Уайтсайд. «Это означает, что организация должна понимать свой риск. Это включает сотрудников, технологии, операционные и финансовые риски, а также влияние кибербезопасности на каждый из них».

Корриган работает с командой топ-менеджеров World Insurance Associates, информируя их о ландшафте угроз и о том, как они могут повлиять на компанию. Он также прислушивается к их отзывам, чтобы понять, «... какие бизнес-процессы следует поддерживать и где следует настроить средства киберконтроля, чтобы защитить организацию, не влияя на ее способность эффективно функционировать». ***(Carrie Pallardy. 6 Ways Cybersecurity Can Boost Revenue // Informa PLC (https://www.informationweek.com/security-and-risk-strategy/6-ways-cybersecurity-can-boost-revenue). 05.04.2023).***

***

«Любая компания может извлечь выгоду из оценки рисков кибербезопасности. Изучение того, где находятся наиболее значительные уязвимости организации, — это первый шаг к устранению этих рисков, чтобы оставаться в безопасности. Однако предприятия сталкиваются с двумя основными вариантами этих оценок — количественным и качественным анализом данных.

Качественный и количественный анализ данных может выявить ваши риски кибербезопасности, но они подходят к этому вопросу по-разному. Поскольку ландшафт рисков каждой организации уникален, оба подхода могут быть более или менее полезными в различных сценариях. Лучший выбор между ними начинается с понимания того, что каждый из них предлагает.

Что такое качественный анализ?

Качественный анализ данных направлен на то, чтобы ответить на вопросы «что, если» о различных сценариях риска. В контексте кибербезопасности это может выглядеть как вопрос: «Какова вероятность того, что мы столкнемся с утечкой данных с наших конечных точек IoT? Что произойдет, если посторонний проникнет через эти устройства?»

Такая оценка риска кибербезопасности является весьма субъективной и основывается на опыте и знаниях людей в этих вопросах. Учитывая, что в мире существует нехватка кадров для кибербезопасности в 3,4 миллиона человек, это может исказить результаты в некоторых компаниях. Без большого или достаточно опытного персонала службы безопасности вы не сможете точно оценить риски, основываясь только на мнении.

Хотя качественный анализ подвержен систематической ошибке, он также имеет ряд преимуществ. Одним из самых больших является его быстрое и относительно простое исполнение. Некоторые инсайдеры также могут иметь ценную информацию о рисках, которые трудно поддаются количественной оценке, и этот подход может быть ценным способом определения того, как и почему что-то происходит.

Что такое количественный анализ?

Другая сторона динамики качественных и количественных данных использует подход, основанный на числах. Вместо того, чтобы просить людей оценивать риски на основе их знаний и опыта, он использует достоверные данные для присвоения конкретных цифр этим проблемам.

Количественная оценка риска кибербезопасности анализирует историю инцидентов и общие тенденции, чтобы определить вероятность риска, а затем присваивает ему долларовую стоимость на основе информации о конкретной компании. Поскольку он фокусируется на реальных цифрах, а не на интуиции, риск предвзятости меньше. Количественный анализ данных также может дать более практическую информацию, предоставляя конкретные цифры о стоимости различных рисков.

Опасность количественного анализа заключается в том, что у предприятий не всегда есть данные, которые им нужны, чтобы быть надежными. Решения, основанные на неточных или неполных данных, обходятся организациям в 12,9

млн долларов в год, поэтому отсутствие доступной информации или ошибки при вводе данных могут серьезно помешать эффективному принятию решений.

Качественный и количественный анализ данных: что лучше?

Учитывая эти преимущества и недостатки, какой вариант лучше при выборе между качественным и количественным анализом данных? Чаще всего лучше использовать немного того и другого.

Качественный анализ данных лучше всего подходит для формирования гипотезы, тогда как количественный анализ лучше подходит для проверки. Предприятия могут применить это в контексте кибербезопасности, используя качественный анализ, чтобы выделить свои наиболее значительные риски, а затем использовать количественные исследования, чтобы присвоить конкретные числовые значения этим уязвимостям, чтобы получить более практическую информацию.

Мнения инсайдеров могут быть ценными источниками информации о вещах, которые может быть трудно количественно оценить с помощью достоверных данных, и могут объяснить, почему что-то представляет собой риск. Затем количественный анализ данных может дать более полное представление об этих проблемах, показывая, куда вкладывать больше всего, чтобы оставаться в максимальной безопасности. Обе стороны имеют решающее значение в быстро меняющемся, часто непредсказуемом мире кибербезопасности.

Сегодня предприятия тратят на 47% больше расходов, связанных с данными, чем до пандемии COVID-19. В свете этих высоких расходов защита этих данных важна как никогда, поэтому лучше всего использовать наиболее целостный подход к оценке рисков. Использование обеих сторон также может помочь управлять затратами на анализ для повышения рентабельности инвестиций.

Найдите правильный путь для оценки рисков кибербезопасности

Оценка рисков кибербезопасности имеет решающее значение, поэтому очень важно подходить к ним правильно. Наилучший путь вперед — отойти от идеи качественного и количественного анализа и рассматривать их как дополняющие друг друга. Комбинируя эти подходы, вы учтете недостатки каждого из них и получите наиболее надежные и содержательные результаты». ***(Shannon Flynn. Qualitative vs. Quantitative Analysis for Cybersecurity // Hackernoon hq (https://hackernoon.com/qualitative-vs-quantitative-analysis-for-cybersecurity). 06.04.2023).***

***

«Национальная федерация розничной торговли (NRF) и Центр обмена и анализа информации о розничной торговле и гостиничном бизнесе (RH-ISAC) объединяют усилия для повышения кибербезопасности розничной торговли. Две ведущие в отрасли организации будут объединять свои усилия в области разведки и мониторинга угроз. Цели этого партнерства, объявленного в январе 2023 года, включают расширение доступа к новостям в области кибербезопасности, руководствам, образованию и ресурсам для предприятий розничной торговли.

Исследования показывают, что 24% кибератак нацелены на розничные организации, и практически все эти атаки имеют финансовую мотивацию. Хакеры

активно атакуют финансовые и платежные данные. Все больше торговли происходит в Интернете, и розничные продавцы становятся более уязвимыми для атак. Это вызывает трения в бизнес-решениях, поскольку потребители предпочитают многоканальные варианты покупок, но электронная торговля увеличивает риски кибербезопасности.

Партнерство NRF и RH-ISAC улучшит доступность точных новостей и информации о розничной кибербезопасности. Обе организации являются отраслевыми лидерами в области данных и рекомендаций в целом. Сотрудничество в области безопасности позволит им удвоить охват и влияние, чтобы помочь как можно большему количеству предприятий и специалистов.

В пресс-релизе NRF за 2023 год образование и поддержка были отмечены как ключевые цели партнерства с RH-ISAC. Обмен и разработка более подробных и актуальных руководств по передовым методам кибербезопасности помогут повысить готовность предприятий розничной торговли и гостиничного бизнеса. Надеемся, что это уменьшит количество успешных кибератак в отрасли.

Помимо сотрудничества в области образования, NRF и RH-ISAC объединят свои платформы для обмена киберугрозами. Портал обмена киберрисками NRF скоро закроется. Все участники будут переведены на систему обмена угрозами RH-ISAC, которая станет новым информационным центром для обеих организаций. Это позволит хранить все в одном месте.

Новости кибербезопасности Партнерство с CyberWire

RH-ISAC также будет сотрудничать с лидером новостей кибербезопасности CyberWire для выпуска розничного подкаста новостей кибербезопасности. Подкасты CyberWire являются одними из самых популярных в отрасли и охватывают широкий круг тем, связанных с безопасностью. Добавление подкаста RH-ISAC в библиотеку CyberWire повысит репутацию CyberWire как поставщика надежных новостей, включая розничную торговлю.

Своевременное обновление сведений о кибербезопасности может сыграть важную роль в обеспечении защиты предприятий розничной торговли. Например, для владельцев бизнеса естественно беспокоиться о расширении своих онлайн-каналов, когда они сталкиваются с высокой стоимостью кибератаки. Исследования показывают, что утечка данных стоит в среднем 4,35 миллиона долларов по состоянию на 2022 год. Этого достаточно, чтобы заставить любого дважды подумать о расширении возможностей электронной коммерции.

Однако эти владельцы бизнеса могут не знать, что они могут использовать инструменты для защиты от успешных кибератак. Например, страхование ответственности за кибербезопасность может покрыть стоимость простоя бизнеса в результате взлома и даже обеспечить судебную поддержку. Это означает, что стоимость найма экспертов будет покрыта, чтобы компании могли расследовать причину и виновных в атаке.

Рост киберпреступности увеличивает рынок инструментов и решений для защиты от хакеров. Это включает в себя новые типы планов страхования и превентивные инструменты, такие как ИИ и мониторинг угроз. Розничные предприятия также могут принять меры для защиты данных своих клиентов.

Например, внедрение методов входа в систему с двухфакторной аутентификацией может повысить безопасность учетной записи клиентов.

Компании должны знать об этих инструментах и ресурсах для их внедрения. Вот почему надежные и своевременные новости кибербезопасности в розничной торговле так важны для отрасли сегодня. Партнерство RH-ISAC и NRF будет поддерживать текущие исследования киберугроз и предоставлять образовательные ресурсы. Между тем, сотрудничество RH-ISAC с CyberWire может выступать в качестве центра для обмена этими регулярными новостями безопасности розничной торговли.

Розничные риски кибербезопасности

От каких угроз безопасности работают такие организации, как NRF и RH-ISAC, чтобы защитить розничный бизнес? Сегодня перед отраслью стоит несколько крупных киберугроз.

Само присутствие и стоимость кибератак неуклонно растут. Годовой глобальный ущерб от киберпреступлений вырос более чем на 900% в период с 2018 по 2022 год, и ожидается, что он продолжит расти в течение следующих нескольких лет. Розничные предприятия сталкиваются с растущими финансовыми рисками от атак, при этом одно нарушение может стоить миллионы долларов.

Потребители также сталкиваются с растущим числом киберугроз. Опросы показывают, что 65% американцев получили хотя бы одно предложение онлайн-мошенничества, и атаки с использованием социальной инженерии являются одними из самых распространенных. Такие тактики, как фишинг и кража учетных данных, могут быть широко распространены в розничной торговле, когда хакеры знают, что они могут получить доступ к финансовым данным.

Кроме того, хакеры с большей вероятностью предполагают, что у розничных предприятий есть лишние деньги. Это означает, что компания может с большей вероятностью заплатить киберпреступникам за атаку программ-вымогателей. Если жертва отказывается платить, преступник, скорее всего, по-прежнему будет иметь доступ к конфиденциальной информации о платежах или счетах клиентов, что само по себе является ценным.

Такие тенденции, как программа-вымогатель как услуга, также расширяют доступность инструментов киберпреступности, позволяя большему количеству людей заниматься взломом. Начинающий хакер теперь может заплатить более опытному преступнику за использование его программы-вымогателя и кражу денег из любой организации, которую он захочет. Это требует минимальных усилий с высокой вероятностью выигрыша в случае успеха атаки.

Все эти факторы делают обязательным для предприятий доступ к розничным новостям, обучению и ресурсам в области кибербезопасности. Знания — это ключ к подготовке и защите от киберугроз». ***(Shannon Flynn. NRF Plans for Cybersecurity in 2023 // Emerald X, LLC (https://www.retailtouchpoints.com/topics/digital-commerce/e-commerce-security/nrf-plans-for-cybersecurity-in-2023). 07.04.2023).***

***

«…Согласно Индексу кибербезопасности 2023 года, подготовленному Cisco, 82% компаний, принявших участие в опросе, заявили, что ожидают нарушения их бизнеса в ближайшие 12–24 месяца из-за инцидента, связанного с кибербезопасностью. И всего 15% организаций по всему миру адекватно подготовлены к потенциальным рискам.

Цена неподготовленности может быть значительной: 60 % респондентов заявили, что за последние 12 месяцев сталкивались с инцидентом кибербезопасности, а 41 % пострадавших заявили, что это стоило им не менее 500 000 долларов.

Эволюция угроз подчеркивает необходимость того, чтобы организации сохраняли бдительность и принимали упреждающие меры для защиты своих систем и сетей от кибератак.

Возрастающая частота и серьезность кибератак подчеркнули важность кибербезопасности для организаций любого размера, и это вызвало растущий спрос на стартапы с соответствующими решениями и услугами, создающими привлекательный рынок для инвесторов.

Растущие проблемы

В связи с пандемией коронавируса компании перешли от в основном статической операционной модели, в которой люди работали с отдельных устройств из одного места, подключаясь к статической сети, к гибридному миру.

Здесь сотрудники все чаще подключаются к нескольким сетям с нескольких устройств в разных местах, получают доступ к приложениям в облаке и в пути и генерируют огромные объемы данных. Это создает новые и уникальные проблемы кибербезопасности для компаний.

В Турции инвестиции правительства и государственных учреждений в продукты и услуги кибербезопасности остаются недостаточными. Поэтому крайне важно увеличить соответствующие инвестиции, учитывая растущую важность кибербезопасности в современном цифровом ландшафте.

Готовность ниже среднего

Между тем, исследование Cisco показало убедительный вывод, что только 15% компаний находятся на стадии «зрелости», в то время как более половины (55%) глобальных компаний попадают на стадии «начинающий» или «формирующийся», то есть они работают. ниже среднего по готовности к кибербезопасности.

Дидем Дуру, генеральный менеджер Cisco Türkiye, сказала, что, как и в остальном мире, гибридная модель получила значительный импульс в Турции после пандемии.

«С появлением мультиоблачных архитектур и гибридной работы компании стали намного более уязвимыми к киберрискам. Для компаний важно быть более гибкими и инвестировать в эту область, чтобы устранить эти риски и закрыть пробел в безопасности. В Cisco мы оказываем им всю необходимую поддержку в этом процессе», — сказал Дуру.

Обучение кибербезопасности

Из компаний, которые были оценены как «зрелые», 53% заявили, что они «очень уверены» в способности оставаться устойчивыми к потенциальным кибератакам в течение следующих 12–24 месяцев.

С другой стороны, только 30% компаний на стадии «Начинающий» и 34% на стадии «Формирование» сказали то же самое.

Кроме того, 86% респондентов заявили, что планируют увеличить свои бюджеты на безопасность как минимум на 10% в течение следующих 12 месяцев.

Türk Telekom, одна из ведущих технологических и коммуникационных компаний Турции, владеет крупнейшим центром кибербезопасности в стране и продолжает делиться своим опытом в этой области с молодежью.

Молодые люди, участвующие в тренинге по защите «киберродины», имеют возможность сформировать свое будущее, став частью будущих «кибергероев». Ожидается, что работы будут продолжены в 2023 году.

Инвестиции в DefensX

Угрозы кибербезопасности являются одними из самых серьезных проблем в мире Интернета и технологий. Многие предприятия предлагают своим клиентам более безопасный доступ в Интернет с помощью инновационных решений.

DefensX, опытный стартап с новой технологией защиты браузера от взломов с использованием браузера, заявил, что на этой неделе получил новые инвестиции. а DefensX объявила о заключении соглашения с Revo Capital, одним из самых важных инвесторов в стартап-экосистему в Турции.

DefensX, основанная Халисом Османом Эрканом и Муратом Демиртеном в США, ориентирована на обеспечение безопасной работы пользователей в любой сети или на любом устройстве.

Он предлагает решение, особенно против угроз кибербезопасности, которые могут исходить через интернет-браузеры. В нем говорится, что он может изолировать угрозы до того, как они достигнут конечных устройств, таких как настольные компьютеры, ноутбуки, смартфоны и планшеты». ***(Timur Sırt. Investors look for startups amid subpar cybersecurity measures // daily sabah (https://www.dailysabah.com/business/tech/investors-look-for-startups-amid-subpar-cybersecurity-measures). 07.04.2023).***

***

«Компания Cobalt Labs Inc., занимающаяся тестированием на проникновение как услугой, сегодня подробно рассказала в новом отчете о влиянии сокращения бюджета и нехватки кадров в индустрии кибербезопасности, и это нехорошие новости: киберкоманды изо всех сил пытаются управлять процессом исправления и отслеживать уязвимости.

Пятый ежегодный отчет Cobalt о состоянии пентестинга показал, что сокращение бюджета и нехватка специалистов подвергают организации более высокому риску нарушений безопасности. Было обнаружено, что макроэкономические сдвиги влияют на стандарты безопасности организаций в США, Европе, на Ближнем Востоке и в Африке.

Было обнаружено, что сокращение рабочих мест в сфере кибербезопасности распределяется неравномерно: более половины (63%) специалистов по кибербезопасности в США сообщили, что бюджет их отдела был сокращен в 2023 году, по сравнению с 28% их коллег из региона EMEA. Также было обнаружено, что две трети американских компаний и 61% компаний в регионе EMEA замедлили набор сотрудников в области кибербезопасности.

Было также установлено, что сокращение численности и замены персонала вызывает «выгорание в кибербезопасности», которое может подтолкнуть работников к увольнению. Из тех, кто столкнулся с увольнениями или сокращениями бюджета, почти все — 95 % в США и 84 % в регионе EMEA — заявили, что за последний год их роли изменились. Более 60 % специалистов по кибербезопасности в США и 29 % в регионе EMEA заявили, что вследствие этого они чувствуют себя выгоревшими.

Половина респондентов в США и 20% в регионе EMEA заявили, что рассмотрят возможность увольнения с работы, если их организации не решат проблему выгорания.

Нехватка персонала означает недостаток внимания: 79 % специалистов по кибербезопасности в США и 66 % в регионе EMEA признают, что они снижают приоритеты своих обязанностей, что приводит к накоплению неустраненных уязвимостей. Почти три четверти в США и 58% в регионе EMEA заявили, что теперь им сложно отслеживать уязвимости и реагировать на них.

Другие выводы в отчете включают неправильные настройки безопасности сервера, указанные как наиболее часто обнаруживаемая уязвимость безопасности (40 %), за которыми следуют межсайтовые сценарии (12 %), раскрытие конфиденциальных данных (10 %), нарушенный контроль доступа (также 10 %), а также аутентификация и сеансы. в 9%.

Наряду с отчетом Cobalt выпустила новую платформу управления пентестами для повышения эффективности и качества программ пентестинга. Платформа позволяет внутренним группам безопасности, управляемым поставщикам услуг и внешним группам безопасности охватывать весь жизненный цикл пентеста, от планирования, запуска и совместной работы над тестами до написания отчетов, отслеживания уязвимостей и принятия мер по исправлению». ***(Duncan Riley. Cybersecurity teams struggle to monitor vulnerabilities amid budget cuts and layoffs // SiliconANGLE Media Inc. (https://siliconangle.com/2023/04/12/cybersecurity-teams-struggle-monitor-vulnerabilities-amid-budget-cuts-layoffs/). 12.04.2023).***

***

«Угрозы кибербезопасности увеличились и диверсифицировались в последние годы, призывая к непрерывному и систематическому развитию кибербезопасности. Недавно опубликованный отчет определяет несколько развития меры, которые могут улучшить способность властей защищать национальные безопасности, бороться с серьезными киберпреступлениями и развивать киберзащиту.

«Наше киберпространство изменилось постоянно. В центральной части Финляндии правительства, информационная безопасность находится на хорошем

уровне и готовность к кибер угроз является частью повседневной деятельности властей. Тем не менее, способность властей подготовиться к серьезным киберугрозам и реагировать на них должны быть доработаны, чтобы обеспечить их эффективное реагирование в случае угрозы материализуются», — говорит Петри Кнапе, директор отдела национальной безопасности министерства интерьера.

15 февраля 2022 года Министерство внутренних дел и Министерство обороны инициировало проект по оценке потенциала власти и разработать предложения по развитию для обеспечения национальной кибербезопасности, борьба с киберпреступностью и внедрение киберзащиты. Этот первый предварительный отчет послужит основой для предложений по мерам.

Финляндия ежедневно подвергается кибервлиянию усилия и кибершпионаж, а также утечки киберданных и программы-вымогатели атаки. Цифровизация и технологическое развитие позволяют правительства и неправительственные операторы для использования киберпространства в качестве все более эффективный канал враждебного воздействия.

Реагирование на киберугрозы требует тесного сотрудничества между административными ветвями

Согласно отчету, властям в настоящее время не хватает возможностей для эффективной подготовки и предотвратить самые серьезные киберугрозы, особенно те, которые представляют риск для национальной безопасности и обороны. Рабочая группа предлагает меры по развитию, касающиеся стратегическая цель кибербезопасности, сотрудничество органов власти и процессы, картина ситуации, обмен информацией, воздействие и контрмеры, сбор разведывательных данных и улучшение защиты власти сети. Некоторые меры развития могут быть инициированы быстро, в то время как другие требуют новых законодательных проектов.

«Поскольку киберпространство продолжает развиваться, нам нужны более тесные и более скоординированные сотрудничество между властями. Более тесное сотрудничество между правительством агентств, с представителями всех соответствующих органов власти, необходимо между группами сотрудничества, работающими на технологическом уровне, и стратегическими сотрудничество на государственном уровне. Цель состоит в том, чтобы сделать возможным властям предоставлять свои наблюдения и информацию, которую они получают в качестве часть их обязанностей по анализу совместных органов. Это улучшит наше общее понимание и ситуационная координация», — говорит Микко Сойккели, Директор отдела управления информационными технологиями Министерства обороны.

Защитой киберпространства занимается несколько административные отделения; он не был и не может быть назначен ни одному одиночная ветвь. Для реагирования на угрозы различные административные ветви должны тесно сотрудничать как на стратегическом, так и на оперативном уровне. уровни. Инцидент, ставящий под угрозу безопасность киберпространства, может одновременно быть угрозой информационной безопасности, преступлением и угрозой национальной безопасности и национальная оборона, влияющая на внешнюю политику и политику безопасности.

Дальнейшее развитие сотрудничества и обеспечение надлежащего обмена информацией между органами власти может помочь гарантировать, что соответствующий орган принимает на себя правильные действия в нужное время, не ставя под угрозу обязанности другого органа и что лучшая компетенция всегда доступна.

Члены рабочей группы представляли Министерство Министерства внутренних дел, Министерства обороны, Министерства транспорта и Связь, Министерство юстиции, Канцелярия Президента Республики Финляндии, Министерство иностранных дел, Министерство финансов и Канцелярия премьер-министра. Специалисты службы безопасности и разведки Финляндии служба, Национальное бюро расследований, Силы обороны Финляндии, Государственный центр ИКТ, Финское агентство транспорта и связи Traficom и Совет национальной полиции, а также директор национальной кибербезопасности также участвовал в работе». ***(Report: Finland's cyber security must be developed systematically – cooperation of the authorities and processes require further improvement // Ministry of Defence (https://www.defmin.fi/en/topical/press_releases_and_news/report_finland_s_cyber_security_must_be_developed_systematically_-_cooperation_of_the_authorities_and_processes_require_further_improvement.13512.news#21cf009d). 11.04.2023).***

***

«Киберпреступность растет, и злоумышленники всегда ищут новые цели. Вашей организации необходимо руководство, которое осознает этот новый бизнес-риск и понимает, что вы несете полную ответственность за свою кибербезопасность.

Поскольку высшее руководство — например, совет директоров — несет фидуциарную ответственность и надзор за управлением рисками, установление приверженности организации кибербезопасности для устранения этого нового вида рисков начинается сверху. Руководителям высшего звена не обязательно становиться экспертами в области кибербезопасности, но они должны активно участвовать в расстановке приоритетов в области безопасности и иметь представление о состоянии безопасности в организации.

Независимо от того, кто отвечает за выполнение фактических задач кибербезопасности — будь то штатный персонал, сторонние поставщики или их сочетание, — конечная ответственность за риски кибербезопасности не подлежит делегированию и возлагается на высшее руководство вашей организации.

Сегодня у всех нас есть тесные цифровые связи с нашими партнерами, клиентами и поставщиками. Эти связи, «цепочка поставок бизнеса», укрепляют отношения в реальном мире, которые делают нас всех сильнее, но они также предоставляют злоумышленникам возможность переходить от одной цели к другой. Это означает, что если один из нас испытывает сбой в системе безопасности, то все мы в цепочке подвергаемся риску.

Чтобы устранить этот риск цепочки поставок, частные компании, правительства и отраслевые группы требуют от своих партнеров более

эффективных методов кибербезопасности. Ваше руководство должно иметь точное представление о вашей кибергигиене и угрозах, с которыми вы сталкиваетесь, а также о ваших обязательствах по соблюдению требований перед вашими партнерами и любых соответствующих нормативных режимах.

Один из способов, с помощью которого ваше руководство может начать понимать основные аспекты кибербезопасности и способы достижения ваших целей в области кибербезопасности и устойчивости, — это оценить свои методы кибербезопасности в сравнении с общепринятой структурой, такой как NIST Cybersecurity Framework. Структура NIST публикуется Национальным институтом стандартов и технологий США (NIST) и состоит из 5 областей: идентификация, защита, обнаружение, реагирование и восстановление.

Организация, приверженная кибербезопасности, должна рассмотреть возможность принятия рекомендаций в каждой из этих областей.

Подводя итог, конечная ответственность за кибербезопасность вашей организации лежит на вашем высшем руководстве. В то время как функции безопасности могут быть делегированы, управление рисками невозможно. Ваше руководство должно понять ваши потребности в кибербезопасности и осознать свою роль в обеспечении безопасности в вашей бизнес-экосистеме. Лидеры должны предпринять необходимые шаги для принятия политик, процедур и методов, отвечающих вашим потребностям и обязательствам; а также сообщить об этих ожиданиях и требованиях к безопасности своим сотрудникам, партнерам, клиентам и поставщикам». ***(John Burgess. Cybersecurity leadership can't be delegated // Talk Business & Politics (https://talkbusiness.net/2023/04/cybersecurity-leadership-cant-be-delegated/). 22.04.2023).***

***

«Рынок кибербезопасности взорвался за последние пару лет, в основном из-за опасений по поводу увеличения частоты разрушительных кибератак. Прогнозируется, что рынок вырастет со 182,3 млрд долларов в 2022 году до 571,1 млрд долларов в 2030 году, при этом совокупный годовой темп роста (CAGR) составит 13,4% в течение прогнозируемого периода.

По мере того, как все больше ценных данных перемещается в сеть, возрастает потребность в защите от цифровых взломов. Технологии движутся к большей интеграции с Интернетом вещей (IoT), искусственным интеллектом (ИИ) и облаком, все зависит от безопасности и защиты пользовательских данных. Попытки злоумышленников завладеть постоянно растущим объемом информации в Интернете также участились: в 2022 году произошло более 4000 утечек данных из-за взлома, что привело к утечке более 22 миллиардов записей. Ожидается, что к 2025 году затраты, связанные с ущербом от кибератак, достигнут 10,5 трлн долларов, что на 300% больше, чем в 2015 году.

Sekur Private Data позиционирует себя как лидер на рынке кибербезопасности и конфиденциальности данных, и его миссия состоит в том, чтобы обеспечить безопасность и конфиденциальность данных следующего поколения для защиты пользователей от кибер-хакеров. Sekur — зарегистрированная в США компания, занимающаяся кибербезопасностью и конфиденциальностью в Интернете, с

набором решений для защиты данных, предназначенных для обеспечения первоклассной конфиденциальности и безопасности в Интернете.

Готовые решения для обеспечения конфиденциальности данных

Его комплексный набор решений для обеспечения конфиденциальности включает в себя зашифрованные электронные письма и сообщения, безопасные системы связи, возможности облачного хранения, а также восстановление и управление документами. Sekur Private Data предлагает эти решения безопасности для всех, от частных лиц до корпораций и государственных учреждений по всему миру. Теперь компания расширила свои предложения, включив собственную систему виртуальной частной сети (VPN).

SekurVPN — это первая в своем классе коммерчески доступная VPN, которая не поддерживается Big Tech. Это захватывающий шаг вперед для защиты личных данных, поскольку это означает, что с VPN не связаны сторонние пакеты. Это устраняет риск утечки или продажи данных пользователя третьей стороне.

VPN — это часто выбираемый вариант, когда речь идет о защите онлайн-активности, такой как отправка электронной почты, выполнение задач электронного банкинга или электронных покупок, поскольку они шифруют данные и скрывают IP-адрес пользователя. 33% всех интернет-пользователей в настоящее время имеют VPN, и две трети пользователей говорят, что используют VPN для защиты своей онлайн-активности.

Компания также недавно добавила двухфакторную аутентификацию в свои системы для дополнительного уровня безопасности. Теперь это представление SekurVPN указывает на то, что компания продолжает предлагать передовые онлайн-безопасность и конфиденциальность для тех, кто ищет абсолютное спокойствие в отношении своих данных…» ***(Cyberattacks Set To Cost $10 Trillion In Damages Annually By 2025 – As The World Rapidly Steps Up Cybersecurity, Sekur Private Data Could Provide What It Needs // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/pr/news/accesswire/cyberattacks-set-to-cost-10-trillion-in-damages-annually-by-2025-as-the-world-rapidly-steps-up-cybersecurity-sekur-private-data-could-provide-what-it-needs). 26.04.2023).***

***

«Мир становится все более цифровым, и лидеры в сфере безопасности в коммунальном секторе сталкиваются с динамичной и сложной ситуацией. Коммунальные предприятия владеют и управляют набором систем, активов, объектов, оборудования и устройств, которые взаимодействуют с физическим миром и связаны между собой через различные сети связи. Помимо традиционной области информационной безопасности, программа кибербезопасности коммунального предприятия должна иметь более широкий охват для защиты от широкого круга целей. Новые технологии, такие как промышленный Интернет вещей (IIoT) и устаревшая среда промышленных систем управления (ICS), создают динамичный ландшафт. Различные уровни риска кибербезопасности и последствия кибератак усложняют защиту среды такого типа. Чтобы помочь лидерам в области безопасности обеспечить цифровую трансформацию в отрасли коммунальных услуг, глобальная исследовательская и

консалтинговая компания в области ИТ Info-Tech Research Group опубликовала свой новый ресурс — отчет Utilities Cybersecurity Report...

Согласно недавно опубликованному отчету компании, на фоне растущего внедрения технологий IIoT коммунальные предприятия борются с огромным количеством устройств, которые им теперь необходимы для защиты от изощренных кибератак или взломов. Многие существующие эксперты по кибербезопасности ИТ не полностью понимают, как работает ОТ или как соблюдать отраслевые правила и стандарты. Кроме того, лидеры могут реагировать на постоянно меняющуюся политику и правила правительства.

Кибербезопасность стала важной темой в повестке дня заседаний исполнительного руководства и совета директоров, но большинство исполнительных руководителей и членов совета директоров не обладают глубокими знаниями в области кибербезопасности. Ожидается, что для защиты организации от кибератак руководители службы безопасности должны преодолеть разрыв между разработкой стратегии и тактической реализацией. В отчете представлен следующий обзор текущей ситуации в области кибербезопасности в коммунальном секторе:

Нехватка талантов создает риск.

Нехватка персонала влияет на повседневную работу и подвергает коммунальное предприятие риску с тремя основными последствиями: неправильной конфигурацией систем, нехваткой времени для оценки рисков и управления ими, а также задержками с исправлением критически важных систем.

Фирма предлагает организациям сосредоточиться на развитии и удержании персонала, чтобы устранить этот пробел. Привлечение талантов с помощью консультационных услуг по мере необходимости может быть рентабельным для небольших коммунальных предприятий.

Повысить надзор и прозрачность.

В отчете также поясняется, что за большинство неправильных конфигураций, таких как неправильные разрешения, отсутствие аутентификации и слабые пароли, ответственны процессы, управляемые человеком. Программа управления кибербезопасностью в масштабах всей компании может обеспечить соблюдение политик и внедрить образ мышления в отношении кибербезопасности в культуру организации. Каждый коммунальный сектор сталкивается с уникальными проблемами и правилами, включая электричество, природный газ, воду и сточные воды.

Помимо всеобъемлющего анализа в масштабах предприятия, фирма рекомендует коммунальным предприятиям использовать отраслевые рамки для оценки зрелости и выявления пробелов.

Экономически эффективное внедрение технологий.

В исследовании фирмы говорится, что, хотя существуют общие методы управления и контроля, применимые к цифровым областям, таким как ИТ, ОТ и IoT, реальность такова, что в среде ОТ также существуют уникальные проблемы, требующие разных подходов. Устаревшие встроенные системы нельзя сканировать на наличие уязвимостей, а ложные срабатывания могут быть столь же

разрушительными. Не все активы в ОТ можно исправить или обновить. В некоторых случаях исходный код отсутствует для эффективного исправления.

Поскольку ландшафт кибербезопасности коммунальных предприятий продолжает развиваться, рынок технологий кибербезопасности станет полем битвы между различными поставщиками.

Развитие правил кибербезопасности коммунальных предприятий.

Еще одна область, которую исследует отчет, — это развивающаяся область правил кибербезопасности коммунальных предприятий. Во всем мире правительственные учреждения по-разному подходят к законам и стандартам кибербезопасности, и обновления продолжают предлагаться и применяться во всем мире. Коммунальные предприятия должны соблюдать законы и постановления о кибербезопасности, принятые правительствами на национальном или региональном уровне. Правила иногда включают стандарты, установленные доверенными организациями.

Принятие стандартов до выполнения обязательств.

Может быть сложно установить хорошо продуманные правила, поскольку они должны уравновешивать преимущества соответствия требованиям кибербезопасности и затраты для коммунального предприятия и клиентов. Каким бы динамичным ни был ландшафт технологий кибербезопасности коммунальных предприятий, правила продолжают развиваться, поскольку регулирующие органы реагируют на обновления или реформы государственного законодательства с течением времени. Законы и нормативные акты часто предусматривают задержки, позволяющие коммунальным предприятиям реализовать определенные детали.

Комплексное обеспечение зрелости кибербезопасности.

Коммунальные предприятия должны в первую очередь сосредоточиться на базовой гигиене кибербезопасности при проведении комплексной оценки рисков. Крайне важно провести оценку для определения текущего состояния организации и будущего состояния кибербезопасности ИТ/ОТ. Стратегическое планирование инициатив необходимо для устранения пробелов, что является непрерывным и итеративным процессом.

Недавние кибератаки на критическую инфраструктуру страны служат предупреждением для коммунальных служб, поскольку они могут привести к разрушительным последствиям. Основываясь на оценке рисков, связанных с различными поверхностями атак, Info-Tech считает, что лидерам по безопасности крайне важно тщательно изучить технические детали и сосредоточить внимание на более широком воздействии…» ***(Emerging Digitalization Possibilities for Utilities Come With Unique Cybersecurity Risks, Says Info-Tech Research Group in New Report // Gray Television, Inc. (https://www.wilx.com/prnewswire/2023/04/25/emerging-digitalization-possibilities-utilities-come-with-unique-cybersecurity-risks-says-info-tech-research-group-new-report/). 25.04.2023).***

***

«Microsoft расширяет свои усилия по привлечению большего числа женщин в сферу кибербезопасности в рамках своей Инициативы по развитию навыков кибербезопасности.

Кибербезопасность — один из самых быстрорастущих сегментов ИТ-индустрии, но предложение изо всех сил пытается удовлетворить спрос.

«За последние несколько лет киберпреступники нацелились на СМИ, предприятия и правительства, и их количество ошеломляет», — пишет Кейт Бенкен, корпоративный вице-президент Microsoft Philanthropies. «Как мы указали в нашем отчете о цифровой защите за прошлый год, объем атак на пароли вырос примерно до 921 атаки в секунду, что на 74% больше всего за один год. Кибератаки часто имеют разрушительные последствия — средняя стоимость кибератаки достигла 4,35 млн долларов.

«В то же время мы сталкиваемся с глобальным кризисом навыков кибербезопасности. Спрос на навыки кибербезопасности вырос в среднем на 35% за последний год. А в некоторых странах, таких как Бразилия, спрос вырос на целых 76%. У нас просто не хватает людей, обладающих навыками защиты от кибератак, что подвергает риску людей, предприятия и правительства по всему миру».

Чтобы помочь удовлетворить постоянно растущие потребности, компания расширяет свою программу на другие страны, уделяя особое внимание обучению недостаточно представленных групп. Как и в большей части технологической отрасли, в кибербезопасности традиционно гораздо меньше женщин, чем в других областях.

«Помимо распространения программы повышения квалификации на большее количество стран, мы также сосредоточены на том, чтобы помочь исторически недостаточно представленным группам населения попасть на работу в области кибербезопасности», — продолжает Бенкен. «В частности, возможности для женщин работать в сфере кибербезопасности огромны. Сегодня женщины составляют лишь 25% глобальной рабочей силы в области кибербезопасности, поэтому как никогда важно поощрять и расширять возможности женщин для продолжения этой карьеры».

Далее Бенкен выделяет несколько конкретных инициатив:

WOMCY, некоммерческая организация, занимающаяся возможностями кибербезопасности для женщин в Латинской Америке.

Women4Cyber, фонд, направленный на повышение роли женщин в кибербезопасности в Европе.

Международный союз электросвязи — агентство ООН — поддерживает их [Программу наставничества женщин в киберпространстве] (Программу наставничества женщин в киберпространстве) с особым акцентом на Африку, Азию и Ближний Восток.

WiCyS, глобальное сообщество женщин, союзников и сторонников, занимающихся набором, обучением и продвижением женщин в области кибербезопасности.

Компания также работает с организациями в Польше, такими как Институт Костюшко, помогая обучать женщин, в том числе украинских беженцев,

кибербезопасности». ***(Microsoft Expanding Efforts to Bring Women Into Cybersecurity // iEntry Network (https://www.webpronews.com/microsoft-expanding-efforts-to-bring-women-into-cybersecurity/). 24.04.2023).***

***

«В наш век цифровых чудес проблема кибербезопасности ложится тяжелым бременем на предприятия любого размера. По всему спектру компаний регулярно борются с инцидентами, такими как взломы, утечки данных, сложные постоянные угрозы и атаки программ-вымогателей. Большие затраты ложатся на тех, кому не посчастливилось подвергнуться нападению, и нападения могут быть разрушительными. Мало того, кибератаки безжалостно агностичны. Киберпреступникам не важен размер организации, и они атакуют всех, от крупного и среднего бизнеса до самых маленьких магазинов, используя те же методы, что и крупные корпорации. Киберпреступники также не делают различий в зависимости от типа продаваемого продукта или услуги.

Удар среднего уровня, мощное воздействие

В начале февраля крупнейший канадский интернет-магазин книг и музыки Indigo несколько дней подвергался атаке. Атаки затронули заказы клиентов как в розничных точках, так и в Интернете. В течение этого времени компания не могла обрабатывать электронные платежи, операции с подарочными картами или возвраты. Недавно представители Indigo предоставили обновленную информацию об атаке программы-вымогателя и сообщили, что во время инцидента был получен доступ к конфиденциальным прошлым и существующим данным сотрудников.

Атаки на розничную сеть среднего уровня, такую как Indigo, поднимают важные вопросы. Они заставляют задуматься о способности Индиго — или любого другого бизнеса — выжить. Крупные компании могут метафорически игнорировать подобные атаки. В их распоряжении дорогостоящая избыточность, передовые инструменты восстановления и дорогостоящая экстренная помощь специалистов по киберкатастрофам. У них также есть глубокие карманы, чтобы расплатиться. Такие компании, как Amazon, Apple, Sony, Target или Disney, например, имеют сильные бренды, которые позволяют им восстанавливаться после компрометации так, как это просто не могут сделать более мелкие и менее узнаваемые компании. Данные показывают, что 60% малых и средних компаний, подвергшихся успешной кибератаке, исчезнут через 6 месяцев.

Экзистенциальные вызовы

Для компаний среднего размера нет подстраховки. Киберстрахование является дорогостоящим и трудным для получения, и когда резина отправляется в путь, полисы оплачивают только часть квалифицированных расходов. В условиях кибер-кризиса вам по-прежнему нужны экстренные наличные, чтобы покрыть расходы, чтобы вернуться к операционному застою. Таким образом, существует огромная разница в устойчивости между крупными компаниями и каждой компанией среднего или меньшего размера.

Одна из основных причин, по которой инциденты кибербезопасности могут быть более опасными для малых и средних компаний, заключается в том, что им часто не хватает ресурсов для эффективного реагирования на инциденты. В этих

компаниях может не быть ИТ-команды, занимающейся кибербезопасностью, или могут не выделяться финансовые ресурсы для найма внешних экспертов для предотвращения и устранения инцидентов. Это может привести к замедлению времени отклика и повышенному риску дальнейшего повреждения систем и данных компании». ***(Emil Sayegh. Cybersecurity: Why The C-Suite Should Care // Forbes (https://www.forbes.com/sites/emilsayegh/2023/04/18/cybersecurity-why-the-c-suite-should-care/?sh=f4c46d93ef61). 18.04.2023).***

***

«…Чтобы увеличить инвестиции в кибербезопасность, малым и средним предприятиям необходимо переосмыслить то, как они выбирают своих партнеров в области кибербезопасности. Вместо того, чтобы следовать за толпой, они должны начать с оценки своих собственных потребностей.

Малые и средние предприятия испытывают потребность в совершенствовании и росте, но они могут чувствовать разочарование из-за отсутствия изменений при привлечении поставщиков управляемых услуг (MSP). Их разочарование в основном связано с предрасположенностью MSP «отмечать свою домашнюю работу» и придерживаться общих областей знаний, а не предлагать более комплексную настройку кибербезопасности. MSP, как правило, применяют традиционный ИТ-подход к бизнес-вопросам, уделяя особое внимание миграции систем в облако и сохранению статус-кво.

Это отсутствие нестандартного мышления не остается незамеченным ни малыми и средними предприятиями, которым требуются комплексные функции безопасности, ни киберпреступниками, которые используют уязвимости нулевого дня и атаки социальной инженерии с большей изощренностью, чем когда-либо прежде. Ничто не радует их больше, чем чувство самоуспокоенности, когда предприятия мало меняют свою позицию в области кибербезопасности.

Чтобы оставаться киберустойчивыми, малые и средние предприятия должны не ограничиваться эффективностью ИТ и применять объединенное мышление в трех одинаково важных областях: люди, процессы и технологии (PPT). Эти три столпа являются фундаментальной частью кибербезопасности бизнеса и помогут малым и средним предприятиям понять, что им нужно от партнера в первую очередь.

Возможно, сотрудникам не хватает знаний, чтобы обнаружить социальную инженерию, или, может быть, бизнес не соответствует современным стандартам соответствия данных, что делает его открытым для огромных штрафов со стороны регулирующих органов в случае утечки данных. Или, возможно, у бизнеса просто нет средств, чтобы инвестировать в технологию, позволяющую отслеживать угрозы и должным образом отражать их. Как только малый и средний бизнес узнает о своих ограничениях и внутренних проблемах, он может начать искать нужную помощь извне.

В отличие от типичных MSP, поставщики управляемых услуг безопасности (MSSP) узко специализируются на решении тройной проблемы PPT.

Важно отметить, что у MSSP есть одна ключевая цель: постоянно защищать своих клиентов и, если произойдет неизбежное, быстро реагировать, чтобы свести

к минимуму любое воздействие. Этого можно достичь, только наняв специализированных специалистов, которые имеют соответствующий опыт в понимании того, что искать, имеют доступ к глобальной информации об угрозах и делают одно и то же изо дня в день, 24 часа в сутки, 7 дней в неделю, 365 дней в году.

Помимо предоставления ряда услуг в области кибербезопасности, таких как услуги Security Operation Center (SOC), обучение осведомленности о фишинге и тестирование на проникновение, современные MSSP также предоставляют доступ к юристам по защите данных, которые могут помочь организациям внедрить правильные политики и процедуры для борьбы с последствиями. от возможного нападения. Эта возможность будет иметь неоценимое значение, поскольку Великобритания намечает новый курс в законодательстве GDPR, и особенно по мере масштабирования малого и среднего бизнеса.

MSSP обеспечивают широкий спектр навыков и знаний в области кибербезопасности и защиты данных в то время, когда малые и средние предприятия чувствуют себя перегруженными и даже невосприимчивыми к ландшафту киберугроз. На самом деле, новый правительственный обзор нарушений кибербезопасности показывает, что доля микропредприятий, считающих кибербезопасность своим высоким приоритетом, упала с 80 процентов в 2022 году до 68 процентов в этом году, а отсутствие улучшения киберустойчивости по всем направлениям, вероятно, связано с «старшие менеджеры в небольших организациях рассматривают кибербезопасность как меньший приоритет в нынешних экономических условиях».

Малым и средним предприятиям необходимо применять упреждающий подход к выбору подходящего партнера по кибербезопасности, отвечающего их уникальным требованиям. Четкое понимание их критериев PPT — отличная отправная точка, которая даст им более четкое представление о том, каких партнеров искать. Только таким образом малые и средние предприятия могут обеспечить дальнейшее развитие своих инвестиций в кибербезопасность и надежную защиту своего бизнеса от новых киберугроз». ***(Pete Bowers. How SMEs can select the right cybersecurity partner // SME Magazine (https://www.smeweb.com/2023/04/26/how-smes-can-select-the-right-cybersecurity-partner/). 26.04.2023).***

***

«В мире, который все больше определяется не физическими, а скорее цифровыми границами, объем инцидентов в области кибербезопасности по всему миру продолжает расти, а вместе с ним и проблемы, с которыми сталкиваются агентства государственного сектора. Ставки защиты данных об учредителях важнее, чем когда-либо прежде. Чтобы защититься от этих цифровых угроз, государственные учреждения используют подход с нулевым доверием к управлению рисками.

Нулевое доверие — это структура или модель, основанная на мышлении «ничему не доверяй и все проверяй». Это позволяет государственным учреждениям защищать свою среду независимо от того, где находятся данные и люди, применять

политики безопасности и лучше готовиться к тому, что может произойти дальше. Самое главное, нулевой уровень доверия помогает правительствам поддерживать общественное доверие. При эффективном внедрении эта структура позволяет государственным учреждениям обеспечивать безопасность данных учредителей, обеспечивая при этом простоту и удобство работы.

В то время как руководители государственных и государственных учреждений продолжают свой путь к нулевому доверию, вот несколько соображений для тех, кто хочет продолжать снижать свою подверженность риску и повышать кибербезопасность:

Установите надежное управление данными

Государственные учреждения должны работать над распознаванием рисков кибербезопасности, принимать основанные на рисках решения относительно распределения ресурсов и изыскивать ресурсы для устранения уязвимостей. Крайне важно, чтобы они применяли корпоративный подход, который включает в себя технологические отделы, такие как директор по информационным технологиям, а также программные и функциональные отделы, включая персонал и закупки. Им необходимо отдавать приоритет информации, требующей наивысшего уровня защиты.

Кроме того, поскольку организации продолжают двигаться к автоматизации, важно понимать, что запросчиком данных может быть не человек. Многие агентства используют разработку, безопасность и эксплуатацию — или DevSecOps — для решения этих проблем. Благодаря DevSecOps безопасность встраивается заранее и на протяжении всего жизненного цикла разработки решения, что в результате снижает киберриски и уязвимость.

Приоритет управления идентификацией

Надежное управление идентификацией использует аутентификацию и права пользователей, чтобы обеспечить доступ только для уполномоченных лиц. Кибераналитика — это всего лишь один из методов улучшения управления идентификацией в организации. Он может анализировать поведение пользователя, например динамику нажатия клавиш, движения мыши и шаблоны навигации; контекстуальные факторы, такие как местоположение, устройство и время суток; а также данные о внешних угрозах, таких как вредоносное ПО, фишинговые атаки и выявление кражи.

Другие решения включают возможности нулевого доверия, уже используемые государственными организациями, такие как управление доступом на основе ролей, многофакторная аутентификация и доступ, при котором каждому пользователю или устройству предоставляется минимальный системный ресурс для выполнения его функций.

Установить подотчетность

Понимание активов данных необходимо для личной и организационной ответственности. Государственные организации должны внедрить действенные и действенные сетевые средства контроля и контролировать их использование и эффективность. Они также должны постоянно исследовать и тестировать возможности кибербезопасности путем имитации атак на данные, приложения и службы.

Внедрение фреймворка с нулевым доверием не должно быть дорогостоящим мероприятием. Благодаря перепрофилированию существующих киберинструментов и возможностей руководители должны иметь возможность добиться экономии средств при одновременном повышении своей кибербезопасности.

Воспитывать образ мышления в области кибербезопасности

Для эффективного укрепления кибербезопасности в этом должны участвовать все сотрудники. Организации, которые успешно внедряют архитектуру с нулевым доверием, гарантируют, что весь персонал осознает важность защиты данных. Кибербезопасность рассматривается всеми сотрудниками как коллективное мышление сверху вниз и снизу вверх. Кроме того, постоянная «гигиена кибербезопасности» используется в качестве бесценного инструмента наряду с лидерством, выступающим в роли «защитников кибербезопасности».

Кибератаки и угрозы защите данных не ослабевают в нашей все более безграничной среде. Правительства должны действовать сейчас, чтобы продолжать укреплять свою киберзащиту, если они надеются защитить информацию об участниках и сохранить доверие общественности». ***(Tony Hubbard, Viral Chawda. Government agencies are embracing a zero-trust approach to risk management // Nextgov (https://www.nextgov.com/ideas/2023/04/rethinking-cybersecurity-boundaryless-world/385677/). 27.04.2023).***

***

«За даними Cybersecurity Ventures, глобальна кількість вакансій у сфері кібербезпеки зросла на 350% - з одного мільйона у 2013 році до 3,5 мільйона у 2021 році.

Кількість незаповнених вакансій вирівнялася у 2022 році та залишилася на рівні 3,5 мільйона у 2023 році, причому понад 750 тис з них - у США. Зусилля галузі щодо пошуку нових талантів та боротьби з вигоранням кадрів тривають, але аналітики прогнозують, що диспропорція між попитом та пропозицією збережеться щонайменше до 2025 року.

За останні два роки технологічні компанії втратили понад 300 тис робочих місць, а 470 технологічних роботодавців скоротили свою робочу силу з початку пандемії.

«Поки Amazon, Meta, Twitter, Microsoft, Google та інші технологічні гіганти проходять через звільнення, наша галузь вивісила величезний знак «Потрібна допомога», - каже Стів Морган (Steve Morgan), засновник Cybersecurity Ventures.

Незважаючи на безлад у технологічній галузі, кібербезпека залишається ринком з майже нульовим рівнем безробіття для людей з великим досвідом, а дефіцит кадрів означає, що IT-команди також повинні нести тягар безпеки. Співробітники повинні бути обізнані про сучасні загрози, включаючи фішинг, соціальну інженерію, компрометацію ділової електронної пошти (BEC) та фінансове шахрайство. Вони також повинні знати, як захищати програми, дані, пристрої, інфраструктуру та людей». ***(За десять років глобально кількість вакансій у сфері кібербезпеки зросла на 350% // Компьютерное Обозрение***

(https://ko.com.ua/za_desyat_rokiv_globalna_kilkist_vakansij_u_sferi_kiberbezpeki_zrosla_na_350_143871). 17.04.2023).

***

«З кожним роком вартість кібератаки знижується, а їх можливості розширюються шляхом численних експлойтів та програм-вимагачів. Однак разом з ними покращується і захист, надалі можна залучати машинне навчання для швидшої реакції на погрози.

З розвитком звітності за даними, що отримуються від інструментів управління інформацією та подіями безпеки (SIEM) та суміжних рішень, будь-який відділ безпеки сьогодні може зіткнутися з інформаційним навантаженням та паралічем. Щоб внести ясність у цей туман, виникла та продовжує розвиватися практика аналізу загроз. З її допомогою фахівці з безпеки можуть знаходити найактуальніші проблеми серед інцидентів у щоденних звітах та усувати їх.

Фокус переклав статтю Іцика Котлера про те, як розвиток звітів про загрози впливає на кібербезпеку.

Занадто чутливі інструменти управління вразливістю можуть генерувати занадто багато завдань, у той час, як погано налаштовані системи аналізу загроз можуть не відфільтрувати сигнал від шуму і надати занадто багато даних, змусивши команду займатися малозначущими завданнями, що повторюються. Десятки точкових рішень з безпеки вимагають спеціальних знань та майстерності, на досягнення та підтримку яких витрачається час. Додайте сюди перехід від концепції захисту периметра до підходів, що ґрунтуються на дотриманні вимог та ризиків. Стає зрозуміло, чому фахівцям стає все важче зосередитися саме на загрозах, які становлять найбільшу небезпеку.

Аналіз кіберзагроз: минуле, сьогодення та майбутнє

Приватні компанії та уряди завжди аналізували погрози, щоб знайти та відсортувати потенційні ризики. Основні питання аналізу загроз залишаються незмінними:

Вплив – які збитки можуть бути завдані?

Мотивація хто стоїть за загрозою?

Ймовірність – які можливості має суб'єкт загрози для здійснення атаки?

Навички – наскільки серйозна загроза та яка її мета?

Чим більше атак та даних, тим складніше швидко відповісти на ці запитання. Хоча система кібербезпеки SIEM дає певні переваги, вона також може погіршити цю проблему.

Чинні особи кіберзлочинності

З розвитком IT-мереж та Інтернету загрози для підприємств та інших організацій перемістилися в кіберпростір. Останні п'ять років джерела кіберзагроз швидко еволюціонували.

Крім звичайних атак кіберзлочинності, які стали звичним явищем за десятиліття, державні структури також здійснюють кібератаки. Останнім часом кількість таких суб'єктів збільшилася з появою передових груп кіберзагроз (APT), які функціонують як знаряддя урядових атак та промислового шпигунства.

Ці APT стають все більш витонченими і демонструють поведінку, схожу на поведінку цифрових злочинців, що ускладнює класифікацію та атрибуцію атак.

Планка кібератак постійно знижується

Крім різноманітних загроз, що походять від національних держав та організованих злочинних угруповань, Інтернет захлеснув нескінченний потік опортуністичних, автоматизованих або сценарних кібератак.

Зростання числа таких випадків зумовлене розвиненим та квітучим підпільним ринком спеціалізованих експлойтів та програм-вимагачів, наборів інструментів для атак, крадіжки платіжних даних, викрадених облікових даних та послуг фішингових кампаній. Зловмисники можуть орендувати бот-мережі зі зламаних комп'ютерів або «розумних» пристроїв (IoT), таких як принтери та камери, для проведення атак.

Кібератаки та всі їх компоненти сьогодні є товаром, що часто працює за моделлю «надання послуги» відповідних технічних навичок та супутніх товарів для тих, хто готовий платити. Планка для проведення атак навіть на найзахищеніші цілі знизилася як ніколи.

Диверсифікація вразливостей

У міру зростання глобального простору атак зростає і кількість та типи вразливостей. У 2019 році було зафіксовано приблизно у 20 разів більше попереджень про загальні вразливості та експлойти (CVE), ніж у 1999 році. У відповідь сучасні організації розгортають десятки елементів управління, які вимагають постійної тонкої настройки, щоб охопити весь спектр потенційних загроз. Не дивно, що відділи безпеки вже не можуть залатати всі можливі проломи або налаштувати всі елементи керування вручну.

Повернення старих погроз

Що ще гірше, старі погрози знову повертаються у новому вигляді. Прикладом може бути відома шкідлива програма Emotet. Вперше виявлена у 2014 році, Emotet адаптувалася у міру того, як зловмисники налаштовували її, щоб уникнути виявлення та видалення. У 2018 та 2019 роках вона стала найактивнішою шкідливою загрозою, а потім пішла у сплячий режим. Останнє відродження відбулося в липні 2020 року, коли ботнети Emotet почали надсилати електронні листи зі шкідливими URL-адресами або вкладеннями.

Атаки Emotet зазвичай супроводжуються додатковими атаками, такими як програма-вимагач Ryuk, що використовує переваги Emotet для власного поширення. Нині Emotet використовується безліччю організованих кіберзлочинних груп, які часто працюють спільно.

Ця нова норма підкреслює причини постійного зростання кількості інцидентів безпеки, які доводиться розбирати та усувати командам, а також їхню наростаючу потребу у якіснішому та найшвидшому визначенні найактуальніших загроз.

Новий виклик в аналізі загроз

Забезпечення надійного та ефективного аналізу кіберзагроз у постійно змінюваному ландшафті потребує навичок, автоматизації, правильних інструментів та визначення пріоритетів загроз. У міру того, як з'являється все більше методів і тактик аналізу, дані оновлюються набагато швидше. Ключовим завданням є

масштабування охоплення без збільшення ресурсів, збереження контексту і точності.

На цьому тлі компанії перейшли від розгляду кібербезпеки як страхового поліса до погляду на неї як на критично важливу частину бізнесу. У відділів безпеки немає часу аналізувати всі звіти та заглиблюватися у всі зміни, необхідні для блокування атак. Вони повинні більше покладатися на автоматизовані інструменти фільтрації та визначення пріоритетів, такі як симуляція злому та атаки (BAS), щоб зрозуміти, які загрози мають викликати реальне занепокоєння, а які покриваються наявними засобами контролю.

Переваги програми BAS при складанні звітів щодо аналізу загроз

Команда аналізу загроз, що використовує платформу BAS, може швидко отримати більше корисних даних для покращення звітності щодо загроз. На основі цих даних аналітики можуть обґрунтовано припустити, що конкретний агент або APT, швидше за все, націлений на їхню галузь (та їхню компанію). Використовуючи модель аналізу загроз BAS, вони можуть отримати більше інформації про техніку, тактику та процедури (TTP). Звуження кола потенційних сценаріїв атак дозволить аналітикам завантажити симуляцію атаки, щоб перевірити захист, який забезпечує поточна система безпеки. Крім того, аналітики можуть побачити, як розвиватиметься атака, намітити потенційні точки входу та оцінити ймовірність поширення. Вони можуть помітити перехід від менш важливих до цінніших цілей, коли зловмисник отримає доступ до систем високого рівня.

Тести також можуть показати групи моделей поведінки, які вказують на більшу ймовірність атаки, навіть якщо кількість явних ознак компрометації (IOC) обмежена.

Такі сигнали, як спроба «грубого фішингу», замаскований шкідливий макрос у вкладенні або інші «сліди з хлібних крихт» можна об'єднати для створення повнішої системи аналізу загроз. Окремі попередження про ці специфічні види поведінки викликають втому від попереджень. Коли вони пов'язані між собою за допомогою інтелектуальних звітів про аналіз загроз, вони створюють повнішу картину атаки, що розвивається.

Такий підхід, заснований на діях, переводить аналіз загроз у проактивніше русло, дозволяючи прогнозувати, куди рухаються зловмисники. Це може скоротити час реагування з кількох днів чи тижнів до кількох годин, чи навіть хвилин. Побачити ці закономірності можна за допомогою систем машинного навчання, які можуть самостійно виявляти нові моделі шкідливої активності на основі попередніх випадків із файлів журналів та інших артефактів. Ці системи поєднують пошук закономірностей за більшою кількістю змінних і навчаються у мережах, що виходять далеко за межі одного об'єкта.

Зберігати спокій та продовжувати розвиватися

Атаки, безумовно, розвиваються, але фахівці з безпеки щодня роблять кроки щодо їх припинення. Ми з надією дивимось у майбутнє аналізу загроз. За останнє десятиліття він розвивається дуже швидко та постійно вдосконалюється.

Наразі фахівці можуть проводити безперервне моделювання атак на основі десятків тисяч відомих уразливостей та сценаріїв атак. Галузеві структури та

інструменти, такі як база знань ATT&CK компанії MITRE, дозволяють швидко розповсюджувати інформацію та оновлювати останні ТТП.

Системи машинного навчання можуть автоматизувати більшу частину дій зі зіставлення шаблонів першого рівня, щоб дозволити аналітикам загроз зосередитися на аналізі, що має вищу цінність. Аналіз загроз вийшов за межі простих сигнатур і став розуміти складові та складні моделі поведінки, які вказують на ймовірність атаки. Це означає, що аналіз загроз, при правильному плануванні та проведенні, може ефективніше послужити аналітикам, керівником уразливістю та реагуванням на інциденти, а також знизити навантаження на відділи безпеки, допомагаючи їм зосередитися саме на експлойтах, APT та атаках, що становлять найбільший ризик для їхнього бізнесу». ***(Ольга Шевченко. Аналіз загроз: як розвиток звітів про загрози впливає на кібербезпеку // Фокус (https://focus.ua/uk/voennye-novosti/560763-analiz-zagroz-yak-rozvitok-zvitiv-pro-zagrozi-vplivaye-na-kiberbezpeku). 14.04.2023).***

***

Сполучені Штати Америки та Канада

«Министерство обороны США призывает хакеров принять участие в их инициативе «Взломать Пентагон» с запуском нового веб-сайта.

Веб-сайт www.hackthepentagon.mil дополняет программу, запущенную в 2016 году, и служит образовательным инструментом и ресурсным центром для тех, кто хочет помочь Министерству обороны с тем, что они называют «Bug Bounty».

«Когда дело доходит до информации и технологий, оборонный истеблишмент обычно полагается на закрытые системы, — сказал министр обороны эпохи Обамы Эш Картер, когда программа была запущена в 2016 году., чем больше брешей мы сможем найти, тем больше уязвимостей мы сможем исправить и тем большую безопасность мы сможем обеспечить нашим бойцам».

Концепция проста: «этичные хакеры», также известные как «белые хакеры», получат денежное вознаграждение за помощь Пентагону в выявлении проблем с его системами.

«Возможность быть уверенным в своих сетях и понимать, в чем заключаются ваши уязвимые места, означает, что вы должны быть в состоянии подвергать тщательной проверке внешние источники, а не просто быть самолизающимся рожком мороженого», — сказал бывший адмирал в отставке Данелл Барретт. заместитель директора по информационным технологиям ВМС и бывший директор по операциям Киберкомандования США, в 2022 году в « Подкасте Defense Scoop».

Помимо того, что программа невероятно рентабельна, она также помогает Пентагону нанимать технических специалистов.

«Благодаря программе Hack the Pentagon мы создаем глобальный поток талантов для экспертов по кибербезопасности, которые будут вносить свой вклад в нашу национальную оборону за пределами традиционной карьеры в правительстве», — сказал Джинён Инглунд, исполняющий обязанности

заместителя директора по цифровым технологиям и искусственному интеллекту Управления цифровых услуг. пресс-релиз.

С момента начала инициативы Hack the Pentagon опытные инженеры-программисты, специалисты по данным, менеджеры по продуктам и дизайнеры исследований пользователей Главного управления цифрового и искусственного интеллекта провели более 40 наград за обнаружение ошибок с участием более 1400 этичных хакеров. В совокупности они отметили более 2100 уязвимостей.

Любой, кто считает, что нашел ошибку, о которой нужно сообщить, может посетить страницу программы раскрытия информации об уязвимостях Министерства обороны США (VDP) на новом веб-сайте. VDP не предлагает денежное вознаграждение, как это делают вознаграждения за обнаружение ошибок». ***(Ryan Garza. Defense Department invites hackers to 'Hack the Pentagon' // Nexstar Media Inc. (https://www.newsnationnow.com/business/tech/defense-department-invites-hackers-to-hack-the-pentagon/). 05.04.2023).***

***

«Космическая кибербезопасность — это быстро растущий нишевый рынок. Он предоставляет малым предприятиям уникальную возможность расширить свой опыт и позиционировать себя в качестве ценных партнеров в государственном и частном секторах. Недавний конкурс Hack-A-Sat, организованный Министерством ВВС США в сотрудничестве с Исследовательской лабораторией ВВС и Командованием космических систем, выдвинул на первый план космическую кибербезопасность. Это позволило малым предприятиям учиться у самых одаренных талантов в отрасли.

Hack-A-Sat — это ежегодное соревнование по взлому спутников, в котором исследователям безопасности предлагается устранить препятствия кибербезопасности в космических технологиях. Эту концепцию придумали ВВС США, Космические силы и исследовательское сообщество в области безопасности. Ранее в нем использовалось физическое лабораторное оборудование или платформа цифровых двойников, но в этом году участники будут экспериментировать на орбитальном спутнике Moonlighter, запуск которого намечен на начало лета.

Космическая кибербезопасность — растущая ниша

Малые предприятия могут извлечь большую пользу, внимательно следя за такими событиями, как Hack-A-Sat. Используя идеи и знания, полученные на этой платформе, они могут способствовать сотрудничеству и обмену знаниями с талантливыми людьми по всему миру. Это улучшит их предложения в области кибербезопасности и поможет им опережать возникающие угрозы. Конкурс дает ценный практический опыт работы с реальными космическими системами. Это позволяет малым предприятиям лучше понять нюансы создания устойчивых космических систем, что делает их более конкурентоспособными на рынке.

Создание сети в сообществе космической кибербезопасности

Конкурс Hack-A-Sat открыт для глобального сообщества исследователей безопасности, а это означает, что малые предприятия могут устанавливать связи и создавать сеть в сообществе космической кибербезопасности. Эти отношения

могут привести к будущему сотрудничеству, совместным предприятиям и ценным партнерским отношениям, стимулируя рост и возможности расширения для малого бизнеса в этой новой области.

Платформа для инноваций и сотрудничества

Участие в громких мероприятиях, таких как Hack-A-Sat, демонстрирует приверженность компании инновациям и передовым технологиям, что делает его привлекательным выбором для профессионалов, ищущих интересные и перспективные карьерные возможности. Внимательно следя за такими событиями, как Hack-A-Sat, малые предприятия могут привлекать и удерживать лучших специалистов в области кибербезопасности.

Получение информации об орбитальных космических системах

Соревнование Hack-A-Sat 2022 Finals было организовано как CTF «атака-защита», где каждая команда контролировала свой собственный спутник. Команды зарабатывали очки, сохраняя контроль над ним, защищая его от атак, атакуя другие спутники и решая задачи по взлому. Проблемы были самыми разными, включая крипто-уязвимости наземных станций, ошибки в программном обеспечении для полетов, цепочки ROP RISC-V, атаки на веб-серверы, интеллектуальный анализ данных, орбитальные научные миссии, планирование контактов наземных станций, наведение антенн и защиту радиоканалов.

Наиболее успешная атака основывалась на двух ключевых столпах: утечке конфигураций радиосвязи, используемых другими командами, и отправке вредоносных команд для злоупотребления встроенным алгоритмом управления ADCS. Poland Can Into Space была первой командой, применившей эту атаку, что дало им конкурентное преимущество. В то время как другие команды справились с последствиями этой атаки, Poland Can Into Space продолжала эксплуатировать свой спутник, набирая очки SLA и работая над другими задачами.

Атака вынуждает другую команду отказаться от своих планов и вместо этого сосредоточиться на восстановлении своего спутника, прерывая их цикл принятия решений и заставляя их перераспределять свои ресурсы для защиты. Это также мешает другим командам атаковать вас, так как они заняты восстановлением своего спутника и у них меньше времени и ресурсов для организации ответных атак. Компании могут извлечь уроки из этих стратегий, чтобы улучшить свои предложения в области кибербезопасности.

Несмотря на то, что квалификационное мероприятие Hack-A-Sat в этом году уже прошло, малые предприятия все еще могут извлечь выгоду из знаний и опыта, которыми они поделились во время конкурса. Внимательно следя за результатами финального мероприятия этого года в августе и взаимодействуя с сообществом космической кибербезопасности, малые предприятия могут улучшить свои предложения услуг, привлечь лучших специалистов и создать прочную сеть в сообществе космической кибербезопасности, прокладывая путь для будущего роста и успех. Следите за предстоящими соревнованиями Hack-A-Sat и подобными мероприятиями, чтобы изучить возможности и возможности, которые они предлагают». ***(Heather Wilde. Harness the Power of Space Cybersecurity for Growth and Opportunity // MANSUETO VENTURES (https://www.inc.com/heather-wilde/harness-power-of-space-cybersecurity-for-growth-opportunity.html). 05.04.2023).***

***

«Исследователи военной информационной безопасности США просят промышленность найти новые способы защиты больших устаревших программных систем от потенциальных кибератак.

Официальные представители Агентства перспективных исследовательских проектов Министерства обороны США (DARPA) опубликовали во вторник широкое объявление агентства (HR001123S0028) о проекте разделения и управления привилегиями (CPM).

DARPA CPM стремится разработать набор инструментов анализа, аппаратной и программной инфраструктуры, чтобы автоматически сегментировать большие устаревшие программные системы на высокопроизводительные детализированные сегменты с ограниченными правами, которые предотвращают превращение первоначальных проникновений в успешные кибератаки. Проект включает в себя автоматизированное разделение, обеспечение привилегий и поддержку оценки.

Успешная кибератака обычно включает в себя последовательность действий, которая переходит от первоначального проникновения в систему к повышению привилегий и горизонтальному перемещению, а затем к полномасштабной кибератаке.

Первоначальное проникновение направлено на повышение уровня привилегий злоумышленника, а затем и на обеспечение бокового перемещения внутри скомпрометированной системы. В конечном счете, целью злоумышленника является использование несанкционированного привилегированного доступа для обнаружения и извлечения конфиденциальной информации или для нарушения нормальной работы.

Традиционные средства защиты от кибератак сосредоточены на недопущении злоумышленника и устранении уязвимых для использования ошибок в коде. Вместо этого программа CPM фокусируется на блокировании повышения привилегий и горизонтального перемещения, даже если имело место первоначальное проникновение.

Технология CPM предоставит возможность реструктурировать систему в такую, которая будет препятствовать распространению таких кампаний за пределы их первоначального проникновения.

На первом этапе программы CPM будет использоваться операционная система Linux с открытым исходным кодом в качестве цели для тестирования и оценки. Второй этап будет сосредоточен на применении инструментов и возможностей для защиты таких приложений, как веб-браузеры, веб-серверы, системы управления базами данных.

CPM разделен на три технические области: автоматическая компартментализация; применение политики привилегий; и поддержка оценки. Новый запрос на четвертую техническую область, эксперименты с системой DOD, ожидается до этапа 2…» ***(John Keller. Researchers ask industry for information security measures to safeguard legacy software from cyber attacks // Endeavor Business Media, LLC. (https://www.militaryaerospace.com/trusted-computing/article/14292018/information-security-cyber-attacks-legacy-software). 06.04.2023).***

***

«…По данным Cyberseek, проекта, поддерживаемого Национальным институтом стандартов и технологий, в настоящее время в Соединенных Штатах открыто более 755 000 вакансий в области кибербезопасности: примерно 710 000 в частном секторе и 45 000 в государственном секторе.

Многие FSI, конечно же, помогают федеральным агентствам укреплять свою кибербезопасность с помощью технологических решений, внедрений и интеграций, кадрового обеспечения или всего этого. Федеральные агентства полагаются на партнеров из частного сектора, чтобы понять кибер-решения, которые могут решить конкретные проблемы агентства, и помочь в их реализации.

Это также означает понимание федеральных требований и того, как лучше всего включить их в дизайн проекта или включить их в интеграцию.

Тем не менее, подрядчики не всегда понимают требуемые стандарты кибербезопасности, не говоря уже о том, чтобы внедрять их в свою собственную среду, что может увеличить потенциальную подверженность агентств киберугрозам и, соответственно, увеличить нагрузку на и без того перегруженный персонал агентства по кибербезопасности.

Например, оборонные подрядчики, работающие с несекретной информацией, находящейся под федеральным контролем, в течение нескольких лет должны были применять 110 методов обеспечения безопасности, изложенных в специальной публикации NIST 800-171, но сотрудники по контрактам не применяли их.

Это может измениться, когда этой весной 110 (плюс 17 средств контроля для уровня 1) средств и методов безопасности станут основными требованиями в соответствии с правилом сертификации модели зрелости кибербезопасности 2.0 Министерства обороны. Это хороший и необходимый шаг.

Федеральные подрядчики должны соответствовать тем же стандартам, которые применяются к их клиентам-агентствам, независимо от того, требуется ли

это по закону или нет. Соблюдение требований NIST SP 800-53 и SP 800-171, например, должно быть простой задачей.

Подрядчики должны иметь глубокие знания требований кибербезопасности, которые они помогают выполнять агентствам. Приобретение этих знаний до заключения контракта позволит FSI не только выиграть контракт, но и более эффективно выполнить его для агентства. Повышение эффективности снижает нагрузку на кибер-персонал агентства.

Национальная стратегия кибербезопасности призывает к расширению государственно-частного партнерства по многим направлениям. В нем признается, что устранение нехватки специалистов в области кибербезопасности «потребует лидерства на федеральном уровне и прочного партнерства между государственным и частным секторами». Инициативы по найму, удержанию и обучению в обоих секторах — это только начало.

Но нехватка кадров настолько велика, а ландшафт киберугроз настолько широк и коварен, что люди сами по себе не являются ответом — и, конечно же, они не являются краткосрочным решением для устранения насущных пробелов в кибербезопасности.

Управляемые службы безопасности в сочетании с облачными решениями кибербезопасности, использующими искусственный интеллект и машинное обучение, представляют собой более реалистичное решение для устранения нехватки специалистов в области кибербезопасности. По некоторым оценкам, до 90 процентов киберданных никогда не анализируются.

Люди просто не успевают за растущими объемами данных. Но AI и ML могут. Использование облачных решений для обеспечения кибербезопасности снимает бремя управления и обслуживания локальной инфраструктуры безопасности.

Модели на основе искусственного интеллекта могут определять характеристики и контекстуальное поведение действий противника и блокировать их — даже атаки, которые никогда раньше не наблюдались. Машинное обучение обеспечивает постоянное обновление моделей, улучшая защиту в режиме реального времени при обнаружении новых угроз.

Управляемые услуги также являются важным инструментом для FSI в их поддержке клиентов агентства. Автономные операции как в государственном, так и в частном секторе просто нежизнеспособны в сегодняшних условиях.

Управляемые службы безопасности предоставляют интегрированные комплексные решения в области кибербезопасности, экономию средств, масштабируемость, круглосуточный мониторинг и разгружают рутинные задачи, чтобы сотрудники службы безопасности могли сосредоточиться на управлении безопасностью.

Ценность управляемых служб безопасности для FSI и их агентских клиентов сродни ценности облачных служб по сравнению с локальными центрами обработки данных. Проще говоря, переход на управляемые услуги — еще одна простая задача.

Вместе промышленность и правительство могут восполнить нехватку специалистов в области кибербезопасности размером с кратер. Для этого потребуются постоянные усилия на многих фронтах.

На переднем крае для получения наиболее немедленных и устойчивых результатов должно быть Zero Trust, поддерживаемое облачными решениями безопасности, которые используют AI и ML, в сочетании с управляемыми службами безопасности и повсеместным соблюдением государственных стандартов безопасности.

Если мы сделаем это сейчас, мы увидим экспоненциально более быстрый прогресс, чем сегодня». ***(Danny Connelly. Industry and government can both fill that crater-sized gap, but doing so will take sustained efforts on many fronts // Government Media Executive Group LLC (https://washingtontechnology.com/opinion/2023/04/closing-cybersecurity-talent-gap-requires-new-approaches/384717/). 07.04.2023).***

***

«Передовые технологии, глобализированная экономика и нестабильность в экономическом и политическом ландшафте смыли когда-то легко определяемые национальные границы. Киберугрозы и вызовы теперь нацелены на пороги нашего штата, местных, племенных и муниципальных сообществ. Этот сдвиг способствует увеличению количества атак на наши школы, больницы, малый бизнес, местные органы власти и критически важную инфраструктуру.

По правде говоря, тонкое сближение внутренней безопасности с нашей более широкой национальной безопасностью предвещает необходимый сейсмический сдвиг в нашем отношении к кибербезопасности — тот, который подчеркивает большую чувствительность к изменчивости вездесущей кибернетики в цифровом взаимосвязанном мире, возвращаясь к простоте фундаментальной кибербезопасности. практики, которые сводятся к минимуму, забываются или часто игнорируются.

Ничто так не выдвинуло эту реальность на передний план, как война России с Украиной и эскалация напряженности в отношениях Китая с Тайванем.

На заре 2022 года российские кибер-силы предприняли десятки кибератак на украинскую инфраструктуру с намерением нанести ущерб ключевым экономическим, политическим и военным объектам в преддверии массированной наземной атаки России. Хотя на сегодняшний день Россия не нанесла серьезного кибердара по Соединенным Штатам, злоумышленники и их доверенные лица, поддерживающие Кремль, продолжают наращивать свои атаки.

Всего несколько недель назад пророссийские хакеры смогли отключить веб-сайты 14 больниц в США, в том числе Stanford Healthcare, Duke University Hospital и Cedars-Sinai. В нашем образовательном секторе Федеральное бюро расследований (ФБР) обнаружило широко распространенный обмен более чем 36 000 просочившихся учетных данных VPN для колледжей США, которые всплыли на российских форумах по киберпреступности в мае этого года. Источники в банковской сфере сообщили об усилении кибератак на технологическую

инфраструктуру сектора после того, как США ввели санкции в связи с вторжением России в Украину.

С другой стороны мира, эскалация языка Китая, продолжающиеся военные учения и политические подшучивания продолжают создавать предлог для возможного вторжения на Тайвань. Тем не менее, согласно данным Dyadic Cyber Incident and Campaign Data (DCID), использование Китаем кибершпионажа является обоснованным и активно используется. С мая 2021 года Mandiant сообщил, что по крайней мере шесть правительств штатов США были скомпрометированы хакерскими группами, спонсируемыми китайским государством.

Любая отдельная атака на любую страну может иметь глобальные последствия. Еще до нынешнего конфликта российская кибератака NotPetya против Украины в 2017 году нанесла неизбирательный ущерб правительствам и критически важной инфраструктуре по всему миру, включая систему здравоохранения Пенсильвании Heritage Valley. Последствия российской кибератаки против спутниковой компании Viasat всего за несколько часов до вторжения страны в Украину привели к нарушению работы критически важной инфраструктуры далеко за пределами Украины.

В этих условиях каждая организация, в том числе предприятия, имеющие решающее значение для цепочек поставок, и местные органы власти, предоставляющие критически важные услуги своим жителям, подвергаются более высокому профилю риска в отношении изощренных угроз со стороны государства.

Принятие мер через партнерство внутри страны и за рубежом

В преддверии вторжения России федеральные правительственные агентства США мобилизовали правительства штатов и местные органы власти, а также частный сектор для активной подготовки киберзащиты в каждой организации. Министерства внутренней безопасности (DHS) Агентства по кибербезопасности и безопасности инфраструктуры (CISA) Кампания «Shields Up» предложила всем организациям надежные рекомендации по внедрению базовых методов кибербезопасности, которые могли бы противодействовать разрушительным киберинцидентам.

DHS активизировал партнерские отношения с правоохранительными органами по всему миру, чтобы обмениваться важной информацией и наращивать потенциал партнеров, чтобы помочь выявлять угрозы задолго до того, как они достигнут американских границ. По данным Государственного департамента США, агентства федерального правительства, включая CISA, ФБР, Агентство США по международному развитию (USAID), Министерство энергетики и Министерство обороны, а также промышленные, академические и иностранные союзники пришли вместе для обмена информацией и идеями.

Кроме того, Кибернетическое командование США направило группу по поиску киберпреступников непосредственно в столицу Украины Киев, чтобы усилить ее киберзащиту и обеспечить уверенность. Гибкий подход CNMF к киберзащите создает уникальные возможности для постоянного совершенствования своих навыков в области кибербезопасности, помощи

союзникам в укреплении киберзащиты и совместной работы над угрозами и аналитическими данными.

Результаты этих совместных усилий уже окупились. По словам директора CISA Джен Истерли, «Россия просчиталась с военными усилиями, недооценив как стойкость, боеспособность и мужество украинской армии, с которыми ей предстоит столкнуться, так и единый фронт, который США и другие союзники выставят против России».

Глобальные коллективные успехи за границей отражают тот же уровень усилий, к которому США должны стремиться внутри страны, расширяя меры по защите своей критически важной инфраструктуры дома и продолжая национальный диалог о важности надлежащего финансирования организационных усилий по кибергигиене. Ранее упомянутые инциденты в сфере здравоохранения, образования и финансовых услуг указывают на то, что еще многое предстоит сделать.

Активная и эффективная киберзащита начинается дома

В настоящее время администрация Байдена настаивает на разработке планов дополнительных обязательных мер безопасности для отраслевых секторов в рамках продолжающегося сдвига парадигмы в сторону более строгих правил в своей национальной директиве по кибербезопасности. Этот общий подход будет в большей степени опираться на агентства с конкретными отраслями промышленности, такими как авиация, химическая промышленность, водное хозяйство и строительство плотин, а также на усиление лидерства CISA для поддержки этих усилий.

На государственном и местном уровнях управления сотрудничество еще более важно. Небольшие организации борются с фрагментированной структурой управления, разрозненными управлениями, отсутствием упорядоченных политик и процедур с малой уверенностью в том, как действительно проверить уровень кибергигиены в масштабе, особенно при работе в условиях ограниченного бюджета на инструменты и таланты, чтобы идти в ногу с текущими киберугрозы.

Чтобы противостоять этим недостаткам, такие штаты, как Аризона, обращаются к общегосударственному подходу к кибербезопасности, который расширяет поддержку управления кибербезопасностью на более мелкие местные органы власти — будь то путем предоставления ключевых сведений об угрозах и безопасных отчетов, предварительно утвержденных инструментов, обучения или финансирование в виде грантов, чтобы помочь укрепить киберзащиту на всех уровнях правительства. Другие штаты, такие как Калифорния, сначала начинают с таких инициатив, как Cal-Secure, на уровне агентств штата, чтобы обеспечить повсеместное распространение среди агентств на уровне штата, прежде чем распространять их на местные и племенные.

Эти очень совместные и дальновидные инициативы надеются остановить растущую озабоченность по поводу повсеместного распространения киберпространства на протяжении всей нашей жизни. В сочетании с продолжающимся разрушением границ национальной безопасности и национальной безопасности основа нашей нации — люди — теперь являются мишенью злонамеренных кибер-актеров, поддерживаемых государством, которые

используют уязвимости нашего оборудования и программного обеспечения, одновременно используя социальную инженерию для своей выгоды.

Борьба с угрозами сегодняшнего и завтрашнего дня требует совместной работы всех нас с глобальными, федеральными, государственными и местными органами власти, частным сектором, некоммерческими организациями, академическими кругами и, конечно же, вкладом каждого человека. Потребность в совместном государственно-частном партнерстве, возможностях и инструментах будет только расти по мере того, как мы сталкиваемся с угрозами завтрашнего дня.

Сохранение бдительности за счет индивидуального смягчения последствий, обнаружения, реагирования и обеспечения устойчивости

На переднем крае киберзащиты все организации должны сыграть свою роль — в каждом секторе — чтобы опережать киберугрозы со стороны враждебных национальных государств и их доверенных лиц.

Абсолютно первая линия защиты организации, направленная на снижение вероятности кибервторжения, начинается с упреждающих мер безопасности и мер кибергигиены, которые в первую очередь предотвращают доступ.

Важно, чтобы организации проверяли все точки удаленного доступа к своим сетям, а также включали многофакторную аутентификацию. Программное обеспечение следует часто обновлять для устранения известных эксплойтов и уязвимостей.

Инвентаризация оборудования и программных приложений должна быть точной. Недавние уязвимости OpenSSL и Log4J подчеркивают важность постоянного обновления спецификации программного обеспечения вашей организации (SBOM), чтобы гарантировать, что все ваше программное обеспечение и его зависимости будут известны и обновлены немедленно, а не в течение нескольких дней или недель. SBOM аналогичны списку ингредиентов на этикетке продукта. Для текущих приложений (продуктов питания) характерно интегрировать программные библиотеки (ингредиенты) от других разработчиков (уменьшая объем разработки разработчиков с использованием нормализованных блоков функционального кода).

Точная видимость каждой конечной точки организации в режиме реального времени имеет решающее значение, потому что вы не можете защитить то, чего не видите. Это означает конвергентную стратегию, которая объединяет инструменты, рабочие процессы и команды для обеспечения видимости, контроля и исправления в масштабе в режиме реального времени. И базируйте свою обычную конфигурацию, чтобы аномалии легко обнаруживались.

Аналитика платформы больших данных помогает выявлять исторические тенденции и анализировать направления атак, но их использование должно быть сбалансировано с их высокими затратами на хранение и транспортировку данных.

Эффективное реагирование на инциденты и поиск угроз требуют осведомленности в режиме реального времени и способности действовать в масштабе предприятия. Максимальная скорость ответных действий (в секундах, а не в днях) значительно сокращает окна уязвимости и воздействие злоумышленников.

Оптимизация и устранение конфликтов ресурсов обнаружения, таких как антивирус, защита от вредоносных программ и программное обеспечение для обеспечения кибербезопасности, чтобы гарантировать, что персонал по безопасности операций может быстро выявлять и оценивать необычное поведение сети и, следовательно, реагировать на вторжения по мере их возникновения. Без этого программное обеспечение для кибербезопасности будет сражаться друг с другом за ресурсы конечных точек, полагая, что другое представляет реальную угрозу.

То, как организации реагируют на атаку, не менее важно. Независимо от масштаба или области деятельности организации, специалисты по ИТ-безопасности должны исходить из того, что в какой-то момент угроза неизбежно возникнет. Таким образом, важно назначить группы реагирования на кризисные ситуации, в том числе технические, коммуникационные и юридические, с ролями и обязанностями, направленными на устранение предполагаемого инцидента кибербезопасности.

Когда такой инцидент неизбежно происходит, важно максимально повысить отказоустойчивость вашей организации в случае взлома. Это делает передовые методы восстановления данных вашей последней линией защиты. Организации должны изолировать резервные копии от сетевых подключений, регулярно тестировать процедуры резервного копирования и применять передовые методы технологии «воздушного зазора», чтобы гарантировать, что любые данные, затронутые утечкой, могут быть восстановлены с ограниченным нарушением.

Как часто организация должна создавать резервные копии своих данных, зависит от ее миссии. Например, архивные данные, которые не имеют решающего значения для операций миссии, относятся к менее частым потребностям. Но резервные копии для систем, которые необходимы для нашей критической инфраструктуры, таких как общественная безопасность, здравоохранение, финансовые службы и исправительные учреждения, должны поддерживаться как можно чаще. Если эти системы недоступны, влияние на общество в целом может быть ужасным, особенно в то время, когда угрозы со стороны враждебных национальных государств более заметны и обостряются, чем когда-либо прежде.

Организационная кибергигиена имеет основополагающее значение для национальной безопасности. Сейчас, как никогда ранее, нет кибергранespeciallyиц. Примеры продолжающейся агрессии России и Китая требуют бдительности в области кибербезопасности, но наша решимость и сосредоточенность на применении этих оборонительных кибермер укрепят наши организации и обезопасят нашу страну». ***(Sam Kinch. How Russia's War on Ukraine Has Converged Cybersecurity Across Homeland and National Security // Homeland Security Today (https://www.hstoday.us/featured/how-russias-war-on-ukraine-has-converged-cybersecurity-across-homeland-and-national-security/). 08.04.2023).***

***

«Американская служба по надзору за кибербезопасностью не уверена в том, что сотовая сеть, используемая американскими службами экстренного

реагирования и военными, защищена от цифровых вторжений, заявил сенатор США Рон Уайден в письме, опубликованном в среду.

Письмо. от Орегонского демократа, члена комитета по разведке, было адресовано Агентству национальной безопасности (АНБ) и Агентству кибербезопасности и безопасности инфраструктуры (CISA) Это касается FirstNet, специализированной мобильной сети для сотрудников органов общественной безопасности, таких как аварийные работники, пожарные и правоохранительные органы.

В прошлом году неизвестный эксперт CISA сообщил сотрудникам Wyden, что «у них нет уверенности в безопасности FirstNet, в значительной степени потому, что они не видели результатов каких-либо проверок кибербезопасности, проведенных в отношении этой правительственной сети», — говорится в письме. утверждая, что властям пора поделиться своими внутренними аудитами с CISA, NSA и Конгрессом.

CISA отказалась от комментариев, заявив, что ответит Уайдену напрямую. АНБ не сразу ответило на сообщения с просьбой прокомментировать. Сотрудник FirstNet, созданной AT&T Inc (TN), передавал вопросы телекоммуникационной компании, которая, в свою очередь, перенаправляла вопросы руководителю FirstNet. Исполнительный директор не сразу ответил на сообщения поздно вечером во вторник.

В письме Уайдена упоминается Signaling System No. 7 (SS7), протокол с многолетней историей, который позволяет международным сотовым сетям обмениваться информацией, например, когда пользователи сотовых телефонов находятся в роуминге. Эксперты по безопасности говорят, что этим протоколом легко злоупотреблять, позволяя шпионам или хакерам перехватывать текстовые сообщения или определять местонахождение пользователей в реальном времени.

Хотя проблемы с безопасностью SS7 хорошо задокументированы, Уайден сказал об отсутствии ясности в отношении мер безопасности в FirstNet, которая была создана после атак 11 сентября 2001 года, чтобы обеспечить надежную линию связи для служб быстрого реагирования. особенно беспокоило.

«Эти недостатки безопасности также являются проблемой национальной безопасности, особенно если иностранные правительства могут использовать эти недостатки для нападения на сотрудников правительства США», — говорится в его письме.

Гэри Миллер, эксперт по безопасности мобильных сетей из Citizen Lab Университета Торонто, сказал, что опасения Уайдена вполне обоснованы, добавив, что его также беспокоит «крайне тревожная» непрозрачность аудиторских проверок.

Уайден призвал FirstNet сообщать о любых проверках безопасности АНБ и CISA или, в качестве альтернативы, правительству проводить собственные проверки.

Федеральная комиссия по связи, Белый дом и Административно-бюджетное управление — все они были скопированы в письме — не сразу ответили на запросы о комментариях». ***(Raphael Satter. US cyber watchdog has 'no confidence' in security of US emergency cell network – senator // Reuters***

(https://www.reuters.com/world/us/us-cyber-watchdog-has-no-confidence-security-us-emergency-cell-network-senator-2023-04-12/). 12.04.2023).

***

«Атаки на кибербезопасность происходят все чаще и чаще, и они могут быть очень дорогостоящими для бизнеса. В Канаде почти все канадские организации сообщили об атаках кибербезопасности в 2022 году, при этом 25 процентов организаций подвергались как минимум одной атаке в день, а большинство организаций подвергались более чем 11-30 атакам в месяц. Сообщается, что средняя стоимость утечки данных составляет 5,64 миллиона долларов США.

Подготовка к утечке данных — это просто хороший бизнес.

Поддерживать строгие политики и практики конфиденциальности и кибербезопасности

Предприятия могут снизить риски, поддерживая надежные протоколы конфиденциальности. Бизнес должен собирать только ту информацию (включая личную информацию), которая разумно необходима для деловых операций. Доступ к информации должен быть ограничен сотрудниками, подрядчиками и поставщиками услуг, которым доступ к ней необходим для выполнения их обязанностей и ответственности перед организацией. Организации должны регулярно проверять этот доступ. Федеральный комиссар рекомендовал системы безопасности, управления событиями, идентификации пользователей и анализа поведения, в которых компании управляют большими объемами конфиденциальной личной информации. Компании также должны внедрить эффективную политику разделения, хранения и уничтожения данных. Необходимо внедрить протоколы управления уязвимостями, предотвращения потери данных и резервного копирования/аварийного восстановления, а сотрудников следует обучить всем политикам и процедурам.

Поскольку бизнес по-прежнему контролирует и несет ответственность за личную информацию, которая передается стороннему поставщику услуг для обработки, важно реализовать ключевые договорные положения, требующие от третьих сторон использовать и защищать информацию надлежащим образом.

Подготовьте эффективный план реагирования на нарушения

У вашего бизнеса должен быть план реагирования на нарушения. Апелляционный суд Квебека недавно отклонил первый коллективный иск против организации по регулированию инвестиционной индустрии Канады (IIROC) в связи с потерей личной информации тысяч канадских инвесторов в результате утечки данных. Суд рассмотрел действия IIROC после нарушения и пришел к выводу, что он действовал усердно при устранении нарушения. Это решение подчеркивает важность наличия хорошо подготовленного и выполненного плана реагирования на нарушения, который может защитить бизнес от гражданской ответственности, возникающей в результате атаки кибербезопасности или других нарушений данных.

Все сотрудники, подрядчики и соответствующие поставщики услуг должны знать, как выявлять, сообщать и передавать информацию об инциденте. План также

должен включать группу реагирования, которая четко понимает свои роли, контактные телефоны для экстренной помощи для всех в команде и резервные копии для всех членов команды в случае отсутствия. В группу реагирования должны входить члены команды из отдела конфиденциальности, ИТ, ключевые менеджеры, штатные консультанты (если применимо), а также могут входить сотрудники отдела кадров и внешние стороны, такие как страховщики, юрисконсульты, внутренние или внешние судебные эксперты и эксперты по коммуникациям. Регулярный просмотр и тестирование плана может помочь вашему бизнесу заблаговременно выявить слабые места в своей кибербезопасности и укрепить свою защиту. План реагирования необходимо периодически проверять и вносить в него поправки с учетом усовершенствований в технологии и изменений во внутренних процессах.

Уведомление о нарушении

В случае нарушения канадские компании должны оценить, требуется ли уведомление о нарушении в соответствии с применимыми федеральными или провинциальными законами о конфиденциальности. Федеральный закон о защите личной информации и электронных документах (PIPEDA) применяется к предприятиям, занимающимся коммерческой деятельностью по всей Канаде, если только такая деятельность не осуществляется полностью в одной из трех провинций Альберта, Британская Колумбия и Квебек. В этих провинциях действуют собственные законы о конфиденциальности, которые считаются по существу аналогичными PIPEDA. PIPEDA также применяется к федеральным работам, предприятиям и предприятиям, действующим в этих провинциях, таким как банковское дело, железная дорога и телекоммуникации. PIPEDA и аналогичные законы Альберты и Квебека содержат обязательные требования к сообщениям о нарушениях.

Существуют также требования к уведомлению о нарушениях в соответствии с различными провинциальными законами о конфиденциальности и медицинской информации в государственном секторе. Для целей этой статьи мы комментируем только требования к уведомлению о нарушениях в частном секторе.

PIPEDA требует, чтобы бизнес уведомлял Уполномоченного по вопросам конфиденциальности Канады и затронутых лиц о нарушении конфиденциальности, которое представляет «реальный риск причинения значительного вреда» затронутым лицам, как можно скорее. Уведомление должно содержать достаточную информацию, чтобы уполномоченный мог понять значимость нарушения и предпринять шаги для снижения риска причинения вреда. Квебека Закон о защите личной информации в частном секторе и Закон Альберты о защите личной информации (PIPA) имеют схожие требования к уведомлению о нарушении конфиденциальности. Таким образом, о нарушении может потребоваться уведомление в нескольких юрисдикциях с разными требованиями.

Когда кибератака приводит к потере личной информации или несанкционированному доступу или раскрытию личной информации, бизнес должен рассмотреть следующие вопросы, чтобы выполнить требования к уведомлению:

Кто несет ответственность за сообщение о нарушении?

Компании, которые «контролируют» или «владеют» личной информацией, должны сообщить о нарушении федеральному уполномоченному по вопросам конфиденциальности и уполномоченному по вопросам конфиденциальности Альберты или Квебека, если к нарушению причастна личная информация лиц, проживающих в этих провинциях. Когда бизнес передает личную информацию третьей стороне для обработки и происходит нарушение конфиденциальности личной информации, находящейся в распоряжении обработчика, основное предприятие сохраняет контроль над личной информацией и, следовательно, несет ответственность за сообщение о нарушении. Тем не менее, требования законодательства Квебека об уведомлении применяются к любой организации, которая сталкивается с утечкой данных в отношении личной информации, которую организация «хранит», и пока не ясно, будут ли регулирующие органы Квебека проводить такое же различие между контролирующей организацией и обработчиками.

Законы о частном секторе в Канаде могут применяться экстерриториально, если существует реальная и существенная связь с Канадой. Поэтому требования об уведомлении о нарушениях будут применяться к иностранным организациям, которые собрали личную информацию канадцев и пострадали от нарушения, затрагивающего эту информацию.

О каких нарушениях необходимо сообщать?

В соответствии с PIPEDA и Alberta PIPA необходимо сообщать только о нарушениях, которые представляют «реальный риск причинения значительного вреда» (RROSH) физическому лицу. Точно так же новый закон Квебека требует сообщать о нарушениях, которые представляют «риск получения травмы». Реальный риск серьезного вреда может включать телесные повреждения, унижение, ущерб репутации или отношениям, потерю работы, бизнеса или профессиональных возможностей., финансовые потери, кража личных данных, негативные последствия для кредитной записи и повреждение или утрата имущества.

Тест RROSH не имеет четкого определения, но PIPEDA предоставляет несколько общих факторов, которые следует учитывать при определении RROSH. Как правило, он включает такие факторы, как конфиденциальность личной информации и вероятность неправомерного использования этой информации. Конфиденциальная информация обычно включает в себя личные данные, финансовую, медицинскую, трудовую и контактную информацию. Личная электронная почта может считаться конфиденциальной информацией, если она может быть использована злоумышленниками для кражи личных данных. Факторы, которые следует учитывать при рассмотрении вероятности неправомерного использования личной информации, могут включать наличие преднамеренного или злонамеренного намерения (например, кража, взлом) с целью вызвать нарушение, что произошло и насколько вероятно, что кто-то пострадает в результате нарушения, как долго личная информация была раскрыта, сколько элементов личной информации находится под вопросом, и была ли личная информация восстановлена или уничтожена сразу после нарушения.

Согласно PIPEDA и законодательству Квебека, предприятия обязаны вести учет каждого нарушения, даже если оно не подлежит сообщению в соответствии с применимым тестом.

Как уведомляются затронутые лица?

Когда происходит утечка данных, PIPEDA требует, чтобы бизнес уведомлял пострадавших лиц как можно скорее, если утечка представляет «реальный риск причинения значительного вреда» этим лицам. Аналогичное требование содержится в новом законе Квебека. В Альберте, после того как компания уведомляет уполномоченного по вопросам конфиденциальности Альберты о нарушении, уполномоченный может потребовать от компании уведомить отдельных лиц. На самом деле, согласно Отчету о нарушениях PIPA Альберты за 2022 год, 80 процентов предприятий уже уведомили пострадавших лиц на момент сообщения о нарушении Уполномоченному.

Уведомления о нарушении для затронутых лиц должны содержать достаточную информацию, чтобы позволить людям понять значимость нарушения для них и предпринять шаги для уменьшения вреда.

Бизнес может рассмотреть возможность предоставления пострадавшим лицам услуг кредитного мониторинга, услуг по защите от кражи личных данных и другой информации и ресурсов, чтобы снизить риск причинения вреда.

Каков штраф, если бизнес не отчитывается?

В соответствии с законодательством Квебека, компания, которая не сообщит о нарушении уполномоченному по вопросам конфиденциальности или пострадавшему лицу, может быть оштрафована на сумму до 25 миллионов долларов США или 4 процента от ее мирового дохода или денежного административного штрафа в размере до 10 миллионов долларов США или 2 процентов от ее мировой доход.

В 2022 году федеральное правительство представило законопроект C-27 «Закон о внедрении цифровой хартии 2022 года» (DCIA), который заменит PIPEDA более надежными законами о конфиденциальности и защите данных. Он также создаст новый Трибунал по защите личной информации и данных и риск значительных административных денежных штрафов или уголовных штрафов за нарушения или правонарушения в отношении неприкосновенности частной жизни. Законопроект в настоящее время находится на стадии второго чтения в Палате общин и подлежит обсуждению, внесению поправок и дальнейшему изучению, прежде чем он может быть принят в качестве закона.

Если DCIA будет принято, несообщение о нарушениях Уполномоченному по конфиденциальности может привести к максимальным штрафам в размере 25 миллионов долларов или пяти процентов валового глобального дохода. Затронутые лица могут иметь частное право на иск, если уполномоченный по вопросам конфиденциальности обнаружит, что бизнес не внедрил соответствующие протоколы безопасности…» ***(Keri Bennett, David Spratley. Privacy and cybersecurity in Canada: What every business needs to know // DLA Piper (https://www.dlapiper.com/en-ca/insights/publications/2023/04/privacy-and-cybersecurity-in-canada). 12.04.2023).***

***

«В рамках усилий правительства по «перераспределению» ответственности в киберпространстве, описанных в Национальной стратегии кибербезопасности, правительство Соединенных Штатов 13 апреля выпустило важный документ в партнерстве с несколькими союзными правительствами, призывающий к серьезным изменениям в способах создания и управления технологиями. В разделе «Изменение баланса рисков кибербезопасности: принципы и подходы к безопасности по умолчанию и безопасности по умолчанию» CISA, ФБР и АНБ сотрудничают с другими агентствами национальной безопасности и регулирующими органами, чтобы предложить рекомендации для частного сектора. Пятнадцатистраничный документ в некоторых местах предполагает, что частный сектор делает недостаточно, и излагает новые ожидания в отношении развертывания исправлений и обновлений.

Документ начинается с критики существующего положения вещей, в котором говорится, что «производители технологий полагались на исправление уязвимостей, обнаруженных после того, как клиенты развернули продукты, требуя, чтобы клиенты применяли эти исправления за свой счет». Эти правительства призывают производителей «взять на себя ответственность за улучшение результатов безопасности своих клиентов», чтобы «разорвать порочный круг создания и применения исправлений». Эти правительства «настоятельно рекомендуют каждому производителю технологий создавать свои продукты таким образом, чтобы клиентам не приходилось постоянно выполнять мониторинг, регулярные обновления и контроль повреждений в своих системах для смягчения последствий кибервторжений».

Документ предлагает операционные и управленческие рекомендации, основанные на идее о том, что «бремя безопасности не должно ложиться исключительно на клиента» и что пришло время «принять радикальную прозрачность и подотчетность». Неясно, проводят ли эти регулирующие органы различие между розничными конечными пользователями «клиентами» и крупными предприятиями и коммерческими клиентами, поскольку некоторые из их рекомендаций, особенно в разделе «безопасность по умолчанию», по-видимому, по-разному применяются к разным типам клиентов.

«Безопасность по умолчанию» предполагает, что провайдеры должны управлять, а в некоторых случаях и отменять выбор безопасности клиентов.

Среди прочего, предложенного в документе, агентства определяют «безопасные по умолчанию конфигурации», которые производители должны соблюдать в новых продуктах, и они «должны стремиться обновлять продукты, чтобы они соответствовали этим практикам по мере их обновления». Цель этих методов — защитить пользователей, сведя к минимуму шаги, которые они — в отличие от разработчиков — должны предпринять. Несколько примеров показывают, как много эти правительства ожидают от поставщиков.

Удалите пароли по умолчанию. Авторы рекомендуют, чтобы «продукты требовали от администраторов установки надежного пароля во время установки и настройки» и чтобы многофакторная аутентификация (MFA) была обязательной для привилегированных пользователей.

Безопасное ведение журнала. Производители должны «предоставлять высококачественные журналы аудита клиентам без дополнительной оплаты».

Профиль авторизации программного обеспечения. «Поставщики программного обеспечения должны предоставлять рекомендации по авторизованным ролям профиля и их назначенному варианту использования. Производители должны включать визуальное предупреждение, которое уведомляет клиентов о повышенном риске, если они отклоняются от рекомендуемой авторизации профиля.

Отдавайте приоритет «дальновидной безопасности, а не обратной совместимости». Отдавайте предпочтение безопасности, а не обратной совместимости, «предоставляя командам безопасности возможность удалять небезопасные функции, даже если это означает внесение критических изменений».

Отслеживайте и уменьшайте размер «руководства по отверждению». «Агентства-разработчики признают, что сокращенные руководства по укреплению безопасности являются результатом постоянного партнерства с существующими клиентами и включают в себя усилия многих групп разработчиков, включая взаимодействие с пользователем (UX)». Но агентства призывают сокращать и упрощать эти документы, поскольку все больше вещей становится стандартными и обязательными.

Учитывайте влияние настроек безопасности на взаимодействие с пользователем. «Каждая новая настройка увеличивает когнитивную нагрузку на конечных пользователей и должна оцениваться в сочетании с выгодой для бизнеса, которую она приносит».

Агентства признают, что эти изменения могут быть разрушительными, но выражают надежду на то, что поставщики программного обеспечения могут заставить или подтолкнуть своих клиентов.

«Хотя вклад клиентов важен, авторские агентства наблюдали важные случаи, когда клиенты не желали или не могли принимать улучшенные стандарты, часто сетевые протоколы. Для производителей важно создать значимые стимулы для клиентов, чтобы они оставались в курсе событий и не позволяли им оставаться уязвимыми на неопределенный срок».

Документ не касается договорного распределения ответственности или обязанностей.

Безопасные по дизайну шаги включают в себя новые кибер-цели США

В документе также определяется тактика «Безопасность по дизайну» и рекламируется полезность «Структуры безопасной разработки программного обеспечения (SSDF), также известной как Национальный институт стандартов и технологий (NIST) SP 800-218, является основным набором безопасные методы разработки программного обеспечения высокого уровня, которые можно интегрировать на каждом этапе жизненного цикла разработки программного обеспечения (SDLC)». Он предоставляет «неполный список иллюстративных передовых практик дорожной карты».

Примечательно, что в рамках текущей работы в Соединенных Штатах документ призывает разработчиков «удовлетворить цели киберпроизводства (CPG)», созданные DHS CISA. Он призывает «[d]разрабатывать продукты,

отвечающие основным принципам безопасности. Цели эффективности кибербезопасности CISA определяют фундаментальные базовые меры кибербезопасности, которые должны реализовать организации». Таким образом, эта рекомендация включает в себя CPG, которые были разработаны для критической инфраструктуры (CI), постоянно обсуждаются и пересматриваются и еще не адаптированы для секторов CI.

Сильная зависимость документа от публикаций США предполагает успешную пропагандистскую деятельность Соединенных Штатов в целях содействия гармонизации и более широкому глобальному использованию национальных структур. Это хорошая новость, как и успешное глобальное внедрение NIST Framework для улучшения кибербезопасности критической инфраструктуры.

Несколько примечательных дополнительных примеров тактики «Secure-by-Design» из документа:

Обзор кода. «Стремитесь к тому, чтобы код, отправленный в продукты, прошел экспертную оценку другими разработчиками, чтобы обеспечить более высокое качество».

Спецификация программного обеспечения (SBOM): «Включите создание SBOM3, чтобы обеспечить видимость набора программного обеспечения, которое входит в продукты».

Программы раскрытия уязвимостей: «Создайте программы раскрытия уязвимостей, которые позволят исследователям в области безопасности сообщать об уязвимостях и получать при этом законную безопасную гавань. В рамках этого поставщики должны установить процессы для определения основных причин обнаруженных уязвимостей. Такие процессы должны включать в себя определение того, предотвратило бы внедрение какой-либо из описанных в этом документе практик безопасного проектирования (или других подобных практик) появление уязвимости».

Полнота CVE: «Убедитесь, что опубликованные CVE включают основную причину или общее перечисление слабых мест (CWE), чтобы обеспечить общеотраслевой анализ основных причин безопасности программного обеспечения».

Безопасные для памяти языки программирования.

Защищенные программные компоненты: «Приобретайте и поддерживайте хорошо защищенные программные компоненты (например, программные библиотеки, модули, промежуточное ПО, фреймворки) от проверенных коммерческих разработчиков, разработчиков с открытым исходным кодом и других сторонних разработчиков для обеспечения надежной безопасности потребительских программных продуктов».

В той мере, в какой американские предприятия готовы использовать Secure Software Development Framework (SSDF) в NIST SP 800-218, а также другие инновации, продвигаемые в правительстве, этот документ предполагает, что они могут получить поддержку и за рубежом.

Что дальше?

Этот документ отличается широким кругом международных авторов, чьи правовые и нормативные системы различаются. Кроме того, судя по всему, общественность не оказала большого влияния, несмотря на то, что предполагалось резкое изменение ожиданий в частном секторе.

Соединенные Штаты продвигаются вперед полным ходом, чтобы реализовать Национальную стратегию кибербезопасности и выполнить несколько исполнительных указов. Сама Стратегия призывала к изменениям в разработке программного обеспечения путем введения ответственности. Этот документ не идет так далеко, но он, вероятно, будет использоваться для призыва к дальнейшим нормативным и правовым изменениям…» ***(Megan L. Brown. The US Government is Working Globally to Shift Cyber Duties: New Report Shows Ambitious Goals // Wiley Rein LLP (https://www.wileyconnect.com/the-us-government-is-working-globally-to-shift-cyber-duties-new-report-shows-ambitious-goals). 13.04.2023).***

***

«15 марта 2023 года Комиссия по ценным бумагам и биржам («SEC») предложила три новых свода правил («Предлагаемые правила»), которые, в случае их принятия, потребуют от различных компаний усиления своей политики кибербезопасности и процедур уведомления об утечке данных. По словам председателя SEC Гэри Генслера, предлагаемые правила направлены на содействие «киберустойчивости» в поддержку «ответственности SEC за помощь в защите финансовой стабильности».

В частности, SEC предложила:

Поправки к Регламенту SP, которые, среди прочего, требуют от брокеров-дилеров, инвестиционных компаний и зарегистрированных инвестиционных консультантов принятия письменных политик и процедур реагирования на утечку данных и предоставления уведомления лицам, «с разумной вероятностью» затронутым в течение тридцати через несколько дней после того, как стало известно, что инцидент имел место с «достаточной вероятностью» («Предлагаемые поправки к Reg SP»).

Новые требования к ряду «Субъектов рынка» (включая брокеров-дилеров, клиринговые агентства и национальные биржи ценных бумаг), среди прочего: (i) внедрять политики и процедуры в отношении рисков кибербезопасности; (ii) ежегодно оценивать дизайн и эффективность этих политик и процедур; и (iii) уведомлять SEC и общественность о любом «значительном инциденте кибербезопасности» («Предлагаемое правило управления рисками кибербезопасности»).

Поправки к Регламенту «Соответствие и целостность систем» («Reg SCI») для расширения объектов, подпадающих под действие Reg SCI («Субъекты SCI»), и добавления дополнительных требований к безопасности данных и уведомлению для Субъектов SCI («Предлагаемые поправки к Регламенту SCI»).

Как заметила комиссар Эстер Пирс, каждое предлагаемое правило «накладывается и пересекается с каждым из других, а также с другими существующими и предлагаемыми правилами». Таким образом, хотя каждое из

предлагаемых правил относится к схожим целям кибербезопасности, каждое из них необходимо рассматривать по очереди, чтобы определить, распространяется ли действие на конкретную компанию и какие шаги необходимо будет предпринять компании, если предлагаемые правила станут окончательными.

Ниже мы более подробно обсудим каждый набор предлагаемых правил и предоставим некоторые выводы и советы по обеспечению готовности к кибербезопасности независимо от отрасли.

Предлагаемые поправки к Reg SP

Reg SP, принятый в 2000 году, требует, чтобы брокеры, дилеры, инвестиционные компании и зарегистрированные инвестиционные консультанты приняли письменные правила и процедуры, касающиеся защиты и уничтожения записей и информации о клиентах. Но, как пояснил председатель Генслер в заявлении в поддержку предлагаемых поправок к Reg SP, «[t] хотя действующее правило требует, чтобы страховые фирмы уведомляли клиентов о том, как они используют свою финансовую информацию, эти фирмы не обязаны уведомлять клиентов о нарушениях», а Предлагаемые поправки к Reg SP призваны «устранить этот пробел».

В частности, «[хотя] в последние годы все 50 штатов приняли законы, требующие от фирм уведомлять отдельных лиц об утечках данных, стандарты различаются в зависимости от штата, при этом некоторые штаты вводят повышенные требования к уведомлению по сравнению с другими штатами», и SEC стремится через Предлагаемые поправки к Reg SP, чтобы обеспечить «минимальный федеральный стандарт для уведомления клиентов» для организаций, на которые распространяется действие. Это включает определение «конфиденциальной информации о клиентах», которое шире, чем то, которое используется как минимум в 12 штатах; 30-дневный крайний срок уведомления, что короче, чем сроки, установленные в настоящее время в 15 штатах (плюс 32 штата, которые не устанавливают крайний срок уведомления или не разрешают отсроченные уведомления для правоохранительных целей); и обязательное уведомление, если охватываемое учреждение не обнаруживает риска причинения вреда, в отличие от 21 штата, которые требуют уведомления только в том случае, если после расследования охваченное учреждение обнаруживает риск причинения вреда.

Кроме того, в то время как Reg SP в настоящее время применяется к брокерам-дилерам, инвестиционным компаниям и зарегистрированным инвестиционным консультантам, предлагаемые поправки к Reg SP расширят сферу действия на трансферных агентов. Он также будет применять правила защиты и уничтожения информации о клиентах к информации о клиентах, которую охватываемое учреждение получает от других финансовых учреждений, и к более широкому набору информации путем нового определения термина «информация о клиенте», который для агентов, не являющихся агентами по передаче, «включать любую запись, содержащую «непубличную личную информацию» (как определено в Регламенте SP) о «клиенте финансового учреждения», будь то в бумажной, электронной или другой форме, которая обрабатывается или поддерживается охватываемым учреждением или от его имени», и для трансфер-агентов, которые

«обычно не имеют потребителей или клиентов» для целей Reg SP, будет иметь аналогичное определение в отношении «любого физического лица, которое является держателем ценных бумаг эмитента, для которого действует или действовал трансфер-агент». в качестве трансфер-агента, который обрабатывается или поддерживается трансфер-агентом или от его имени».

Предлагаемое правило управления рисками кибербезопасности

Предлагаемое правило управления рисками кибербезопасности повлияет на множество «различных типов организаций, выполняющих различные функции» на финансовых рынках, определяемых как «Субъекты рынка», включая «брокеров-дилеров, брокеров-дилеров, которые управляют альтернативной торговой системой, клиринговые агентства, основные участники свопов на основе ценных бумаг, Муниципальный совет по разработке правил по ценным бумагам, национальные ассоциации ценных бумаг, национальные биржи ценных бумаг, хранилища данных о свопах на основе ценных бумаг, дилеры по свопам на основе ценных бумаг и трансфер-агенты».

Как пояснил председатель Генслер, Предлагаемое правило управления рисками кибербезопасности предназначено для «решения проблемы кибербезопасности субъектов рынка финансового сектора», среди прочего, требуя от субъектов рынка принятия письменных политик и процедур для устранения своих рисков кибербезопасности, чтобы уведомить SEC о значительных киберинцидентов, и, за исключением более мелких брокеров-дилеров, обнародовать краткое описание рисков кибербезопасности, которые могут существенно повлиять на организацию, и значительных инцидентов кибербезопасности в текущем или предыдущем календарном году.

Согласно SEC, эти политики и процедуры «не предназначены для навязывания универсального подхода к устранению рисков кибербезопасности» и предназначены для предоставления субъектам рынка «гибкости для обновления и изменения своих политик и процедур по мере необходимости». Однако существуют определенные минимальные политики и процедуры, которые потребуются, такие как периодическая оценка рисков кибербезопасности, средства контроля, предназначенные для минимизации рисков, связанных с пользователями, и предотвращения несанкционированного доступа к системе, периодическая оценка информационных систем, надзор за поставщиками услуг, которые получают, хранят или обрабатывают информацию организации (включая письменные контракты между организацией и ее поставщиками услуг), меры, предназначенные для обнаружения, смягчения и устранения угроз кибербезопасности. и уязвимости, меры, предназначенные для обнаружения инцидентов кибербезопасности, реагирования на них и восстановления после них, и ежегодный обзор структуры и эффективности политик и процедур кибербезопасности (с письменным отчетом). Для большинства регулируемых организаций такие меры уже действуют.

Предлагаемые поправки к Reg SCI

Наконец, SEC предложила поправки к Reg SCI, правилу, принятому в 2014 году, чтобы «укрепить технологическую инфраструктуру рынков ценных бумаг США, уменьшить возникновение системных проблем на этих рынках, повысить их

отказоустойчивость при возникновении технологических проблем и установить обновленную и формализованная нормативная база» для надзора SEC за этими системами. Reg SCI применяется к «Организациям SCI», к которым относятся саморегулируемые организации, некоторые крупные Альтернативные торговые системы и некоторые другие участники рынка, которые, как считается, обладают «потенциалом влияния на инвесторов, рынок в целом или торговлю отдельными ценными бумагами при возникновении определенных типов системных проблем».

Предлагаемые поправки к Reg SCI расширят определение субъекта SCI, включив в него зарегистрированные репозитории данных о свопах на основе безопасности, зарегистрированных брокеров-дилеров, размеры которых превышают пороговое значение, и дополнительные клиринговые агентства, освобожденные от регистрации. Они также расширят требования, которым подчиняются организации SCI, в том числе обязательное уведомление SEC и затронутых лиц о любых «вторжениях в системы», которые будут включать «ряд событий кибербезопасности».

Выводы

Хотя предлагаемые правила еще не приняты, компании, которые могут быть охвачены, должны воспользоваться возможностью пересмотреть свои методы и политики в области кибербезопасности, чтобы максимально снизить риск кибератаки и быть готовыми к ее устранению. атака, в том числе соблюдение всех требований к уведомлению, если таковая произойдет.

Среди прочего, передовой опыт включает в себя:

Письменная оценка кибер-рисков, которая классифицирует и приоритизирует кибер-риски на основе инвентаризации компонентов информационных систем, включая тип информации, находящейся в сети, и потенциальное влияние инцидента кибербезопасности;

Оценка уязвимости кибербезопасности для оценки угроз и уязвимостей; определять отклонения от допустимых конфигураций, корпоративной или локальной политики; оценить уровень риска; и разработать и/или рекомендовать соответствующие контрмеры по смягчению последствий как в рабочих, так и в нерабочих ситуациях;

Письменный план реагирования на инциденты, определяющий, как компания будет реагировать и восстанавливаться после инцидента кибербезопасности, включая время и способ сообщения о таком инциденте регулирующим органам, лицам или другим организациям;

План обеспечения непрерывности бизнеса, разработанный для разумного обеспечения непрерывности операций при столкновении с инцидентом кибербезопасности и сохранения доступа к информации;

Кабинетные учения по анализу и тестированию планов реагирования на инциденты и обеспечения непрерывности бизнеса;

Ежегодный обзор политик и процедур.

В качестве следующего шага каждое из предлагаемых правил будет опубликовано в Федеральном реестре и открыто для комментариев в течение шестидесяти дней после публикации. Независимо от того, будут ли приняты предлагаемые правила, они отражают растущую осведомленность Комиссии по

ценным бумагам и биржам об инцидентах кибербезопасности и желание их смягчить, и компании должны быть соответствующим образом подготовлены». ***(Tracee E. Davis, Daphne Morduchowitz, Scott Carlson, Matthew Catalano. SEC Proposes Sweeping New Cybersecurity Rules: Is Your Company Prepared? // Seyfarth Shaw LLP (https://www.seyfarth.com/news-insights/sec-proposes-sweeping-new-cybersecurity-rules-is-your-company-prepared.html). 10.04.2023).***

***

«В ответ на крупные кибератаки, вызванные недостатками безопасности программного обеспечения, такими как взлом SolarWinds, администрация Байдена готовится принять жесткие меры в отношении поставщиков программного обеспечения, которые распространяют продукты с недостатками безопасности, которые делают клиентов уязвимыми для кибератак.

Одной из целей администрации, как указано в ее Национальной стратегии кибербезопасности от марта 2023 года, является разработка законодательства для переноса ответственности за кибератаки на компании-разработчики программного обеспечения, которые «не принимают разумных мер предосторожности для защиты своего программного обеспечения» и предотвращения компаниям, обладающим влиянием на рынке, полностью отказаться от ответственности по контракту. Заявленная цель администрации состоит в том, чтобы «подтолкнуть рынок к производству более безопасных продуктов и услуг, сохраняя при этом инновации и способность стартапов и других малых и средних предприятий конкурировать с лидерами рынка».

Администрация планирует включить «безопасную гавань», которая защищает компании от ответственности, если они предпримут разумные шаги для «безопасной разработки и обслуживания своих программных продуктов и услуг». Безопасная гавань предположительно потребует лучших практик, которые аналогичны тем, которые включены в платформу разработки безопасного программного обеспечения Национального института стандартов и технологий (NIST) и будут развиваться с течением времени. Это действие будет стимулировать разработчиков программного обеспечения следовать принципам безопасности при разработке и выполнять предварительное тестирование, что приведет к повышению уровня безопасности как для потребителей, так и для бизнеса.

Администрация намерена преобразовать эти предложения в законодательство при содействии как Конгресса, так и частного сектора. Тем временем разработчики программного обеспечения должны рассмотреть возможность оценки и обновления своих продуктов и внимательно следить за тем, какие шаги потребуются для создания безопасных продуктов и снижения ответственности за кибератаки. Субъектам, покупающим программные продукты, также следует обратить внимание, поскольку они могут потребовать компенсацию от разработчиков программного обеспечения за кибератаки». ***(Kathleen McGee, Ken Fishkin, Mikayla Berliner. Biden Administration Aims to Shift Liability for Cyberattacks to Software Developers // NYU Law's Program on Corporate Compliance and Enforcement***

(https://wp.nyu.edu/compliance_enforcement/2023/04/12/biden-administration-aims-to-shift-liability-for-cyberattacks-to-software-developers/). 12.04.2023).

***

«Администрация Байдена опубликовала свою обновленную Национальную стратегию кибербезопасности в начале марта — и хотя это первая стратегия Байдена, это третья стратегия кибербезопасности, выпущенная США в этом столетии. И это, вероятно, будет иметь самые реальные последствия.

В отличие от киберстратегий прошлого, в этой последней за успех непосредственно отвечают несколько групп и секторов. Он указывает на одного высокопоставленного государственного чиновника, который должен будет отвечать за его реализацию и успех. Национальный директор по кибербезопасности будет нести ответственность за обеспечение контроля и измерения реализации, за то, чтобы межведомственные группы работали в ногу, а федеральное правительство располагало ресурсами и разрешениями, необходимыми для реализации стратегии.

Это большая задача: Крис Инглис недавно ушел с этой должности спустя чуть менее двух лет, и хотя Кемба Уолден заменяет исполняющую обязанности официального лица, президент Байден, надеюсь, в ближайшие недели назначит постоянного директора, будь то Уолден или кто-то еще.

Повышенная ответственность технологического сектора

Еще одна цель — возложить повышенную ответственность на технологический сектор в целом, в том числе возложить на поставщиков критически важного оборудования и программного обеспечения ответственность за создание более безопасных продуктов. В рамках обнародованной стратегии администрация обязалась работать как с Конгрессом, так и с частным сектором над «разработкой законодательства, устанавливающего ответственность за программные продукты и услуги» — усилия, которые наверняка вызовут разногласия в нынешнем Конгрессе.

По праву, стратегия администрации Байдена фокусируется на критической инфраструктуре и, делая шаг вперед по сравнению с предыдущими киберстратегиями, связывает соблюдение кибертребований с финансированием инвестиций в инфраструктуру. Эти средства «могут привлечь инвестиции в критически важные продукты и услуги, которые являются безопасными и отказоустойчивыми по своей конструкции, а также поддерживать и стимулировать безопасность и отказоустойчивость на протяжении всего жизненного цикла критически важной инфраструктуры», — говорится в стратегии.

Реализация этого будет непростой задачей, поскольку для достижения конечной цели различных государственных учреждений потребуется связать требования к финансированию с продемонстрированными кибер-методами.

Сосредоточьтесь на реализации в масштабах всего сообщества

В то время как обнародованная стратегия содержала много ожидаемых элементов, администрация Байдена ясно дала понять одну вещь: основное внимание будет уделяться реализации в масштабах всего сообщества не только для

еще не назначенного национального директора по кибербезопасности, но и для законодательных органов, политиков и технологические компании.

Даже в отдельных компаниях существует тенденция возлагать ответственность за кибербезопасность на всех, но не всегда существует общая ответственность. Эта стратегия направлена на поощрение участия всех участников: тех, кто разрабатывает технологию, тех, кто находится в цепочке поставок до конечного пользователя, тех, кто создает мандаты и стимулы, и, наконец, финансовый рынок. Этот многоаспектный подход, несомненно, даст более последовательные и оптимизированные результаты, но для этого потребуется реальное сотрудничество и общение.

Наконец, стратегия ориентирована на регулирование, поскольку без стратегического управления по всем направлениям изменения были непредсказуемыми. В то время как разрешение добровольных подходов привело к улучшениям, «отсутствие обязательных требований привело к неадекватным и непоследовательным результатам», говорится в стратегии.

С точки зрения политики, это самая сильная позиция по регулированию киберпространства, которую правительство США приняло за более чем десятилетие, и реализовать ее будет непросто. Республиканская палата представителей избегает регулирования, и добиться надлежащего согласования с палатой будет сложно, особенно по таким темам, как привлечение технологических компаний к ответственности и связь соблюдения требований с федеральным финансированием.

Таким образом, остается вопрос: не слишком ли смелая стратегия Байдена сработает? Получить одобрение от политиков (включая Палату представителей) и координировать постоянную прозрачность и связь между государственным и частным секторами — и все это при новом директоре — далеко не просто.

Но, учитывая высокие ставки — киберпреступники постоянно развиваются и переходят к использованию оружия для своих атак — правительства должны провести четкую черту на песке и реализовать смелые стратегии. Если все заинтересованные стороны смогут работать над тем, чтобы эта стратегия была успешной, наша страна от этого выиграет». ***(Bob Kolasky. Biden's cybersecurity strategy is bold, but it may get held up in Congress // VentureBeat (https://venturebeat.com/security/bidens-cybersecurity-strategy-is-bold-but-it-may-get-held-up-in-congress/). 23.04.2023).***

***

«Двухпартийная группа федеральных законодателей вновь приняла закон, который, по их мнению, усилит кибербезопасность в школах.

Закон об усилении кибербезопасности K-12 предоставит школам и округам лучший доступ к ресурсам кибербезопасности и улучшит отслеживание кибератак K-12 на национальном уровне. Спонсорами законопроекта являются представители Дорис Мацуи, штат Калифорния, и Зак Нанн, штат Р-Айова, а также сенаторы Марша Блэкберн, штат Теннесси, и Марк Уорнер, штат Вирджиния.

Предложение приходит как кибератаки ориентация на школы становится все более распространенной и сложной. По данным некоммерческой организации K12

Security Information Exchange (K12 SIX), которая помогает школам предотвращать кибератаки, в период с 2016 по 2022 год было зарегистрировано 1619 публично раскрытых кибер-инцидентов. Хакеры атаковали районы всех размеров, в том числе Объединенный Лос-Анджелес., второй по величине в стране.

«Киберпреступники быстро развивают свои стратегии, чтобы вызвать хаос и разрушение, но нехватка ресурсов для наших школ вынуждает их делать больше с меньшими затратами», — сказал Мацуи, высокопоставленный член подкомитета по коммуникациям и технологиям Палаты представителей по энергетике и торговле. заявление. «Закон об усилении кибербезопасности K-12 создаст важную дорожную карту для подготовки нашей киберинфраструктуры K-12 к будущим атакам».

Закон предписывает федеральному агентству кибербезопасности и безопасности инфраструктуры (CISA) создать реестр инцидентов кибербезопасности для отслеживания инцидентов кибератак на школы K-12. Отправка информации об инцидентах в реестр будет добровольной, и эта информация будет использоваться для проведения анализа тенденций, повышения осведомленности и разработки стратегий предотвращения инцидентов и реагирования на них.

«Есть много очень веских причин, по которым мы хотим, чтобы школьные системы делились информацией о своем опыте в области кибербезопасности», — сказал Дуг Левин, национальный директор K12 SIX. Он информирует политиков, помогает правоохранительным органам, помогает другим школьным системам защищаться от подражательных атак и информирует общественность в случае несанкционированного доступа к конфиденциальным данным.

Хотя «режимы добровольной отчетности не являются чем-то необычным, неизвестно, насколько эффективными они могут быть», — сказал Левин. «Если нет прямого возврата к организации, которая представляет эту информацию, это просто похоже на нефинансируемый мандат. Если данные попадают в черную дыру и если они не видят пользы, может быть трудно убедить людей выполнять эту работу».

По словам Левин, наличие систем добровольной отчетности также означает, что округа могут занижать информацию об инцидентах.

В некоторых штатах, таких как Нью-Йорк и Техас, школы K-12 обязаны сообщать об утечках данных и кибератаках. И федеральный отчет об инциденте кибербезопасности закон, принятый в 2022 году, может включать школы в число организаций, которые должны отчитываться, но, по словам Левина, он все еще находится в процессе разработки правил.

Закон об усилении кибербезопасности K-12 также учредит программу, которая будет финансироваться до 20 миллионов долларов в течение двух финансовых лет, которая поможет округам устранять риски и угрозы кибербезопасности для их информационных систем и сетей.

Законодательство также предписывает CISA создать систему обмена информацией о кибербезопасности для публикации информации, передового опыта и предоставления возможностей для повышения кибербезопасности.

«Эти [20 миллионов долларов] — капля в море с точки зрения потребности. Я бы, конечно, не сказал, что этого достаточно», — сказал Левин. «Но если

инвестировать разумно на национальном уровне, это может иметь огромное значение».

Законопроект был впервые внесен в Палату представителей США в 2021 году при поддержке обеих партий. Хотя это не продвинулось, Конгресс вместо этого принял Закон о кибербезопасности K-12, который обязал CISA опубликовать отчет о рисках, с которыми сталкиваются школы K-12, а также рекомендации и ресурсы, чтобы помочь школам снизить риски и поддерживать устойчивые программы кибербезопасности.

CISA Отчет был опубликован в январе и показал, что сектор K-12 становится все более уязвимым и нуждается в помощи. Агентство рекомендовало принять эффективные меры безопасности, устранить нехватку ресурсов и сосредоточиться на сотрудничестве.

Образовательные организации, такие как Государственная ассоциация директоров по образовательным технологиям и Консорциум школьных сетей, поддержали законопроект…» ***(Lauraine Langreo. Schools Are Major Targets of Cyberattacks. A Bipartisan Effort in Congress Aims to Help // Education Week (https://www.edweek.org/technology/schools-are-major-targets-of-cyberattacks-a-bipartisan-effort-in-congress-aims-to-help/2023/04). 20.04.2023).***

***

Країни ЄС та Великобританія

«Европейский комиссар по внутреннему рынку Тьерри Бретон объявил о проекте выявления киберугроз Европейскому Союзу и противодействии им, на который будет израсходовано более 1 млрд евро.

«Наша цель — создать «европейский киберщит», который позволит гораздо лучше выявлять кибератаки на высшем уровне. Сегодня между началом распространения вредоносного программного обеспечения и началом атаки может пройти до 190 дней», — пояснил еврокомиссар в интервью изданию Les Echos.

Бретон добавил, что инвестиции в «киберщит» ЕС составят более 1 млрд евро, две трети из которых будут выделены из европейского бюджета.

В интервью французскому каналу LCI Бретон анонсировал создание нескольких оперативных центров для усиления кибербезопасности государств-членов.

«В результате в Украине количество кибератак в Европе в прошлом году возросло на 140%. В этом контексте объединение и координация наших сил на европейском уровне становится более необходимым, чем когда-либо, поскольку угроза будет расти», — подчеркнул еврокомиссар.

«По стечению обстоятельств, эта активность растет в странах, отправляющих оружие в Украину», — добавил он.

В середине апреля Европейская Комиссия также должна представить Акт о киберсолидарности, который будет предусматривать ответные действия на кибератаку государств-членов Европейского Союза». ***(Евросоюз выделит более 1 млрд евро на проект обнаружения киберугроз // Укррудпром***

(https://ukrrudprom.com/news/Evrosoyuz_videlit_bolee_1_mlrd_evro_na_proekt_obnarugeniya_kiberugroz.html). 06.04.2023).

***

«Європейська комісія оголосила про план протидії зростаючим загрозам для кібербезпеки вартістю 1,1 мільярда євро, підкресливши все більше занепокоєння з приводу серії гучних хакерських атак…

Для швидкого та ефективного виявлення основних кіберзагроз Єврокомісія пропонує створити «Європейський кіберщит» – загальноєвропейську інфраструктуру, що складається з національних і транскордонних оперативних центрів безпеки (SOC) по всьому ЄС.

Це організації, на які покладено завдання виявляти кіберзагрози і реагувати на них. Вони використовуватимуть найсучасніші технології, такі як штучний інтелект (ШІ) і передовий аналіз даних, для виявлення і своєчасного попередження про кіберзагрози та інциденти на транскордонному рівні. Своєю чергою, органи влади і відповідні організації зможуть більш ефективно і оперативно реагувати на серйозні інциденти.

Ці центри можуть запрацювати на початку 2024 року. На підготовчому етапі створення «Європейського кіберщита» у квітні 2023 року Комісія в рамках програми «Цифрова Європа» відібрала три консорціуми транскордонних оперативних центрів безпеки (SOC), що об'єднують державні органи з 17 країн-членів ЄС та Ісландії.

Механізм реагування на кібернетичні надзвичайні ситуації перевірятиме організації в таких критично важливих секторах, як охорона здоров'я, транспорт та енергетика, на предмет потенційної вразливості.

План також передбачає створення Резерву кібербезпеки ЄС, що складається зі служб реагування на інциденти, які втручатимуться на прохання країни або установи ЄС у разі значного або масштабного інциденту в сфері кібербезпеки.

Загальний бюджет усіх заходів, передбачених Актом ЄС про кіберсолідарність, становить 1,1 мільярда євро, з яких близько 2/3 буде профінансовано Євросоюзом через програму «Цифрова Європа»…» ***(Єврокомісія запропонувала створити «Європейський кіберщит» вартістю 1,1 млрд євро // Європейська правда (https://www.eurointegration.com.ua/news/2023/04/19/7160105/). 19.04.2023).***

***

«Сегодня Комиссия приняла предложение о Законе ЕС о киберсолидарности для укрепления потенциала кибербезопасности в ЕС. Он будет поддерживать обнаружение и информирование об угрозах и инцидентах кибербезопасности, повышать готовность критически важных объектов, а также укреплять солидарность, согласованное управление кризисами и возможности реагирования в государствах-членах. Закон о киберсолидарности устанавливает возможности ЕС, чтобы сделать Европу более устойчивой и реактивной перед киберугрозами, укрепляя при этом существующий механизм сотрудничества. Это будет способствовать обеспечению безопасного и надежного цифрового ландшафта

для граждан и предприятий, а также защите критически важных объектов и основных служб, таких как больницы и коммунальные службы.

Комиссия также представила Академию навыков кибербезопасности в рамках Европейского года навыков 2023 года, чтобы обеспечить более скоординированный подход к сокращению нехватки кадров в области кибербезопасности, что является необходимым условием для повышения устойчивости Европы. Академия объединит различные существующие инициативы, направленные на развитие навыков кибербезопасности, и сделает их доступными на онлайн-платформе, тем самым повысив их узнаваемость и увеличив количество квалифицированных специалистов по кибербезопасности в ЕС.

В рамках Европейского союза безопасности ЕС стремится обеспечить надежную защиту всех европейских граждан и предприятий как в Интернете, так и в автономном режиме, а также продвигать открытое, безопасное и стабильное киберпространство. Тем не менее, растущие масштабы, частота и влияние инцидентов кибербезопасности представляют серьезную угрозу для функционирования сетей и информационных систем, а также для единого европейского рынка. Военная агрессия России против Украины еще больше усугубила эту угрозу, наряду с многочисленными государственными, криминальными и хактивистскими субъектами, вовлеченными в нынешнюю геополитическую напряженность.

Опираясь на. уже существующую прочную стратегическую, политическую и законодательную базу, предлагаемый Закон ЕС о кибер-солидарности и Академия навыков кибербезопасности будут способствовать дальнейшему повышению эффективности обнаружения киберугроз, устойчивости и готовности на всех уровнях экосистемы кибербезопасности ЕС

Закон ЕС о киберсолидарности

Закон ЕС о кибер-солидарности укрепит солидарность на уровне Союза, чтобы лучше обнаруживать, готовиться и реагировать на значительные или крупномасштабные инциденты в области кибербезопасности, создавая Европейский щит кибербезопасности и всеобъемлющий механизм защиты от киберугроз.

Для быстрого и эффективного обнаружения крупных киберугроз Комиссия предлагает создать Европейский киберщит, который представляет собой общеевропейскую инфраструктуру, состоящую из национальных и трансграничных центров операций по обеспечению безопасности (SOC) по всему ЕС. Это организации, которым поручено обнаруживать киберугрозы и реагировать на них. Они будут использовать самые современные технологии, такие как искусственный интеллект (ИИ) и расширенный анализ данных, для обнаружения и обмена своевременными предупреждениями о киберугрозах и инцидентах через границы. В свою очередь, органы власти и соответствующие органы смогут более эффективно и действенно реагировать на крупные инциденты.

Эти центры могут начать работу к началу 2024 года. В качестве подготовительного этапа Европейского киберщита в апреле 2023 года Комиссия выбрала в рамках программы «Цифровая Европа» три консорциума

трансграничных центров обеспечения безопасности (SOC), объединяющих государственные органы. из 17 государств-членов и Исландии.

Закон ЕС о киберсолидарности также предусматривает создание Механизма экстренного реагирования в киберпространстве для повышения готовности и расширения возможностей реагирования на инциденты в ЕС. Он будет поддерживать:

Меры по обеспечению готовности, в том числе тестирование объектов в особо важных секторах (здравоохранение, транспорт, энергетика и т. д.) на наличие потенциальных уязвимостей на основе общих сценариев и методологий риска.

Создание нового резерва кибербезопасности ЕС, состоящего из служб реагирования на инциденты от доверенных поставщиков, предварительно заключенных и, следовательно, готовых вмешаться по запросу государств-членов или институтов Союза, органов и агентств в случае значительного или крупномасштабного инцидента кибербезопасности.

Предоставление финансовой поддержки для взаимной помощи, когда государство-член может предложить поддержку другому государству-члену.

Кроме того, предлагаемый Регламент устанавливает Механизм проверки инцидентов кибербезопасности для повышения устойчивости Союза путем рассмотрения и оценки значительных или крупномасштабных инцидентов кибербезопасности после того, как они произошли, извлечения уроков и, при необходимости, выдачи рекомендаций по улучшению состояния кибербезопасности Союза.

Общий бюджет всех действий в рамках Закона ЕС о киберсолидарности составляет 1,1 миллиарда евро, из которых около 2/3 будет финансироваться ЕС через программу «Цифровая Европа».

Академия навыков кибербезопасности ЕС

Академия навыков кибербезопасности ЕС объединит частные и государственные инициативы, направленные на повышение квалификации в области кибербезопасности на европейском и национальном уровнях, делая их более заметными и помогая ликвидировать нехватку специалистов в области кибербезопасности.

Первоначально Академия будет размещаться онлайн на платформе Комиссии по цифровым навыкам и вакансиям. Граждане, заинтересованные в карьере в области кибербезопасности, смогут найти обучение и сертификаты со всего ЕС в одном месте в Интернете. Заинтересованные стороны также смогут заявить о своей поддержке для улучшения навыков кибербезопасности в ЕС, инициируя конкретные действия, такие как проведение тренингов и сертификаций по кибербезопасности.

Академия будет развиваться, чтобы включать в себя общее пространство для академических кругов, поставщиков услуг обучения и промышленности, помогая им координировать образовательные программы, тренинги, финансирование и отслеживать эволюцию рынка труда в области кибербезопасности.

Схемы сертификации для управляемых услуг безопасности

Комиссия также предложила сегодня целевую поправку к Закону о кибербезопасности, чтобы обеспечить принятие в будущем европейских схем

сертификации для «управляемых услуг безопасности». Это очень важные и конфиденциальные услуги, предоставляемые поставщиками услуг кибербезопасности, такие как реагирование на инциденты, тестирование на проникновение, аудит безопасности и консультирование, чтобы помочь компаниям и другим организациям предотвращать, обнаруживать, реагировать или восстанавливаться после киберинцидентов.

Сертификация является ключевой и может играть важную роль в контексте Резерва кибербезопасности ЕС и Директивы о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе (Директива NIS 2), облегчая также трансграничное предоставление этих услуг.

Следующие шаги

Европейский парламент и Совет теперь рассмотрят предложенное Положение о Законе ЕС о киберсолидарности, а также целевую поправку к Закону о кибербезопасности.

Европейский центр компетенции в области кибербезопасности организует совместные закупки инструментов и инфраструктур с выбранными трансграничными центрами операций по обеспечению безопасности для создания возможностей киберобнаружения.

Агентство ЕС по кибербезопасности (ENISA) и Европейский центр компетенции в области кибербезопасности продолжат работу над навыками кибербезопасности, способствуя реализации Академии навыков кибербезопасности в соответствии со своими соответствующими мандатами и в тесном сотрудничестве с Комиссией и государствами-членами.

Комиссия предлагает, чтобы Академия приняла форму европейского консорциума цифровой инфраструктуры (EDIC), новой правовой базы для реализации многострановых проектов. Теперь эта возможность будет обсуждаться с государствами-членами.

Также необходимо обеспечить, чтобы специалисты проходили необходимое качественное обучение. В связи с этим ENISA разработает пилотный проект, изучая создание европейской схемы аттестации навыков кибербезопасности…» ***(Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience // European Commission (https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243). 18.04.2023).***

***

Китай

«Пекин объявил о проверке кибербезопасности Micron Technology, ведущего американского производителя микросхем, сообщает The New York Times. Эта мера, которую ожидали многие отраслевые аналитики, является самым значительным ответным ударом Китая против Вашингтона за его кампанию по ограничению доступа Китая к высокопроизводительным чипам.

Когда на прошлой неделе высокопоставленные китайские чиновники устраивали приемы для десятков американских и европейских бизнесменов в

рамках ежегодных экономических форумов, их цель была ясной: Китай открыт для бизнеса. Но к концу недели устрашающие регуляторы Китая подали совсем другой сигнал.

Китайская служба по надзору за интернетом — Администрация киберпространства Китая (CAC) — заявила, что проводит проверку продуктов Micron, продаваемых в стране, для «обеспечения безопасности цепочки поставок информационной инфраструктуры». Мао Нин, пресс-секретарь министерства иностранных дел Китая, охарактеризовала проверку как «обычную меру регулирования», направленную на продукты, которые могут повлиять на национальную безопасность, сообщает NYT.

Компания Micron Technology, базирующаяся в Бойсе, штат Айдахо, производит микросхемы памяти, используемые в телефонах, компьютерах, центрах обработки данных, автомобилях и другой электронике. По данным NYT, компания имеет давние связи в Китае и является символом лидирующего положения Америки в мировой полупроводниковой промышленности. Но теперь Micron попала в ловушку стремления Китая стать самостоятельным в передовых технологиях.

Сенатор Джим Риш, республиканец из Айдахо, раскритиковал расследование Китая в отношении Micron, назвав его попыткой подорвать позиции США в полупроводниковой промышленности, сообщает NYT.

«Этот шаг еще больше помогает американскому народу увидеть Китай таким, какой он есть — агрессором и хулиганом, который никогда не был заинтересован в настоящем экономическом партнерстве», — говорится в заявлении Риша.

Ежедневная газета сообщила, что акции Micron упали на 9% после этой новости. В заявлении Micron говорится, что ее бизнес в Китае работает в обычном режиме и «полностью сотрудничает» с властями.

Смешанные сообщения из Китая отражают то, по какому канату идет руководство страны. Согласно The New York Times, они пытаются поддержать переживающую трудности экономику, которая лишь недавно вновь открылась после трех лет строгих ограничений, связанных с пандемией, и в то же время пытаются представить непреклонный политический имидж все более враждебному Вашингтону.

Согласно NYT, на одном из праздников на прошлой неделе для руководителей иностранных компаний, включая Тима Кука из Apple, новый премьер-министр Китая Ли Цян пообещал, что Китай будет продолжать «открывать свои двери все шире и шире».

«Китай не стесняется использовать различные тактики в отношениях с иностранными фирмами», — сказал Дэн Ван, приглашенный научный сотрудник Йельской школы права и технологический аналитик исследовательской фирмы Gavekal Dragonomics. «Иногда это как бы говорит: ну, если вам не нравится эта морковь, у нас есть и большая клюшка».

Решение Китая подвергнуть Micron пересмотру последовало за радикальными ограничениями, наложенными США на китайскую полупроводниковую промышленность. Согласно NYT, эти меры, обнародованные в октябре, были направлены против некоторых китайских конкурентов Micron.

Micron открыла свой первый завод в Китае в 2007 году в Сиане. NYT сообщила, что у производителя чипов по всей стране работает около 3000 сотрудников, работающих в сфере обслуживания клиентов, продаж и проектирования. У нее есть центр в Шанхае, где разрабатываются чипы, а также филиалы в Пекине и Шэньчжэне.

«Мы рады быть растущей частью технологической индустрии Китая», — заявил в 2007 году бывший председатель Micron Стив Эпплтон.

Но по мере того, как амбициозный план Китая стать глобальным конкурентом в области технологий усилился, Micron оказалась в центре технологического соревнования страны с США, пишет ежедневная газета. В 2018 году Министерство юстиции США начало расследование в отношении производителей чипов из Китая и Тайваня по подозрению в краже коммерческой тайны у Micron. По данным NYT, одна из компаний признала себя виновной, дело другой продолжается.

За последние два года Micron дала «очень четкие сигналы» о своем намерении сократить свое влияние на Китай, сказал Хуэй Хэ, руководитель отдела исследований полупроводников в Китае для Omdia, исследовательской фирмы в области технологий.

«Micron была одной из самых быстро реагирующих на политику правительства США компаний», — сказала она, добавив, что компания «относительно не зависит от Китая».

Micron начала сокращать количество китайского персонала и закрывать операции в своем Шанхайском центре проектирования микросхем в январе 2022 года. Согласно ежедневной газете, как и многие западные производители микросхем, Micron имеет сильное производственное присутствие в Азии, в том числе в Сингапуре и Тайване, но объявила о планах строительства завода по производству микросхем стоимостью 100 миллиардов долларов США в Нью-Йорке. Президент Байден назвал это «одной из самых значительных инвестиций в американской истории».

Согласно отчетам компании, в 2022 году на материковый Китай приходилось примерно 11% продаж по сравнению с примерно половиной пятью годами ранее.

В своем последнем отчете о прибылях и убытках за март Micron предупредила инвесторов, что правительство Китая может «ограничить нас от участия на китайском рынке или может помешать нам эффективно конкурировать с китайскими компаниями». Это также подчеркнуло конкурентные риски, с которыми она столкнулась со стороны китайских полупроводниковых конкурентов, финансируемых государством.

По словам отраслевых аналитиков, действия против Micron, по-видимому, были направлены на то, чтобы послать сигнал американским политикам в области технологий, а также защитить отечественную промышленность. Инвесторы в Китае приветствовали эту новость, подтолкнув акции отечественных полупроводниковых компаний вверх. По данным NYT, аналитики говорят, что китайские клиенты Micron, вероятно, будут передавать заказы китайским поставщикам, чтобы застраховать свои ставки.

Но дело Micron стало предупреждением для иностранных компаний и оставило будущее Micron неопределенным, сказал Сэмм Сакс, старший научный сотрудник Йельской школы права. Согласно ежедневной газете, она назвала процесс проверки кибербезопасности «черным ящиком». ***(Cybersecurity review of Micron is Beijing's most significant stroke of retaliation against Washington: NYT // Printline Media Pvt. Ltd. (https://theprint.in/economy/cybersecurity-review-of-micron-is-beijings-most-significant-stroke-of-retaliation-against-washington-nyt/1498630/). 05.04.2023).***

***

Кіберстрахування

«Сегодня многие компании сокращают бюджеты и увольняют сотрудников перед лицом текущих экономических трудностей и геополитической неопределенности. Между тем кибератаки не замедляются; во всяком случае, уровень атак и уровень риска продолжают расти.

Несмотря на эти растущие угрозы, многие компании по киберстрахованию также срезают углы, сужая покрытие. В результате директора по информационной безопасности и бизнес-лидеры сталкиваются с трудным выбором. Как они должны распределять средства? Должны ли они улучшить свою безопасность? Должны ли они покупать больше кибер-страховки? Или оба?

Недавнее соглашение в размере 100 миллионов долларов между страховым гигантом Zurich и Mondelez International (производитель Oreos, крекеров Ritz и десятков других закусок) проливает свет на этот вопрос. В 2017 году вредоносное ПО NotPetya нанесло ущерб примерно в 10 миллиардов долларов по всему миру, и Mondelez стал одной из жертв.

Вполне вероятно, что российские военные хакеры запустили NotPetya в украинскую компанию до того, как она распространилась по всему миру. Вот что побудило Цюрих требовать освобождения от войны. Они отказались оплачивать иск, пока дело не будет передано в суд. Был ли Mondelez жертвой военных действий или жертвой «сопутствующего ущерба», который должен покрываться страховкой?

Сейсмические сдвиги в киберстраховании

Еще до решения Цюриха и Монделеза индустрия киберстрахования претерпела серьезные изменения. В августе 2022 года Lloyd's, крупнейшая в мире страховая площадка, попросила всех киберстраховщиков, торгующих через ее платформу, переписать свои полисы.

Согласно рыночному бюллетеню Y5381, Lloyd's теперь требует, чтобы все отдельные политики кибератак (согласно определенным кодам и условиям) включали соответствующий пункт, исключающий ответственность за убытки, возникающие в результате любой кибератаки, поддерживаемой государством.

Это вызвало драматический волновой эффект в отрасли. Страховщики теперь должны бороться за то, чтобы оставаться конкурентоспособными, несмотря на

сужение охвата. Этот шаг также может подтолкнуть перевозчиков, не входящих в Ллойд, исключить покрытие кибер-инцидентов, связанных с войной.

Между тем, в условиях растущих рисков страхование от кибератак пользуется большим спросом у корпоративных клиентов. В 2021 году 20 крупнейших страховых компаний США получили прямые премии в области кибербезопасности на сумму более 3,9 млрд долларов. Кроме того, в 2021 году отдельные премии в области кибербезопасности выросли на 95%.

Киберстраховщики проигрывают?

По данным Fitch Ratings, в период с 2018 по 2021 год убытки киберстраховщиков выросли на 300%. Тем не менее, в 2021 году рост заработанных премий превысил изменение понесенных убытков, а коэффициент отдельных киберубытков улучшился до 65% с 72% в год. ранее.

Все это было до того, как разразилась война на Украине. Давление на страховые компании также возникает после крупных судебных решений в пользу истцов. Например, в декабре 2021 года суд Нью-Джерси постановил, что страховое подразделение Chubb не может отказать в покрытии убытков Merck & Co. в размере 1,4 миллиарда долларов от NotPetya. Суд постановил, что исключение Чабба из войны запрещает только физическую войну, а не кибератаки. Более того, решение Merck было основано на заявлении о страховании имущества, а не на страховом покрытии в киберпространстве.

Учитывая все эти факторы, очевидно, что Ллойд счел необходимым изменить способ покрытия заявлений о кибератаках.

Как зародилось киберстрахование

В недавнем блоге Lawfare содержится обзор новой книги Жозефины Вольф «Политика киберстрахования: переосмысление риска в эпоху программ-вымогателей, компьютерного мошенничества, утечки данных и кибератак» (MIT Press, 2022). Вольф — профессор политики кибербезопасности, информатики и инженерии в Университете Тафтса.

По словам Вольфа, до того, как киберстрахование стало популярным, компании предъявляли киберпретензии в отношении общей коммерческой ответственности, имущества и других видов традиционного страхования. Но судебные решения часто принимали решения против страхователей. Это позволило страховщикам избежать уплаты судебных издержек по коллективным искам, связанным с кибербезопасностью. В конце концов, эта тенденция подтолкнула рынок к разработке продуктов, специально предназначенных для киберстрахования.

Киберстрахование раскрывает сложность кибербезопасности

В наши дни все крупные бренды в любой отрасли также являются технологическими брендами. Что происходит, когда компания является жертвой взлома, но также и виновником кибератак? Вольф подчеркивает, насколько сложно «распутать, кто несет ответственность за инциденты, в которых было несколько, часто пересекающихся слоев жертв, пособников и потенциальных защитников».

По словам Вольффа, для страховой отрасли существуют постоянные трудности с моделированием и ценообразованием киберрисков. Например, как страховая компания влияет на то, как компьютерные сети и данные все больше

переплетаются друг с другом и с другими зонами покрытия? Страховщики неоднократно жалуются на отсутствие надежных актуарных данных, критериев моделирования и ценообразования.

Вольф также отмечает, что разработка полиса страхования от киберрисков сильно отличается от страхования автомобилей или пожарных рисков. В отличие от автомобиля и риска возгорания, практически невозможно сформулировать все способы причинения вреда киберугрозами.

Специалисты по безопасности понимают боль

Проблемы, с которыми сталкиваются киберстраховщики, отражают повседневную реальность групп кибербезопасности. Периметра больше нет. Тысячи приложений, устройств, третьих лиц и пользователей запрашивают подключение к вашим сетям в любое время. Переплетающаяся природа сетей и конечных точек требует, чтобы безопасность применяла совершенно разные подходы, что может принести пользу индустрии киберстрахования и наоборот.

Например, подход к безопасности расширенного обнаружения и реагирования (XDR) работает путем сбора и сопоставления данных в различных точках сети, таких как серверы, электронная почта, облачные рабочие нагрузки и IoT.

Затем данные, собранные с помощью XDR, анализируются и сопоставляются, придавая им наглядность и контекст. Это позволяет идентифицировать продвинутые угрозы. Затем можно приоритизировать угрозы, проанализировать и отсортировать их, чтобы предотвратить сбои в системе безопасности и утечку данных. XDR помогает организациям повысить уровень осведомленности о кибербезопасности и позволяет специалистам по безопасности выявлять и устранять уязвимости.

Дополнительные преимущества между кибербезопасностью и страхованием

Все эти данные и понимание могут также улучшить понимание и разработку полиса киберстрахования. Точно так же обмен данными об инцидентах позволит более точно оценивать риски и цены.

Киберстраховщики также рассматриваются как тип регулятора де-факто. Чтобы претендовать на киберстрахование (что очень желательно для многих предприятий), необходимо соблюдать определенные стандарты. Кроме того, компании с более надежной защитой, такие как системы XDR, могут настаивать на более низких надбавках.

Индустрия киберстрахования будет продолжать развиваться. Если между страховщиками, охранными фирмами и организациями происходит тесное сотрудничество, все стороны должны выйти вперед». ***(Jonathan Reed. Cyber Insurance Companies Adapt to the Security Crisis // IBM Security (https://securityintelligence.com/news/cyber-insurance-companies-adapt-security-crisis/). 10.04.2023).***

***

«На сайт парламенту Фінляндії у вівторок здійснено DoS-атаку.

Про це повідомляє Yle, передає Укрінформ.

Зазначається, що ІТ-фахівці парламенту та Центру кібербезпеки Фінляндії вживають заходів для запобігання кібератаці.

Раніше російська хакерська група NoName 057(16) повідомила у соцмережах, що Фінляндія стала мішенню серії кібератак через вступ до Північноатлантичного альянсу.

«Фінляндія офіційно стала 31-м членом НАТО... «Проводжаємо» Фінляндію в НАТО серією кібератак», – заявили в NoName 057(16).

Ця російська хакерська група поки не взяла на себе відповідальність за кібератаку на сайт парламенту, але оголосила, що їй вдалося зробити недоступним сайт державного науково-дослідного центру VTT…» ***(Сайт парламенту Фінляндії атакували хакери, ймовірно російські // Укрінформ (https://www.ukrinform.ua/rubric-world/3691475-sajt-parlamentu-finlandii-atakuvali-hakeri-jmovirno-rosijski.html). 04.04.2023).***

***

«Служба военной контрразведки Польши и ее Группа реагирования на компьютерные чрезвычайные ситуации связали спонсируемых государством хакеров APT29, входящих в состав Службы внешней разведки (СВР) правительства России, с широкомасштабными атаками, направленными против стран НАТО и Европейского Союза.

В рамках этой кампании группа кибершпионажа (также известная как Cozy Bear и Nobelium) стремилась собирать информацию от дипломатических учреждений и министерств иностранных дел.

«На момент публикации отчета кампания все еще продолжается и находится в разработке», — предупреждает опубликованный сегодня бюллетень.

«Служба военной контрразведки и CERT.PL рекомендуют всем субъектам, которые могут находиться в сфере интересов субъекта, внедрить механизмы, направленные на повышение безопасности используемых систем ИТ-безопасности и увеличение обнаружения атак».

Злоумышленники нацелены на дипломатический персонал, используя фишинговые электронные письма, выдающие себя за посольства европейских стран, со ссылками на вредоносные веб-сайты или вложения, предназначенные для развертывания вредоносного ПО через файлы ISO, IMG и ZIP.

Веб-сайты, контролируемые APT29, заражали жертв дроппером EnvyScout посредством контрабанды HTML, который помогал развертывать загрузчики, известные как SNOWYAMBER и QUARTERRIG и предназначенные для доставки дополнительного вредоносного ПО, а также стейджер CobaltStrike Beacon под названием HALFRIG.

SNOWYAMBER и QUARTERRIG использовались для разведки, чтобы помочь злоумышленникам оценить актуальность каждой цели и определить,

скомпрометированы ли они приманками или виртуальными машинами, используемыми для анализа вредоносных программ.

в опубликованном сегодня отдельном отчете об анализе вредоносных программ «Если зараженная рабочая станция прошла ручную проверку, вышеупомянутые загрузчики использовались для доставки и запуска коммерческих инструментов COBALT STRIKE или BRUTE RATEL», — говорится.

«HALFRIG, с другой стороны, работает как так называемый загрузчик — он содержит полезную нагрузку COBALT STRIKE и запускает ее автоматически».

APT29 — это хакерское подразделение Службы внешней разведки России (СВР), которое также было связано с атакой цепочки поставок SolarWinds, которая привела к компрометации нескольких федеральных агентств США три года назад.

С тех пор хакерская группа взломала сети других организаций, используя скрытое вредоносное ПО, которое годами оставалось незамеченным, включая новое вредоносное ПО, отслеживаемое как TrailBlazer, и вариант бэкдора GoldMax Linux.

Подразделение 42 также наблюдало, как средство моделирования противоборствующих атак Brute Ratel использовалось в атаках, предположительно связанных с российскими кибершпионами СВР.

Совсем недавно Microsoft сообщила, что хакеры APT29 используют новое вредоносное ПО, способное взламывать службы федерации Active Directory (ADFS) для входа в систему под любым именем в системах Windows.

Они также атаковали учетные записи Microsoft 365 в странах НАТО, пытаясь получить доступ к информации о внешней политике, и организовали волну фишинговых кампаний, нацеленных на правительства, посольства и высокопоставленных чиновников по всей Европе». ***(Sergiu Gatlan. Russian hackers linked to widespread attacks targeting NATO and EU // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/russian-hackers-linked-to-widespread-attacks-targeting-nato-and-eu/). 13.04.2023).***

***

«Двухпартийная группа законодателей хочет применить американские технологии и методы кибербезопасности для защиты Тайваня, объекта китайских кампаний влияния, цифровых нападений и потенциального военного переворота.

Сенаторы Джеки Розен, штат Невада, и Майк Раундс, RS.D., и представители Крисси Хулахан, D-Pa., и Майк Галлахер, R-Wis., 20 апреля представили Тайваньский закон об устойчивости кибербезопасности, который потребует от Пентагона активизировать свою деятельность в области кибербезопасности и сотрудничество с широко обсуждаемым независимым островом.

Такое расширенное партнерство будет включать в себя учения и искоренение злонамеренной киберактивности, по словам Розена, который упомянул закон на слушаниях в комитете Сената по вооруженным силам с участием высшего военного командующего США в Индо-Тихоокеанском регионе адмирала ВМС Джона Акилино.

Китай считает Тайвань отступнической провинцией и пообещал вернуть его силой, если это будет необходимо. США десятилетиями поставляли Тайваню военную технику и программное обеспечение на миллиарды долларов. Правительство Тайваня ранее заявляло, что его агентства еженедельно подвергаются тысячам кибератак.

Розен в четверг заявил, что США «остро осознают угрозу, которую Китай представляет в киберпространстве», и назвал Тайвань «испытательным полигоном» Пекина, что также используется для описания динамики российско-украинских отношений. Галлахер, возглавляющий специальный комитет Палаты представителей по Китаю, в своем заявлении заявил, что законопроект поможет «вооружить Тайвань до зубов в киберпространстве».

Официальные лица США считают Китай главной киберугрозой наряду с Россией. администрации Байдена Национальная стратегия кибербезопасности, опубликованная в начале прошлого месяца, называет Китай самой постоянной цифровой угрозой, способной искажать повествования и выкачивать интеллектуальную собственность, а Россию — иностранным вмешивающимся лицом, убежищем для хакеров.

По словам Акилино, отвечающего за всю военную деятельность США в Индо-Тихоокеанском регионе, крайне важно усилить кибербезопасность дома и за рубежом.

С помощью Киберкомандования, сказал он Розену, США работают над «укреплением сетей союзников, партнеров и друзей, чтобы они были в безопасности и чтобы они могли быть уверены в том, что то, что они размещают в своих собственных сетях, не читаются и не подвергаются влиянию со стороны других стран».

Список необеспеченных финансированием приоритетов INDOPACOM на 2024 финансовый год на общую сумму почти 3,5 миллиарда долларов включает 184 миллиона долларов на наступательные кибервозможности, 90 миллионов долларов на кибербезопасность и укрепление сети и 39 миллионов долларов на так называемую среду партнеров миссии, которая позволяет получать данные из ряда вооруженных сил. сопоставлены, защищены, разделены и приняты меры.

Военные лидеры представляют необеспеченные запасы, часто называемые списками пожеланий, в Конгресс, чтобы выделить проекты, которые не вошли в план бюджета Белого дома, но были бы полезны, если бы деньги были доступны…» ***(Colin Demarest. Bipartisan bill would ‘arm Taiwan to the teeth’ with US cyber tech // Defense News (https://www.defensenews.com/cyber/2023/04/21/bipartisan-bill-would-arm-taiwan-to-the-teeth-with-us-cyber-tech/). 21.04.2023).***

***

«Когда в пятницу веб-сайты израильских банков, телекоммуникационных компаний, почтовых служб и т.д. были закрыты хакерами, атака не стала неожиданностью.

В течение многих лет последняя пятница Рамадана, посвященная антиизраильским митингам, проводимым Ираном под лозунгом «День

Иерусалима», сопровождалась хакерскими группами, пытающимися нарушить жизнь Израиля. Как и в прошлые годы, кибератака в пятницу едва зафиксировала всплеск, вызвав лишь незначительные перебои в обслуживании, по словам израильских властей. Однако важно то, кто мог нести за это ответственность и какой сигнал это посылает Израилю.

Ответственность за атаку взяла на себя группа под названием «Анонимный Судан», которая, как считается, не имеет значимой связи с хакерским коллективом Анонимус или сахарской страной, в настоящее время охваченной смертоносными гражданскими беспорядками.

Скорее, эксперты полагают, что группа имеет тесные связи с Россией, и, учитывая видную роль Ирана в направлении антиизраильской деятельности в ознаменование Дня Иерусалима, многие видят его следы и за кибератакой.

В случае подтверждения ирано-российское сотрудничество в киберпространстве станет новым этапом в давней теневой войне между Израилем и Ираном, которая в основном ведется с помощью компьютерного кода. Такой прорыв существенно повлиял бы на региональный баланс сил — в пользу Исламской Республики.

Кибервойна между Ираном и Израилем обострилась за последние шесть лет. Считается, что Израиль, преисполненный решимости помешать Ирану получить ядерное оружие и передовые ракетные возможности, стоит за кибератаками, которые нарушили функционирование Исламской Республики и нанесли ущерб иранским объектам. Среди самых известных случаев — ошибка Stuxnet 2010 года, которая, как считается, привела к уничтожению центрифуг, используемых для разработки ядерной программы Ирана. С тех пор нападения продолжаются.

Иран также полон решимости наращивать свои кибервозможности, чтобы реагировать на хакерские атаки Израиля и инициировать собственные атаки. Кибератака 2020 года, нацеленная на израильские водные объекты, была, вероятно, первым иранским набегом на кибервойну.

Киберзащита Израиля до сих пор предотвращала крупный ущерб, но Тегеран не отказывается от попыток. Учитывая, что военное сотрудничество между Тегераном и Москвой уже набирает обороты на фоне войны на Украине, Исламской Республике казалось бы уместным обратиться к России, чтобы модернизировать свои кибервозможности и искать возможности для совместных инициатив.

Большинство кибератак, совершенных Израилем и Ираном друг против друга на сегодняшний день, представляют собой формы психологической войны, операции, направленные на то, чтобы повлиять на общественное мнение в стране-мишени, чтобы оказать давление на правящий режим или спровоцировать дестабилизирующие протесты.

Такие атаки обычно не наносят необратимого ущерба целям и не заканчиваются гибелью ни в чем не повинных мирных жителей. Список уязвимых целей, которые, как считается, были взломаны Ираном в последние годы, включает Технион — Израильский технологический институт (2023 г.), сирены ракетного оповещения, которые были запущены в Иерусалиме и Эйлате (2022 г.), взломанные

камеры видеонаблюдения (2022 г.), веб-сайт ЛГБТК Atraf (2021 г.) и страховой компании «Ширбит» (2020 г.).

Маловероятно, что иранцам понадобилась помощь России для взлома израильских веб-сайтов в пятницу, которые представляли собой довольно рудиментарные распределенные атаки типа «отказ в обслуживании» или DDoS. Но проведение скоординированной атаки с участием российских хакеров пошлет сильный сигнал Израилю.

Анонимный Судан впервые взял на себя ответственность за хакерские атаки в январе и, по-видимому, сосредоточился на европейских странах в отместку за предполагаемую антимусульманскую деятельность. Эксперты отмечают, что большинство сообщений Telegram от Anonymous Sudana на русском или английском языках и связывают группу с российской хакерской группировкой Killnet, которая запустила DDoS-атаки в европейских странах, поддерживающих Украину.

Killnet и Анонимный Судан также часто распространяют сообщения друг друга в социальных сетях. В феврале Killnet опубликовал сообщение от Anonymous Sudan, в котором утверждалось, что сайт израильской фирмы Radware, занимающейся кибербезопасностью, закрыт.

В рамках растущего военного сотрудничества между Ираном и Россией во время войны на Украине Москва снабжает Тегеран ноу-хау в области кибербезопасности и помогает ему получить передовые возможности цифрового наблюдения, сообщила в прошлом месяце Wall Street Journal.

Иран перебросил в Россию беспилотники, ракеты малой дальности и другие боеприпасы, подкрепив свои ослабевающие военные усилия. Сообщается также, что он надеется приобрести российские ударные вертолеты и реактивные истребители.

Сотрудничество, похоже, является частью новой иранской стратегии по укреплению своих позиций в регионе, превращая бывших соперников в партнеров, как это недавно произошло с Саудовской Аравией.

В то же время Иран также все более активно участвует в координации антиизраильской деятельности террористических группировок в секторе Газа, Ливане и Сирии. Это сотрудничество было замечено ранее в этом месяце, когда террористы в Газе и Ливане выпустили большие залпы ракет по Израилю. Несколькими днями ранее глава экспедиционного подразделения «Аль-Кудс» Корпуса стражей исламской революции встретился в Ливане с руководителями «Хизбаллы» и ХАМАС. А в пятницу президент Ирана выступил с беспрецедентным виртуальным обращением к палестинцам на митинге в честь Дня Иерусалима в подконтрольной ХАМАС Газе.

Интенсивное киберсотрудничество между Ираном и Россией представляет угрозу для Израиля, США и их союзников. Россия, а не Иран, находится у руля в том, что касается определения того, насколько далеко зайдет сотрудничество, и на нее могут оказать давление, чтобы ограничить его.

Хотя в прошлом Россия игнорировала израильское лоббирование сотрудничества с Ираном, ей может угрожать перспектива того, что Тегеран в будущем применит свое кибер-мощь против Москвы.

Но пока Россия и Иран все еще хакерят его вместе, Израиль должен быть готов противостоять кибернападениям, которые могут вызвать настоящие проблемы». ***(Avi Davidi. Iranian-Russian cooperation on hack attacks may challenge Israeli cyber supremacy // The Times of Israel (https://www.timesofisrael.com/iranian-russian-cooperation-on-hack-attacks-may-challenge-israeli-cyber-supremacy/). 18.04.2023).***

***

«Компанії у Фінляндії все частіше стають об'єктами російських кібератак.

Як пише «Європейська правда», про це заявили на спільній пресконференції Агентство транспорту і зв'язку Фінляндії (Traficom) та Служба безпеки і розвідки Фінляндії (Supo), повідомляє Yle.

Керівник Supo Антті Пелттарі зазначив, що Росія все частіше намагається збирати розвіддані у кіберсфері. За даними відомства російське кібершпигунство, спрямоване проти Фінляндії, перевищило попередні рівні.

У службі повідомляють, що Росія намагається використовувати кібершпигунство, щоб компенсувати зменшення кількості співробітників розвідки.

«Щодня Фінляндія стає мішенню цілого ряду кіберзагроз – від DDoS атак до витоку даних і спроб поширення шкідливого програмного забезпечення», – сказала генеральна директорка Traficom Кірсі Карламаа.

Зокрема, жертвами кібератак стали фінське інформаційне агентство STT, а також державні установи, в тому числі ті, що пов'язані з критичною інфраструктурою.

Крім того, у Фінляндії спостерігається зростання хактивізму – груп, які використовують комп’ютерні системи для просування певних ідей.

Також зросла з використанням програм-шантажистів (Ransomware), які вимагають щось у користувачів.

Але, попри збільшення кількості кібератак, малоймовірно, що вони зможуть паралізувати життєдіяльність країни…» ***(У Фінляндії фіксують все більше російських кібератак // Європейська правда (https://www.eurointegration.com.ua/news/2023/04/21/7160315/). 21.04.2023).***

***

«Від початку повномасштабного російського вторгнення в Україну РФ регулярно здійснює кібератаки на Молдову…

Коли російські війська збиралися для повномасштабного вторгнення в Україну на початку минулого року, комп’ютерні системи, які сусідня Молдова використовувала для управління своїми операціями безпеки вздовж кордону з Україною, зазнали атаки.

За нападом, про який раніше не повідомлялося, який міг порушити здатність Молдови впоратися з потоком українських вимушених біженців і зерна, послідувала серія подібних атак. В ході війни проросійські облікові записи у соціальних мережах поширювали неправдиві заяви, спрямовані на дискредитацію

молдовського уряду, а «тролі» бомбардували владу Молдови тисячами фальшивих погроз про вибухи.

У серпні хакери зламали сервери електронної пошти, які використовуєся офіс президентки Молдови; у листопаді хакери також опублікували тисячі приватних повідомлень, які, як вони стверджували, викрали у Анни Ревенко, міністерки внутрішніх справ Молдови, та Сергія Литвиненка, який тоді обіймав посаду міністра юстиції.

Офіційні особи Молдови кажуть, що кампанія кібератак і дезінформації триває, оскільки війна затягується. Вони описують це як навмисну спробу підірвати – або навіть усунути – дружній до Заходу уряд у країні, яка межує із зоною бойових дій. Кібервійна в поєднанні з економічною шкодою, спричиненою війною, має потенціал для глибокої дестабілізації.

«Вони хочуть налякати населення, щоб викликати постійне відчуття паніки, страху. Це випробування, якого ми ніколи не проходили з часів нашої незалежності», – сказала Ревенко.

Російські хакери не мали великого успіху в самій Україні, де багато експертів передбачали, що режим президента РФ Володимира Путіна використовуватиме кібератаки, щоб дестабілізувати уряд або вивести з ладу інші важливі системи.

Експерти пояснюють здатність України захистити свої комп'ютерні системи частково допомогою американських технологічних компаній, зокрема Google і Microsoft Corp.

У Молдові Росія та пов'язані з нею хакерські групи, схоже, грубо поводяться з відносно слабким захистом країни.

«Росія більше навіть не хоче маскувати атаки; вони просто жорстоко атакують будь-якими способами», – зазначив Густав Грессель, старший науковий співробітник Європейської ради з міжнародних відносин.

Паніше Молдова була республікою Радянського Союзу, але стала незалежною з 1991 року. Нація з населенням 2,6 мільйона осіб є однією з найбідніших у Європі, і вона сильно постраждала від повномасштабного вторгнення Росії в Україну.

За даними ООН, з початку війни в країну в'їхало близько 800 тисяч українців. Україна перенаправила близько 60% свого експорту зерна через територію Молдови після закриття чорноморських морських шляхів, – повідомляє уряд Молдови. Окрім контролю над довгим українським кордоном, Молдова має справу з регіоном, контрольованим російськими сепаратистами – Придністров'ям.

Кібератака на інструменти управління кордонами могла порушити управління біженцями, безпеку кордонів і потік зерна, але її було зірвано до того, як вона завдала значної шкоди.

Представник Служби інформаційних технологій і кібербезпеки Молдови (Stisc) каже, що найпоширеніші атаки, з якими стикається країна, – це спроби відмови в обслуговуванні переповнених трафіком урядових вебсайтів Молдови та вивести їх із мережі.

Також триває тривала кампанія фішингових електронних листів, націлених на державні облікові записи. На початку 2023 року їх було отримано понад 1300.

Державна Moldtelecom, найбільша телекомунікаційна компанія Молдови, «постійно зазнавала кібератак», за словами Сергіу Тіу, менеджера з інформаційної безпеки. Вони варіюються за складністю від атак на відмову в обслуговуванні до «розширених постійних» атак, які частіше пов'язують з російськими урядовими хакерами.

У період з лютого по листопад минулого року компанія зазнала щонайменше дев'яти інцидентів, які її команда безпеки позначила як «значні» або «критичні», згідно з документом, який перевірив Bloomberg Businessweek. Тіу каже, що компанія не виявила жодних витоків даних унаслідок атак.

Український уряд заявив, що має документальні докази російського плану повалити уряд Молдови, а координатор Білого дому з національної безпеки Джон Кірбі попередив у заяві в березні, що Росія намагається послабити молдовський уряд.

Через два дні після цієї заяви молдовська влада заявила, що розбила підтримувані Росією групи, яким нібито пообіцяли виплати в розмірі 10 000 доларів США за організацію заворушень під час протестів у столиці Молдови Кишиневі. Поліція заарештувала десятки осіб і вилучила готівку на мільйони євро.

Україна створила захист від кібератак у відповідь на багаторічні хакерські дії Росії. За словами речника агентства, Молдова – набагато менш підготовлена, що робить її більш уразливою до зовнішніх загроз, і має лише чотирьох осіб, які відповідають за кіберзахист і працюють у Stisc. У молдовській розвідці та військових працюють окремі невеликі групи кіберекспертів.

Наталія Спіну, яка очолювала команду кіберзахисту Stisc до травня минулого року, каже, що країні потрібне набагато потужніше агентство реагування на кібернетичні ситуації.

«Немає нікого, хто відповідає. Погані речі відбуваються за лаштунками, і люди просто не знають», – сказала вона…» ***(Росія вдарила кібервійною по непідготовленій Молдові – Bloomberg // Букви (https://bykvu.com/ua/bukvy/rosiia-vdaryla-kiberviinoiu-po-nepidhotovlenii-moldovi-bloomberg/). 20.04.2023).***

***

«У Великій Британії заявили, що хакери, які пов'язані з РФ планують кібератаки на критичну інфраструктуру Заходу. Зокрема, йдеться про Сполучене Королівство…

Зазначається, що в Агентстві кіберзахисту Великої Британії (GCHQ) попереджають про загрозу критичній національній інфраструктурі Заходу через активність з боку хакерів, які пов'язані з Росією.

Прихильники-хакери РФ раніше проводили в основному онлайн-кампанії, які спотворювали загальнодоступні вебсайти або виводили їх з ладу. Однак зараз деякі з них планують завдати більшої шкоди.

«Деякі заявили про бажання досягти більш руйнівного та руйнівного впливу на західну критично важливу національну інфраструктуру, зокрема у Великій Британії», — заявили в Британському національному центрі кібербезпеки (NCSC), що є частиною розвідувального агентства GCHQ.

Хоча такі групи є ідеологічно вмотивованими та пов’язані з інтересами РФ, вони «не підлягають формальному державному контролю».

«Це робить їх менш передбачуваними», — додали в повідомленні.

Кібернаступ РФ минулого року був швидким та затятим, водночас не викликав захоплення. У ньому хакери провели, мабуть, найбільшу в історії атаку на комп’ютерні мережі. Україна, добре підготовлена та підтримувана іноземними технологічними компаніями та союзниками, відбила багато з цих ударів, попри всі очікування, зберігши зв’язок та найважливіші державні служби онлайн. Але кібервійна, як і фізична, розвивається.

За даними пошукової системи Google, російські кібератаки в країнах НАТО за минулий рік зросли в чотири рази проти показника 2020 року. В Україні кількість російських кібератак за той самий період зросла втричі.

19 січня президент Microsoft Бред Сміт заявив, що кібератаки Росії проти українських цілей послабилися, проте попередив, що це може змінитися з початком весни». ***(Пов’язані з РФ хакери планують кібератаки на критичну інфраструктуру Заходу // Букви (https://bykvu.com/ua/bukvy/pov-iazani-z-rf-khakery-planuiut-kiberataky-na-krytychnu-infrastrukturu-zakhodu/). 19.04.2023).***

***

«Мерія Праги опинилась під атакою російських хакерів. У Чехії кажуть, що це помста за допомогу Україні.

Про це повідомив директор одного з департаментів інформатики муніципалітету Їржі Каролі, пише видання "Чеські новини".

Сервери празького муніципалітету сьогодні зазнали атаки російської хакерської групи через підтримку України.

Через ранковий напад не працював сайт столиці та онлайн-трансляція сьогоднішнього засідання ради.

Близько 16:00 Каролі заявив, що «всі системи працюють».

За інформацією муніципалітету, це була так звана DDoS-атака, іншими словами, перевантаження серверів великою кількістю запитів. За словами Каролі, IP-адреса атаки була в Росії.

«Ми зараз розслідуємо, яка хакерська група стоїть за атакою, і аналізуємо техніку атаки», — сказав Каролі.

Відзначимо, що кількість атак російських хакерів на Чехію зросла після російської атаки на Україну в лютому минулого року.

«У зв'язку з президентськими виборами хакери атакували, серед іншого, сайти тодішнього кандидата та чинного президента Петра Павла та сервер Міністерства закордонних справ Чехії. Нещодавно, наприклад, сайт інтегрованого транспорту Праги також зазнав DDoS-атаки», — пише видання…» ***(Даріна Глущенко. Росіяни завдали хакерської атаки по чеській міській раді // ТОВ «МЕДІАМЕРЕЖІ» (https://it.novyny.live/rosiiani-zavdali-khakerskoyi-ataki-po-cheskii-miskii-radi-90657.html). 27.04.2023).***

***

«…что такое ответственная кибердержава? 4 апреля Национальные киберсилы Великобритании (NCF) попытались ответить на этот вопрос, опубликовав документ, в котором излагаются их взгляды на цель и принципы «наступательной кибербезопасности» — нарушения работы компьютерных сетей в отличие от кибершпионажа. Это также раскрыло личность командира НКФ Джеймса Бэббиджа, который дал свое первое интервью The Economist.

Прозрачность Великобритании является долгожданным шагом вперед. Кибероперации окутаны тайной. Они могут распространяться на компьютерные сети, от которых зависит современная экономика и общество: российская кибератака в 2017 году нанесла ущерб более чем на 10 миллиардов долларов. Их потенциал также плохо изучен. Многие политические лидеры ошибочно рассматривают их как стратегическое оружие для сдерживания врагов.

Новый документ NCF важен, потому что в нем изложен реалистичный и ограниченный взгляд на кибермощь. В нем говорится, что его основная цель не столько кинетическая — цифровая замена ударам с воздуха — сколько когнитивная. Российская кибердезинформация часто нацелена на все население. Великобритания заявляет, что ее целями обычно являются отдельные лица и небольшие группы. Кибератака может, например, нарушить их связь, так что они будут парализованы замешательством или нападут друг на друга.

Британский пример предлагает несколько критериев для оценки того, ответственно ли используется кибермощь. Во-первых, какие цели выбираются. Северокорейские хакеры однажды атаковали американскую киностудию за то, что она выпустила нелицеприятный фильм о Ким Чен Ыне, лидере страны. Иран атаковал американские банки в ответ на санкции. Россия использовала кибертактику для вмешательства в выборы в Америке и Европе.

Другое дело, насколько хорошо откалиброваны атаки. Являются ли они точными в своих последствиях и помнят об эскалации? Или они дико швыряют вредоносный код? Должностные лица и эксперты годами спорили о том, как международное право, включая законы о вооруженных конфликтах, применимо к киберпространству. Таллиннское руководство, связанное с НАТО, является одним из таких руководств. Российские спецслужбы не обращают особого внимания на такие вещи, но ответственным киберкомандирам нужны юристы.

Третьим тестом является то, насколько хорошо киберсилы защищают свои арсеналы. Хакерские инструменты, используемые государствами, часто бывают мощными и опасными. Они могут причинить значительный вред, если станут широко доступными. В 2017 году северокорейская кибератака привела к распространению программ-вымогателей по всему миру, в том числе путем перепрофилирования вредоносного кода, просочившегося из Агентства национальной безопасности США (nsa). По мере того, как все больше стран прибегают к наступательным кибероперациям, безопасность их инструментов станет более серьезной проблемой.

Наконец, киберсилам нужна подотчетность. Взгляд Британии на наступательный киберпространство как на средство целенаправленного

психологического разрушения, а не как на универсальное оружие проецирования силы, заслуживает высокой оценки. Но это также толкает кибер-мощь в мрачную сферу тайных действий. Надзор за этим вдвойне труден: работа одновременно очень секретная и высокотехнологичная. Законодатели и судьи часто с трудом улавливают детали.

В настоящее время подход Великобритании следует приветствовать. Десять лет назад Эдвард Сноуден, бывший подрядчик nsa, шокировал АНБ и gchq, его британского коллегу, публично обнародовав информацию об их сборе разведывательных данных в промышленном масштабе в киберпространстве. Десять лет спустя призраки, похоже, поняли, что ответственность требует проверки». ***(What is a responsible cyber power? // The Economist Newspaper Limited (https://www.economist.com/leaders/2023/04/05/what-is-a-responsible-cyber-power). 05.04.2023).***

***

«Команда Швеції та Ісландії перемогла на навчаннях із кібербезпеки Locked Shields – 2023, організованих Північноатлантичним Альянсом в Естонії.

Про це повідомила пресслужба шведського уряду в п’ятницю…

Швеція була головним організатором команди, тоді як Ісландія брала участь у Locked Shields – 2023 вперше. Ця команда показала найкращі результати й перемогла в навчаннях, що завершились у п’ятницю.

Швецію на навчаннях представляли військовослужбовці шведських збройних сил, а шведсько-ісландська команда складалась із цивільних і військових представників, які відпрацьовували питання оборонної співпраці, і налічувала понад 100 людей.

«Я дуже пишаюсь шведськими учасниками. Кібербезпека є важливою частиною загальної оборони Швеції. Це наочно демонструє, що Швеція як член оборонного альянсу НАТО може зробити значний внесок в ще одну сферу», – заявив міністр цивільної оборони Швеції Карл-Оскар Болін.

Під час навчань Locked Shields – 2023 учасники мали протистояти різноманітним атакам в умовах обмеженого часу. Атаки відбувались в умовах змодельованої реальної події в галузі кібербезпеки, протистояли їм як індивідуально, так і спільно з іншими.

Locked Shields – найбільші у світі навчання з кібербезпеки. Навчаннями керував і розробляв Центр передового досвіду НАТО з питань кібербезпеки в Таллінні. Цього року в них узяли участь 33 країни у складі 24 різних команд…» ***(Швеція та Ісландія перемогли в найбільших у світі навчаннях НАТО з кібербезпеки // Європейська правда (https://www.eurointegration.com.ua/news/2023/04/21/7160316/). 21.04.2023).***

***

«Просочившаяся оценка американской разведки содержит резкое напоминание об угрозе, которую хакеры могут представлять для критической инфраструктуры.

Оценка, которая в основном сосредоточена на военных действиях Украины против российских войск и которую высокопоставленный американский чиновник считает достоверной, включает в себя предупреждение о том, что российские хактивисты взломали в этом году канадскую газовую инфраструктуру и получили указания от российской разведки.

В оценке отмечается, что такой доступ может привести к значительному ущербу и, возможно, к взрыву. Такое нападение считается чрезвычайно трудным для осуществления, но оно остается одним из самых больших опасений разведывательного сообщества. И хотя таких крупных атак пока не обнаружено, эксперты говорят, что они представляют постоянную угрозу.

«Это не первый случай, когда кто-то получает доступ к критически важной инфраструктуре, — сказал Джон Халтквист, вице-президент по анализу угроз в компании по кибербезопасности Mandiant, принадлежащей Google. «Это происходит постоянно. Российские спецслужбы делают это постоянно».

Хактивисты, русскоязычная группа под названием «Заря», в феврале взломали компьютерную сеть неназванного канадского газораспределительного предприятия и отправили российской разведке скриншоты того, что, по ее утверждению, было средствами управления «для повышения давления в клапанах, отключения сигнализации и инициирования аварийная операция [которая] вызовет взрыв», — говорится в оценке США.

NBC News не подтвердила это утверждение, и неясно, какая компания была замешана. Чиновник также сказал, что некоторые документы могли быть изменены до того, как они были размещены в Интернете, хотя эта часть оценки не показывает явных признаков изменений.

«Если «Заря» добьется успеха, это будет первый раз, когда IC наблюдает, как пророссийская хакерская группа осуществляет подрывную атаку на западные промышленные системы управления», — говорится в оценке с использованием аббревиатуры разведывательного сообщества.

Похоже, что такой катастрофы не произошло. Но оценка показывает, как США обеспокоены деструктивными взломами западной энергетической инфраструктуры, так и то, как российская разведка может полагаться на местных хакеров-преступников, которые будут работать на них.

Оценка с пометкой «Совершенно секретно» взята из кэша из более чем 50 страниц секретных документов, которые появились в сети в последние дни после того, как томились в темных уголках Интернета. Официальные лица США отказались комментировать подлинность конкретных документов, но один чиновник сказал NBC News, что они действительно кажутся реальными. Неясно, кто изначально слил документы и почему.

Об оценке «Зари» впервые сообщила журналист Ким Зеттер. Представитель посольства России в Вашингтоне не сразу ответил на запрос о комментариях.

США обычно рассматривают хакерские атаки для ведения шпионажа как обычную тактику, используемую всеми сторонами, в то время как кибератаки, приводящие к физическому разрушению, рассматриваются как драматическая эскалация.

«Я думаю, что большая проблема здесь заключается в том, решат ли они использовать этот доступ для какой-то подрывной или разрушительной атаки», — сказал Халтквист.

Канадский центр кибербезопасности отказался рассматривать конкретное утверждение в оценке США. Но представитель агентства заявил, что обеспокоен тем, что хакеры получат доступ к критически важной инфраструктуре.

«Мы по-прежнему глубоко обеспокоены этой угрозой и призываем владельцев и операторов критической инфраструктуры связаться с нами для совместной работы по защите своих систем», — сказал представитель.

Лесли Кархарт, руководитель отдела реагирования на инциденты в Северной Америке компании Dragos, специализирующейся на кибербезопасности промышленных систем, сказал, что они считают правдоподобным, что такая группа хактивистов, как «Заря», могла получить доступ к газораспределителю, но для этого потребовалось бы гораздо больше усилий, чтобы вызвать взрыв.

«Такой процесс имеет избыточность. Человеческий контроль. Цифровые и физические элементы управления безопасностью. Он спроектирован так, чтобы не взорваться, даже если кто-то совершит ошибку», — написал Кархарт в текстовом сообщении.

«Заря» — одна из нескольких пророссийских хакерских групп, которые часто пристают к целям, связанным с НАТО и странами-союзниками Украины. Хотя они часто выводят веб-сайты из строя на короткий период, они редко демонстрируют способность нанести серьезный ущерб.

Таких групп около 20, большинство из которых появились за последние два года, начиная примерно с того времени, когда Россия начала вторжение в Украину, сказал Сергей Шикевич, который отслеживает информацию об угрозах для израильской компании по кибербезопасности Check Point Software.

«Заря» ведет хронику своих подвигов в своем Telegram-канале, где в основном хвастается отключением сайтов. В его сообщениях не упоминается атака на энергетическую инфраструктуру Канады, и группа прямо заявляет, что не связана с российским правительством.

Крис Пейнтер, посол Госдепартамента в администрации Обамы по кибербезопасности, сказал, что российская разведка часто опирается на свой богатый пул отечественных киберпреступников для достижения своих целей.

«Это один из инструментов в их наборе инструментов для использования этих прокси-серверов, потому что в некотором смысле он уклоняется от прямой ответственности», — сказал Пейнтер. «Они всегда могут сказать: «Ну, это были не мы. Это была преступная группа». ***(Kevin Collier. Leaked U.S. assessment includes warning about Russian hackers accessing sensitive infrastructure // NBC UNIVERSAL (https://www.nbcnews.com/tech/security/leaked-us-assessment-includes-warning-russian-hackers-accessing-sensit-rcna79011). 11.04.2023).***

***

«Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США (FDA) выпустило новое руководство для производителей медицинского оборудования о важности мер кибербезопасности при разработке продуктов. В необязательном руководстве под названием «Кибербезопасность в медицинских устройствах: отказаться от принятия политики для киберустройств в соответствии с разделом 524B Закона FD&C» подчеркивается острая необходимость для производителей устранять риски кибербезопасности в медицинских устройствах и обеспечивать безопасность устройств, прежде чем они могут быть одобрены. для использования.

Раздел 524B «Обеспечение кибербезопасности устройств» был добавлен в Федеральный закон о пищевых продуктах, лекарствах и косметических средствах (Закон FD&C) 29 декабря 2022 г. посредством Закона о сводных ассигнованиях 2023 г. (Сводной). Согласно Омнибусу, поправки к Закону о FD&C вступят в силу через 90 дней после вступления закона в силу, то есть 29 марта. Требования кибербезопасности, изложенные в поправках, не будут применяться к любым заявкам или материалам, поданным в FDA до этого. дату в соответствии с положениями Омнибуса. FDA также продлило льготный период до 1 октября, когда оно, как правило, не будет отказывать в каких-либо предварительных представлениях от компаний, которые не соблюдают требования, а вместо этого будет работать с фирмами для достижения соответствия.

Руководство FDA является частью более широких усилий по снижению растущего риска киберугроз в индустрии медицинского оборудования. В последние годы агентство все больше внимания уделяло кибербезопасности медицинских устройств, признавая, что по мере того, как устройства становятся более связанными и сложными, они также становятся более уязвимыми для кибератак.

В новом руководстве указана информация, которая должна быть включена в предпродажную документацию для устройств, содержащих программное или микропрограммное обеспечение, включая конкретную документацию по кибербезопасности, такую как анализ опасностей, оценка рисков и рекомендуемые средства контроля для снижения выявленных рисков. Руководство также содержит подробную информацию о том, как FDA планирует оценивать документацию по кибербезопасности и что производители могут ожидать в процессе проверки.

В рамках руководства FDA также выпустило политику «Отказ в приеме» для медицинских устройств в соответствии с разделом 524B Закона FD&C). Раздел 524B «Обеспечение кибербезопасности устройств» был добавлен в Закон FD&C 29 декабря 2022 г. посредством Закона о сводных ассигнованиях 2023 г. («Омнибус»). Политика отказа в принятии описывает ожидания FDA в отношении документации по кибербезопасности, которая должна быть включена в предварительные заявки. Если документация не соответствует стандартам агентства, в представлении будет отказано, и процесс рассмотрения не начнется.

Политика «Отказаться от принятия» важна, поскольку подчеркивает важность кибербезопасности медицинских устройств и подчеркивает приверженность FDA обеспечению безопасности и безопасности пациентов. Производители медицинского оборудования должны уделять первоочередное внимание кибербезопасности в процессе разработки своей продукции и обеспечивать соответствие своих устройств стандартам кибербезопасности FDA, чтобы избежать санкций регулирующих органов, ответственности за ущерб и ущерба репутации.

Руководство и новые политики FDA представляют собой дорожную карту, которой производители должны следовать, чтобы соответствовать ожиданиям агентства в отношении документации по кибербезопасности. Невыполнение этих ожиданий может привести к задержкам в процессе утверждения и дополнительным расходам для производителей.

По мере того, как индустрия медицинского оборудования продолжает развиваться, риски кибербезопасности будут становиться все более сложными и сложными. Действия FDA являются важными шагами к тому, чтобы медицинские устройства оставались безопасными для пациентов. Производители должны предпринять необходимые шаги для соблюдения руководства и уделять кибербезопасности приоритетное внимание в процессе разработки своей продукции, чтобы избежать нормативных и юридических последствий». ***(Laura E. Macherelli, Lee H. Rosebush, Lynn Sessions. Cybersecurity in Medical Devices // Baker & Hostetler LLP (https://www.bakerlaw.com/alerts/cybersecurity-in-medical-devices). 10.04.2023).***

***

«Давно рекомендуется, чтобы при заключении контракта с поставщиком технологий вы включали в контракт пункт о возмещении убытков, согласно которому поставщик возместит вам ущерб, если его продукт будет скомпрометирован и приведет к утечке данных в вашей компьютерной сети. Эта рекомендация была недавно подтверждена как киберорганами США, так и Великобритании, Германии, Канады, Австралии, Новой Зеландии и Нидерландов. Основой для правительственной рекомендации было использование рынка для обеспечения безопасности технологических продуктов по своей конструкции и по умолчанию. В настоящее время технологические продукты разрабатываются с учетом уязвимостей, что приводит к тому, что конечный пользователь несет основную тяжесть кибербезопасности с постоянным мониторингом, регулярными обновлениями и контролем повреждений для предотвращения кибератак.

Государственные киберорганы хотят, чтобы производители и разработчики технологий вместо нынешней практики проектирования уязвимостей применяли принцип защиты по дизайну. Это включает в себя переход на языки программирования, которые устраняют широко распространенные уязвимости. Хотя первоначальная защита по дизайну обходится дороже, в долгосрочной перспективе она может снизить затраты на обслуживание и установку исправлений. Защищенные протоколы включают в себя:

Безопасные для памяти языки программирования, такие как Rust, Ruby, Java, Go, C# и Swift;

Надежная аппаратная основа, обеспечивающая точную защиту памяти;

Защищенные программные компоненты, включая библиотеки, модули, промежуточное ПО и фреймворки от коммерческих разработчиков, разработчиков с открытым исходным кодом и сторонних разработчиков;

Фреймворки веб-шаблонов, которые автоматически избегают пользовательского ввода, чтобы избежать атак с использованием межсайтовых сценариев;

Параметризованные запросы для предотвращения атак путем внедрения SQL-кода;

Статическое и динамическое тестирование безопасности приложений для выявления подверженных ошибкам практик;

Экспертные обзоры кода;

Спецификация программного обеспечения;

Программы раскрытия уязвимостей, которые позволяют исследователям в области безопасности сообщать об уязвимостях, не опасаясь юридической опасности;

Полная информация о CVE, включая перечисление первопричин или общих недостатков;

Инфраструктура, разработанная в соответствии с принципами глубокоэшелонированной защиты, поэтому компрометация одного элемента управления не приводит к компрометации всей системы; и

Меры и методы, которые соответствуют целям эффективности кибербезопасности CISA.

Используя эти предлагаемые принципы обеспечения безопасности, производители и разработчики технологий могут эффективно устранять первопричины существующих уязвимостей технологий.

В дополнение к безопасности по дизайну правительственные киберорганы также рекомендуют безопасность по умолчанию, что означает, что безопасные конфигурации являются базовым уровнем по умолчанию. Если клиенты хотят отклониться от базовых параметров безопасности по умолчанию, им сообщается, что изменение базовых параметров безопасности по умолчанию повысит вероятность компрометации их систем. Правительственные органы по кибербезопасности выступают за безопасность в соответствии с дизайном, потому что «сложность конфигурации безопасности не должна быть проблемой для клиентов». К безопасным по умолчанию протоколам относятся:

Устранение общедоступных паролей по умолчанию;

Мандат многофакторной аутентификации для привилегированных пользователей;

Единый вход для ИТ-приложений;

Предоставление качественных журналов аудита клиентам без дополнительной оплаты;

Рекомендации по авторизованным ролям профиля и их назначенному варианту использования;

Приоритет безопасности над обратной совместимостью;

последовательное уменьшение размеров направляющих закалки; и

Оценка бремени взаимодействия с пользователем, вызванного настройками безопасности.

Принимая эти рекомендации, государственные киберорганы хотят дать организациям возможность привлекать производителей и разработчиков технологий к ответственности за кибербезопасность их продуктов.

Рекомендация о том, что компании должны включать в свои контракты положения о возмещении убытков от кибератак, не должна ограничиваться только контрактами с поставщиками технологий. Поставщиков услуг все чаще просят использовать определенные программы или приложения в их компьютерных сетях или сотовых телефонах компании, чтобы более эффективно предоставлять услуги по контракту. Это должно быть предметом переговоров при заключении любого контракта. Если указанная программа или приложение могут быть использованы в качестве средства атаки на компьютерную сеть поставщика или сотовые телефоны компании злоумышленниками в будущем, поставщик должен включить в контракт пункт о возмещении убытков. Положение о возмещении убытков будет предусматривать, что если требуемая программа или приложение приведет к взлому компьютерной системы поставщика или сотовых телефонов компании, то сторона, требующая использования этой технологии, возместит поставщику ущерб. Эта компенсация должна включать восстановление сети поставщика до ее состояния до атаки, а также защиту и возмещение убытков поставщику от любых судебных исков, которые могут возникнуть в результате кибератаки, совершенной с помощью требуемой программы или приложения. Эти типы положений о возмещении убытков должны быть включены в начале договорных отношений, даже если другая сторона в настоящее время не требует от поставщика использования конкретной программы или приложения для оказания помощи в предоставлении услуг по договору, поскольку это может измениться в течение срока действия договора. Если это не было заключено в контракте в начале отношений, а поставщика позже попросили использовать конкретную программу или приложение в течение срока действия контракта, это представляет собой существенное изменение контракта, и тогда можно договориться о возмещении убытков. Однако легче провести такие переговоры в начале договорных отношений, чем в середине их.

Могут быть случаи, когда компания просит сотрудников разместить приложение на своих личных телефонах, которое будет использоваться для помощи им в выполнении своих служебных обязанностей. Допустимо требовать от сотрудников установки рабочих приложений на личные устройства, если компания не предоставляет корпоративные устройства. Однако работодатель все же должен защитить себя от возможности того, что требуемое приложение может стать средством атаки на личное устройство работника, что приведет к утечке персональных данных работника. Компания, требующая установки приложения на личные устройства сотрудников, должна рассмотреть вопрос о субсидировании части ежемесячного счета за мобильный телефон каждого сотрудника за данные, которые использует приложение, в обмен на то, что сотрудники подпишут

соглашение о возмещении убытков, удерживающее компанию от ответственности в случае что установка необходимого приложения приводит к утечке данных. Это соглашение о возмещении убытков также должно информировать сотрудников о том, какие данные собирает приложение, для чего используются собранные данные, как долго эти данные будут храниться и кто их собирает. Всю эту информацию можно найти в уведомлении о конфиденциальности для приложения…» ***(Alexander L. Turner. Tech Vendors and Cybersecurity – Are They Responsible? // spilmanlaw (https://www.spilmanlaw.com/dataentry/resources/attorney-articles/technology/tech-vendors-and-cybersecurity-%E2%80%93-are-they-responsi). 25.04.2023).***

***

«Программа-вымогатель — это «самая быстрорастущая угроза вредоносного ПО». Исследование показало, что в 2022 году количество атак в сфере здравоохранения увеличилось на 328%. В другом недавнем исследовании сообщается, что с 2016 по 2021 год «ежегодное количество здравоохранения в сфере атак программ-вымогателей увеличилось более чем вдвое», раскрывающих электронную личную медицинскую информацию (ePHI) «почти 42 миллионов пациентов».

Программа-вымогатель «относится к типу вредоносного ПО, используемого злоумышленниками, которые сначала шифруют файлы, а затем пытаются вымогать деньги в обмен на ключ [дешифрования], чтобы разблокировать файлы, требуя «выкупа»». В секторе здравоохранения это определяется как «вредоносное ПО, предназначенное для блокировки больниц от их записей о пациентах»... с простым ультиматумом: заплатите или навсегда потеряйте доступ ко всей информации о пациентах». Хакеры также используют программы-вымогатели для уничтожения или эксфильтрации данных в сочетании с развертыванием других заразных вредоносных программ.

Без надлежащих планов кибербезопасности, аварийного восстановления и резервного копирования атака программ-вымогателей может иметь разрушительные последствия для больницы или системы здравоохранения. В большинстве случаев, чтобы восстановить доступ к ePHI и возобновить работу, уплата выкупа является единственным вариантом. Тем не менее, делая это, больница или система здравоохранения рискуют подвергнуться денежным штрафам, если группа вымогателей попадет под санкции Управления по контролю за иностранными активами Министерства финансов США. Федеральное бюро расследований (ФБР) не поощряет выплаты выкупа, но не запрещает их. Однако ФБР поощряет сообщения о выплатах выкупа, чтобы оно могло оказать помощь жертвам и провести дальнейшее расследование действий хакеров.

Те больницы или системы здравоохранения, которые применяют меры по профилактике и реагированию, по-видимому, добились успеха: число жертв, платящих выкуп, сократилось с 85% в 2019 году до всего 37% в 2022 году. Необходимо принять комплексные меры безопасности как для защитить сети систем здравоохранения и подключенные устройства, а также обеспечить соответствие правилам безопасности Закона о переносимости и подотчетности

медицинского страхования (HIPAA) и Руководству по кибербезопасности Министерства здравоохранения и социальных служб США (HHS) от 2023 года.

Надвигающаяся угроза системам здравоохранения

Новая эра для систем здравоохранения началась в 2016 году, когда они стали основной целью атак программ-вымогателей. Этому развитию способствовали два фактора: (1) масштабы ePHI и (2) «дыры в безопасности в системах информационных технологий (ИТ)». К основным дырам в безопасности — или уязвимостям — относятся фрагментированные инфраструктуры, устаревшие системы, сотрудники, подключенные устройства и большое количество беспроводных приложений.

Атаки программ-вымогателей затрагивают не только больницы и системы здравоохранения, но и их бизнес-партнеров (BA). Значительный процент этих атак возникает из-за внешних угроз. Однако внутренние угрозы, такие как ошибки сотрудников, также являются важным фактором. Действительно, исследование показало, что 36% организаций здравоохранения и 55% бизнес-аналитиков становятся жертвами нарушений в результате непреднамеренных действий сотрудников.

Недостаточная безопасность электронной почты повышает уязвимость к атакам программ-вымогателей. Сообщалось, что «более 75% [систем здравоохранения] не используют инструменты сканирования и фильтрации электронной почты». Это упущение вызывает беспокойство, учитывая, что «91% атак программ-вымогателей являются результатом фишинговых атак» через замаскированные электронные письма. Многие больницы и системы здравоохранения признают, что не проявляют бдительности, не инвестируют в надлежащие технологии, не нанимают достаточно квалифицированных специалистов по ИТ-безопасности и просто не выделяют организации достаточный бюджет на обеспечение безопасности для сокращения или сведения к минимуму нарушений. Недостаточная безопасность электронной почты только усугубляет борьбу больницы или системы здравоохранения, чтобы защитить себя от атак программ-вымогателей и уменьшить ущерб, причиненный такими атаками.

Подключенные медицинские устройства системы здравоохранения: Disruptionware

Системы здравоохранения все больше полагаются на подключенные устройства в своей работе. Хакеры нацелены на эти устройства, чтобы вызвать крупномасштабное нарушение работы. «Подрывное ПО», как его теперь называют некоторые, может поставить медицинское учреждение почти на колени, ставя под угрозу целостность ePHI и совместимость подключенных медицинских устройств, необходимых для обеспечения беспрепятственного ухода за пациентами. Такая атака может вынудить систему здравоохранения и все ее учреждения отменить основные услуги, перенаправить и перевести пациентов в другие больницы и использовать аварийное резервное или ручное оборудование для поддержания жизни пациентов. Особое беспокойство вызывает то, что большое количество подключенных устройств «работают на устаревших системах, которые оставляют эти уязвимые конечные точки открытыми для злоумышленников». В то время как новые технологии улучшили безопасность данных, многие организации не могут

позволить себе заменить все свои технологии сразу и могут постепенно отказываться от устаревших устройств.

Иллюстрируя потенциальное влияние программ-вымогателей, в 2020 году произошли первые смерти, связанные с атаками программ-вымогателей. В одном случае новорожденный умер из-за того, что врачи якобы не провели критическое предродовое тестирование из-за кибератаки на больницу. Еще одна атака программы-вымогателя в 2020 году вынудила больницу перенаправить машину скорой помощи, и пациент умер, когда его перенаправили в другую больницу. Из-за возросшей угрозы и риска, связанного с подрывным программным обеспечением, федеральное правительство недавно начало уделять больше внимания кибербезопасности системы здравоохранения.

Ранее в этом году раздел 3305 Закона о сводных ассигнованиях от 2023 года внес поправки в федеральный закон о пищевых продуктах, лекарствах и косметических средствах, добавив раздел 524B «Обеспечение кибербезопасности устройств». Раздел 524B уполномочивает Управление по санитарному надзору за качеством пищевых продуктов и медикаментов (FDA) требовать от производителей медицинских устройств разработки и поддержания обновлений и исправлений «для мониторинга, выявления и устранения, при необходимости, в разумные сроки уязвимостей и эксплойтов кибербезопасности после выхода на рынок [.]» Новый раздел применяется к медицинским устройствам, определяемым как «киберустройство», которое «имеет возможность подключения к Интернету». Назначая производителей медицинских устройств сторонами, ответственными за мониторинг, выявление и устранение рисков кибербезопасности, связанных с их продуктами, Раздел 524B и аналогичные законы позволяют системам здравоохранения более эффективно сосредоточивать свои ресурсы.

Применимость правила безопасности HIPAA

В соответствии с HIPAA система здравоохранения — застрахованная организация (CE) или ее BA — должна внедрять «меры безопасности, которые могут помочь предотвратить внедрение вредоносных программ, включая программы-вымогатели». В соответствии с Правилом безопасности системы здравоохранения должны проводить анализ рисков «потенциальных рисков и уязвимостей в отношении конфиденциальности, целостности и доступности всей электронной PHI, которую организации создают, получают, поддерживают или передают, а также внедряют меры безопасности. достаточно для снижения этих выявленных рисков и уязвимостей до разумного и надлежащего уровня». Правило безопасности устанавливает только минимальный уровень безопасности ePHI, а дополнительные стандарты настоятельно рекомендуются и приветствуются в случае нарушения. Кроме того, «HHS считает любую успешную атаку программы-вымогателя нарушением [ePHI] и поэтому требует, чтобы застрахованная организация сообщала в HHS в соответствии с HIPAA».

В результате системы здравоохранения должны обеспечить защиту ePHI на внешнем интерфейсе за счет использования шифрования в соответствии с правилом безопасности HIPAA и руководством HHS, а также иметь план на случай непредвиденных обстоятельств для устранения нарушения в случае его возникновения, или, более уместно, когда происходит нарушение. Системы

здравоохранения должны активно разрабатывать сеть с надлежащим шифрованием, а также план действий в чрезвычайных ситуациях для устранения нарушений. Эти усилия не только снизят стоимость нарушения, но также снизят ответственность в соответствии с правилом безопасности HIPAA.

Использование руководства по внедрению HHS Cybersecurity Framework и NIST-CSF

В соответствии с усилением контроля со стороны правительства в области кибербезопасности системы здравоохранения, HHS выпустила в марте 2023 года всеобъемлющее руководство «Руководство по внедрению концепции кибербезопасности» для обеспечения соблюдения требований кибербезопасности в системах здравоохранения. Цель руководства состоит в том, чтобы помочь организациям сектора здравоохранения и общественного здравоохранения понять и использовать информационные справочники [Национального института стандартов технологий] Cybersecurity Framework [(NIST-CSF)] при реализации надежных программ кибербезопасности и управления киберрисками, охватывая пять основных функциональных областей NIST[-CSF] для обеспечения соответствия национальным стандартам, помощи организациям в оценке и повышении их уровня киберустойчивости, а также предоставления предложений о том, как связать кибербезопасность с их общей деятельностью по управлению информационной безопасностью и рисками для конфиденциальности.

Процесс из семи шагов сводится к следующему:

Определение стратегии риска кибербезопасности и проведение инвентаризации.

Выбор стандартов риска кибербезопасности.

Создание целей и задач с использованием фреймворков NIST.

Проведение оценки риска.

Выявление расхождений между результатами оценки и целями, созданными на шаге 3.

Оценка выявленных пробелов, проведение анализа затрат и результатов и выбор действий для устранения выявленных пробелов.

Реализация плана действий, который включает в себя отслеживание, мониторинг и оценку после реализации.

Заключение

Распространение программ-вымогателей и подрывных программ означает, что системы здравоохранения должны устанавливать или обновлять политики для предотвращения и обработки инцидентов и нарушений безопасности, включая: (1) как и когда раскрывать соответствующую информацию внутренним и внешним заинтересованным сторонам; и (2) планирование и управление ресурсами. Эти политики должны включать обучение по кибербезопасности для группы реагирования на инциденты/нарушения безопасности, а также соответствующее обучение сотрудников.

Ключом к успешному управлению рисками кибербезопасности является включение, внедрение и обучение всех заинтересованных сторон, сотрудников, систем и устройств. Сектор здравоохранения, считающийся «критически важным сектором инфраструктуры» и «основной услугой» во время пандемии COVID-19,

имеет решающее значение для здоровья и безопасности населения. Таким образом, для больниц и систем здравоохранения важно внедрять надежные программы, политики и процедуры кибербезопасности». ***(Mitchell J. Surface. Managing Ransomware Risk in Health Systems // Maynard Nexsen PC (https://www.maynardnexsen.com/publication-managing-ransomware-risk-in-health-systems). 18.04.2023).***

***

Захист персональних даних та соціальні мережі

«Всего через три дня после того, как Twitter опубликовал часть своего исходного кода в сети, которая включала алгоритм рекомендаций приложения, исследователь безопасности обнаружил, что злоумышленники могут манипулировать программным обеспечением, чтобы эффективно заглушить определенные учетные записи на платформе социальных сетей.

Аргентинский разработчик отметил проблему в сервисе хостинга программного обеспечения GitHub 1 апреля после того, как Twitter опубликовал код в паре репозиториев на сайте. «Текущая реализация позволяет скоординировано наносить ущерб репутации аккаунта без права регресса», — написал разработчик.

В результате некоммерческая корпорация Mitre присвоила частям кода Twitter общие уязвимости и уязвимости, или CVE, обозначение на основе того, как злоумышленники могут нацеливаться на определенные учетные записи, чтобы уменьшить их уязвимость на платформе. Неясно, кто отправил CVE в базу данных Mitre, и компания не будет идентифицировать того, кто отправил его на проверку, в соответствии с политикой компании.

CVE, который представляет собой обозначение, которое сообщество информационной безопасности использует для выявления и отслеживания публично раскрытых недостатков программного обеспечения, отмечает, что текущий алгоритм рекомендаций Twitter «позволяет злоумышленникам вызывать отказ в обслуживании (снижение оценки репутации), организуя несколько учетных записей Twitter для координировать негативные сигналы в отношении целевой учетной записи, такие как отмена подписки, отключение звука, блокировка и сообщение, которые использовались в дикой природе в марте и апреле 2023 года».

В тот же день, когда аргентинский разработчик отметил проблему, пользователь Twitter под именем «el gato malo» указал, по сути, на ту же проблему, отметив, что «именно так армии ботнетов/активистов уничтожают учетные записи». Пользователь отметил владельца Твиттера Илона Маска предложением учитывать только «синюю галочку: отключение звука/блокировка/отчеты». Маск ответил, спросив, кто стоит за ботнетами. «Награда в миллион долларов в случае осуждения», — написал Маск, хотя неясно, что означает «осужден» в этом контексте.

Twitter распустил свою пресс-группу и немедленно ответил на запрос о комментариях по поводу CVE и проблемы с алгоритмом: «💩».

В неподписанном блоге, размещенном на веб-сайте компании на прошлой неделе, Twitter заявил, что выпуск кода был «первым шагом в новую эру прозрачности», и что, как «городская площадь Интернета, мы в конечном итоге делаем это, чтобы способствовать прозрачности. и завоевать доверие наших пользователей, клиентов и широкой публики».

Позже Маск сказал на сеансе в Twitter Spaces, что релиз «будет довольно неловким, и люди будут штрафовать много ошибок, но мы собираемся исправить их очень быстро», согласно TechCrunch. Он добавил, что компания «стремится к отличному примеру Linux как операционной системы с открытым исходным кодом», где можно найти эксплойты, но «сообщество выявляет и исправляет эти эксплойты».

Существует около 650 CVE, в которых упоминается какой-либо алгоритм в базе данных Национального института стандартов и технологий, который отражает базу данных CVE, управляемую и поддерживаемую корпорацией Mitre. Представитель Mitre сообщил CyberScoop во вторник, что CVE, связанные с социальными сетями, присваивались в прошлом, в том числе CVE-2022-46405 и CVE-2022-48364, которые имеют отношение к сервису Mastodon». ***(AJ Vicens. Twitter's recommendation algorithm opens platform to manipulation, bot attacks, researcher finds // cyberscoop.com (https://cyberscoop.com/twitter-algorithm-cve-bots-elon-musk/). 04.04.2023).***

***

«Министерство торговли при президенте Байдене обдумывает принудительные меры в соответствии со своими правилами онлайн-безопасности против «Лаборатории Касперского», российской компании, занимающейся кибербезопасностью, которая, по словам людей, знакомых с этим вопросом, уже давно сталкивается с обвинениями в том, что она представляет угрозу для США.

Это действие — если оно будет реализовано — может стать проверкой растущей роли Министерства торговли в борьбе с онлайн-угрозами, по словам некоторых людей, которые заявили, что США могут применить те же правила онлайн-безопасности против технологий, контролируемых Китаем, включая, возможно, ТикТок.

Московская компания «Лаборатория Касперского» не сразу ответила на запрос о комментариях. Фирма, чье программное обеспечение было удалено из сетей федерального правительства США при администрации Трампа, неоднократно отрицала, что работает с Россией или каким-либо правительством для содействия кибершпионажу или другой злонамеренной киберактивности.

Представитель Министерства торговли заявил, что министерство не комментирует «какие-либо потенциальные конкретные действия компании», но заявило, что оно «привержено полному использованию своих полномочий для защиты конфиденциальных данных американцев и двухпартийной работе с Конгрессом для адаптации к меняющимся рискам».

Эти шаги были предприняты в связи с тем, что США также обдумывали, что делать с TikTok, принадлежащим пекинской компании ByteDance Ltd. На данный момент обсуждение TikTok сосредоточено в Комитете по иностранным инвестициям в США, межведомственном органе, который наблюдает за угрозами безопасности в трансграничные сделки.

Представитель Commerce сказал, что агентство работает над пересмотром правил онлайн-безопасности, известных как правила в области информационных и коммуникационных технологий и услуг. Правила направлены на защиту интернет-пользователей США от целого ряда угроз, включая шпионаж и дезинформацию, которые могут исходить от технологий и интернет-сервисов, базирующихся в потенциально враждебных странах, таких как Россия и Китай. Правила разрешают полный запрет определенных приложений, среди прочих средств правовой защиты.

Знакомые люди сказали, что решение о применении правил ICTS еще не принято, но некоторые говорят, что дискуссии в этом направлении недавно набрали обороты после длительного периода бездействия.

Некоторые республиканцы в Конгрессе раскритиковали Министерство торговли за «несоблюдение» правил ICTS Согласно августовскому письму 18 законодателей на имя министра торговли Джины Раймондо.

Чиновники торговли призывают Конгресс принять закон, чтобы укрепить свои позиции в борьбе с угрозами безопасности, исходящими от технологий, контролируемых из-за рубежа.

Некоторые законодатели во главе с сенатором Марком Уорнером (D., VA) и Джоном Тьюном (R., SD) недавно представили закон, который кодифицирует большую часть регулирующих полномочий департамента в отношении онлайн-безопасности, одновременно укрепляя правовые основы правил.

Администрация Байдена год назад — вскоре после вторжения России в Украину — обдумывала введение санкций в отношении «Лаборатории Касперского», как сообщал в то время журнал, но в конечном итоге не предприняла никаких действий из-за сопротивления со стороны некоторых официальных лиц США, которые были обеспокоены размером и размах такого шага.

Продукты «Лаборатории Касперского», в том числе антивирусное ПО, используют сотни миллионов клиентов по всему миру, в том числе в США.

Любые принудительные действия со стороны Министерства торговли, вероятно, должны быть узконаправленными, чтобы запретить программное обеспечение компании только в определенных контекстах, таких как его использование в компьютерных сетях, которые управляют критически важной инфраструктурой, сказал один из людей, знакомых с этим вопросом.

Частично сложность подачи иска заключается в неуверенности в том, насколько широко продукты «Лаборатории Касперского» внедрены в сети США, и в возможности того, что слишком широкое ограничение может привести к непредвиденным последствиям, например поставить под угрозу функциональность другого программного обеспечения, сказал этот человек.

Правила ICTS также позволяют другим федеральным агентствам передавать потенциальные дела на рассмотрение в Министерство торговли. Отдел национальной безопасности Министерства юстиции передал дело Касперского в

Министерство торговли в 2021 году, но, по словам человека, знакомого с этим вопросом, до недавнего времени эта передача практически не действовала.

Министерство юстиции отказалось от комментариев.

«Лаборатория Касперского» была основана в 1990-х годах Евгением Касперским, ученым-компьютерщиком и предпринимателем, прошедшим обучение в технической школе, спонсируемой КГБ. Фирма быстро превратилась в один из самых известных брендов в области кибербезопасности в мире. Многие западные исследователи кибербезопасности рассматривают «Лабораторию Касперского» как важного участника глобальных усилий по пониманию и смягчению киберугроз.

Американские, немецкие и другие западные разведчики годами заявляли, что программное обеспечение «Лаборатории Касперского» может быть использовано в качестве оружия для слежки за клиентами по указанию Кремля. Под влиянием этих опасений в 2017 году бывший президент Дональд Трамп приказал удалить программное обеспечение фирмы из всех гражданских и военных федеральных сетей США. Позже Конгресс кодифицировал запрет как закон.

В том же году журнал сообщил, что хакеры, работающие на российское правительство, украли информацию о программах киберразведки США после того, как подрядчик Агентства национальной безопасности удалил секретные материалы и поместил их на свой домашний компьютер.

По всей видимости, компьютер подрядчика был заражен в результате использования подрядчиком антивирусного программного обеспечения «Лаборатории Касперского». Было неясно, в какой степени «Лаборатория Касперского» была осведомлена о хакерской деятельности, и в заявлении «Лаборатории Касперского» говорится, что «ей не было предоставлено никакой информации или доказательств, подтверждающих этот предполагаемый инцидент, и в результате мы должны предположить, что это еще один пример ложного обвинения».

После запрета доступа к сетям федерального правительства США «Лаборатория Касперского» сообщила о двузначном снижении доходов в Северной Америке». ***(John D. McKinnon, Dustin Volz. Biden Administration Weighs Action Against Russian Cybersecurity Firm // Dow Jones & Company, Inc. (https://www.wsj.com/articles/biden-administration-weighs-action-against-russian-cybersecurity-firm-b84afcd7). 07.04.2023).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Кибербезопасность — это тема, которая затрагивает все сферы бизнеса. Согласно недавнему отчету Accenture, кибератаки могут стоить предприятиям более 5,2 триллиона долларов в виде упущенной выгоды и дополнительных расходов. Появление искусственного интеллекта (ИИ) принесло с собой некоторые решения, а также новые угрозы, которых не существовало некоторое время назад.

Давайте посмотрим на горько-сладкие отношения между ИИ и кибербезопасностью и на то, что с этим можно сделать.

Что такое искусственный интеллект?

Искусственный интеллект — это разработка и теория компьютерных систем, которые позволяют им справляться с задачами, обычно требующими человеческого интеллекта. К таким задачам относятся распознавание речи, визуальное восприятие, перевод и принятие решений. Эти возможности могут быть улучшены как положительно, так и отрицательно, как описано ниже.

Хорошо

Увеличение числа атак на кибербезопасность привело к росту числа продуктов для кибербезопасности на основе ИИ, которые, по оценкам, вырастут до 133,8 млрд долларов к 2030 году. По состоянию на 2022 год они стоили чуть более 14,9 миллиардов долларов. Организации могут использовать эти инструменты искусственного интеллекта для более эффективного обнаружения вредоносных программ и других угроз, а также использовать модель прогнозирования для прогнозирования будущих атак и подготовки к ним.

Управление уязвимостями

Организация часто подвергается нескольким уязвимостям. К сожалению, компания не может обрабатывать все уязвимости одновременно. Он должен придумать способ определить наиболее серьезные угрозы и справиться с ними в первую очередь. ИИ помогает сортировать угрозы и определять порядок приоритета.

Поиск угроз

Вместо того, чтобы просто проверять угрозы, которые были обнаружены ранее, ИИ помогает организациям выявлять другие угрозы, которые, возможно, не были обнаружены ранее. Он может использовать большие данные и другую доступную информацию для определения вероятных проблем, которые обычные инструменты могут не обнаружить, пока не произойдет событие.

Сетевая безопасность

Сетевая безопасность проверяет политики, чтобы убедиться, что не создаются вредоносные приложения для подключения, и отслеживает среду, чтобы убедиться, что нет лазеек, которые могут быть использованы. ИИ улучшает мониторинг окружающей среды и улучшает разработку политик, повышая безопасность.

Оптимизация процессов центра обработки данных

ИИ также можно использовать для оптимизации критически важных процессов в центре обработки данных, таких как резервное питание, энергопотребление, использование полосы пропускания, внутренняя температура и охлаждение. Он обеспечивает наилучшие значения для обеспечения эффективной работы инфраструктуры.

Плохо

К сожалению, даже несмотря на то, что ИИ хорошо справляется с кибербезопасностью, он открывает новые возможности для злоумышленников и хакеров, чтобы использовать и получать доступ к системам компании способами, которые они не могли бы получить с помощью традиционных методов

проникновения. Мы ожидаем увеличения числа кибератак с использованием ИИ в ближайшем будущем.

Киберпреступники могут использовать ИИ для сканирования сети организации на наличие уязвимых приложений, сетей и устройств, на которые они могут нацелиться для получения доступа. Фишинговые электронные письма, созданные с помощью ИИ, имеют больше шансов быть принятыми, чем другие электронные письма, что увеличивает риск того, что компания может быть атакована с использованием методов, которые в противном случае считались малорисковыми.

Хакеры также могут перепроектировать системы искусственного интеллекта и узнать наборы данных, которые использовались для создания систем. Затем они могут использовать эту информацию, чтобы найти способы получить доступ к системам.

Киберпреступники также могут использовать постоянно меняющиеся сигнатуры вирусов, чтобы обойти настроенные вами статические средства защиты, такие как обнаружение периметра и брандмауэры. Кроме того, ИИ может помочь вредоносным программам оставаться в системе, наблюдая за действиями пользователя и собирая другие важные данные до тех пор, пока не будут собраны все данные, необходимые для проведения атаки. Его также можно использовать для отправки данных хакерам с небольшим риском обнаружения.

Со временем компании, скорее всего, найдут средства защиты от различных угроз, связанных с ИИ. Тем не менее, хакеры могут настойчиво изобретать методы обхода установленных систем безопасности. Следовательно, использование ИИ — это лучший подход к решению проблем кибербезопасности. Компании должны помнить о том, что хакерский инструмент, управляемый искусственным интеллектом, может представлять более серьезные, опасные и неуловимые вредоносные программы или другие формы угроз.

Вывод: у ИИ есть преимущества и угрозы для кибербезопасности. В то время как это повышает способность компании справляться с угрозами и предсказывать их заранее, это также увеличивает площадь поверхности для хакеров, чтобы получить доступ к сети, использовать ресурсы, которые обычно им недоступны, и лучше обнаруживать слабые места в терминалах и системах компании. чем они были бы в традиционной установке». ***(Jim Goldman. AI For Cybersecurity Is Here To Stay—The Good And The Bad // Forbes (https://www.forbes.com/sites/tylerroush/2023/04/05/north-carolina-democrat-flips-to-republican-party-grants-state-gop-a-supermajority/?sh=19172ed65d29). 06.04.2023).***

***

«Образцовый набор возможностей и препятствий возник с наступлением цифровой эпохи. Тестирование кибербезопасности становится все более важным, поскольку организации стремятся защитить свои сети, данные и системы от вредоносных атак…

Одним из основных преимуществ использования ИИ в тестировании кибербезопасности является его способность обнаруживать и анализировать аномалии. Решения на основе искусственного интеллекта могут обнаруживать

аномальные действия и закономерности в данных, что может помочь организациям выявить потенциальные угрозы и уязвимости кибербезопасности.

Еще одним преимуществом является его способность быстро и точно выявлять вредоносные угрозы. Используя решения на основе ИИ, организации могут обнаруживать потенциальные атаки до того, как они произойдут, и предпринимать необходимые шаги для их смягчения.

1. Искусственный интеллект со временем становится умнее

Поскольку технология искусственного интеллекта может постепенно повышать безопасность сети, она более эффективна и сложна, чем можно было бы предположить из ее названия. Искусственный интеллект использует машинное обучение и глубокое обучение, чтобы лучше понять поведение организации в сети с течением времени. Они определяют шаблоны, присутствующие в сети, и после этого технология искусственного интеллекта группирует их вместе, прежде чем двигаться дальше, чтобы определить, произошли ли какие-либо отклонения от типичного трафика или инциденты безопасности. Когда он закончил обработку трафика, он реагирует на них.

2. ИИ помогает идентифицировать неизвестные угрозы

Из-за роста атак вредоносных программ и изощренной социальной инженерии, когда злоумышленники пробуют новые тактики для разрушения системы, становится жизненно важным перейти на обновленные решения, чтобы предотвратить повреждение системы кибератаками. Искусственный интеллект в сочетании с кибербезопасностью оказался одним из лучших сочетаний технологий безопасности с точки зрения обнаружения и предотвращения неизвестных угроз от разрушения сетевой инфраструктуры организации.

3. ИИ способен обрабатывать большие объемы данных

Искусственный интеллект выходит на сцену, чтобы выявить любые потенциальные риски, которые могут быть ошибочно истолкованы как рутинные действия. Это оказывается идеальным вариантом, потому что это так полезно. Он сканирует огромные объемы данных и анализирует трафик на наличие потенциальных рисков, потому что он автоматизирован, что позволяет ему делать это.

Резидентный прокси — это технология, использующая искусственный интеллект для облегчения передачи данных. Кроме того, он способен обнаруживать угрозы и идентифицировать поток трафика.

4. Искусственный интеллект лучше справляется с уязвимостями

Искусственный интеллект работает быстрее и может помочь нам в оценке наших систем быстрее, чем персонал по кибербезопасности, что снижает нашу рабочую нагрузку и увеличивает нашу способность решать проблемы в несколько раз. ИИ также выявляет слабые места в работе программного обеспечения и бизнес-сетях, позволяя организациям сосредоточиться на более важных задачах, связанных с безопасностью. Это обеспечивает своевременную защиту корпоративных систем и управление уязвимостями.

Более того, решения на основе ИИ могут обеспечивать анализ угроз безопасности и уязвимостей в режиме реального времени. Это позволяет организациям быстро реагировать на любые потенциальные угрозы и

предпринимать необходимые шаги для защиты своих сетей от атак. Наконец, решения на основе ИИ могут помочь организациям автоматизировать многие процессы тестирования кибербезопасности, высвобождая ресурсы для других задач.

Кибербезопасность и искусственный интеллект: три ключевые функции

Три ключевые цели ИИ в области кибербезопасности заключаются в следующем:

Prediction: функция прогнозирования используется второй по частоте. Около 35% предприятий в значительной степени полагаются на ИИ для прогнозирования кибератак. Основываясь на своем обучении, ИИ делает прогнозы, просеивая различные типы данных.

Предприятия, которые используют ИИ для прогнозирования, могут использовать эту технологию для автоматического анализа своих активов и топологии сети, выявления существенных слабых мест и постоянного усиления защиты своей сети от любых потенциальных катастрофических атак.

Обнаружение: организации теперь в значительной степени полагаются на ИИ для выявления киберугроз. Высокий уровень использования для обнаружения присутствует более чем в 50% организаций, использующих решения для кибербезопасности на основе ИИ. При обнаружении искусственный интеллект (ИИ) использует поведенческий анализ для непрерывного выявления необычного трафика. Это одна из отличительных особенностей ИИ, которая обеспечивается машинным или глубоким обучением.

Ответ: И последнее, но не менее важное: ИИ все еще развивается, когда речь идет о защите от угроз. Только 18% предприятий широко используют ИИ для защиты от кибератак. Это влечет за собой создание новых защитных механизмов в режиме реального времени или автоматизацию разработки виртуального патча для идентификации угроз.

Атаки могут быть легко обнаружены и остановлены в режиме реального времени с помощью стратегии реагирования ИИ. Это решение предотвратило аномальное поведение, вызванное ботами, например использование украденных учетных данных или несанкционированные покупки, совершенные с учетных записей клиентов.

Независимо от того, как предприятие использует ИИ для кибербезопасности, он помогает сократить расходы, сократить время реагирования на угрозы и реагировать на нарушения.

Проблемы ИИ в тестировании кибербезопасности

Несмотря на множество преимуществ использования ИИ в тестировании кибербезопасности, необходимо учитывать несколько проблем. Одной из основных проблем является стоимость внедрения и обслуживания решений на основе ИИ. Решения на основе ИИ требуют значительного количества ресурсов, как аппаратных, так и кадровых, и это может стать препятствием для некоторых организаций.

Еще одна проблема — сложность решений на основе ИИ. Решения на основе ИИ часто сложны и требуют значительного количества времени и ресурсов для настройки и обслуживания. Кроме того, решения на основе ИИ требуют серьезного

обучения, чтобы быть эффективными, и это может быть проблемой для некоторых организаций.

Наконец, решения ИИ эффективны настолько, насколько доступны данные. Если данные, используемые для обучения решений на основе ИИ, являются неполными или неточными, результаты могут быть ненадежными. Это может привести к ложноположительным и ложноотрицательным результатам, что может привести к неэффективным или неточным результатам тестирования безопасности.

Услуги по тестированию безопасности на основе ИИ

На рынке доступно множество решений для тестирования безопасности на основе ИИ. Некоторые из наиболее популярных решений включают в себя:

Системы обнаружения вторжений (IDS): IDS — это системы на базе ИИ, которые используются для обнаружения вредоносных действий в сети и реагирования на них. Они используют алгоритмы для анализа сетевого трафика и выявления подозрительных действий.

Системы управления уязвимостями (VMS): VMS — это система на базе ИИ, которая используется для оценки и выявления потенциальных уязвимостей в сети. Они используют алгоритмы для поиска слабых мест в сети и предоставляют рекомендации по смягчению любых потенциальных угроз.

Поведенческая аналитика. Поведенческая аналитика — это системы на базе искусственного интеллекта, которые используются для обнаружения и анализа подозрительного поведения пользователей. Они используют алгоритмы для мониторинга действий пользователей и выявления любых потенциальных вредоносных действий.

Системы аудита безопасности. Системы аудита безопасности — это системы на базе ИИ, которые используются для оценки состояния безопасности организации. Они используют алгоритмы для анализа сетей и выявления любых потенциальных слабых мест или уязвимостей.

Это лишь некоторые из доступных на рынке решений для тестирования безопасности на основе ИИ. Конечно, с помощью правильного решения для тестирования безопасности на основе ИИ организации могут лучше понять свое состояние кибербезопасности и снизить риск атак.

Как использовать ИИ в тестировании кибербезопасности

Чтобы использовать ИИ в тестировании кибербезопасности, важно понимать различные типы доступных решений для тестирования безопасности на основе ИИ. Во-первых, как только вы лучше поймете различные решения на основе ИИ, вы сможете начать оценивать, какие решения лучше всего соответствуют вашим потребностям в безопасности.

При оценке решений для тестирования безопасности на основе ИИ необходимо учитывать несколько ключевых факторов. К ним относятся:-

Стоимость: важно оценить стоимость внедрения и обслуживания решений для тестирования безопасности на основе ИИ.

Масштабируемость. Важно оценить масштабируемость решения для тестирования безопасности на основе ИИ.

Точность: важно оценить точность решения для тестирования безопасности на основе ИИ.

Простота использования: важно оценить простоту использования решения для тестирования безопасности на основе ИИ.

Оценивая эти факторы, вы можете определить, какое решение для тестирования безопасности ИИ лучше всего соответствует вашим потребностям.

Варианты использования тестирования кибербезопасности на основе ИИ

Решения для тестирования безопасности ИИ полезны в самых разных случаях использования. Некоторые из наиболее популярных вариантов использования включают в себя:

Мониторинг сетевой безопасности. Решения для тестирования безопасности на основе ИИ можно использовать для мониторинга сетей на предмет вредоносных действий и подозрительного поведения.

Обнаружение и устранение уязвимостей. Решения для тестирования безопасности на основе ИИ можно использовать для обнаружения и устранения потенциальных уязвимостей в сети.

Обнаружение и предотвращение вторжений. Решения для тестирования безопасности на основе ИИ можно использовать для обнаружения и предотвращения вредоносных действий в сети.

Аудит безопасности: решения для тестирования безопасности на основе ИИ можно использовать для оценки уровня безопасности организации.

Используя решения для тестирования безопасности на основе ИИ, организации могут лучше понять свою кибербезопасность и предпринять необходимые шаги для защиты своих сетей от атак.

Как улучшить стратегию тестирования безопасности на основе ИИ

Чтобы улучшить свою стратегию тестирования безопасности на основе ИИ, важно понимать различные типы доступных решений для тестирования безопасности на основе ИИ. Как только вы лучше поймете различные решения на основе ИИ, вы сможете начать оценивать, какие решения лучше всего соответствуют вашим потребностям в безопасности.

Хотя также важно оценить точность и масштабируемость ваших решений для тестирования безопасности на основе ИИ. Это гарантирует, что вы сможете точно обнаруживать и анализировать потенциальные угрозы и уязвимости. Кроме того, важно оценить стоимость внедрения и обслуживания ваших решений для тестирования безопасности на основе ИИ. Это гарантирует, что вы сможете использовать наиболее экономичные решения для своих нужд.

Наконец, важно убедиться, что ваши решения для тестирования безопасности на основе ИИ регулярно тестируются и обновляются. Это обеспечит точность и актуальность результатов. Кроме того, важно убедиться, что ваши решения для тестирования безопасности ИИ правильно настроены и поддерживаются. В целом это гарантирует, что они смогут обнаруживать и анализировать потенциальные угрозы и уязвимости.

Будущее ИИ в тестировании кибербезопасности

Будущее ИИ в тестировании кибербезопасности светлое. По мере того, как организации продолжают вкладывать средства в решения для тестирования безопасности на основе ИИ, эта технология будет становиться все более продвинутой и эффективной. Решения на основе ИИ станут более эффективными и

точными, что позволит организациям быстрее и точнее обнаруживать и анализировать потенциальные угрозы и уязвимости.

Более того, решения на основе ИИ станут более рентабельными. Поскольку организации продолжают инвестировать в решения для обеспечения безопасности на основе ИИ, стоимость внедрения и обслуживания будет снижаться. Это сделает решения на основе ИИ более доступными для организаций любого размера.

Наконец, решения на основе ИИ станут более изощренными. По мере того как организации продолжают инвестировать в решения на основе ИИ, эта технология будет становиться все более продвинутой и функциональной. Это позволит организациям более точно обнаруживать и анализировать вредоносные действия, а также выявлять потенциальные векторы атак…» ***(Timothy Joseph. The Future of AI in Cyber Security Testing: Unlock the Potential // ReadWrite, INC (https://readwrite.com/the-future-of-ai-in-cyber-security-testing-unlock-the-potential/). 05.04.2023).***

***

«…В недавнем исследовании IBM обнаружила, что средняя общая стоимость утечки данных достигла 4,35 млн долларов в 2022 году во всем мире и 9,44 млн долларов в США. Это подчеркивает потребность в более эффективных и упреждающих решениях в области кибербезопасности, которые обеспечивают более совершенные возможности обнаружения и реагирования.

В то время как традиционные системы управления информацией и событиями безопасности (SIEM) были стандартной частью арсенала кибербезопасности бизнеса, киберпреступники в настоящее время становятся все более изощренными, разрабатывая методы атак, которые все чаще способны скомпрометировать системы. Таким образом, организациям необходимо будет рассмотреть альтернативы SIEM, чтобы оставаться на шаг впереди. AI и ML становятся мощными инструментами, устраняющими ограничения традиционных систем SIEM.

В частности, AI и ML предоставляют инновационные альтернативы SIEM, предназначенные для защиты предприятий от растущих киберугроз. Это особенно важно для предоставления лицам, принимающим решения, ценных сведений об информационной безопасности и кибербезопасности, которые улучшат состояние безопасности. Одним из ключевых отличий является способ управления безопасностью. Традиционные системы SIEM предназначены для управления и анализа данных о событиях безопасности. Это приводит к проблемам, связанным с тем, как быстро развиваются векторы атак.

Однако по мере того, как организации генерируют больше данных из более широкого круга источников, системы SIEM часто сталкиваются с проблемами при обработке этой информации в режиме реального времени. Это приводит к задержке обнаружения угроз и реагирования на них.

Кроме того, такие традиционные системы основаны на методах, основанных на правилах, что затрудняет выявление новых или неизвестных угроз. Более продвинутые альтернативы традиционным системам SIEM гарантируют, что

средства защиты от кибербезопасности могут эффективно противостоять этим современным угрозам.

ИИ и машинное обучение революционизируют подход организаций к кибербезопасности, используя мощь алгоритмов, основанных на данных, и возможности самообучения. Они способны более эффективно обнаруживать угрозы и реагировать на них, а также учиться и адаптироваться к постоянно меняющемуся характеру кибератак.

Во-первых, AI и ML могут анализировать огромные объемы данных на высоких скоростях. Это позволяет обнаруживать угрозы и реагировать на них в режиме реального времени, что особенно важно, поскольку киберпреступники также начинают использовать одни и те же стратегии и инструменты для проведения своих атак. Быстрое выявление и устранение таких атак может значительно снизить потенциальный финансовый и репутационный ущерб для бизнеса.

AI и ML могут выявлять шаблоны и аномалии, которые могут указывать на ранее неизвестные угрозы. Тайский язык дает организациям преимущество в усилении своих мер безопасности, таким образом, оставаясь на шаг впереди киберпреступников и злоумышленников.

Как альтернативы SIEM используют ИИ для борьбы с угрозами

В связи с растущим спросом на альтернативные и интеллектуальные решения для кибербезопасности появились такие альтернативы SIEM, основанные на искусственном интеллекте и машинном обучении, которые предлагают инновационные подходы к борьбе с киберугрозами. Они выходят за рамки традиционных возможностей SIEM, поскольку включают в себя технологии, улучшающие обнаружение угроз, реагирование и прогнозный анализ.

Некоторые из них включают:

Организация безопасности, автоматизация и реагирование (SOAR). Эти платформы используют искусственный интеллект и машинное обучение для автоматизации повторяющихся задач, оптимизации процессов реагирования на инциденты и предоставления организациям более обоснованных возможностей для принятия решений в случае кибератаки. Интеграция с другими инструментами позволяет решениям SOAR создавать целостную экосистему безопасности, способную адаптироваться к новым угрозам по мере их появления.

Анализ поведения пользователей и объектов (UEBA): в этих решениях используются алгоритмы искусственного интеллекта и машинного обучения для отслеживания моделей поведения пользователей и объектов в цифровой среде организации. UEBA выявляет отклонения от нормы и, следовательно, может обнаруживать потенциальные внутренние угрозы, скомпрометированные учетные записи и другие риски безопасности. Это добавляет дополнительный защитный слой к защите кибербезопасности бизнеса.

Обнаружение конечных точек и реагирование (EDR): решения EDR сосредоточены на мониторинге и сборе данных с конечных точек, включая устройства IoT, смартфоны и устройства BYOD, для выявления потенциальных угроз. С помощью решений AI и ML EDR может проводить анализ в режиме реального времени и, таким образом, реагировать на угрозы также в режиме

реального времени. Это позволяет предприятиям снижать риски, связанные с расширением зоны атаки, в соответствии с растущей сегодня тенденцией использования BYOD и механизмов удаленной работы.

Некоторые проблемы впереди

Хотя альтернативы SIEM на основе ИИ и машинного обучения предлагают значительные преимущества, организации также должны учитывать потенциальные проблемы и риски, связанные с внедрением этих технологий, и, следовательно, должны учитывать следующие передовые практики:

Обеспечьте конфиденциальность данных и соблюдение нормативных требований. Решения на основе искусственного интеллекта и машинного обучения для эффективного функционирования полагаются на большие объемы данных, поэтому организации должны убедиться, что они соблюдают правила конфиденциальности данных и отраслевые требования соответствия.

Улучшите возможности человеческих ресурсов, чтобы восполнить пробел в навыках ИИ и машинного обучения. Согласно недавнему исследованию, только 10 процентов мировой рабочей силы обладают востребованными навыками, связанными с ИИ, которые будут полезны в эти меняющиеся времена. Поскольку новые технологии также потребуют высокоспециализированных навыков и опыта, отрасли должны обеспечить, чтобы их человеческие ресурсы не отставали.

Баланс между безопасностью, эффективностью и пользовательским интерфейсом. Поддержание положительного пользовательского опыта является ключом к более широкому принятию и внедрению любой технологии. По мере того, как организации внедряют передовые решения в области кибербезопасности, они должны найти баланс между повышением безопасности и поддержанием операционной эффективности.

Поскольку альтернативы SIEM, основанные на искусственном интеллекте и машинном обучении, продолжают набирать обороты, для лиц, принимающих решения, крайне важно осознавать потенциал этих технологий и расставлять приоритеты в их внедрении в своих организациях, особенно в тех, которые сосредоточены на информационной безопасности и кибербезопасности. Ключевой персонал должен быть в курсе последних разработок в области искусственного интеллекта и машинного обучения и понимать преимущества, которые они могут принести с точки зрения улучшения стратегий кибербезопасности. Таким образом, лица, принимающие решения, могут сделать более осознанный выбор инструментов и решений, которые они внедряют для защиты своего бизнеса от киберугроз.

Чтобы обеспечить успешный переход к решениям для кибербезопасности, основанным на искусственном интеллекте и машинном обучении, организации также должны инвестировать в создание квалифицированной рабочей силы, которая понимает эти технологии и может эффективно их использовать. Это может включать предоставление возможностей для обучения и развития, а также сотрудничество с академическими учреждениями и отраслевыми партнерами для устранения пробелов в навыках искусственного интеллекта и машинного обучения.

Внимательно изучая эти проблемы и работая над их преодолением, организации могут успешно использовать потенциал альтернатив SIEM на основе

искусственного интеллекта и машинного обучения для повышения своей кибербезопасности во все более сложной цифровой среде». ***(Evan Morris. Machine Learning and AI: The Future of SIEM Alternatives in Cybersecurity // TechTarget (https://www.datasciencecentral.com/machine-learning-and-ai-the-future-of-siem-alternatives-in-cybersecurity/amp/). 11.04.2023).***

***

«Согласно отчету израильской венчурной фирмы Team8, компании, использующие инструменты генеративного искусственного интеллекта, такие как ChatGPT, могут подвергать риску конфиденциальную информацию о клиентах и коммерческую тайну.

Широкое внедрение новых чат-ботов с искусственным интеллектом и инструментов для письма может сделать компании уязвимыми для утечек данных и судебных исков, говорится в отчете, который был предоставлен Bloomberg News до его публикации. Есть опасения, что чат-боты могут быть использованы хакерами для доступа к конфиденциальной корпоративной информации или совершения действий против компании. Есть также опасения, что конфиденциальная информация, поступающая в чат-боты сейчас, может быть использована ИИ-компаниями в будущем.

Крупные технологические компании, в том числе Microsoft Corp. and Alphabet Inc. спешит добавить возможности генеративного искусственного интеллекта для улучшения чат-ботов и поисковых систем, обучая свои модели на данных, взятых из Интернета, чтобы предоставить пользователям универсальное решение для их запросов. В отчете говорится, что если эти инструменты будут передавать конфиденциальные или частные данные, будет очень сложно стереть информацию.

«Корпоративное использование GenAI может привести к доступу и обработке конфиденциальной информации, интеллектуальной собственности, исходного кода, коммерческой тайны и других данных посредством прямого ввода пользователем или API, включая информацию о клиентах или личную информацию и конфиденциальную информацию», — говорится в отчете. классифицируя риск как «высокий». Он описал риски как «управляемые», если будут введены надлежащие меры безопасности.

В отчете Team8 подчеркивается, что запросы чат-ботов не передаются в широкоязычные модели для обучения ИИ, в отличие от недавних отчетов о том, что такие запросы потенциально могут быть замечены другими.

«На момент написания этой статьи большие языковые модели не могут обновляться в режиме реального времени и, следовательно, не могут возвращать чьи-то входные данные к чужому ответу, эффективно развенчивая эту проблему. Однако это не обязательно верно для обучения будущих версий этих моделей», — говорится в сообщении.

В документе отмечены три другие проблемы «высокого риска» при интеграции генеративных инструментов искусственного интеллекта и подчеркнута повышенная угроза обмена информацией через сторонние приложения. Microsoft

внедрила некоторые функции чат-бота AI в свою поисковую систему Bing и инструменты Microsoft 365.

«Например, на стороне пользователя сторонние приложения, использующие API GenAI, в случае взлома потенциально могут предоставить доступ к электронной почте и веб-браузеру и позволить злоумышленнику выполнять действия от имени пользователя», — говорится в сообщении.

По его словам, существует «средний риск» того, что использование генеративного ИИ может усилить дискриминацию, нанести ущерб репутации компании или подвергнуть ее судебному иску по вопросам авторского права.

Энн Джонсон, корпоративный вице-президент Microsoft, участвовала в составлении отчета. Microsoft вложила миллиарды в Open AI, разработчика ChatGPT.

«Microsoft поощряет прозрачное обсуждение развивающихся киберрисков в сообществах безопасности и искусственного интеллекта», — сказал представитель Microsoft.

Десятки главных сотрудников по информационной безопасности американских компаний также указаны в качестве соавторов отчета. Отчет Team8 также был одобрен Майклом Роджерсом, бывшим главой Агентства национальной безопасности США и Киберкомандования США». ***(Marissa Newman. ChatGPT Poised to Expose Corporate Secrets, Cyber Firm Warns // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2023-04-18/chatgpt-poised-to-expose-corporate-secrets-cyber-firm-warns). 18.04.2023).***

***

«С момента своего запуска в ноябре 2022 года ChatGPT, чат-бот с искусственным интеллектом (ИИ), вызвал настоящий ажиотаж из-за удивительно человечных и точных ответов программного обеспечения.

Автогенерирующая система достигла рекордных 100 миллионов активных пользователей в месяц всего через два месяца после запуска. Однако, хотя его популярность продолжает расти, в настоящее время в индустрии кибербезопасности обсуждается вопрос о том, поможет ли этот тип технологии сделать Интернет более безопасным или сыграет на руку тем, кто пытается создать хаос.

Программное обеспечение AI имеет множество вариантов использования в области кибербезопасности, включая расширенный анализ данных, автоматизацию повторяющихся задач и помощь в расчете оценок риска. Однако вскоре после его дебюта было быстро установлено, что этот простой в использовании, свободно доступный чат-бот может также помочь хакерам проникнуть в программное обеспечение и разработать сложные фишинговые инструменты…

Как и любое новое технологическое достижение, всегда будут некоторые негативные последствия, и ChatGPT ничем не отличается.

В настоящее время наиболее обсуждаемая проблема, связанная с чат-ботом, связана с простотой создания очень убедительных фишинговых текстов, которые, вероятно, будут использоваться во вредоносных электронных письмах., чей родной язык может быть не английским, было легко. Из-за отсутствия мер безопасности

злоумышленникам использовать механизм ChatGPT для создания красноречивого, заманчивого сообщения, написанного с почти идеальной грамматикой за считанные секунды.

И поскольку американцы потеряли 40 миллиардов долларов в 2022 году из-за этих мошенников, легко понять, почему преступники использовали ChatGPT, чтобы получить кусок этого прибыльного незаконного пирога.

Чат-боты на базе ИИ также поднимают вопрос о безопасности труда. Конечно, существующая система не может заменить высококвалифицированного специалиста, но эта технология позволяет значительно сократить количество журналов и отчетов, которые необходимо проверить сотруднику. Это может повлиять на то, сколько аналитиков потребуется нанять операционному центру безопасности (SOC).

Хотя программное обеспечение действительно предлагает несколько преимуществ для предприятий, занимающихся кибербезопасностью, будет много компаний, которые примут эту технологию просто из-за ее нынешней популярности и попытаются привлечь с ее помощью новых клиентов. Однако использование технологии исключительно из-за ее причудливого статуса может привести к неправильному использованию. Компании могут не устанавливать надлежащие меры безопасности, что препятствует прогрессу в создании эффективной программы безопасности.

Как и в случае с любой новой технологией, сбой является неизбежным компонентом, но это не должно быть чем-то плохим.

Компании, занимающиеся кибербезопасностью, могут добавить дополнительный уровень интеллекта к своим ручным усилиям по просеиванию журналов аудита или проверке сетевых пакетов, чтобы отличить угрозы от ложных тревог.

Благодаря способности ChatGPT обнаруживать шаблоны и выполнять поиск по определенным параметрам, его также можно использовать для повторяющихся задач и создания отчетов. Затем киберкомпании могут более разумно рассчитывать оценки риска для угроз, влияющих на организации, используя ChatGPT в качестве сверхмощного помощника по исследованиям.

Например, Orca Security, израильская компания по кибербезопасности, начала использовать превосходные аналитические возможности ChatGPT, чтобы проникнуть в океан данных и помочь с оповещениями безопасности. Заранее поняв, как чат-бот может улучшить свою повседневную работу, компания также может извлечь уроки из этой технологии, что дает ей уникальное преимущество в настройке своих моделей для оптимизации того, как ChatGPT работает для ее бизнеса.

Кроме того, обработка естественного языка чат-ботом, благодаря которой он так хорошо пишет фишинговые электронные письма, означает, что он также идеально подходит для создания сложных политик безопасности. Эти четко сформулированные тексты можно использовать на веб-сайтах по кибербезопасности и в учебных документах, экономя драгоценное время для ценных членов команды.

Технология искусственного интеллекта ChatGPT легкодоступна для большей части мира. Поэтому, как и в любой другой битве, это просто гонка, чтобы увидеть, какая сторона лучше использует технологию.

Компании, занимающиеся кибербезопасностью, должны будут постоянно бороться с гнусными пользователями, которые найдут способы использовать ChatGPT для причинения вреда способами, которые компании, занимающиеся кибербезопасностью, еще не поняли. И все же этот факт не отпугнул инвесторов, и будущее ChatGPT выглядит очень радужным. Поскольку Microsoft инвестирует 10 миллиардов долларов в Open AI, становится ясно, что знания и возможности ChatGPT будут продолжать расширяться.

Для будущих версий этой технологии разработчикам программного обеспечения необходимо обратить внимание на отсутствие в ней мер безопасности, а дьявол будет кроться в деталях.

ChatGPT, вероятно, не сможет в значительной степени решить эту проблему. У него могут быть механизмы для оценки привычек пользователей и обнаружения людей, которые используют очевидные подсказки, такие как «напишите мне фишинговое письмо, как будто я чей-то начальник», или пытаются подтвердить личность людей.

Открытый ИИ может даже работать с исследователями, чтобы обучить свои наборы данных оценивать, когда их текст использовался в атаках в других местах.

Однако все эти идеи создают множество проблем, включая рост затрат и проблемы с защитой данных.

Чтобы остановить нынешнюю эпидемию фишинга, большему количеству людей необходимо образование и осведомленность для выявления таких атак. И индустрия нуждается в дополнительных инвестициях со стороны операторов сотовой связи и провайдеров электронной почты, чтобы смягчить количество атак, происходящих в дикой природе…» ***(Taylor Hersom. ChatGPT may hinder the cybersecurity industry // VentureBeat (https://venturebeat.com/security/chatgpt-may-hinder-the-cybersecurity-industry/). 22.04.2023).***

***

«Европол обеспокоен тем, что хакеры могут использовать сервисы генеративного искусственного интеллекта (ИИ), такие как ChatGPT и Google Bard, для кодирования вредоносных программ и других поддельных приложений, которые могут обмануть ничего не подозревающих пользователей. И исследователи безопасности уже показали, как легко с помощью ChatGPT создавать необнаруживаемое вредоносное ПО, несмотря на средства защиты OpenAI, встроенные в его большую языковую модель.

Но существует еще один опасный тип вредоносных атак, который на самом деле не использует возможности ChatGPT для создания поддельных приложений. Вместо этого исследователи безопасности обнаружили, что злоумышленники используют расширения и приложения, маскирующиеся под законные приложения ChatGPT или Google Bard. Затем они могут использовать эти приложения в качестве векторов для развертывания вредоносного ПО для кражи данных.

Атака довольно проста и является неудачным результатом бизнес-модели OpenAI ChatGPT. Тот, которому также следуют Microsoft и Google.

У OpenAI нет специализированных приложений ChatGPT для разных операционных систем. Генеративный ИИ доступен через веб-браузеры на любом устройстве. Но многие компании создали законные приложения ИИ для различных платформ. Одним из таких примеров является iOS, так как iPhone предлагает доступ ко множеству отличных приложений ChatGPT.

Также появляется все больше расширений для браузера, которые упрощают использование ChatGPT, чем посещение веб-сайта OpenAI.

Таким образом, пользователи уже обучены искать более простые способы доступа к ChatGPT. Google Bard даже не широко доступен, но поддельные приложения привлекли бы много внимания. Злоумышленникам нужно только заставить ничего не подозревающих пользователей установить поддельные расширения или приложения ChatGPT или Google Bard на свои компьютеры.

YouTuber Джон Хаммонд показал в видео множество приложений и расширений ChatGPT, доступных для загрузки прямо сейчас. Ролик основан на отчете Guardio, в котором подробно описывается поддельное расширение ChatGPT Chrome, которое распространяло вредоносное ПО среди целей.

Пользователи, которые установили приложение, подвергались риску кражи вредоносной программой доступа к их учетным записям Facebook. Злоумышленники могут захватить эти учетные записи для вредоносных целей, в том числе для оплаты рекламы деньгами пользователя. Вредоносная программа также будет извлекать пользовательские данные, которые хакеры могут продавать через Интернет или использовать для дополнительных атак.

Более того, вредоносное ПО может даже развернуть поддельное приложение Facebook, которое может дополнительно контролировать ваш профиль и страницы. Приложение выглядит как настоящее, но в нем включены все разрешения, что дает хакерам полный контроль над профилем и страницей Facebook.

Отдельно охранная фирма Verity обнаружила еще одну атаку с использованием поддельных приложений ChatGPT и Google Bard.

Атака состоит из двух этапов и не имеет ничего общего с огромными возможностями ChatGPT. ИИ вообще не участвует в этом процессе.

Во-первых, хакеры развертывают программное обеспечение «вредоносное ПО как услуга». В частности, мы рассматриваем вредоносное ПО RedLine Stealer, которое продается в даркнете по цене около 150 долларов.

Затем злоумышленники пытаются украсть учетные данные бизнес-аккаунта Facebook или учетной записи сообщества с тысячами подписчиков. После этого они используют страницы Facebook для размещения спонсируемых сообщений, которые продвигают бесплатные загрузки приложений ChatGPT и Google Bard. Когда пользователи загружают поддельные приложения, они на самом деле получают вредоносное ПО RedLine Stealer.

Затем вредоносное ПО может украсть конфиденциальную информацию у пользователей, установивших поддельные приложения. Данные вашей кредитной карты и другие сохраненные учетные данные в браузере могут быть под угрозой. То же самое касается и других данных на вашем компьютере.

Согласно информации Veriti, количество атак, основанных на популярности приложений с искусственным интеллектом, таких как ChatGPT и Google Bard, с января неуклонно растет, а в марте резко возросло. Тенденция, вероятно, сохранится до тех пор, пока ничего не подозревающие пользователи продолжают попадаться на поддельные приложения с искусственным интеллектом.

Вы должны запускать антивирусное программное обеспечение на своих устройствах и устанавливать последние исправления безопасности, чтобы повысить вероятность обнаружения вредоносных приложений, работающих на ваших компьютерах. Вы также можете запустить ChatGPT в браузере, отличном от того, который вы используете для Facebook и других популярных сайтов. Таким образом, вы можете уменьшить масштабы атак.

Но самый простой способ защитить себя от таких атак — не загружать какое-либо приложение или расширение ChatGPT, пока вы не убедитесь, что оно подлинное. Поищите в Интернете дополнительную информацию о приложении и узнайте, кто за ним стоит.

Вы не должны доверять какой-либо рекламе Facebook, рекламирующей такие приложения, так как вы рискуете загрузить вредоносное ПО ChatGPT или Google Bard вместо реального.

Кроме того, убедитесь, что вы загружаете приложения и расширения из надежных магазинов только после проверки их подлинности.

Вам следует избегать открытия любых подозрительных файлов и электронных писем, которые вы получаете, чтобы снизить риск установки вредоносных программ, которые могут украсть учетные данные Facebook.

Наконец, вы должны использовать надежный уникальный пароль для своей учетной записи Facebook, особенно если вы управляете страницами и сообществами с большим количеством подписчиков. И вы можете часто менять этот пароль, чтобы усложнить работу злоумышленников». ***(Chris Smith. How to avoid ChatGPT and Google Bard malware attacks // BGR Media, LLC. (https://bgr.com/tech/how-to-avoid-chatgpt-and-google-bard-malware-attacks/). 14.04.2023).***

***

«В области генеративного ИИ появляется новая тенденция — генеративный ИИ для кибербезопасности — и Google входит в число тех, кто хочет войти в число первых.

Сегодня на конференции RSA 2023 Google анонсировала Cloud Security AI Workbench, пакет кибербезопасности, основанный на специализированной языковой модели «безопасности» AI под названием Sec-PaLM. По словам Google, ответвление модели Google PaLM, Sec-PaLM «точно настроено для случаев использования в сфере безопасности», включая анализ уязвимостей программного обеспечения, вредоносных программ, индикаторов угроз и поведенческих профилей субъектов угроз.

Cloud Security AI Workbench включает в себя ряд новых инструментов на основе ИИ, таких как ИИ Mandiant Threat Intelligence, который будет использовать Sec-PaLM для поиска, обобщения и устранения угроз безопасности. (Напомним,

что Google приобрела Mandiant в 2022 году за 5,4 миллиарда долларов.) VirusTotal, еще одна собственность Google, будет использовать Sec-PaLM, чтобы помочь подписчикам анализировать и объяснять поведение вредоносных скриптов.

В другом месте Sec-PaLM будет помогать клиентам Chronicle, облачной службы кибербезопасности Google, в поиске событий безопасности и «консервативном» взаимодействии с результатами. Тем временем пользователи Google Security Command Center AI получат «удобочитаемые» объяснения подверженности атакам от Sec-PaLM, включая затронутые активы, рекомендуемые меры по смягчению последствий и сводки рисков для безопасности, соответствия и конфиденциальности.

«Несмотря на то, что генеративный ИИ в последнее время захватывает воображение, Sec-PaLM основан на многолетних фундаментальных исследованиях ИИ, проведенных Google и DeepMind, а также на глубоком опыте наших команд по безопасности», — написал Google сегодня утром в своем блоге. «Мы только начали осознавать возможности применения генеративного ИИ для обеспечения безопасности, и мы с нетерпением ждем возможности продолжать использовать этот опыт для наших клиентов и продвигать достижения в сообществе безопасности».

Это довольно смелые амбиции, особенно если учесть, что VirusTotal Code Insight, первый инструмент в Cloud Security AI Workbench, на данный момент доступен только в ограниченной предварительной версии. (Google заявляет, что планирует развернуть остальные предложения для «доверенных тестировщиков» в ближайшие месяцы.) Честно говоря, неясно, насколько хорошо Sec-PaLM работает — или не работает — на практике. Конечно, «рекомендуемые меры по смягчению последствий и сводки рисков» звучат полезно, но стали ли эти предложения лучше и точнее, потому что их создала модель ИИ?

В конце концов, языковые модели ИИ, какими бы передовыми они ни были, допускают ошибки. И они подвержены таким атакам, как быстрое внедрение, что может привести к тому, что они будут вести себя не так, как предполагали их создатели.

Конечно, это не останавливает технологических гигантов. В марте Microsoft запустила Security Copilot, новый инструмент, предназначенный для «обобщения» и «придания смысла» информации об угрозах с использованием генеративных моделей искусственного интеллекта от OpenAI, включая GPT-4. В материалах для прессы Microsoft, как и Google, заявила, что генеративный ИИ лучше вооружит специалистов по безопасности для борьбы с новыми угрозами.

Присяжные очень не согласны с этим. По правде говоря, генеративный ИИ для кибербезопасности может оказаться более шумным, чем что-либо еще — исследований его эффективности не хватает. Если повезет, мы скоро увидим результаты, а пока отнеситесь к заявлениям Google и Microsoft с изрядной долей скептицизма». ***(Kyle Wiggers. Google brings generative AI to cybersecurity // Yahoo (https://techcrunch.com/2023/04/24/google-brings-generative-ai-to-cybersecurity/). 24.04.2023).***

***

«…ИИ недавно оказался в центре внимания индустрии кибербезопасности. Он начинался как интеллектуальный агент, который искал вредоносные программы и другие аномалии в системах безопасности, но позже расширил свой арсенал для решения более сложных проблем безопасности.

ИИ может выявлять новые штаммы вредоносных программ, обнаруживать слабые звенья, скрытые в бесчисленных строках кода, и предсказывать киберпреступления до их совершения (возможно, даже кибератаки в космосе).

Это наиболее важные роли, которые ИИ играет в укреплении кибербезопасности.

Автоматическое обнаружение активов

Поскольку ИТ-активы являются основной целью киберпреступников, очень важно иметь актуальную информацию обо всем оборудовании, программном обеспечении и облачных активах, таких как данные.

Поскольку в сети организации постоянно что-то меняется, например постоянно добавляются и удаляются новые устройства, обнаружение активов может стать серьезной проблемой для ИТ-менеджеров. Здесь в игру вступает ИИ. Автоматизируя обнаружение активов, ИИ делает весь процесс более эффективным и менее подверженным человеческим ошибкам. Кроме того, ИИ укрепляет кибербезопасность организации путем поиска уязвимостей как в инфраструктуре, так и в системах, таких как устаревшее программное обеспечение, утечки данных и уязвимые приложения.

Сетевой мониторинг и управление

Целью мониторинга сети является предоставление релевантной информации в режиме реального времени (такой как поток трафика, использование полосы пропускания и время безотказной работы), которая информирует сетевых администраторов об оптимальной работе сети. С помощью ИИ система мониторинга сети может выиграть от автоматизации, которая упростит и ускорит процесс мониторинга и обслуживания.

ИИ может отслеживать сеть без остановки и оперативно предупреждать администраторов о любых серьезных проблемах, которые необходимо решить, избегая при этом ложных тревог (хотя некоторые ИИ склонны к ложным срабатываниям). Кроме того, ИИ может определять приоритеты проблем, поэтому администраторы знают, какие из них требуют немедленного внимания.

Прогнозирование и предотвращение кибератак

Используя прогнозный ИИ, администраторы могут получать предупреждения об уязвимостях нулевого дня в программном обеспечении организации до того, как произойдет успешная кибератака и будет нанесен непоправимый ущерб. Без него киберпреступники могли бы атаковать эти уязвимости, запуская так называемые атаки нулевого дня с использованием эксплойтов нулевого дня, неизвестных даже самим поставщикам программного обеспечения.

Кроме того, ИИ можно использовать для обнаружения киберугроз и подозрительной кибератвности. Стандартные системы безопасности не могут справиться с новыми, более сложными вредоносными программами, которые появляются с беспрецедентной скоростью. Однако с помощью искусственного

интеллекта и его сложных алгоритмов он может распознавать закономерности, обнаруживать вредоносные программы и обнаруживать даже малейшие признаки атак вредоносных программ или программ-вымогателей до того, как они проникнут в ИТ-систему.

Если вы думаете, что ваш бизнес слишком мал для серьезных киберугроз, подумайте еще раз. Существуют кибератаки, с которыми обычно сталкиваются предприятия независимо от их размера.

Реагирование на инцидент

Реагирование безопасности на киберугрозы, автоматизированное с помощью ИИ, требует меньше времени и снижает риск человеческой ошибки. ИИ помогает сотрудникам службы безопасности управлять оповещениями о безопасности в больших масштабах, выявлять конкретные угрозы, определять приоритеты рисков и находить нужные ресурсы для реагирования на угрозы высокого риска.

Это может быть особенно полезно в ситуации, когда сотрудники службы безопасности не знают, как реагировать на малоизвестный инцидент. В таком случае защитное решение на основе ИИ может взять на себя управление, автоматически отключить скомпрометированные системы и уменьшить ущерб, нанесенный кибератакой.

Устранение человеческих ошибок

Хорошо, мы не можем ожидать, что ИИ полностью устранит фактор человеческой ошибки, по крайней мере, на данный момент. Тем не менее, ИИ может свести к минимуму человеческие ошибки, взяв на себя ручные и полуручные задачи, которые иногда страдают от метода проб и ошибок.

В конце концов, большинство нарушений кибербезопасности можно отнести к человеческим ошибкам, что подтверждает тот прискорбный факт, что мы являемся самым слабым звеном в цепочке кибербезопасности. Если мы посмотрим на крупнейшие утечки данных 2022 года, мы заметим одну общую черту: человеческий фактор, которого можно было бы избежать.

Плюсы использования ИИ в кибербезопасности

Решения на базе ИИ способны выявлять, анализировать и устранять киберугрозы быстрее, чем традиционное программное обеспечение для обеспечения безопасности, что делает их мощным инструментом в борьбе с киберпреступностью. Некоторые из основных преимуществ использования ИИ в кибербезопасности включают в себя:

ИИ может работать круглосуточно: ИИ не нужно находить баланс между профессиональной и личной жизнью, делать перерывы и сопротивляться прокрастинации. ИИ может работать 24/7/365 без отдыха.

Со временем ИИ становится все более интеллектуальным: ИИ использует преимущества машинного и глубокого обучения, поэтому технология, стоящая за ним, также становится более продвинутой.

ИИ может анализировать данные быстрее, чем что-либо другое: даже если мы говорим о быстро развивающемся бизнесе с большими объемами данных, ИИ может просмотреть их за очень короткое время и найти любую угрозу, скрытую в трафике.

ИИ способен выявлять неизвестные угрозы: хотя люди могут быть не в состоянии идентифицировать неизвестные им угрозы, ИИ гораздо более активен — иногда даже склонен к ложным срабатываниям — когда дело доходит до выявления новых киберугроз.

Минусы использования ИИ в кибербезопасности

Как и у большинства вещей в жизни, у ИИ есть и темная сторона, и во многом это связано с тем, что его могут использовать и киберпреступники. Итак, вот несколько минусов использования ИИ в кибербезопасности.

Плохие парни тоже могут использовать ИИ: к сожалению, у ИИ нет морального компаса, а это означает, что киберпреступники могут использовать его технологию для создания более изощренных автоматизированных кибератак. Например, ИИ можно использовать для поиска слабых мест в системах безопасности, что позволяет киберпреступникам использовать их.

ИИ не может мыслить нестандартно: хотя ИИ способен накапливать и анализировать информацию, он не креативен в своем подходе к обучению. Без участия человека он может оказаться неэффективным в ситуациях, требующих творческого подхода, таких как атаки со стороны противника.

ИИ не застрахован от ошибок: хотя люди более склонны к ошибкам, ИИ тоже можно обмануть. Например, состязательные атаки создаются, чтобы перехитрить алгоритм машинного обучения, в результате чего ИИ неправильно интерпретирует данные, созданные со злым умыслом, и начинает совершать ошибки, которые ставят под угрозу общую безопасность.

Кто больше выигрывает от роли ИИ в кибербезопасности: хорошие или плохие парни?

Хотя обе стороны выигрывают от роли ИИ в кибербезопасности, нельзя отрицать, что ИИ обладает огромным потенциалом для того, чтобы сделать онлайн-мир более безопасным.

ИИ может помочь нам обнаруживать и определять приоритеты рисков, непосредственно реагировать на инциденты и обнаруживать киберугрозы до того, как будет нанесен ущерб. Хотя у ИИ есть недостатки, такое программное обеспечение играет решающую роль в укреплении кибербезопасности. Но наша роль — следить за тем, чтобы распространение ИИ не вышло из-под контроля. ***(Sead Fadilpašić. Is the Use of AI in Cybersecurity Making the World More Secure? // www.makeuseof.com (https://www.makeuseof.com/ai-cybersecurity-making-world-more-secure/). 25.04.2023).***

***

Кіберзлочинність та кібертероризм

«В новом отчете, опубликованном в среду, говорится, что более половины (52%) организаций пострадали от утечки данных за последние два года во всем мире, увеличившись с 49% в 2022 году до 39% в 2021 году.

Согласно отчету State of Security 2023, подготовленному компанией-разработчиком программного обеспечения Splunk, около 62 % респондентов

заявили, что их критически важные бизнес-приложения страдали от незапланированных простоев из-за инцидента кибербезопасности не реже одного раза в месяц, по сравнению с 54 % в 2022.

«В организациях, с которыми мы работали, устойчивость была наибольшей благодаря совместному подходу во всем, от разработки программного обеспечения и мониторинга инфраструктуры до планирования обеспечения непрерывности бизнеса. Этот подход объединяет всех, в том числе руководителей по безопасности с ИТ-руководителями и бизнес-лидерами, поэтому все они могут сосредоточиться на защите организации», — сказал Райан Ковар, выдающийся стратег безопасности Splunk и руководитель SURGe.

Более того, в Индии около 42 % организаций сообщают, что они перегружены атаками с утечкой данных, по сравнению с 23 % в остальном мире.

Почти 48% индийских организаций говорят, что их стек безопасности слишком сложен, по сравнению с 28% в остальном мире.

В отчете также упоминается, что организации в Индии чаще сообщают о взломах за последние два года: 59% по сравнению с 45% респондентов в других странах Азиатско-Тихоокеанского региона.

В отчете также говорится, что, хотя предприятия сталкиваются с серьезными препятствиями в области кибербезопасности, многие организации предпринимают шаги для решения этих проблем.

Около 95% респондентов говорят, что их бюджеты на безопасность увеличатся в течение следующих двух лет, при этом 56% заявили, что их бюджеты увеличиваются «значительно».

Почти 81% организаций говорят, что они объединяют аспекты своей безопасности и ИТ-операций.

Около 95% респондентов говорят, что они уделяют больше внимания оценке рисков третьими сторонами». ***(About 52% of organisations suffered data breach in past 2 years globally // The Statesman Limited. (https://www.thestatesman.com/technology/about-52-of-organisations-suffered-data-breach-in-past-2-years-globally-1503169546.html). 06.04.2023).***

***

«Угрозы кибербезопасности растут угрожающими темпами по всему миру, и в то же время киберпреступники становятся все более изощренными в своих методах атак. Между тем, нехватка специалистов в области кибербезопасности мешает организациям и отраслям удовлетворять эти постоянно меняющиеся требования безопасности.

Таким образом, ландшафт кибербезопасности становится все более сложным. На самом деле, ожидается, что к 2025 году киберпреступность будет обходиться миру в 10,5 трлн долларов в год, но организации изо всех сил пытаются развить специальные навыки, необходимые для борьбы с этими растущими угрозами. Согласно последнему отчету ISACA о состоянии кибербезопасности, 63 процента предприятий имеют незанятые должности в области кибербезопасности, в то время как нехватка рабочей силы в Великобритании стала особенно острой. На самом деле, несмотря на то, что в настоящее время в Великобритании насчитывается

около 339 000 специалистов по кибербезопасности (рост на 13% в годовом исчислении), по-прежнему не хватает 56 811 работников (рост на 70% в годовом исчислении).

И все же, несмотря на эту растущую потребность в талантах в области кибербезопасности, мы также по-прежнему наблюдаем значительную недопредставленность и исключение женщин в секторе кибербезопасности. Недавний отчет о женщинах в сфере кибербезопасности показал, что по состоянию на сентябрь 2022 года женщины составляли лишь 25 процентов рабочей силы в глобальной индустрии кибербезопасности, при этом в Великобритании дела обстоят немного лучше, поскольку женщины составляют 36 процентов национальной рабочей силы в области кибербезопасности. Но ожидается, что к 2025 году женщины будут составлять лишь 30 процентов глобальной рабочей силы в области кибербезопасности, а к 2031 году — 35 процентов. Это означает, что всего за десятилетие количество женщин в отрасли вырастет всего на 10 процентов.

Такое отсутствие участия женщин в рабочей силе в области кибербезопасности наносит ущерб не только сектору и безопасности предприятий, поскольку способствует постоянной нехватке столь необходимых навыков в области кибербезопасности, но и потому, что создает белые пятна в кибербезопасности через суженную призму перспектив. в поле.

Вот почему, если предприятия хотят ужесточить свою кибербезопасность, они должны начать осмысленно и серьезно сокращать гендерный разрыв.

Гендерное равенство как двигатель прогресса

Обеспечение более широкого включения женщин в сферу кибербезопасности не только заполнит пустующие стулья в отрасли, но и сыграет ключевую роль в расширении и укреплении возможностей организации в области безопасности, привнося различные точки зрения на решение проблем и инновации.

На самом деле хорошо доказано, что включение женщин помогает обеспечить лучшие результаты технологических решений, позволяя организациям подходить к функциональным возможностям технологий с другой точки зрения, тем самым уменьшая любые белые пятна, которые иначе не были бы обнаружены. Например, женщины-пользователи Интернета чаще сталкиваются с киберпреступлениями, но при этом подвергаются повышенному риску потери финансовых данных, нарушения конфиденциальности и безопасности.

Кроме того, более разнообразная рабочая сила в конечном итоге повышает эффективность бизнеса, поскольку компании с гендерно разнообразной базой сотрудников, как правило, имеют более высокую финансовую отдачу, чем в среднем по отрасли.

Но самое главное, предоставив большему количеству женщин возможность работать в сфере кибербезопасности, которая является хорошо оплачиваемой, высокопроизводительной и перспективной отраслью для трудоустройства, мы сможем укрепить и диверсифицировать национальную экономику.

Привлечение большего числа женщин к кибербезопасности

По данным Всемирного экономического форума, существует мнение, что женщины мало осведомлены о кибербезопасности и что низкое участие женщин в

кибербезопасности связано с отсутствием доступа к образованию в области кибербезопасности. Это неправда.

На самом деле, 82 процента респондентов глобального опроса студенток бакалавриата STEM заявили, что у них есть некоторые или большие знания о кибербезопасности, в то время как 58 процентов сказали, что у них есть доступ к образованию в области кибербезопасности, а 68 процентов уже прошли курс, связанный с кибербезопасностью.

Итак, что именно служит барьером для входа женщин в сферу кибербезопасности и как нам создать более инклюзивную рабочую силу в области кибербезопасности?

Ну, это не так просто, как просто нанять больше женщин на должности в сфере кибербезопасности. Акцент должен быть сделан на обучении и образовании, а также на поощрении женщин и молодых девушек заниматься кибербезопасностью в качестве карьерного пути, предоставляя наставничество и доступ к другим женским образцам для подражания в отрасли.

Одна из основных причин, по которой женщины не рассматривают возможность карьеры в сфере кибербезопасности, часто заключается в том, что они просто не видят для себя такой возможности. Таким образом, остается значительная возможность привлечь больше женщин в эту область, предоставляя им широкие и разнообразные должности, доступные в сфере кибербезопасности с раннего возраста (от средней школы до высших учебных заведений), а также через стажировки, проекты и другие мероприятия, связанные с кибербезопасностью, такие как хакатоны

Недопредставленность женщин в секторе кибербезопасности оказывает прямое негативное влияние на безопасность и защиту людей, организаций, отраслей и экономики в целом. Вот почему вовлечение большего числа женщин в сферу кибербезопасности имеет решающее значение не только для решения проблемы нехватки специалистов в области кибербезопасности, но и для создания более безопасного киберпространства, а также для создания более инклюзивной индустрии кибербезопасности». ***(Debi Dowling. If businesses are to get a grip on their cybersecurity, they need to close the gender gap // BetaNews, Inc. (https://betanews.com/2023/04/03/cybersecurity-gender-gap/). 03.04.2023).***

***

«Кибератаки стали одной из главных проблем для руководителей технологических компаний и владельцев бизнеса. К 2025 году киберпреступность будет стоить компаниям 10,5 млрд долларов в год. Предполагаемая стоимость киберпреступности в 2021 году составила 6,1 трлн долларов, и ожидается, что она будет расти на 15% каждый год.

Компании увеличивают свои кибербюджеты, чтобы защитить свои активы. За 12-месячный период, закончившийся в декабре 2022 года, количество онлайн-объявлений о вакансиях на должности в области кибербезопасности превысило 755 000. По данным Gartner, к 2026 году расходы на кибербезопасность вырастут до 267,3 млрд долларов. уровень кибербезопасности компании был «удовлетворительным», очень немногие считали его «весьма

удовлетворительным». Почти все респонденты считают, что есть возможности для улучшения.

В отчете говорится, что тремя основными проблемами, касающимися кибербезопасности, являются: растущее число киберпреступников, проблемы с конфиденциальностью, укрепление доверия и, наконец, множество атак из разных источников. В этой статье мы обсудим три основные проблемы кибербезопасности:

Растущее число киберпреступников

Среднее количество кибератак и утечек данных увеличилось на 15,1% в период с 2020 по 2021 год. В то время как бюджеты и усилия в области кибербезопасности растут горизонтально, кибератаки и угрозы растут экспоненциально.

Исследования показывают, что внешние злоумышленники могут нарушить периметр и получить доступ к ресурсам сети в 93% случаев. После этого требуется всего два дня, чтобы взломать внутреннюю сеть этой организации. С ростом числа и сложности кибератак организации чувствуют, что они недостаточно хорошо оснащены, чтобы защитить себя. Кроме того, преследование и обнаружение киберпреступников в США составляет всего 0,05%.

Вопросы конфиденциальности и укрепление доверия

Конфиденциальность данных относится к этичному и безопасному обращению, хранению и совместному использованию пользовательских данных. Кибератаки носят глобальный характер и не регулируются конкретными юрисдикционными нормами. Однако организации должны соблюдать сложные системы правил и положений, таких как Общий регламент по защите данных (GDPR) и многие другие.

В то время как правила конфиденциальности и защиты данных необходимы, организациям часто приходится ориентироваться в сложных, а иногда даже противоречащих друг другу правилах. Такая сложность регулирования иногда создает проблемы для усилий организаций в области кибербезопасности, а не дополняет их. Это заставляет организации постоянно поддерживать стандарты безопасности и конфиденциальности, чтобы завоевать доверие клиентов.

Разнообразие атак

Кибератаки стали более разнообразными и изощренными. Существует множество кибератак, которые угрожают предприятиям. К ним относятся программы-вымогатели, проблемы безопасности IoT, атаки на блокчейн и криптографию, фишинг, атаки на цепочки поставок, облачные атаки, уязвимости программного обеспечения, инсайдерские атаки и так далее. По мере того, как эти атаки становятся все более сложными, организации необходимо постоянно внедрять инновации, чтобы смягчить эти атаки.

Вот несколько наиболее распространенных типов атак:

Вредоносное ПО. Вредоносное ПО — это вредоносное программное обеспечение, которое может заражать компьютерные системы и причинять вред, например, путем кражи конфиденциальной информации или нарушения работы. Типы вредоносных программ включают вирусы, трояны и программы-вымогатели.

Фишинг. Фишинг — это атака, в которой используются поддельные электронные письма, веб-сайты или текстовые сообщения, чтобы обманным путем

заставить людей раскрыть конфиденциальную информацию, такую как учетные данные для входа или номера кредитных карт.

Атаки типа «отказ в обслуживании» (DoS) и «распределенный отказ в обслуживании» (DDoS): атаки типа «отказ в обслуживании» и «DDoS» пытаются нарушить доступ к веб-сайту или онлайн-сервису, перегрузив цель трафиком.

SQL-инъекция: SQL-инъекция — это тип атаки, использующий уязвимости в программном обеспечении базы данных для получения несанкционированного доступа к конфиденциальной информации.

Атаки «человек посередине» (MitM): атаки MitM происходят, когда злоумышленник подслушивает и изменяет сообщения между двумя сторонами, причем ни одна из сторон не знает об этом.

Межсайтовый скриптинг (XSS): атаки XSS используют уязвимости в веб-приложениях для внедрения вредоносного кода на веб-сайт, который может быть выполнен ничего не подозревающими посетителями.

Атаки на пароли. Атаки на пароли включают в себя такие методы, как атаки полным перебором, атаки по словарю и другие, которые пытаются взломать пароли, чтобы получить доступ к конфиденциальной информации.

В заключение

Приведенное выше обсуждение показывает, что кибербезопасность стала одной из главных проблем для организаций. Рост числа киберпреступников, растущая сложность и разнообразие кибератак, а также проблемы, связанные с доверием и конфиденциальностью, являются неотложными проблемами, которые необходимо решать современным предприятиям. Ясно, что индустрия кибербезопасности будет расти в ближайшие пару лет благодаря высоким организационным расходам на кибербезопасность и увеличению числа рабочих мест в сфере кибербезопасности». ***(Gordon Pelosse. Three issues driving cybersecurity // Endeavor Business Media, LLC. (https://www.securityinfowatch.com/cybersecurity/article/53056578/three-issues-driving-cybersecurity). 06.04.2023).***

***

«…Фирма по обеспечению безопасности электронной почты Armorblox сообщила о росте почти всех форм атак на электронную почту в прошлом году. В своем втором ежегодном отчете об угрозах безопасности электронной почты за 2023 год Armorblox обнаружил рост компрометации поставщиков, мошенничества и серой почты, массовых рассылок — законных или нет — в прошлом году впустую 27 часов времени команд безопасности в неделю.

Armorblox, который заявил, что его отчет основан на данных из четырех миллиардов электронных писем и 800 000 предотвращенных угроз каждый месяц в 2022 году, обнаружил:

Рост числа фишинговых атак на 70% по сравнению с 63% в 2021 году.

Малые и средние предприятия особенно уязвимы для мошенничества с поставщиками и атак по электронной почте в цепочке поставок.

Пятьдесят три процента компрометационных атак поставщиков нацелены на технологические организации.

Пятьдесят два процента атак были связаны с конфиденциальными пользовательскими данными, такими как учетные данные пользователя.

Семьдесят семь процентов BEC-атак используют язык и социальную инженерию.

Пятьдесят восемь процентов атак были нацелены на малый и средний бизнес.

Двадцать процентов атак BEC были связаны с серой почтой или нежелательным запросом.

Пятьдесят шесть процентов атак обходили устаревшие фильтры безопасности.

В прошлом году количество атак финансового мошенничества увеличилось на 72%.

Фирма предсказала, что генеративные инструменты искусственного интеллекта также будут способствовать увеличению BEC.

«Исходя из угроз, проанализированных Armorblox в нашей клиентской базе из более чем 58 000 организаций, мы видим, что более половины атак по электронной почте, нацеленных на критически важные бизнес-процессы, направлены на кражу конфиденциальных пользовательских данных», — сказал DJ Sampath, соучредитель и генеральный директор Armorblox. заявление.

«В этих атаках часто участвуют злоумышленники, которые проникают в законные деловые коммуникации, чтобы изменить конфиденциальную деловую информацию, например, назначить новые номера маршрутизации для платежных запросов», — сказал он.

Он добавил, что они используют язык в качестве основного вектора атаки, чтобы выдать себя за доверенное программное обеспечение как сервисные приложения, поставщиков и VIP-персон…

В исследовании также отмечается, что гибридные схемы работы увеличивают риски для сотрудников, работающих дома. Респонденты нового исследования, основанного на опросе компании Red Access, посвященной гибридной работе и безопасности просмотра, признали, что, хотя они рассматривают гибридную работу как постоянную парадигму работы, они также считают ее наиболее уязвимой точкой входа для злоумышленников.

В ходе опроса 72% из 300 директоров по информационной безопасности из США и Великобритании из компаний с 5000 и более сотрудников заявили, что гибридная и удаленная рабочая сила негативно влияет на состояние безопасности их организации. Они также утверждали, что тактика, включающая безопасные веб-шлюзы и изоляцию удаленных браузеров, недостаточна перед лицом разнообразных угроз, исходящих от злоумышленников.

Ситуация усложняется тем, что, согласно опросу, внедрение этих методов также ниже в организациях, которые переводят сотрудников на преимущественно удаленную модель, чем в компаниях, где сотрудники в основном находятся в офисе…» ***(Karl Greenberg. Cybersecurity leaders see risk from email attacks, hybrid work // TechnologyAdvice (https://www.techrepublic.com/article/cybersecurity-leaders-see-risk-from-email-attacks-hybrid-work/amp/). 12.04.2023).***

***

«Новый отчет компании JupiterOne, занимающейся обзором и управлением киберактивами, показывает, что количество корпоративных киберактивов увеличилось на 133% по сравнению с прошлым годом, в среднем со 165 000 в 2022 году до 393 419 в 2023 году.

Согласно отчету, в котором проанализировано более 291 миллиона ресурсов, результатов и политик, организации также заметили, что количество уязвимостей в системе безопасности или нерешенных проблем увеличилось на 589 процентов, чтобы установить текущее состояние корпоративных облачных активов, включая облачные и физические среды устройства, сети, приложения, данные и пользователи.

Жасмин Генри, старший директор по безопасности данных и конфиденциальности в JupiterOne и ведущий исследователь отчета о состоянии киберактивов за 2023 год, говорит: «Если прошедший год нас чему-то научил, так это критической важности безопасности для общего состояния организации и общественная безопасность. Кибербезопасность больше не является просто вопросом CISO; генеральный директор, совет директоров и инвесторы уделяют пристальное внимание. Историки могут написать, что атака программы-вымогателя WannaCry в 2017 году была тогда, когда руководители осознали важность безопасности и колониального трубопровода 2021 года. Событием стало то, что средний человек понял, что безопасность имеет значение, но, несмотря на то, что все согласны с важностью безопасности, этот отчет показывает нам, на какую большую гору нам еще предстоит взобраться».

В среднем в крупных организациях на одного сотрудника приходится 2011 киберактивов, в малых организациях — 681, а в организациях среднего размера — 489. Специалисты по безопасности несут ответственность в среднем за 334 уникальных учетных записи поставщиков облачных услуг (CSP) в 2023 г. для организаций всех размеров или в среднем 225 и 559 уникальных учетных записей в крупных и средних организациях соответственно…» ***(Ian Barker. Vulnerable cloud attack surface grows almost 600 percent // BetaNews, Inc. (https://betanews.com/2023/04/12/vulnerable-cloud-attack-surface-grows-almost-600-percent/). 12.04.2023).***

***

«По мере того как мир становится все более цифровым, киберпреступность становится все более серьезной угрозой для предприятий по всему миру, в том числе в спортивной экосистеме.

Согласно исследованию, проведенному поставщиком программного обеспечения Check Point Research,в прошлом году число кибератак во всем мире увеличилось на 38%, при этом в годовом исчислении рост составил более 60% в таких областях, как отдых, гостиничный бизнес и розничная торговля.

Еженедельные кибератаки на организацию увеличились на 22% в Азиатско-Тихоокеанском регионе, на 26% в Европе, на 29% в Латинской Америке и на огромные 52% в Северной Америке. В Африке рост составил более скромные 4%, хотя на этом континенте произошло самое большое количество кибератак на организацию — невероятные 1875 в неделю.

Более подробное изучение статистики показывает, что два крупнейших географических рынка спортивной индустрии были одними из самых целевых: количество атак в США увеличилось на 57%, а в Соединенном Королевстве — на 77%.

Тем не менее, глобальная траектория подчеркивает тревожные масштабы проблемы во всем мире, при этом эксперты сходятся во мнении, что резкое увеличение числа киберпреступлений обусловлено тремя основными факторами:

Растущее число более мелких и ловких преступных групп, занимающихся использованием организаций с помощью программ-вымогателей;

Более широкий охват хакеров, которые теперь обычно атакуют средства делового сотрудничества и коммуникации с помощью фишинга;

Дело в том, что академические учреждения стали популярными мишенями для преступников из-за их цифровой трансформации в последние годы, ускоренной глобальной пандемией. Наряду с образованием/исследованиями в последнее время больше всего атак подвергались секторы государственного управления и здравоохранения.

Угроза спорту

Однако, собирая и управляя личными данными посредством продажи билетов, членства и товаров, а также контролируя крупные бюджеты и банковские переводы, легко понять, почему спорт находится на переднем крае киберпреступности.

Действительно, в последние годы спортивная индустрия подверглась интенсивному нападению. Согласно исследованию, проведенному Национальным центром кибербезопасности правительства Великобритании в 2020 году, по крайней мере 70% спортивных организаций столкнулись с киберинцидентами или взломом, что более чем вдвое превышает средний показатель по всем британским предприятиям в то время.

Зловещий отчет также назвал спорт «важной целью» и описал, как неназванный клуб Английской футбольной лиги подвергся нападению, которое привело к отключению видеонаблюдения и турникетов на его стадионе, а матч был отложен.

Кроме того, среди жертв были такие громкие имена, как «Манчестер Юнайтед», поскольку хакеры атаковали онлайн-систему и операции футбольного клуба английской премьер-лиги.

Между тем, в Соединенных Штатах франшиза американского футбола NFL San Francisco 49ers в прошлом году пострадала от взлома, когда, как сообщается, были получены данные более 20 000 человек.

Использование слабых сторон

Атаки нацелены не только на правообладателей, поскольку разросшаяся спортивная индустрия предоставляет преступникам различные возможности для использования слабых мест в системах безопасности.

Например, в январе 2023 года розничный продавец спортивной одежды JD Sports столкнулся с нарушением безопасности, которое, как считается, поставило под угрозу личные данные около 10 миллионов клиентов.

Возможно, наиболее известная кибератака так называемого «олимпийского разрушителя» нарушила работу ИТ-инфраструктуры, поддерживающей церемонию открытия зимних Олимпийских игр 2018 года в Пхенчхане, Южная Корея.

«Растущая зависимость от технологий сделала спортивные организации более уязвимыми для киберугроз, включая вирусы, вредоносные программы, программы-вымогатели, распределенные атаки типа «отказ в обслуживании», спам и фишинг», — говорит Сатиндер Сони, управляющий директор глобальной консалтинговой компании Ankura.

«Спортивные организации должны обеспечить наличие у них надежных мер кибербезопасности, как и у других сопоставимых организаций в коммерческом секторе, для защиты от этих угроз.

Однако некоторые сферы спортивной индустрии сопряжены с более высокими рисками и требуют усиленных мер безопасности. Например, организации, участвующие в антидопинговом тестировании, такие как испытательные лаборатории, одобренные Всемирным антидопинговым агентством, должны иметь безопасные системы для защиты целостности процедур тестирования и предотвращения любых попыток фальсификации результатов.

Точно так же спортивные юридические фирмы и арбитражные комиссии должны защищать конфиденциальную информацию своих клиентов, включая юридические стратегии и расчеты. Участники торгов и местные организационные комитеты крупных спортивных мероприятий также подвергаются более высокому риску, поскольку они обрабатывают конфиденциальные данные, включая личную и финансовую информацию спортсменов, персонала и зрителей, а также логистические детали событий.

Кроме того, некоторые виды деятельности в отрасли, такие как системы безбилетного доступа на стадионы и системы управления результатами соревнований, представляют более высокую уязвимость к киберугрозам с потенциалом катастрофического сбоя».

Влияние

Последствия кибератаки могут быть ужасными для процветания и устойчивости профиля, определенных Глобальным устойчивым спортом, нанося ущерб финансовым перспективам спортивного предприятия или организации, а также потенциально их репутации.

Согласно отчету IBM и Ponemon Institute, средняя стоимость взлома данных для бизнеса с менее чем 500 сотрудниками составляет невероятные 2,98 млн долларов. Эта средняя сумма может включать в себя выкуп, а также дополнительные расходы, такие как:

Устранение немедленных повреждений и ремонт;

Предоставление бесплатного кредитного мониторинга;

Подбор персонала по работе с клиентами для обработки запросов клиентов;

Предложение бесплатных или льготных продуктов и услуг;

Оплата штрафов;

Наем дополнительных экспертов, в том числе консультантов по ИТ-безопасности, консультантов по управлению рисками, юристов, аудиторов и

бухгалтеров, консультантов по управлению и консультантов по связям с общественностью.

Одна из проблем заключается в том, что киберпреступность постоянно меняется и становится все более технологичной.

Еще десять лет назад, до того, как многие организации прошли цифровую трансформацию, 46% организаций сообщили в опросе Forbes, что их репутация и ценность бренда пострадали из-за нарушения кибербезопасности за предыдущие 24 месяца.

Десять лет спустя, во все более цифровом ландшафте, проблемы будут только усиливаться, особенно по мере того, как преступники становятся все более организованными. В недавнем отчете, подготовленном в соавторстве с ФБР в США, говорится, что преступники, работающие удаленно, даже создают внутренние арбитражные системы для разрешения споров об оплате между разными хакерами.

Кроме того, есть ожидания, что кибератаки будут только возрастать по частоте и сложности из-за появления технологий искусственного интеллекта, которые позволяют хакерам создавать вредоносные коды и электронные письма быстрее, чем когда-либо прежде, по словам эксперта по этой теме Чака Брукса, президента. Брукс Консалтинг Интернэшнл.

В равной степени следует отметить, что ИИ рассматривается как потенциальная часть решения, а также проблемы.

Решение проблемы

Таким образом, угроза спортивным организациям, их профилю и основам устойчивости процветания значительна. Однако есть предположения, что подавляющее большинство операторов отрасли просто недостаточно серьезно к этому относятся.

По словам Екатерины Караянис, директора по кибербезопасности и управлению рисками компании Maple Leaf Sports & Entertainment, базирующейся в Торонто, которая является оператором нескольких команд и стадионов высшей лиги, только около 1% профессиональных команд и лиг имеют адекватную инфраструктуру кибербезопасности.

Выступая в прошлом году на симпозиуме Sports Business Journal AXS Sports Facilities & Franchises and Ticketing Symposium, Караянис изложил широкий план из шести пунктов, который спортивная организация должна принять в отношении угрозы киберпреступности:

Подготовьтесь к атаке, потому что она, вероятно, неизбежна;

Знайте свою терпимость к риску;

Поговорите с другими, например, с коллегами в отрасли;

Задавайте вопросы – доверяйте, но проверяйте;

Можно сказать нет;

Выйдите за рамки коммерческого предложения и прочитайте мелкий шрифт в договоре.

Она также выделила Высшую футбольную лигу и Национальную баскетбольную ассоциацию за их усилия в области кибербезопасности, но предупредила, что ответственность за активную деятельность лежит на спортивных

организациях, учитывая, что провайдеры «больше не хотят страховать спортивные команды [с помощью страхования кибербезопасности в качестве] … мы слишком рискуем».

В качестве первого шага, по словам Check Point, поставщика решений для ИТ-безопасности, «необходимо думать в первую очередь о предотвращении, а не об обнаружении», при этом жизненно важные усилия включают обучение кибербезопасности, своевременное обновление исправлений и внедрение технологии защиты от программ-вымогателей.

С практической точки зрения Генри Дойл, соучредитель поставщика услуг кибербезопасности Altinet, предупреждает, что в залах заседаний спортивных организаций следует обсуждать тройную угрозу захвата электронной почты, программ-вымогателей и подражательного кибермошенничества.

Он также предлагает шесть главных советов, применимых во всех организациях, а не только в спортивной индустрии:

Поддерживайте программное обеспечение в актуальном состоянии с помощью последних исправлений;

Защитите учетные записи электронной почты, так как 91% кибератак начинаются с фишингового письма;

Внедрение и управление антивирусным программным обеспечением и брандмауэрами нового поколения;

Используйте инструмент управления паролями для всех платформ и пользователей;

Используйте двухфакторную аутентификацию;

Внедрите услугу обучения кибербезопасности…» ***(Satinder Soni. Sustainability Challenges: Cybersecurity // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102ic70/sustainability-challenges-cybersecurity). 12.04.2023).***

***

«Когда вы слышите слово «кибератака», вы думаете об атаках на банки, крупные магазины или медицинские учреждения. Вы должны добавить в этот список строительную отрасль, поскольку она является третьей по распространенности целью кибератак. Эти типы атак только увеличиваются, потому что злоумышленники создали процессы, которые упростили атаки на бизнес. Им нравится нападать на строительную отрасль, потому что большие суммы денег переводятся на банковские счета и с банковских счетов с помощью электронных переводов. Недавно мы стали свидетелями того, как компании сталкиваются с тем, что недобросовестные лица сидят на корпоративных учетных записях электронной почты, ожидая перенаправления банковских переводов или прямых депозитов. Злоумышленники будут использовать фишинговую или спуфинговую атаку, чтобы обмануть сотрудника и предоставить ему информацию, которая позволит злоумышленникам получить административный доступ к системе электронной почты компании. С этим административным доступом злоумышленники будут получать электронные письма, перенаправленные им, и они будут ждать получения информации, связанной с банковским переводом или

прямым депозитом, по электронной почте. Затем злоумышленник перехватит этот платеж, отправив отправителю электронное письмо с новой информацией о проводке с законной учетной записи в компании, удалит электронное письмо из почтового ящика законного владельца учетной записи и направит платеж на другую учетную запись. Только потом, когда бизнес увидит, что оплата за услуги не поступила, или сотрудник увидит, что зарплата не зачислена, нарушение будет обнаружено. Однако к тому времени уже слишком поздно, и плохие актеры уже ушли со средствами.

Чтобы не стать жертвой кибератаки, кибербезопасность должна стать частью корпоративной культуры. Для борьбы с этим типом атак необходимо тщательное обучение и обновление политик и процедур. Сотрудникам необходимо улучшить обучение важности кибербезопасности, тому, как защитить систему компании от атак и как распознать атаку и сообщить о ней. Компании необходимо инвестировать в обновление программного обеспечения и обучение, а также быть в курсе последних методов, которые злоумышленники используют для проникновения в компьютерные системы, и способов предотвращения атаки. Наконец, компании необходимо провести аудит всех данных, которые она хранит. Компания должна знать, какие данные у нее есть, какие данные ей нужно сохранить, от каких данных она может избавиться и кто имеет доступ ко всем этим данным. Хранение большого количества данных, особенно данных, которые вам больше не нужны, только увеличивает риск и ответственность компании в случае утечки данных, поэтому бизнес должен установить политику периодического удаления данных, которые компании больше не нужны. Кроме того, не каждому сотруднику нужен доступ ко всем данным, хранящимся в вашей компании, поэтому компания должна ограничить доступ сотрудников только к тем данным, которые необходимы сотруднику для выполнения его или ее работы…» ***(Alexander L. Turner. Cyberattacks and Construction – A Hard Hit Industry // Spilman Thomas & Battle, PLLC (https://www.spilmanlaw.com/dataentry/resources/attorney-articles/construction/cyberattacks-and-construction-%E2%80%93-a-hard-hit-industr). 04.04.2023).***

***

«Одна из опасностей всех взломов и кибератак заключается в том, что они могут повлиять на вас спустя долгое время после того, как произошли. Ни с того ни с сего вы можете начать получать фишинговые электронные письма, поскольку мошенники пытаются собрать больше информации о вас, например, год спустя. Или испытайте цепочку подозрительных событий в своих учетных записях в Интернете, банковские счета могут указывать на кражу личных данных. Другими словами, у нарушения нет срока давности. Как только ваши личные данные раскрываются, всегда существует риск того, что кто-то их использует в какой-то момент.

Вот некоторые из крупнейших кибератак в Нидерландах:

Вы заметите, что большинство из них произошли в 2021 году и ранее. Это связано не с отсутствием более свежих инцидентов, а с тем, что, согласно

исследованию IBM, на выявление и локализацию нарушения уходит в среднем 277 дней — около 9 месяцев. Кроме того, некоторые из них никогда не публикуются.

1. Утечки из программы отслеживания коронавируса

В 2021 году органы здравоохранения Нидерландов сообщили о массовой утечке данных, которая затронула медицинские данные тысяч людей. Личная информация многих людей, участвовавших в программе отслеживания коронавируса в Нидерландах, была раскрыта в результате двух отдельных утечек.

2. Данные о 7,3 млн голландских автовладельцев, проданных на хакерском форуме

В марте 2021 года RDC, голландская компания, предоставляющая услуги гаража и технического обслуживания владельцам автомобилей, подтвердила утечку данных после того, как личные данные и данные о транспортных средствах миллионов клиентов были выставлены на продажу на известном форуме по киберпреступности.

3. На Booking.com просочилась информация о 4000 гостей.

В марте 2021 года Booking.com был оштрафован на 475 000 евро за то, что не уложился в срок, чтобы сообщить детали нарушения регулирующему органу. Кибер-мошенники получили доступ к конфиденциальной информации, такой как данные кредитной карты и коды CVV клиентов, которые забронировали поездку на отдых через Booking dot com.

4. Хакер украл файлы пациентов из голландских психиатрических клиник.

Пациентов голландских психиатрических клиник предупредили, что их личные записи попали в руки хакеров после нарушения безопасности на онлайн-портале, который «гарантировал» их конфиденциальность.

25 октября 2022 года нидерландская технологическая компания Nedap сообщила о взломе своего портала Carenzorgt.nl, который использовался тысячами медицинских учреждений по всей стране для обмена цифровыми медицинскими картами и личными данными.

5. «Этический хакер» среди арестованных по делу о программе-вымогателе в Нидерландах.

В феврале 2023 года полиция Нидерландов арестовала трех человек в связи с атаками программ-вымогателей и шантажом тысяч компаний.

Предполагается, что хакеры украли десятки миллионов единиц личной информации. Сообщается, что украденная конфиденциальная информация включала не только имена, адреса и номера телефонов отдельных лиц, но также даты рождения, номера банковских счетов, кредитные карты, пароли, данные номерных знаков, служебные номера и паспортные данные…» ***(Cristina POPOV. Top 5 biggest cyberattacks in the Netherlands. Were you affected? You can still do something about it. // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/top-5-biggest-cyberattacks-in-the-netherlands-were-you-affected-you-can-still-do-something-about-it/). 24.04.2023).***

***

«…В период с 2021 по 2022 год количество глобальных кибератак выросло на 38 процентов. Ожидается, что эта сумма будет продолжать расти, и по

этой причине неудивительно, что мы наблюдаем значительный рост расходов на решения для кибербезопасности, поскольку организации отчаянно пытаются найти новые способы смягчения последствий развивающегося ландшафта атак.

Исследование Gartner предсказало, что в течение 2023 года расходы на безопасность и управление рисками вырастут на 11,3%. Дополнительные исследования показали, что повышение кибербезопасности бизнеса является основной мотивацией для двух из пяти организаций инвестировать в ИТ, а две трети планируют увеличить свои расходы на кибербезопасность в этом году…

В ответ на эти различные угрозы в области кибербезопасности было создано множество решений для обеспечения безопасности. Каждый из них работает отдельно и затрагивает разные области ИТ-среды, а решения нацелены на:

Безопасность конечной точки (opens in new tab) — направлена на защиту устройств пользователей от угроз программ- вымогателей (opens in new tab) и фишинга.

Сетевая (открывается в новой вкладке) безопасность — направлена на защиту от вирусов и попыток кражи данных.

Безопасность приложений (открывается в новой вкладке) — направлена на защиту веб-приложений, которые, как и все, что напрямую связано с Интернетом, представляют собой цель для злоумышленников.

Однако многие лидеры в области безопасности не имеют четкой стратегии того, как их бизнес должен интегрировать их в существующий арсенал безопасности организации. Это отсутствие целостного и всеобъемлющего представления означает, что организации уязвимы для неэффективности, избыточности и пробелов в охвате. И это делает их уязвимыми для дальнейших киберугроз.

Лучший подход к управлению ресурсами

Каждая компания будет надеяться избежать этого уязвимого положения. Вот почему лидерам по безопасности необходимо предпринять важные шаги, которые позволят им свести на нет последствия разрозненного подхода к кибербезопасности.

Для этого им нужно будет проанализировать свою защиту. Предприятиям с несколькими разнообразными решениями для обеспечения безопасности часто не хватает последовательного объединенного подхода. Это не только создает риск возникновения пробелов в охвате, что делает эти организации более уязвимыми, чем раньше, но также и то, что новые решения могут дублировать возможности существующего программного обеспечения, которое не используется в полной мере. Чтобы избежать этого, компаниям необходимо определить области, в которых решения, выполняющие аналогичные или дублирующие функции, могут привести к перерасходу средств.

Следующим шагом является определение потенциальных областей для оптимизации ресурсов. Расходы, необходимые для управления каждым аспектом процедуры безопасности организации, могут быть высокими. Это означает, что лучшие в своем классе решения не обязательно являются лучшими в своем классе подходами в целом. Вместо этого компаниям следует подумать о том, могут ли существующие решения, которые могут быть не лучшими для решения каждой

конкретной проблемы, по-прежнему обеспечивать достаточную защиту, повышая при этом простоту управления и контроля. Этот подход улучшит общий контроль состояния безопасности, снизит потребность в расходах на отдельные лицензии и уменьшит потребность в квалифицированных специалистах для управления разрозненными решениями.

Решение для оптимизации безопасности

Окончательный ответ исходит от перехода к оптимизации безопасности. После того, как организация обратилась к описанным выше областям, оптимизация становится решающим шагом, который позволит ей точно определить, где они дублируют решения, предлагающие аналогичные услуги. Затем он может решить, как обеспечить более широкий охват, применяя каждое решение по-разному, чтобы избежать ненужных покупок в будущем.

Конечно, это может быть легче сказать, чем сделать для компаний без директора по информационной безопасности, которые имеют стратегическое понимание того, как создать оптимизированный портфель безопасности. Для этих компаний решением может стать поиск партнеров, которые могут либо предоставить временного директора по информационной безопасности, либо выступить в роли консультанта.

Какой бы подход ни выбрала организация, растущие проблемы с экономикой и безопасностью указывают на то, что предприятия должны дистанцироваться от распространенного реактивного подхода к закупкам кибербезопасности. Скорее, им нужно будет принять более связанный и стратегический взгляд, который учитывает как интеграцию новых решений с существующими, так и общее влияние, которое это оказывает на их состояние безопасности.

Этот подход позволит компаниям оптимизировать свою систему кибербезопасности, рационализировать свои операции и гарантировать, что их команда будет иметь ресурсы и инструменты, необходимые для эффективной защиты своей организации от развивающегося ландшафта киберугроз». ***(Jonathan Wright. Optimizing cybersecurity within an evolving threat environment // Future US, Inc. (https://www.techradar.com/opinion/optimizing-cybersecurity-within-an-evolving-threat-environment). 26.04.2023).***

***

На прошлой неделе кибератака нарушила работу компьютерных систем коммерческой и оборонной судостроительной компании Fincantieri Marine Group.

Компания в четверг признала инцидент в заявлении для Green Bay Press-Gazette, но не предоставила подробностей о типе произошедшей атаки. В заявлении указано, что сервер электронной почты компании и некоторые сетевые операции остаются в автономном режиме и что компания работает с федеральными агентствами и партнерами над расследованием инцидента.

«На прошлой неделе Fincantieri Marine Group столкнулась с инцидентом кибербезопасности, который привел к временному нарушению работы определенных компьютерных систем в ее сети. Сотрудники службы сетевой безопасности компании немедленно изолировали системы и сообщили об

инциденте соответствующим агентствам и партнерам», — говорится в заявлении компании. «Fincantieri привлекла дополнительные ресурсы для расследования инцидента и скорейшего восстановления полной функциональности пострадавших систем».

Fincantieri Marine Group заявила, что ремонтно-строительные работы на ее верфях продолжаются. Компания добавила, что у нее нет доказательств того, что инцидент скомпрометировал личную информацию сотрудников.

Новости USNI в четверг сообщили более подробные сведения об атаке программ-вымогателей 12 апреля, которая затронула данные на серверах верфи и затронула некоторые производственные машины. USNI News, часть Военно-морского института США, подтвердили детали в интервью с двумя источниками, знакомыми с сводкой ВМС США об инциденте, и подтвердили это ВМС.

В заявлении для USNI военно-морской флот заявил, что ему «узнали о кибер-инциденте с участием Fincantieri Marine Group», позже добавив, что «FMG приняла меры для предотвращения дальнейшего вторжения и проводит необходимые действия по реагированию, исправлению и отчету». активно следит за усилиями».

Fincantieri Marine Group является частью итальянской компании Fincantieri SpA, расположенной в Триесте, но инцидент с кибербезопасностью затронул только офисы и системы Marine Group в США. Fincantieri Marine Group состоит из верфей в Маринетт, Стерджен-Бей и Грин-Бей, на которых работает около 2300 человек.

Персонал компании из Висконсина строит коммерческие грузовые суда в Стерджен-Бей, прибрежный боевой корабль и фрегат с управляемыми ракетами класса Constellation для ВМС США в Маринетт…

ФБР Центр жалоб на интернет-преступления в 2022 году получил 800 944 жалобы, что на 5% меньше, чем в 2021 году, но потенциальные убытки от этих жалоб увеличились с 6,9 млрд долларов в 2021 году до 10,2 млрд долларов в 2022 году. Жалобы, которые расследует ICCC, включают вопросы прав интеллектуальной собственности, хакерские атаки, экономический шпионаж., экстерьер в Интернете, отмывание денег и кража личных данных». ***(Jeff Bollier. Fincantieri Marine Group confirms cybersecurity incident is under investigation // Green Bay Press-Gazette (https://www.greenbaypressgazette.com/story/money/2023/04/20/fincantieri-marine-group-hit-by-cyberattack-impacting-computer-systems/70135610007/). 20.04.2023).***

***

«…Ветеран-кіберзлочинець розповів, що насправді відбувається в даркнет, де хакери, вбивці та наркоторговці безладно діють. Зокрема, він розповів, що будь-яка система, підключена до Інтернету, під загрозою атаки.

«Я бачив, як шифрувалися лікарні, і люди стояли перед вибором: заплатити за розшифрування даних або ризикувати життями?», - сказав чоловік, приховуючи свою особу за маскою.

Попри те, що хакер не займався незаконною діяльністю, він переймається «значними наслідками (вимагання викупу), які можуть відчутно вплинути на

фінансові ринки або мати потенційні наслідки для таких речей, як електроенергетичні установки».

Філіп Інґрам, колишній полковник військової розвідки у Великій Британії, минулого року сказав: «Даркнет все частіше використовується серйозними та організованими злочинцями для різноманітних цілей. Вони шукають вразливість у дітей, коли збираються привернути їх до таких речей, як доставка наркотиків від місцевості до місцевості, експлуатація в педофільських колах чи набір до терористичних та екстремістських груп».

До даркнету надають доступ одразу кілька мереж, серед них - i2p, FreeNet та Tor.

Tor — скорочення від The Onion Router — це густа матриця шифрованих веб-сайтів, яка дозволяє користувачам переглядати Інтернет в повній анонімності. Він використовує численні шари безпеки та шифрування, щоб забезпечити анонімність користувачів в Інтернеті.

За дослідженням, щоденно користувачів Tor налічується близько 2,6 мільйонів осіб.

«Це ж дослідження виявило, що з одного збору даних приблизно 80% трафіку до головних сервісів направлялося на сервіси, які надавали незаконну порнографію, зображення насильства та/або матеріали про дитяче сексуальне збочення», — зазначили дослідники з Австралійського національного університету в The Conversation.

Інтерв'ю з хакером було проведене Vice в 2021 році, але відео з'явилося знову як нагадування про те, що існує темний світ людей, чиє єдине завдання — викликати хаос за допомогою Інтернету.

Чоловік розпочав свою кар'єру хакера як «чорний шапочник», який є типом кіберзлочинця, який не дотримується законів і здійснює атаки для своїх власних цілей. Згодом він перейшов на білу сторону, ставши “білою шапочкою”, де використовує свої навички з добрими намірами, відслідковуючи злочинців в Інтернеті і шукаючи вразливості в системах, щоб виправити їх, а не використовувати на власну користь.

«Якби я хотів отримати доступ до захищеної компанії, я б не ходив та не ламав двері», — сказав він на початку інтерв'ю.

Перша атака рансомвіру була написана Джозефом Поппом в 1989 році і використовувалась для атак на сектор охорони здоров'я.

Атака, яка називалась «AIDS Trojan», була здійснена Поппом, який роздав 20 000 інфікованих дисків учасникам конференції Всесвітньої організації охорони здоров'я щодо СНІДу. На дисках були написи «Інформація про СНІД — Вступні дискети».

Коли дискету завантажували на комп'ютер, на екрані з'являлася велика картинка, на якій було написано, що програмне забезпечення «негативно впливає на інші програмні застосування. Ви будете зобов'язані відшкодувати можливі збитки для PC Cyborg Corporation, а ваш мікрокомп'ютер перестане працювати нормально».

Програма підраховувала кількість запусків комп'ютера, і якщо їх кількість досягала 90, то вона ховала теки та шифрувала або блокувала назви файлів на

диску C. Щоб отримати доступ знову, користувачі повинні були відправити 189 доларів на PC Cyborg Corporation на скриньку в Панамі.

З тих пір, як розроблено розшифровувальний код, хакерам не потрібно залишати своє житло — все можна зробити у даркнеті.

«Колись, щоб довести до розладу країну таку велику, як Сполучені Штати, потрібні були б мільйони доларів інвестицій, щоб щось зробити», — заявив чоловік журналістам Vice.

Кевін Мітнік вважається "найвідомішим хакером у світі" через свою атаку на 40 великих компаній, включаючи IBM, Nokia та та Motorola. Чоловік вкрав комп'ютерні коди, вартість яких дехто оцінює майже в 330 мільйонів доларів, за що провів у в'язниці п'ять років.

Після звільнення 2000 року Мітнік заявив, що він "виправився" і тепер працює як «біла шапочка» - етичний хакер з безпеки. Чоловік, який спілкувався з Vice, теж заявив, що займається цією роботою.

«Колись я вважав себе «чорною шапкою» і перейшов на «білу», — сказав чоловік.

Він стверджує що кожна західна країна зверталася до даркнету у пошуках допомоги від «спільноти».

Хакер “біла шапка” також згадував про ринок початкового доступу, на якому злочинці можуть придбати доступ до корпоративних мереж.

«За середню ціну близько 2 800 доларів, так звані брокери початкового доступу (IAB) продавали вкрадені дані облікових записів VPN та протоколу віддаленого робочого столу (RDP) та інші облікові дані, які злочинці могли використовувати для вторгнення до мереж понад 2 300 організацій по всьому світу», — повідомляє Dark Reading.

Після випуску відео Vice ринок початкового доступу отримав значне поширення.

Дослідники кібербезпеки повідомили про 2 348 випадки продажу доступу до корпоративних мереж через IAB протягом другої половини 2021 року та першої половини 2022 року. Кількість брокерів також зросла з 262 до 380.

За звітний період на сайтах витоків даних через рансомвер було опубліковано чутливу інформацію 2886 компаній, що становить збільшення на 22% порівняно з попереднім роком, повідомляє InfoSecurity Magazine.

ФБР не залишається осторонь незаконної діяльності, але має проблеми з усуненням великих гравцівЗараз агенція шукає операторів та. користувачів цих сайтів.

«Ми намагаємося не тільки атакувати сторону постачальника, але й сторону попиту з користувачами», — заявив старший службовець ФБР цього місяця під час операції з ліквідації Genesis Market, великого онлайн-ринку злочинців.

Якщо ви збираєтесь використовувати ці типи сайтів для залучення в таку діяльність, будуть наслідки. Міжнародні правоохоронні органи, очолювані ФБР, захопили розкішний темний веб-ринок, популярний серед кіберзлочинців, де викрадені паролі продавалися за $1 кожний.

Хакерський кібер-базар, відомий як Genesis Market, був захоплений в рамках міжнародної операції під назвою «Операція Монстр Кукі», оскільки сайт спеціалізується на викраденнях цифрових відбитків пальців, відомих як кукі.

За даними ФБР, Genesis Market пропонував доступ до даних, викрадених з більш ніж 1,5 мільйона комп'ютерів по всьому світу, що містять понад 80 мільйонів облікових записів.

У викрадених даних були збережені паролі до послуг, таких як онлайн-банкінг, Facebook, Amazon, PayPal і Netflix, а також цифрові відбитки пальців, які кримінальні елементи можуть використовувати для обману онлайн-перевірок безпеки, підробивши пристрій жертви.

У координованих обшуках по всьому світу було проведено понад 200 обшуків та було затримано близько 120 осіб, з них 24 затримання в районі британського міста Грімсбі, повідомили представники правоохоронних органів Великої Британії.

Старший посадовець ФБР повідомив DailyMail.com, що підозрювані були також затримані в США у зв'язку з розгорнутим розслідуванням, але не надав деталей щодо кількості затриманих та звинувачень.

Додамо, у п’ятницю, 31 березня, офіційні особи НАТО повідомили співробітникам про заборону завантажувати китайську програму соціальних мереж TikTok, посилаючись на проблеми безпеки». ***(Христина Головчак. Був хакером упродовж 30 років: колишній кіберзлочинець розповів, як працює даркнет // ТСН.ua (https://tsn.ua/tsikavinki/buv-hakerom-uprodovzh-30-rokiv-kolishniy-kiberzlochinec-rozpoviv-yak-pracuye-darknet-2310301.html). 18.04.2023).***

***

«Сьогодні, 22 квітня, російські хакери атакували авіадиспетчерську службу Європи. Компанія Eurocontrol заявляє, що змін для цивільних немає.

Про це інформує The Wall Street Journal.

Нападу зазнало агентство Eurocontrol, яке координує діяльність національних авіаційно-диспетчерських служб Європи. Кібератака з боку проросійського угруповання розпочалася в середу і триває досі.

Компанія заявляє, що повітряному руху та системам управління ніщо не загрожує, жодних змін у розкладі маршрутів немає. Однак агентство зазнає певних технологічних складнощів, включаючи збої в системах зв'язку, а деяким авіакомпаніям для управління рейсами довелося використовувати стару систему…» ***(Анна-Каріна Білоткач. Хакери РФ атакували авіадиспетчерську службу Європи: що відомо // ТОВ «МЕДІАМЕРЕЖІ» (https://accident.novyny.live/crime/khakeri-rf-atakuvali-aviadispetchersku-sluzhbu-ievropi-shcho-vidomo-89590.html). 22.04.2023).***

***

«Группа анализа угроз Google LLC сегодня опубликовала новую информацию о подмножестве северокорейской хакерской группы, известной как APT43, и о том, что она делает для защиты пользователей от этой группы.

Как подробно описано в отчете Mandiant, принадлежащем Google в прошлом месяце, APT43 был впервые обнаружен в 2018 году и имеет приоритеты сбора, которые соответствуют миссии Главного разведывательного бюро, службы внешней разведки Северной Кореи. APT43 крадет и отмывает криптовалюту для покупки операционной инфраструктуры в соответствии с государства чучхе в Северной Корее. идеологией самообеспечения

Подмножество группы, названное исследователями Google TAG «Архипелагом», нацелено на людей, обладающих опытом в вопросах политики Северной Кореи, таких как санкции, права человека и вопросы нераспространения. Целями были учетные записи Google и других компаний, принадлежащие правительственным и военным, аналитическим центрам, политикам, ученым и исследователям в Южной Корее, США и других странах.

Archipelago обычно рассылает фишинговые электронные письма, в которых члены группы изображают из себя представителей СМИ или аналитических центров и просят экспертов по Северной Корее принять участие в интервью для СМИ или запросить информацию. В электронных письмах получателям предлагается щелкнуть ссылку, чтобы просмотреть вопросы интервью или запросить информацию.

Неудивительно, что ссылки в электронном письме являются вредоносными и ведут получателей на фишинговый сайт, который маскируется под запрос на вход в систему. Фишинговая страница записывает нажатия клавиш, введенные в форму входа, и отправляет информацию на URL-адрес, контролируемый злоумышленником. После того, как получатели вводят свой пароль, фишинговая страница перенаправляется на безобидный документ с контекстно-подходящими вопросами для интервью или запросом информации в соответствии с содержанием исходного фишингового письма.

Исследователи обнаружили, что Archipelago тратит время и усилия на установление взаимопонимания с целями, часто отправляя им электронные письма в течение нескольких дней или недель, прежде чем, наконец, отправить вредоносную ссылку или файл. В одном случае группа выдавала себя за журналиста южнокорейского информационного агентства и разослала вежливые электронные письма с просьбой об интервью экспертам по Северной Корее.

Первоначальные кампании Archipelago были сосредоточены на проведении традиционных кампаний по фишингу учетных данных, но в последнее время было замечено, что группа включает вредоносное ПО в большее количество своих операций, включая усилия по уклонению от обнаружения и разработку новых и новаторских методов вредоносного ПО. Archipelago защищает свое вредоносное ПО паролем и передает пароль получателям в фишинговой электронной почте, чтобы защитить свое вредоносное ПО от антивирусного сканирования.

Интересно, что Archipelago также использует учетные записи Google Диска как часть своей деятельности, используя файлы Диска для управления и контроля. Google принял меры, чтобы предотвратить использование Диска злоумышленником.

Также было обнаружено, что Archipelago использует вредоносные расширения Chrome в сочетании с фишингом и вредоносным ПО. Функции расширения включали возможность кражи имен пользователей, паролей и файлов cookie браузера. С тех пор Google внес несколько изменений в экосистему расширений Chrome, в том числе повышенную прозрачность через Интернет-магазин Chrome и Manifest V3, которые эффективно мешают злоумышленникам распространять вредоносные расширения через Интернет-магазин Chrome». ***(Duncan Riley. Google threat analysis researchers detail activities of North Korean 'Archipelago' hackers // SiliconANGLE Media Inc. (https://siliconangle.com/2023/04/05/google-tag-researchers-detail-activities-north-korean-archipelago-hackers/). 05.04.2023).***

***

«Пророссийская хакерская группа взяла на себя ответственность за кибератаку на веб-сайт Hydro-Quebec в четверг утром.

По состоянию на 11:00, некоторые части сайта энергетической компании Квебека все еще не работали. Hydro-Quebec сообщает, что никакие личные данные не были скомпрометированы.

В онлайн-сообщении группа NoName057 (16) объявила, что стоит за взломом, но не уточнила, почему она, как сообщается, нацелена на Hydro-Quebec.

«Продолжаем визиты в Канаду», — написала хакерская группа в переводе с русского. «Веб-сайт Hydro-Québec, компании, отвечающей за производство и транспортировку электроэнергии в Квебеке, был закрыт».

Hydro-Quebec подтвердил CTV News, что веб-сайт подвергся «кибератаке» ночью в среду, но не может сказать, стоит ли за этим NoName057 (16).

«Наша служба безопасности быстро обнаружила атаку, поэтому наши критически важные системы не пострадали», — заявила пресс-секретарь Линн Сен-Лоран.

Сен-Лоран заявил, что не было никаких «проникновений» или «эксфильтрации» конфиденциальных данных или информации о клиентах.

Веб-сайт Hydro-Quebec подвергся атаке типа «отказ в обслуживании», которая возникает, когда система перегружается излишними запросами.

По словам технического аналитика Кармы Леви, эти типы атак могут быть эффективными, даже если они не особенно сложны.

«Это одна из самых простых атак, которые существуют во всем режиме кибербезопасности. Так что в этом смысле это хорошая новость, но она очень разрушительна», — пояснил он.

«Это похоже на то, как будто толпа с вилами появляется у вашей входной двери и начинает часами стучать в дверь. Они не взламывают, ничего не крадут, ничего не портят, но вы не можете приходить и уходить. Вы ничего не можете сделать, и ваша жизнь, по сути, приостановлена».

Некоторые страницы на веб-сайте Hydro все еще были доступны в четверг утром, например, карта отключений. Другие разделы, например страница Customer Space, не загружались. Также пострадало приложение Hydro-Quebec.

Представитель Hydro Линн Сен-Лоран сообщил, что в команде Hydro по кибербезопасности 300 сотрудников, которые следят за сайтом «24/7».

Hydro-Quebec входит в число немногих канадских организаций, подвергшихся кибератакам в последние дни.

Ранее на этой неделе были совершены атаки на веб-сайт премьер-министра Джастина Трюдо, веб-сайт Laurentian Bank of Canada и веб-сайты различных канадских портов, в том числе портов Монреаля и Порт-де-Квебек.

Как сообщает The Canadian Press, ответственность за эти теракты взяли на себя и пророссийские группировки.

Поскольку мы выступили вперед, чтобы помочь Украине [...] Россия ясно дала понять, что Канада находится в списке стран, на которые она будет нацелена в цифровой сфере», — сказал Леви…». ***(Lillian Roy. Pro-Russia hackers say they were behind Hydro-Quebec cyberattack // Bell Media (https://montreal.ctvnews.ca/cyber-attack-at-hydro-quebec-pro-russia-hackers-claim-responsibility-1.6353627). 13.04.2023).***

***

«Массированная кибератака, совершенная группой суданских хакеров, отключила веб-сайты крупного порта аэропорта, а также крупнейшего поставщика электроэнергии на оккупированных Израилем территориях на фоне растущих кибероперациий, направленных против компаний и объектов израильского режима.

Средства массовой информации на иврите сообщили, что хакерская группа, называющая себя Anonymous Sudan, в субботу взломала веб-сайты международного аэропорта Бен-Гурион и Israel Electric Corporation (IEC).

В отчетах добавлено, что атаки распределенного отказа в обслуживании (DDoS), во время которых веб-сайты становятся мишенью, перегружая их серверы слишком большим количеством запросов на подключение, сделали веб-сайты недоступными на некоторое время, прежде чем они были возвращены в работу.

«Мы не забыли наш праздничный подарок Израилю. Произойдет крупная [кибератака], которая разрушит большую часть инфраструктуры в Израиле. Мы нападем в любой момент», — написала группировка в своем Telegram-канале.

Ранее на этой неделе группа индонезийских хакеров осуществила массированную кибератаку на ряд израильских веб-сайтов, в том числе на веб-сайты министерств иностранных дел, образования и здравоохранения.

Газета «Джерузалем пост» сообщила, что группа, называющая себя VulzSecTeam, объявила 17 апреля, что в последние дни ей удалось взломать веб-сайты израильского министерства образования, здравоохранения и иностранных дел, а также израильской полиции и автобусных и железнодорожных компаний. и снял их.

События произошли всего через несколько дней после того, как пропалестинские хакеры отключили веб-сайты десятков известных израильских

компаний и учреждений в знак солидарности с палестинским народом по случаю Международного дня Кудс и в осуждение чудовищных преступлений, совершенных израильским режимом. против угнетенной нации.

Согласно сообщению, опубликованному ивритоязычной газетой Israel Hayom, хакеры за 48 часов вывели из строя не менее 60 израильских веб-сайтов, а беспрецедентные масштабы кибератак привели к массовым нарушениям на оккупированных территориях.

В отчете добавлено, что помимо израильских банков, подвергшихся кибератакам в День Кудса, среди пострадавших оказались веб-сайты международной службы заказа такси Yango и частного Колледжа права и бизнеса в Рамат-Гане.

Специалисты и эксперты в области информационных технологий подчеркивают, что методы, использованные для взлома, были значительно более совершенными, чем применявшиеся в предыдущие годы». ***(Sudanese hackers knock offline websites of major Israeli airport, electric company // PressTV (https://www.presstv.ir/Detail/2023/04/22/702046/Websites-of-major-Israeli-airport,-electric-company-knocked-offline-by-Sudanese-hackers). 22.04.2023).***

***

Вірусне та інше шкідливе програмне забезпечення

«Исследователи кибербезопасности из Trustwave SpiderLabs обнаружили новый вид вредоносного ПО нацеленного на криптовалютные кошельки жертв.

На основе Chromium, Вредоносное ПО, получившее название Rilide, выдает себя за расширение для браузеров таких как Google Chrome, Microsoft Edge, Brave или Opera.

Вредоносное ПО выдает себя за законное расширение для Google Диска, и если люди установят его на свои конечные точки, они дадут вредоносному ПО возможность отслеживать их историю просмотров, делать снимки экрана и даже внедрять вредоносные скрипты, которые будут вытягивать все их найденные деньги. на биржах криптовалют.

Что делает эту вредоносную программу уникальной, так это ее способность использовать «поддельные диалоги», чтобы обманом заставить людей выдать свои ключи многофакторной аутентификации, а затем получить криптовалюту, работая в фоновом режиме. Если вредоносное ПО обнаружит, что у пользователя есть учетная запись на бирже криптовалют, оно попытается сделать запрос на снятие средств в фоновом режиме, предоставив пользователю поддельное диалоговое окно аутентификации устройства, чтобы получить код 2FA.

Обычно криптовалютные биржи также уведомляют пользователей о запросах на вывод по электронной почте, что также пытается скрыть это вредоносное ПО. По словам исследователей, эти подтверждения электронной почты заменяются «на лету», пока пользователь входит в почтовый ящик, используя тот же веб-браузер.

Электронное письмо с запросом заменяется запросом на авторизацию устройства, обманом заставляя жертву выдать код 2FA.

Для исследователей стилер Rilide является «ярким примером» того, как вредоносные расширения для браузеров становятся все более изощренными и опасными. Исследователи заключают, что как компании, так и потребители должны сохранять бдительность в то время, когда слишком много информации может притупить наши чувства…». ***(Sead Fadilpašić. This dangerous malware disguises itself as a legit browser extension to steal your cash // Future US, Inc. (https://www.techradar.com/news/this-dangerous-malware-disguises-itself-as-a-legit-browser-extension-to-steal-your-cash). 06.04.2023)***.

***

«Хакеры снова используют поддельные обновления Google Chrome, чтобы заразить ничего не подозревающих пользователей вредоносными программами.

Однако на этот раз они сначала преследуют веб-сайты и внедряют в них скрипты, которые отображают поддельные ошибки автоматического обновления Chrome согласно BleepingComputer (открывается в новой вкладке).

Сама кампания началась еще в ноябре прошлого года, но в новом отчете (открывается в новой вкладке) аналитик NTT по безопасности Ринтаро Койке объясняет, что ответственные за нее хакеры расширили ее масштабы в феврале 2023 года, чтобы охватить еще больше пользователей.

В ходе расследования этого вопроса BleepingComputer обнаружил множество сайтов, которые были взломаны в ходе этой кампании по распространению вредоносных программ, включая новостные сайты, интернет-магазины, блоги и сайты для взрослых.

Как только веб-сайт был скомпрометирован путем внедрения в него вредоносного кода JavaScript, взломанный сайт выполняет сценарии, способные загружать дополнительные сценарии, когда пользователь посещает сайт.

Хакеры, стоящие за этой кампанией, используют службу Pinana IPFS (InterPlanetary File System) для доставки этих дополнительных сценариев, поскольку она скрывает происхождение сервера, на котором размещены файлы, что затрудняет их блокировку.

Если целевой пользователь действительно посещает один из этих взломанных сайтов, сценарии отображают поддельный экран ошибки Google Chrome, в котором говорится, что им необходимо установить автоматическое обновление, чтобы продолжить работу на сайте. Отсюда сценарии автоматически загружают ZIP-файл с именем «release.zip», который замаскирован под обновление Chrome.

Ничего не подозревающие пользователи, которые попадаются на эту уловку, в конечном итоге устанавливают на свой ПК майнер Monero вместо законного обновления Chrome. Опасность установки такого криптомайнера на вашем компьютере заключается в том, что ваша система будет работать медленнее, поскольку на самом деле она выполняет довольно много работы в фоновом режиме. В то же время, это также может создать дополнительную нагрузку на ваш

процессор, графический процессор и другие компоненты, которые затем необходимо будет заменить раньше, чем позже.

Еще одна интересная особенность этой вредоносной кампании заключается в том, что устанавливаемый ею крипто-майнер закрепляется на компьютере жертвы, добавляя запланированные задачи и выполняя изменения в реестре. Он также исключает себя из Защитника Windows, и в результате антивирусное программное обеспечение Microsoft не знает, как удалить его из вашей системы.

Что еще хуже, вредоносное ПО даже останавливает Центр обновления Windows, что может сделать ваш компьютер уязвимым для других штаммов вредоносных программ и вирусов.

Как защититься от вредоносных программ, распространяемых через поддельные обновления

Поддельные обновления — это один из самых простых способов, с помощью которых хакеры обманом заражают свои устройства вредоносными программами. Таким образом, вы никогда не должны устанавливать какие-либо обновления, которые появляются во всплывающем окне, и это особенно верно для Google Chrome.

Вместо того, чтобы приставать к вам всплывающими окнами, когда доступно новое обновление Chrome, Google вместо этого отображает всплывающую подсказку рядом с изображением вашего профиля в правом верхнем углу своего браузера. Цвет кружка указывает, когда было выпущено последнее обновление: зеленым — обновление двухдневной давности, оранжевым — обновление четырехдневной давности и красным — обновление, выпущенное не менее недели назад.

Нажав на это облачко, вы обновите свой браузер до последней версии, но вы также можете сделать это вручную, щелкнув меню из трех точек справа от изображения вашего профиля. Отсюда вам нужно спуститься в нижнюю часть этого меню и нажать «Справка», затем «О Google Chrome». Вы перейдете на страницу настроек Chrome, и если доступно обновление, оно будет загружено автоматически и применено при следующем перезапуске браузера.

Помимо регулярного обновления Chrome и избегания всплывающих окон с предложением обновить браузер, вы также должны использовать одно из лучших антивирусных программных решений на своем ПК, чтобы предотвратить заражение вредоносным ПО и другие кибератаки.

Хотя в настоящее время эта кампания в основном нацелена на говорящих на японском, корейском и испанском языках, NTT предупреждает, что хакеры, стоящие за ней, могут стремиться к дальнейшему расширению, поскольку они недавно добавили новые языки. В любом случае, если вы избегаете всплывающих окон или сообщений об ошибках, предлагающих обновить Google Chrome, вы должны быть в безопасности». ***(Anthony Spadafora. Hackers are using fake Chrome updates to spread malware — don't fall for this // Future US, Inc. (https://www.tomsguide.com/news/hackers-are-using-fake-chrome-updates-to-spread-malware-dont-fall-for-this). 12.04.2023).***

***

«…Исследователь безопасности Forcepoint Аарон Малгрю рассказал, как ему удалось создать это вредоносное ПО с помощью генеративного чат-бота OpenAI. Несмотря на то, что ChatGPT имеет некоторые средства защиты, которые не позволяют людям просить его создать вредоносный код, Аарон смог найти лазейку.

Он подсказал ChatGPT создать код функция за функцией с отдельными строками. Как только все отдельные функции были скомпилированы, он понял, что у него в руках незаметный исполняемый файл для кражи данных, который был столь же изощрен, как и любое вредоносное ПО национального государства.

Это невероятно тревожно, потому что Малгрю смог создать это очень опасное вредоносное ПО без помощи команды хакеров, и ему даже не пришлось самому создавать код.

Вредоносное ПО начинает с того, что маскируется под приложение-заставку, которое затем автоматически запускается на устройствах Windows. Оказавшись на устройстве, он просматривает все типы файлов, включая документы Word, изображения и PDF-файлы, и ищет любые данные, которые сможет украсть с устройства.

Как только вредоносное ПО получает данные, оно может разбить их на более мелкие части и скрыть эти части в других изображениях на устройстве. Затем изображения избегают обнаружения, загружаясь в папку Google Диска. Код был сделан сверхнадежным, потому что Малгрю смог усовершенствовать и усилить свой код против обнаружения, используя простые подсказки в ChatGPT.

Хотя все это было сделано Малгрю в частном тестировании, и вредоносная программа не атакует никого публично, действительно тревожно знать, какие опасные действия могут быть совершены с использованием ChatGPT. Малгрю утверждал, что у него нет опыта программирования, но защита ChatGPT все еще недостаточно сильна, чтобы заблокировать его тест. Будем надеяться, что защита будет усилена до того, как настоящий хакер получит шанс сделать что-то, как это сделал Малгрю…». ***(Kurt Knutsson. AI-created malware sends shockwaves through cybersecurity world // FOX News Network, LLC. (https://www.foxnews.com/tech/ai-created-malware-sends-shockwaves-cybersecurity-world). 13.04.2023).***

***

«Microsoft показывает, как ИТ-специалисты могут обнаружить «невидимую» и упорно сохраняющуюся часть вредоносного ПО под названием BlackLotus, поскольку гигант из Редмонда публикует подробное руководство по защите от буткита UEFI.

BlackLotus — это сложный вариант вредоносного ПО, нацеленный на Unified Extensible Firmware Interface или UEFI, который загружает практически все компоненты современных компьютеров.

Поскольку он запускается перед операционной системой компьютера, размещение вредоносного ПО здесь означает, что оно может отключить антивирусную защиту или даже оставаться в рабочем состоянии, пока работают решения безопасности. Это также означает, что вредоносное ПО останется на

устройстве даже после переустановки операционной системы — и даже если жертва заменит жесткий диск.

Злоумышленники обычно стремятся развернуть BlackLotus, используя уязвимость, отслеживаемую как CVE-2022-21894. Как сообщает BleepingComputer, вредоносное ПО продается на темных форумах по цене около 5000 долларов. Реконструкция доступна примерно за 200 долларов.

Все это очень затрудняет обнаружение и удаление. Однако с руководством Microsoft это должно быть несколько проще. Согласно отчету, анализ этих артефактов может помочь определить, заражена ли ваша система буткитом BlackLotus UEFI:

Недавно созданные и заблокированные файлы загрузчика

Наличие промежуточного каталога, используемого во время установки BlackLotus, в файловой системе EPS:/

Изменение ключа реестра для обеспечения целостности кода, защищенного гипервизором (HVCI).

Сетевые журналы

Журналы конфигурации загрузки

Артефакты загрузочного раздела

Чтобы очистить устройство от компрометации BlackLotus, необходимо удалить его из сети и переустановить с чистой операционной системой и разделом EFI, инструктируют исследователи. Кроме того, они могут восстановить его из чистой резервной копии с разделом EFI.

Также стоит упомянуть, что злоумышленникам необходимо использовать определенную уязвимость — CVE-2022-21894 — для развертывания BlackLotus. Установка исправления, устраняющего эту уязвимость, также может помочь защитить устройство от заражения в будущем.

Наконец, как заявляет компания: «Избегайте использования сервисных учетных записей на уровне домена и администратора. Ограничение прав локального администратора может помочь ограничить установку троянов удаленного доступа (RAT) и других нежелательных приложений». ***(Sead Fadilpašić. Microsoft gives tips on spotting this undetectable malware // Future US, Inc. (https://www.techradar.com/news/microsoft-gives-tips-on-spotting-this-undetectable-malware). 13.04.2023).***

***

«Теоретически большинство вредоносных приложений для Android поступают с подозрительных веб-страниц или сторонних магазинов приложений, но исследователи безопасности часто находят их скрытыми в официальном магазине Google Play. В новом отчете «Лаборатории Касперского» говорится, что взломанные приложения Play Store становятся все более изощренными.

В новом отчете, опубликованном на этой неделе, компания по безопасности Kaspersky описывает рынок темной сети, предлагающий услуги по взлому целей с помощью вредоносных и шпионских программ для Android. Хакеры могут

проникнуть большую часть этого вредоносного кода в магазин Google Play, обойдя самые строгие меры защиты Google.

Первый шаг в этом процессе и, возможно, самый опасный для конечных пользователей — это взлом учетных записей разработчиков Play Store. Потенциальный злоумышленник может заплатить хакеру от 25 до 80 долларов за учетную запись разработчика, которая была либо украдена, либо зарегистрирована с украденными учетными данными. Это позволяет киберпреступникам превращать ранее доверенные приложения в векторы для вредоносных программ.

Если злоумышленник загружает новое приложение, он может не сразу загружать его шпионским ПО, чтобы не привлекать внимание Google, а вместо этого будет ждать, пока оно не наберет достаточное количество загрузок. Хакеры также предлагают услуги по увеличению числа загрузок и запуску рекламных кампаний Google, чтобы мошеннические приложения выглядели более законными.

Затем хакеры могут использовать загрузчики для передачи вредоносного кода на целевые устройства через, казалось бы, законные обновления, но они могут не содержать окончательной полезной нагрузки вредоносного ПО. Приложение может запрашивать у пользователя разрешение на загрузку приложений или другой информации из-за пределов магазина Google Play, что затем полностью заражает устройство, чтобы получить полный контроль или украсть информацию. Скомпрометированные приложения иногда перестают работать должным образом, пока пользователь не предоставит разрешение на загрузку полной полезной нагрузки.

Хакеры предлагают широкий спектр услуг и сделок при продаже вредоносных программ, включая демонстрационные видеоролики, пакеты, аукционы и различные планы оплаты. Продавцы вредоносного ПО могут потребовать единовременный платеж, процент от прибыли от мошеннической операции или абонентскую плату.

Чтобы увеличить шансы на успешное заражение, хакеры продают сервисы запутывания, которые усложняют полезную нагрузку, чтобы защитить ее от безопасности Google. И наоборот, существуют более дешевые варианты для служб привязки, которые пытаются заразить цели с помощью APK-файлов, отличных от Play Store, которые имеют более низкий уровень успеха, чем загрузчики.

Самая простая мера предосторожности для пользователей — никогда не позволять приложениям Play Store загружать что-либо из-за пределов Play Store, особенно если эти приложения обычно не запрашивают такое разрешение. Всегда будьте осторожны с тем, какие разрешения предоставляются приложениям. Тем временем разработчики должны быть особенно осторожны в защите своих учетных записей с помощью общих передовых методов, таких как многофакторная аутентификация и общая бдительность. Наиболее часто уязвимыми приложениями являются трекеры криптовалюты, сканеры QR-кода, приложения для знакомств и финансовые приложения». ***(Daniel Sims. On the dark web, cybercriminals are selling services to hack Google Play Store apps // TechSpot, Inc. (https://www.techspot.com/news/98278-dark-web-cybercriminals-selling-services-hack-google-play.html). 11.04.2023).***

***

«Согласно новому отчету канадского исследовательского института Citizen Lab, опубликованному во вторник, шпионское ПО, разработанное израильской киберкомпанией QuaDream, использовалось ее клиентами для нападения на журналистов и активистов оппозиции по всему миру и для взлома их iPhone.

Отчет был выпущен в сотрудничестве с исследователями из Microsoft, которые первыми выявили начальные признаки взлома QuaDream. QuaDream — одна из нескольких наступательных киберфирм, действующих из Израиля, специализирующаяся на заражении iPhone шпионским ПО для государственных клиентов.

В ходе совместного расследования Citizen Lab и Microsoft обнаружили, что iPhone как минимум пяти человек, включая журналистов, политиков и активиста гражданского общества, были взломаны с использованием эксплойта, использующего календарь iPhone для проникновения на устройство и заражения его современным шпионским ПО. В отчете не указаны жертвы, но сказано, что они были из Северной Америки, Азии, Европы и Ближнего Востока.

QuaDream специализируется на взломе iPhone с помощью заражения «нулевым щелчком», которое не требует никаких действий со стороны жертвы. Фирма считается крупнейшим конкурентом NSO Group, известной своей печально известной шпионской программой Pegasus, и Paragon в этой области. Но в то время как эти две конкурирующие фирмы сосредоточены на взломе различных устройств, QuaDream занимается только использованием iPhone и разработкой новых методов взлома популярного и, казалось бы, безопасного устройства.

Развитие возможностей «нулевого клика» — метода, который заражает устройство без ведома жертвы и без каких-либо действий с ее стороны — считается самым дорогим видом взлома на рынке. Такой эксплойт для iPhone можно продать за несколько миллионов долларов, а найти такие хаки для Android-устройств сегодня практически невозможно. Высокопоставленные чиновники из QuaDream не ответили на запрос Haaretz о комментариях.

Шпионский инструмент QuaDream называется Reign, и уязвимость, которую он использовал (обнаруженная впервые), связана с службой цифрового календаря Apple, iCloud Calendar. Рейн использовал календари пользователей, чтобы отправить фиктивное приглашение на мероприятие на телефоны целей и впоследствии получить к ним доступ. Этот метод напоминает методы, используемые шпионским ПО Pegasus от NSO Group, которое использовало аналогичную уязвимость в системе обмена сообщениями Apple для заражения устройства, отправляя изображение с внедренным в него вредоносным кодом.

В 2021 году Гур Мегиддо сообщил TheMarker, что QuaDream продала свои хакерские технологии Саудовской Аравии. Компания также владеет дочерней фирмой на Кипре под названием InReach, через которую в свое время была совершена сделка. Согласно источникам, знакомым с этим вопросом, кипрская компания не находится под контролем Израиля.

Проверка серверов компании выявила потенциальных операторов в таких странах, как Израиль, Сингапур, Объединенные Арабские Эмираты, Болгария, Чехия, Венгрия, Гана, Мексика и Румыния.

По оценкам экспертов, QuaDream является одной из компаний, наиболее сильно пострадавших от ограничений, введенных Министерством обороны Израиля на продажу наступательных кибервозможностей. Ряд израильских фирм в этой области имеют филиалы на Кипре, известном регуляторном убежище, где также была основана компания по наблюдению за Circles — одна из первых наступательных кибер-компаний, появившихся в Израиле. Минобороны не ответило на вопрос «Гаарец» о том, ведется ли мониторинг QuaDream.

В отчете Citizen Lab утверждается, что он также связан с другими израильскими компаниями, включая Verint, с которой он разделяет собственность, а также с израильской компанией NFV Systems.

После серии инцидентов, в том числе дела Project Pegasus и внесения Министерством торговли США в черный список NSO Group и израильской фирмы-шпиона Candiru, Израиль начал усиливать контроль над продажей наступательных киберинструментов, разработанных в стране. Это сократило количество стран, которым разрешено продавать эти наступательные технологии, только 37 странам, большинство из которых являются западными демократиями, что значительно сократило потенциал рынка шпионского ПО и привело к закрытию ряда израильских киберфирм.

Однако, согласно отраслевым источникам, в последние месяцы ограничения на процесс выдачи лицензий на продажу этих инструментов были ослаблены до такой степени, что эти технологии можно продавать даже в страны, в которых продажи по-прежнему запрещены. Сообщается, что после возвращения премьер-министра Биньямина Нетаньяху к власти министерство обороны, как сообщается, продлит объем этих разрешений — в основном, чтобы разрешить продажи в страны Южной Америки и Центральной Азии, говорят источники в отрасли.

Израильская наступательная кибериндустрия использует широкий спектр технологий наблюдения и шпионажа. Некоторые из них — это инструменты, продаваемые полицейским органам, которые раскрывают географическое местоположение цели. Существуют также более продвинутые технологии, продаваемые правоохранительным и разведывательным органам, которые позволяют клиентам взламывать компьютеры, мобильные телефоны и зашифрованные приложения для обмена сообщениями, извлекая всю информацию, хранящуюся на устройстве, и тайно включая его микрофон и камеру, чтобы создать инструмент, который шпионит за своим хозяином». ***(Omer Benjakob. Israeli Firm QuaDream's Spyware Used to Hack Journalists, Activists Around the World // Haaretz Daily Newspaper Ltd. (https://www.haaretz.com/israel-news/security-aviation/2023-04-12/ty-article/spyware-made-by-israeli-cyber-firm-quadream-used-to-hack-journalists-activists-worldwide/00000187-73c0-d024-a5ef-f7dc6a1d0000). 12.04.2023).***

***

«Исследователи предупреждают, что хакеры используют совершенно новый инструмент для отключения антивирусных программ, установленных

на устройствах, перед развертыванием более сомнительных вредоносных программ, а иногда даже программ-вымогателей.

Исследователи кибербезопасности из Sophos X-Ops недавно наблюдали за злоумышленниками, использующими метод Bring Your Own Vulnerable Driver (BYOVD) для развертывания инструмента под названием AuKill, способного отключать программы безопасности.

Во-первых, им нужно сбросить законный, но уязвимый драйвер на целевую конечную точку. Обычно это делается с помощью атак по электронной почте, распространяя драйвер через фишинговые электронные письма. Драйвер, способный работать с привилегиями ядра, называется procexp.sys и обычно поставляется рядом с фактическим драйвером, используемым Microsoft Process Explorer v16.32 (законная программа, которая собирает данные об активных процессах Windows).

Как только законная программа запустит вредоносную DLL, она сначала проверит, работает ли она с системными привилегиями, и убедится в этом, выдавая себя за установщика модулей Windows TrustedInstaller. Затем он запускает несколько потоков, тестируя и отключая различные процессы и службы безопасности.

После отключения программ безопасности на компьютере операторы AuKill развертывают вредоносное ПО второго уровня. Согласно отчету Sophos X-Ops, иногда злоумышленники используют Medusa Locker или LockBit — чрезвычайно мощные и популярные варианты программ-вымогателей.

«С начала 2023 года этот инструмент использовался как минимум в трех инцидентах с программами-вымогателями для саботажа защиты цели и развертывания программ-вымогателей», — предупреждают исследователи. «В январе и феврале злоумышленники развернули программу-вымогатель Medusa Locker после использования инструмента; в феврале злоумышленник использовал AuKill непосредственно перед развертыванием программы-вымогателя Lockbit».

Хотя инструмент кажется относительно новым и был только что обнаружен, один из его вариантов имеет временную метку ноября 2022 года. Исследователи заключают, что новейшая обнаруженная версия была составлена в середине февраля. Его код аналогичен коду Backstab, инструмента с открытым исходным кодом, который также может отключать антивирусные программы. Исследователи видели, как операторы LockBit использовали Backstab в прошлом.

«Мы обнаружили много общего между инструментами с открытым исходным кодом Backstab и AuKill», — говорят в Sophos. «Некоторые из этих сходств включают похожие характерные строки отладки и почти идентичную логику потока кода для взаимодействия с драйвером». ***(Sead Fadilpašić. This evil malware disables your security software, then goes in for the kill // Future US, Inc. (https://www.techradar.com/news/this-evil-malware-disables-your-security-software-then-goes-in-for-the-kill). 20.04.2023).***

***

«После проверки аномального DNS-трафика, отличающегося от обычной интернет-активности, был обнаружен новый набор вредоносных программ для предприятий под названием «Decoy Dog».

Decoy Dog помогает злоумышленникам обходить стандартные методы обнаружения за счет стратегического устаревания доменов и клонирования DNS-запросов, стремясь создать хорошую репутацию у поставщиков средств безопасности, прежде чем переключиться на содействие операциям киберпреступности.

Исследователи из Infoblox обнаружили этот инструментарий в начале апреля 2023 года в рамках ежедневного анализа более 70 миллиардов записей DNS для поиска признаков ненормальной или подозрительной активности.

Infoblox сообщает, что отпечаток DNS Decoy Dog чрезвычайно редок и уникален среди 370 миллионов активных доменов в Интернете, что упрощает его идентификацию и отслеживание.

Таким образом, расследование инфраструктуры Decoy Dog быстро привело к обнаружению нескольких доменов C2 (управления и контроля), которые были связаны с одной и той же операцией, при этом большая часть сообщений с этих серверов исходила от хостов в России.

Дальнейшее расследование показало, что туннели DNS в этих доменах имели характеристики, указывающие на Pupy RAT, троян удаленного доступа, развернутый набором инструментов Decoy Dog.

Pupy RAT — это модульный набор инструментов для пост-эксплуатации с открытым исходным кодом, популярный среди спонсируемых государством злоумышленников за скрытность (без файлов), поддержку зашифрованных коммуникаций C2 и помощь им в объединении их действий с другими пользователями инструмента.

Проект Pupy RAT поддерживает полезные нагрузки во всех основных операционных системах, включая Windows, macOS, Linux и Android. Как и другие RAT, он позволяет злоумышленникам удаленно выполнять команды, повышать привилегии, красть учетные данные и распространяться по сети.

Менее опытные участники не используют Pupy RAT, так как развертывание инструмента с правильной конфигурацией DNS-сервера для связи C2 требует знаний и опыта.

«Эта сигнатура, состоящая из нескольких частей (DNS), вселила в нас уверенность в том, что (связанные) домены не только использовали Pupy, но и все они были частью Decoy Dog — большого единого набора инструментов, который очень специфическим образом развертывал Pupy на предприятиях или крупные организационные, непотребительские устройства», — говорится в отчете Infoblox.

Кроме того, аналитики обнаружили различное поведение DNS-маяков на всех доменах-приманках, которые настроены на следование определенному шаблону периодического, но нечастого создания DNS-запросов.

Расследование деталей хостинга и регистрации домена показало, что операция Decoy Dog проводилась с начала апреля 2022 года, поэтому она оставалась незамеченной более года, несмотря на то, что домены инструментария показывают крайние выбросы в аналитике…

Открытие Decoy Dog демонстрирует возможности использования крупномасштабного анализа данных для обнаружения аномальной активности на просторах Интернета.

«Компания Infoblox перечислила домены Decoy Dog в своем отчете и добавила их в свой список «Подозрительные домены», чтобы помочь защитникам, аналитикам безопасности и целевым организациям защититься от этой изощренной угрозы», — объясняют исследователи InfoBlox.

«Открытие Decoy Dog и, что наиболее важно, тот факт, что несколько, казалось бы, не связанных между собой доменов использовали один и тот же редкий инструментарий, было результатом этой комбинации автоматических и человеческих процессов».

Поскольку ситуация сложная, и мы были сосредоточены на аспектах открытия DNS, мы ожидаем, что в будущем больше информации будет поступать не только от нас самих, но и от отрасли».

Компания также поделилась индикаторами компрометации в своем общедоступном репозитории GitHub, который можно использовать для ручного добавления в черные списки». ***(Bill Toulas. Decoy Dog malware toolkit found after analyzing 70 billion DNS queries // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/decoy-dog-malware-toolkit-found-after-analyzing-70-billion-dns-queries/). 23.04.2023).***

***

«Фирма по кибербезопасности Secureworks обнаружила новый штамм вредоносного ПО, выдающий себя за Google Ads, и он быстро распространяется.

Вредоносная программа, известная как Bumblebee, была первоначально обнаружена более года назад и обычно распространялась с помощью фишинговых атак, но Secureworks предупредила, что злоумышленник, стоящий за вредоносной загрузкой, теперь становится более изобретательным и использует новую тенденцию.

В недавнем отчете Securework о состоянии угроз за 2022 год было обнаружено увеличение числа атак троянского программного обеспечения, которое распространяется через Google Ads или отравление SEO, и Bumblebee — лишь один из многих экспериментов с этим все более популярным методом.

Сфера действия вредоносного ПО выходит далеко за пределы поисковой системы, и его примеры можно найти во многих популярных бизнес-приложениях, таких как Zoom, Cisco AnyConnect, ChatGPT и Citrix Workspace. Жертвы, устанавливающие, по их мнению, законное программное обеспечение с поддельных страниц загрузки, затем заражаются вредоносным ПО.

Директор по разведке компании Майк Маклеллан объяснил, что до 1% онлайн-рекламы содержат вредоносный контент. Маклеллан описал типичный сценарий, при котором жертва подвергается атаке: вместо того, чтобы загружать программное обеспечение через ИТ-команду компании, многие удаленные работники сами берут на себя управление и выходят в интернет, не подозревая о потенциальных рисках.

В отчете подробно описывается загрузка законного установщика Cisco AnyConnect VPN, «который был изменен, чтобы содержать вредоносное ПО Bumblebee». В результате злоумышленник не только получил доступ к системе жертвы, но и развернул дополнительные инструменты, такие как Cobalt Strike.

Маклеллан объясняет, что новые результаты только демонстрируют, насколько важно, чтобы компании имели строгую политику ограничения доступа к веб-рекламе и управления привилегиями при загрузке программного обеспечения.

Помимо этого, работникам рекомендуется создать свой собственный прямой путь к законному веб-сайту, а не следовать потоку ссылок или рекламы, или полностью исключить себя из процесса и попросить, чтобы ИТ-команда их компании взяла на себя управление». ***(Craig Hale. This painful malware targets new victims through Google Ads // Future US, Inc (https://www.techradar.com/news/this-painful-malware-targets-new-victims-through-google-ads). 21.04.2023).***

***

«Новый вариант вредоносного ПО PingPull для Linux, используемый китайской группой продвинутых постоянных угроз (APT) Alloy Taurus (Gallium), был признан активной угрозой для телекоммуникационных, финансовых и государственных организаций в Юго-Восточной Азии, Европе и Африке.

В сообщении в блоге от 26 апреля подразделение 42 Palo Alto Networks сообщило, что, отслеживая инфраструктуру, используемую группой APT для варианта PingPull Linux, они также выявили использование ею другого бэкдора, названного ими Sword2033.

Исследователи Unit 42 заявили, что первые образцы вредоносного ПО PingPull относятся к сентябрю 2021 года. Отслеживая его использование в нескольких кампаниях, Unit 42 опубликовала в июне исследование, в котором описываются функциональные возможности PingPull, и приписывает использование этого инструмента Alloy Taurus. По словам исследователей, китайская группа APT работает как минимум с 2012 года.

По состоянию на 26 апреля Unit 42 сообщил, что трое из 62 поставщиков сочли образец вредоносного ПО PingPull для Linux вредоносным. Это определение было сделано на основе соответствующей структуры связи HTTP, параметров POST, ключей AES и команд C2, которые описаны в сообщении блога. Исследователи также обнаружили, что Sword2033 работает как простой бэкдор, который делает следующее: загружает файл в систему (#up); загружает файл из системы (#dn); выполняет команду, но добавляет перед ее выполнением (exc /c:).

Китайские злоумышленники известны тем, что используют APT для ведения шпионажа, в отличие от других преступных групп или национальных государств, чьи мотивы более мотивированы деньгами, сказал Тимоти Моррис, главный советник по безопасности в Tanium. Но это не означает, что они не могут использовать вредоносное ПО для других гнусных целей, сказал Моррис.

«Как и у других вредоносных программ, у этого есть очень всеобъемлющая система управления, которая технически совершенна, полна тактик запутывания, использующих IPv6, что затрудняет обнаружение», — сказал Моррис. «Три

используемых варианта (TCP, HTTPs и ICMP) делают его универсальным и более незаметным. Unit 42 предоставил несколько IOC, чтобы помочь обнаружить вредоносное ПО».

Эндрю Барратт, вице-президент Coalfire, добавил, что, хотя специфика этой вредоносной программы относительно хорошо изучена, на макроуровне она показывает, что бизнес-сообществу необходимо более тщательно отслеживать атаки, в которых используются не-Windows-системы, такие как Linux. Барратт отметил, что, поскольку очень легко развертывать рабочие нагрузки Linux с помощью инструментов оркестрации общедоступного облака, это потенциально делает технологию более доступной для менее опытных системных администраторов, которые могут пропустить индикаторы вредоносного ПО и совершать ошибки по незнанию.

«Это также свидетельствует о необходимости проявлять большую бдительность в отношении трафика, который вы «выпускаете» из своих систем», — сказал Барратт. «Многие организации имеют очень слабую фильтрацию исходящего трафика из-за устаревших приложений или нежелания проводить анализ. Это дает вредоносному ПО возможность установить свой командно-контрольный канал, а затем предоставить ценность злоумышленнику. PingPull прячется, используя ICMP-трафик, и, хотя это семейство протоколов в основном используется для устранения неполадок, он все равно не должен свободно управлять сетью. Относительно небольшие расходы на управление выходом часто имеют огромную отдачу с точки зрения безопасности».

Крейг Берланд, директор по информационной безопасности Inversion6, согласен с тем, что командам по безопасности следует уделять больше внимания системам Linux. Берланд сказал, что, хотя компании разработали дисциплинированные и эффективные процессы для защиты своей инфраструктуры Windows, они в значительной степени игнорировали Linux и встроенный Linux, создавая слабые места, которыми могут легко воспользоваться хакеры.

«От серверов приложений до сетевого оборудования — Linux везде, — сказал Берланд. «И для обеспечения безопасности и поддержки требуется такая же самоотверженность и дисциплина, как и для Windows. Будем надеяться, что организации видят эту угрозу и быстро масштабируют свои программы исправления. В противном случае плохие парни быстро захватят верх в битве за Linux-устройства». ***(Steve Zurier. Chinese APT group Alloy Taurus unleashes new Linux variant of PingPull malware // CyberRisk Alliance (https://www.scmagazine.com/news/cybercrime/chinese-apt-group-alloy-taurus-new-linux-variant-pingpull-malware). 26.04.2023).***

***

«Хакерське угруповання LockBit, скандально відоме своїми вірусами-вимагачами, створило перше шкідливе програмне забезпечення для комп'ютерів Apple. Про це повідомили журналісти порталу 9to5Mac із посиланням на дослідників, які виявили розробку зловмисників.

LockBit стало першим угрупуванням хакерів, якому вдалось створити вірус-вимагач для пристроїв Apple. Зазвичай LockBit використовує однойменний

шкідливий софт і працює за моделлю «програма-вимагач як послуга» (RaaS) — партнери угрупування вносять депозит для використання інструменту, а потім ділять отримані кошти з операторами LockBit.

Збірка вірусу для Mac отримала назву «locker_Apple_M164». Початкові методи атак LockBit включають соціальну інженерію: фішинг, компрометацію ділової електронної пошти, використання загальнодоступних додатків та вкрадених облікових даних.

Цікава особливість додатка LockBit: він запрограмований таким чином, що його не можна використовувати для атак на росію чи країни СНД. Це наводить на деякі думки про походження учасників угрупування…». ***(Хакери розробили першу в історії програму-вимагач для комп'ютерів Apple // No worries (https://noworries.news/hakery-rozrobyly-pershu-v-istoriyi-programu-vymagach-dlya-kompyuteriv-apple/#). 17.04.2023).***

***

Програми-вимагачі

«Исследователи кибербезопасности недавно обнаружили новый вид программ-вымогателей, который, по их мнению, является самым быстрым.

Расследуя кибер-инцидент в американской компании, специалисты Check Point обнаружили неизвестный вариант программы-вымогателя, который после более тщательного анализа получил название Rorshach.

Исследователи пришли к выводу, что Rorshach является самым быстрым штаммом программ-вымогателей, когда дело доходит до шифрования, протестировав код, предоставив ему 220 000 файлов на машине с 6-ядерным процессором, чтобы увидеть, сколько времени потребуется для шифрования файлов. Rorshach выполнил задание за четыре с половиной минуты. Для сравнения, ранее LockBit 3.0 удерживал рекорд — семь минут для той же задачи.

Хотя операторы программы-вымогателя до сих пор неизвестны, у исследователей есть несколько идей относительно того, кто может стоять за этим. Они говорят, что записка с требованием выкупа использует формат, аналогичный тому, который используется программой-вымогателем Yanlowang. Они также сказали, что в предыдущих версиях вредоносного ПО использовалась записка о выкупе, аналогичная той, что использовала DarkSide, что обманом заставило других исследователей поверить в то, что Rorshach на самом деле был DarkSide.

Что касается технических характеристик программы-вымогателя, исследователи обнаружили, что Rorshach поддерживает аргументы командной строки, которые могут расширить его функциональность. Однако параметры скрыты, и к ним нельзя получить доступ без обратного проектирования вредоносного ПО. Они также обнаружили, что шифровальщик начнет работать только в том случае, если обнаружит, что целевая машина настроена с языком за пределами Содружества Независимых Государств (СНГ).

Что касается схемы шифрования, то это смесь алгоритмов шифра Curve25519 и eSTREAM hc-12. Вредоносное ПО шифрует только части файла, что также

используется другими разработчиками программ-вымогателей для ускорения процесса шифрования.

Процедура шифрования Роршаха предполагает «высокоэффективную реализацию планирования потоков через порты завершения ввода-вывода», — заключили исследователи». ***(Sead Fadilpašić. This new ransomware could be the fastest encryptor ever seen // Future US, Inc. (https://www.techradar.com/news/this-new-ransomware-could-be-the-fastest-encryptor-ever-seen). 05.04.2023).***

***

«Серия кибератак группы вымогателей под названием Clop затронула ряд отраслей, от товаров для дома до здравоохранения.

Группа нацелилась на уязвимость нулевого дня в инструменте Fortra для передачи файлов GoAnywhere MFT, который позволяет компаниям безопасно обмениваться файлами. Fortra выпустила исправление 7 февраля. По данным Fortra, более 3000 организаций используют GoAnywhere.

Procter & Gamble сообщила, что хакеры использовали уязвимость в GoAnywhere MFT для кражи информации о сотрудниках. Между тем, Hatch Bank сообщил о несанкционированном доступе к GoAnywhere с 30 по 31 января, сообщает The Washington Post. Другие затронутые организации включают Community Health Systems, Hitachi Energy, компанию по обеспечению безопасности данных Rubrik и Saks Fifth Avenue.

Клоп, впервые появившийся в феврале 2019 года, утверждает, что у него 130 жертв. По данным BleepingComputer. Национальный институт стандартов и технологий идентифицирует уязвимость GoAnywhere как CVE-2023-0669.

Журналист по кибербезопасности Брайан Кребс сообщил об атаках Clop.

Согласно исследовательскому отчету Enterprise Strategy Group «Долгий путь к обеспечению готовности к программам-вымогателям», программы-вымогатели представляют собой ключевую проблему для организаций. На самом деле, 79% организаций заявили, что готовность к программам-вымогателям является одним из пяти главных бизнес-приоритетов для их исполнительной команды и/или совета директоров, говорится в отчете ESG.

Вот некоторые ключевые выводы об атаках Clops и советы о том, как ИТ-директора должны реагировать на эти типы программ-вымогателей.

Проверка использования GoAnywhere

ИТ-руководители должны проверить, используется ли инструмент передачи файлов GoAnywhere, и если да, удалить или обновить его, говорит Ян МакШейн, вице-президент по стратегии компании Arctic Wolf Networks, занимающейся кибербезопасностью.

«Если они еще не были выкуплены, ищите индикаторы компрометации, меняйте все пароли и особенно те, у которых есть административные или повышенные привилегии», — говорит МакШейн.

Пользователям также следует применить последний патч от Fortra.

«У вас действительно нет оправдания тому, что вы попали под удар после выхода исправления, кроме того, что вы просто не применили его», — говорит Мак Макмиллан, основатель фирмы по кибербезопасности CynergisTek.

Подготовьтесь к возрождению

Макмиллан предупреждает, что угрозы со стороны таких групп вымогателей, как Clop, никуда не делись.

«Я думаю, что это первый урок для ИТ-директоров; те, кого я называю профессиональными хакерами организованной преступности, никуда не делись», — говорит Макмиллан. «Они возвращаются. Это похоже на другие виды организованной преступности. Здесь можно отрубить голову змее, но она выскакивает в другом месте».

Итак, что должны делать ИТ-директора? «Сконцентрируйтесь на управлении своей средой и определите свой уровень готовности к обнаружению киберугроз и реагированию на них, когда они возникают», — говорит Макмиллан.

Знайте, как разговаривать с конечными пользователями

Ключевой стратегией реагирования на атаки программ-вымогателей, таких как инцидент с GoAnywhere, является информирование конечных пользователей о том, как сообщать о подозрительных инцидентах, когда они их видят. По словам МакШейна, для этого требуется хорошо документированный план реагирования.

«С точки зрения конечных пользователей убедитесь, что они знают, как позвонить и сообщить об этом как можно быстрее, и убедитесь, что сотрудники чувствуют себя в безопасности, сообщая об инцидентах, зная, что они не будут наказаны за ошибки или несчастные случаи», — советует он.

Уилл Таунсенд, вице-президент и главный аналитик исследовательской компании Moor Insights & Strategy, также советует ИТ-руководителям иметь готовый план, который включает надлежащую связь на случай атаки нулевого дня или программы-вымогателя.

«Немедленно будьте прозрачными с клиентами и сообщайте план действий по раскрытию конкретной информации», — говорит Таунсенд. «Двусмысленность может привести к катастрофическим последствиям».

Подтяните свою осанку соответствия

По словам Игоря Воловича, вице-президента по стратегии соответствия компании Qmulos, отвечающей за соблюдение нормативных требований, усиление соблюдения нормативных требований должно помочь укрепить доверие к режиму безопасности компании.

«Этого можно добиться за счет постоянного мониторинга, регулярной отчетности и открытого общения с клиентами и регулирующими органами», — говорит Волович. «Будучи активными и прозрачными, компании могут продемонстрировать свою приверженность безопасности и соответствию требованиям».

Рассмотрите инструменты наблюдения

По словам Таунсенда, компании могут обеспечить более глубокую проверку своих сетей с помощью инструментов наблюдения. Примеры включают AppDynamics, Dynatrace и Gigamon.

Следуйте модели нулевого доверия

Некоторые эксперты называют стратегию нулевого доверия способом защиты от таких угроз, как программы-вымогатели. Стратегия нулевого доверия

состоит из «никогда не доверяй, всегда проверяй». Компании должны полностью аутентифицировать и авторизовать пользователей перед предоставлением доступа.

«Повсеместный доступ к сети с нулевым доверием — лучший подход, — говорит Таунсенд. «Аутентификация пользователей в приложениях по сравнению с плоской сетью снизит угрозы».

Выполнение активного мониторинга

По словам Макмиллана, поскольку атака Клопа была происшествием нулевого дня, это делает необходимым активный мониторинг.

«Все, что вы можете сделать, чтобы изначально оградить себя от попадания этих вещей и иметь хорошие возможности обнаружения для реагирования, позволит вам смягчить последствия, если вы один из тех немногих несчастных, которые пострадали первыми», — говорит Макмиллан. «Ваша способность реагировать и реагировать и использовать все, что происходит после атаки, чтобы смягчить ее, — это то, что вы можете контролировать».

Макмиллан предполагает, что динамический мониторинг, который постоянно отслеживает среду компании, может помочь обнаружить такие угрозы, как уязвимость GoAnywhere.

«Когда [службы безопасности] начинают замечать ненормальную связь, они предупреждают кого-то, кто говорит, что происходит», — говорит Макмиллан. «Тогда, если это какая-то вредоносная полезная нагрузка, очевидно, у них есть возможность обнаружить и это».

Ограничьте ненужное подключение к Интернету

Макмиллан предлагает ограничить подключение к Интернету для приложений только теми, которые наиболее важны. Административный интерфейс, подключенный к инструменту передачи GoAnywhere, должен оставаться отключенным от доступа.

«Есть часть этой конкретной технологии, которая должна быть доступна в Интернете, чтобы иметь возможность передавать файлы — эта конкретная часть этой системы, по-видимому, очень безопасна», — говорит Макмиллан. «Уязвимость была обнаружена в этом административном интерфейсе, который, я думаю, по определению, вероятно, никогда не должен был быть доступен в Интернете».

«Те организации, которые реализовали эту технологию более безопасным образом, не имели внутреннего административного интерфейса, доступного через Интернет, — говорит Макмиллан.

Разделите критически важные активы

Наряду с ограничением доступа в Интернет ИТ-руководители должны также изолировать критически важные активы в сети.

Если вы действительно разделили свои критически важные активы, реализовали средства контроля безопасности, такие как доступ к сети с нулевым доверием, вы действительно можете ограничить горизонтальное движение, если кто-то проникнет в другие системы...

Удалить данные из инструмента переноса

Знайте, что влечет за собой ваша политика хранения и управления данными, и при использовании инструмента передачи данных, такого как GoAnywhere,

удаляйте данные из инструмента передачи данных каждую ночь, особенно важные активы…» ***(Brian T. Horowitz. Clop Ransomware Attacks: How Should CIOs Respond? // Informa PLC (https://www.informationweek.com/security-and-risk-strategy/clop-ransomware-attacks-how-should-cios-respond-). 06.04.2023).***

***

«Сегодня поставщик облачных сетей обнаружения и реагирования ExtraHop опубликовал Глобальный индекс кибербезопасности за 2023 год, который показал, что не только среднее количество атак программ-вымогателей увеличилось с четырех до пяти с 2021 по 2022 год, но также и то, что 83% организаций-жертв платили выкуп хотя бы один раз.

В отчете говорится, что в то время как такие организации, как ФБР и CISA, выступают против выплаты выкупа, многие организации решают погасить первоначальные затраты на выплату выкупа, стоимость которых в среднем составляет 925 162 доллара, вместо того, чтобы терпеть дальнейшие сбои в работе и потерю данных.

Организации «платят выкуп, потому что считают, что это самый быстрый и простой способ восстановить и запустить свой бизнес», — сказал Джейми Моулс, старший технический менеджер ExtraHop.

В то же время популярный метод двойного вымогательства многих кибер-банд «включает в себя кражу данных перед их шифрованием и угрозу опубликовать их в Интернете, если вы не заплатите выкуп», — сказал Моулс, тем самым оказывая дополнительное давление на организации, чтобы они оплатить.

Исследование проводится сразу после того, как KFC, Taco Bell и материнская компания Pizza Hut Yum! Бренды объявили о взломе программы-вымогателя.

Одна из основных тем отчета ExtraHop, опубликованного сегодня, заключается в том, что организации дают злоумышленникам-вымогателям возможность использовать свои данные, не устраняя уязвимости, созданные неисправленным программным обеспечением, неуправляемыми устройствами и теневыми ИТ.

Например, 77% лиц, принимающих решения в области ИТ, утверждают, что устаревшие методы обеспечения кибербезопасности являются причиной не менее половины инцидентов, связанных с безопасностью.

Со временем эти неустраненные уязвимости множатся, предоставляя злоумышленникам больше потенциальных точек входа, которые они могут использовать, и больше рычагов, чтобы заставить компании платить.

«Вероятность атаки программы-вымогателя обратно пропорциональна площади незащищенной поверхности атаки, что является одним из примеров долга кибербезопасности», — сказал Марк Боулинг, главный специалист по рискам, безопасности и информационной безопасности в ExtraHop. «Обязательства и, в конечном итоге, финансовый ущерб, возникающий в результате такого снижения приоритетов, усугубляют задолженность по кибербезопасности и подвергают организации еще большему риску». ***(Tim Keary. 83% of organizations paid up in ransomware attacks // VentureBeat (https://venturebeat.com/security/83-of-organizations-paid-up-in-ransomware-attacks/). 12.04.2023).***

***

«Злоумышленники удваивают бэкдор-атаки, которые доставляют программы-вымогатели и вредоносное ПО, доказывая, что компаниям требуется нулевое доверие для защиты своих конечных точек и удостоверений.

Индекс безопасности X-force за 2023 год IBM предупреждает, что злоумышленники отдают приоритет этим бэкдор-атакам, поскольку они пытаются вымогать деньги у последующих жертв, чьи данные были скомпрометированы. Двадцать один процент всех атак вторжения начался с попытки взлома бэкдора. Две трети попыток бэкдора включали в себя элементы программ-вымогателей.

Команда IBM X-Force Intelligence также обнаружила, что в феврале и марте прошлого года резко возросло количество бэкдор-атак, о чем свидетельствует значительный всплеск инцидентов с вредоносным ПО Emotet. Всплеск был настолько значительным, что в 2022 году на его долю пришлось 47% всех попыток бэкдоров, выявленных во всем мире.

«Хотя вымогательство в основном связано с программами-вымогателями, кампании по вымогательству также включают множество других методов оказания давления на их цели», — сказал Крис Кариди, аналитик киберугроз из IBM Security Threat Intelligence. «К ним относятся такие вещи, как DDoS-атаки, шифрование данных и, в последнее время, некоторые угрозы двойного и тройного вымогательства, сочетающие в себе несколько ранее замеченных элементов».

Злоумышленники с программами-вымогателями опережают инновационные компании, которые полагаются на защиту на основе периметра. За два года им удалось сократить среднее время развертывания атаки программ-вымогателей на 94 %. То, на что злоумышленникам-вымогателям потребовалось два месяца в 2019 году, в 2021 году ушло чуть меньше четырех дней.

Бэкдорный доступ к инфраструктуре предприятия является одним из самых востребованных и дорогих активов, выставленных на продажу в даркнете.

Отчет CrowdStrike о глобальных угрозах за 2023 год показал, что брокеры доступа продолжают создавать процветающий бизнес, массово перепродавая украденные учетные данные и удостоверения злоумышленникам-вымогателям. CrowdStrike Уважаемая группа разведки обнаружила, что правительство, финансовые службы, промышленные и инженерные организации имеют самую высокую среднюю запрашиваемую цену за доступ. Доступ к академическому

сектору стоил в среднем 3827 долларов, а доступ к государственному сектору - в среднем 6151 доллар.

Команда IBM отмечает в индексе 2023 года, что «брокеры первоначального доступа обычно пытаются продать свои доступы с аукциона, который X-Force видел по цене от 5000 до 10 000 долларов, хотя конечная цена может быть меньше. Другие сообщают, что доступ продается по цене от 2000 до 4000 долларов, а один из них достигает 50 000 долларов».

Почти каждый четвертый инцидент, который IBM отслеживает в своем индексе аналитики угроз, нацелен на производство — отрасль, которая известна очень низким уровнем простоев. Это повышает их мотивацию оплачивать требования программ-вымогателей быстро и часто в больших количествах.

Этот сектор также заработал репутацию легкой мишени, потому что многие производители недооценивают безопасность. Системы производителей не работают в среднем пять дней после кибератаки. Из них 50% реагируют на сбой в течение трех дней, и только 15% реагируют в течение дня или меньше.

Атаки с использованием бэкдора основаны на ложном чувстве безопасности, которое создают и увековечивают системы, основанные на периметре. Книга Эдварда Сноудена «Постоянная запись» развеяла любые сомнения в сообществе кибербезопасности, которые считали доверие смертельным. Это доказало, что слишком большое доверие может поставить под угрозу разведывательную сеть. Директора по информационной безопасности сообщают VentureBeat, что они хранят копию этой книги в своих офисах и цитируют ее, когда возникают сомнения в их бюджете на безопасность с нулевым доверием.

Вот проверенные способы, с помощью которых компании могут противостоять бэкдор-атакам, начиная с рассмотрения каждой новой конечной точки и удостоверения как нового периметра безопасности.

Отчет Ivanti о состоянии кибербезопасности за 2023 год показал, что 45% предприятий считают, что бывшие сотрудники и подрядчики по-прежнему имеют активный доступ к системам и файлам компании из-за непоследовательных или отсутствующих процедур отмены доступа. Отмена подготовки выполняется нечасто, и сторонние приложения по-прежнему имеют встроенный в них доступ.

«Крупные организации часто не учитывают огромную экосистему приложений, платформ и сторонних сервисов, которые предоставляют доступ после увольнения сотрудника», — сказал Сринивас Муккамала, директор по продуктам Ivanti. «Мы называем эти учетные данные зомби, и поразительно большое количество специалистов по безопасности — и даже руководителей высшего звена — все еще имеют доступ к системам и данным бывших работодателей».

Старший аналитик Forrester Эндрю Хьюитт (Andrew Hewitt) сказал VentureBeat, что лучшее место для начала защиты личных данных — это «всегда применять многофакторную аутентификацию». Это может иметь большое значение для обеспечения безопасности корпоративных данных. Оттуда он регистрирует устройства и поддерживает строгий стандарт соответствия с помощью инструмента унифицированного управления конечными точками (UEM).

Forrester также советует предприятиям, чтобы преуспеть в реализации MFA, им следует подумать о добавлении факторов «что вы есть» (биометрические данные), «что вы делаете» (поведенческие биометрические данные) или «что у вас есть» (токены) к устаревшим факторам «что вы делаете». знать (пароль или PIN-код) реализации однофакторной аутентификации. Это область, в которой директора по информационной безопасности добиваются быстрых результатов с нулевым доверием уже сегодня, что экономит завтрашний бюджет.

В качестве одного из основных элементов любой стратегии нулевого доверия директора по информационной безопасности и их команды должны отслеживать, сканировать и анализировать сетевой трафик, чтобы выявлять любые бэкдор-угрозы, прежде чем они увенчаются успехом. Почти все поставщики управления безопасностью и информационными событиями (SIEM) и управления безопасностью в облаке (CSPM) включают мониторинг в качестве стандартной функции.

Объем и масштабы инноваций на рынках SIEM и CPSM продолжают расти. Ведущие поставщики SIEM включают CrowdStrike Falcon, Fortinet, LogPoint, LogRhythm, ManageEngine, QRadar, Splunk и Trellix.

Одной из основополагающих концепций нулевого доверия является микросегментация. NIST В структуре нулевого доверия микросегментация упоминается на том же уровне важности, что и управление на основе удостоверений, аутентификация и управление безопасностью сети и конечных точек.

Airgap, AlgoSec, ColorTokens, Illumio, Prisma Cloud и облачная платформа Zscaler доказали свою эффективность в выявлении и предотвращении вторжений и попыток взлома на раннем этапе, используя свои уникальные подходы к микросегментированию удостоверений и сетей.

Платформа изоляции Airgap с нулевым доверием построена на микросегментации, которая определяет конечную точку каждого удостоверения как отдельный объект, а затем применяет контекстно-зависимые политики, предотвращая горизонтальное перемещение. Архитектура AirGap «доверяй везде» включает в себя автономную сеть политик, которая немедленно масштабирует политики микросегментации по всей сети.

Поскольку предпочтительным инструментом злоумышленника является вредоносное ПО Emotet, каждая конечная точка должна быть отказоустойчивой, самовосстанавливающейся и способной отслеживать трафик в режиме реального времени. Цель должна состоять в том, чтобы обеспечить доступ с наименьшими привилегиями по удостоверению для любого ресурса, запрошенного в каждой конечной точке.

Чем более устойчива конечная точка, тем больше вероятность того, что она сможет отразить атаку на удостоверения. Самовосстанавливающаяся конечная точка выключится и проверит свои основные компоненты, начиная с ОС. После исправления версии конечная точка автоматически вернется к оптимизированной конфигурации. Absolute Software, Akamai, CrowdStrike Falcon, Ivanti Neurons, Malwarebytes, Microsoft Defender, SentinelOne, Tanium, Trend Micro и другие поставщики предлагают самовосстанавливающиеся конечные точки.

Платформы конечных точек быстро обновляются в ответ на угрозы. Уникальный подход платформы отказоустойчивости Absolute предоставляет ИТ-специалистам и специалистам по безопасности доступ к информации в режиме реального времени, а также к данным контроля и управления активами для любого устройства, подключенного к сети или нет. Компания демонстрирует стабильно высокий уровень инноваций.

Компания Absolute также изобрела и запустила первую самовосстанавливающуюся платформу с нулевым доверием для управления активами, устройствами и приложениями, аналитики конечных точек, отчетов об инцидентах, обеспечения устойчивости и соответствия требованиям. Неудаляемая цифровая привязка компании доказала свою эффективность в мониторинге и проверке запросов данных и транзакций каждой конечной точки на базе ПК в режиме реального времени.

ИТ-директора сообщают VentureBeat, что их команды достаточно напряжены, не имея возможности заниматься инвентаризацией устройств, требующих исправления. В результате исправление отодвигается на второй план в списке приоритетов, поскольку ИТ-специалисты и специалисты по безопасности слишком часто тушат пожары.

«Управление конечными точками и возможности самовосстановления позволяют ИТ-командам обнаруживать каждое устройство в своей сети, а затем управлять каждым устройством и обеспечивать его безопасность с помощью современных передовых методов, обеспечивающих продуктивность работы конечных пользователей и безопасность ресурсов компании», — Шринивас Муккамала, руководитель директор по продукту Ivanti, сказал в недавнем интервью VentureBeat.

Управление исправлениями в нужном масштабе требует подхода, основанного на данных. Ведущие поставщики в этой области извлекают выгоду из сильных сторон ИИ и машинного обучения (МО) для решения задач по поддержанию тысяч устройств в актуальном состоянии. Ведущие поставщики включают Broadcom, CrowdStrike, SentinelOne, McAfee, Sophos, Trend Micro, VMWare Carbon Black и Cybereason.

Один из самых инновационных подходов к управлению исправлениями реализован в платформе нейронов Ivanti, которая использует ботов на основе ИИ для поиска, идентификации и обновления всех исправлений на конечных точках, которые необходимо обновить. Ivanti Управление облачными исправлениями на основе рисков примечательно тем, как оно интегрирует рейтинг риска уязвимостей (VRR) компании, чтобы помочь аналитикам центра управления безопасностью (SOC) предпринимать действия с приоритетом риска. Иванти обнаружил, как обеспечить отслеживание соглашения об уровне обслуживания (SLA), которое также обеспечивает видимость устройств, приближающихся к соглашению об уровне обслуживания, что позволяет командам предпринимать упреждающие действия.

Бэкдор-атаки процветают, когда организация сокращает свой бюджет на безопасность и полагается на безопасность на основе периметра — или вообще не использует, просто надеясь, что взлома не произойдет.

Определение структуры нулевого доверия, которая соответствует бизнес-стратегии и целям организации, является ставкой на кону. И используемые технологии и подходы не обязательно должны быть дорогими, чтобы быть эффективными». ***(Louis Columbus. Defending against backdoor attacks with zero trust // VentureBeat (https://venturebeat.com/security/defending-against-backdoor-attacks-with-zero-trust/). 12.04.2023).***

***

«Эксперты по кибербезопасности обнаружили новую хакерскую кампанию, использующую слабо защищенные серверы MS-SQL для доставки программы- вымогателя Trigona.

Исследователи из южнокорейской фирмы AhnLab наблюдали, как злоумышленники сканировали серверы Microsoft SQL, открытые в Интернете, а затем пытались получить к ним доступ либо с помощью грубой силы, либо атак по словарю. Эти атаки работают, если на серверах установлены простые, легко угадываемые пароли, а автоматизировав процесс входа в систему, хакеры могут легко взламывать множество серверов.

Как только они получат доступ к конечной точке, злоумышленники сначала установят часть вредоносного ПО, которое исследователи назвали CLR Shell. Эта вредоносная программа собирает системную информацию, изменяет конфигурацию скомпрометированной учетной записи и повышает привилегии до LocalSystem через уязвимость в службе вторичного входа в систему Windows.

«CLR Shell — это тип вредоносного ПО сборки CLR, которое получает команды от злоумышленников и выполняет вредоносные действия, аналогичные WebShells веб-серверов», — говорят исследователи.

Следующим шагом будет использование дроппера svcservice.exe для развертывания программы-вымогателя Trigona. На этом этапе все файлы на устройстве шифруются, и остается записка о выкупе, инструктирующая жертв о том, как связаться с злоумышленниками и договориться о выпуске ключа дешифрования. Исследователи также заявили, что Trigona отключает восстановление системы и удаляет все теневые копии тома Windows, чтобы жертвы не могли восстановить свои системы с помощью резервной копии.

Хотя у предприятий может возникнуть соблазн заплатить выкуп, думая, что это будет самый простой и дешевый способ решить проблему, все согласны с тем, что им следует воздерживаться от уступок криминальным требованиям. Недавние данные от Rubrik Zero Labs показали, что из всех организаций, которые пострадали от атаки программ-вымогателей и заплатили за дешифратор, только 16% действительно удалось восстановить все свои данные.

Выплата выкупа также финансирует будущую преступную деятельность, что является еще одной причиной не поддаваться требованиям хакеров». ***(Sead Fadilpašić. Microsoft SQL servers hacked to spread ransomware // Future US, Inc (https://www.techradar.com/news/microsoft-sql-servers-hacked-to-spread-ransomware). 20.04.2023).***

***

«По данным группы Global Threat Intelligence Team NCC Group, атаки программ-вымогателей участились. В своем ежемесячном отчете об угрозах NCC Group сообщила об увеличении числа атак программ-вымогателей в марте на 91 % по сравнению с февралем и увеличении на 62 % по сравнению с месяцем прошлого года — самое большое количество ежемесячных атак программ-вымогателей, которые когда-либо измеряла группа…

Поставщик программ-вымогателей Cl0p, самый активный субъект угроз, составил 28% всех жертв в марте. NCC Group заявила, что Cl0p впервые стала лучшим RaaS для киберпреступных групп.

Cl0p, связанная с Россией организация, специализирующаяся на двойном вымогательстве, извлекает данные, а затем угрожает опубликовать их, если не будет выкупа. Хакерская группа существует с 2019 года, когда она успешно атаковала крупные компании, такие как Hitachi, Shell и ряд других предприятий.

LockBit 3.0 занял второе место, на его долю приходится 21% атак. NCC Group заявила, что март 2023 года стал вторым месяцем с сентября 2021 года, когда LockBit не был главным субъектом угрозы программ-вымогателей. По данным NCC, число жертв группы уменьшилось на 25% по сравнению с февралем.

Неприсоединившаяся атакующая группа Royal, появившаяся в сентябре прошлого года и нацеленная на сектор здравоохранения, стала третьим по активности злоумышленником с увеличением количества атак в марте по сравнению с февралем на 106%...

Группа NCC заявила, что увеличение количества атак со стороны CL0p отражает использование ею уязвимости в управляемой передаче файлов Fortra GoAnywhere, используемой тысячами организаций по всему миру, что привело к крупномасштабным сбоям.

Как сообщалось, Fortra обнаружила уязвимость нулевого дня в январе и сообщила об этом только своим аутентифицированным пользователям, но ей не присваивали CVE ID на Mitre и не исправляли до начала февраля.

Защита для организаций, использующих GoAnywhere MFT

По данным NCC Group, существуют действенные тактики защиты от атак со стороны Cl0p и других пользователей сторонних инструментов и сервисов:

Ограничьте доступ к портам 8000 и 8001, где расположена административная панель GoAnywhere MFT.

После входа в GoAnywhere выполните действия, описанные в рекомендациях по безопасности GoAnywhere.

Установите патч 7.1.2.

Проверяйте учетные записи пользователей-администраторов на предмет подозрительной активности, уделяя особое внимание учетным записям, созданным системами, подозрительному или нетипичному времени создания учетных записей или отключенным суперпользователям, создающим несколько учетных записей.

Свяжитесь со службой поддержки GoAnywhere MFT напрямую через портал, по электронной почте или по телефону, чтобы получить дополнительную помощь.

Североамериканский промышленный сектор - двойное яблочко

Регионы

Повторяя тенденции анализа прошлого месяца, Северная Америка была целью почти половины мартовской активности, жертвами которой стали 221 человек (48%). В Европе (28%) и Азии (13%) следуют 126 и 59 атак соответственно.

Секторы

Промышленность была наиболее целевым сектором в прошлом месяце: 147 забастовок, что составляет 32% атак. Consumer Cyclicals заняла второе место с 60 атаками (13%), за ними следует Technology, вернув себе третье место с 56 атаками (12%).

В промышленном секторе:

Количество жертв в сфере профессиональных и коммерческих услуг увеличилось на 120%.

Атаки на машины, инструменты, тяжелые транспортные средства, поезда и корабли увеличились на 127%.

Атаки на строительные и инженерные участки увеличились на 16%...

Мэтт Халл, глава глобального отдела анализа угроз в NCC Group, сказал, что огромный всплеск атак программ-вымогателей в прошлом месяце, вероятно, будет нормальным курсом в этом году. «Если операции [Cl0p] останутся стабильными, мы можем ожидать, что они останутся преобладающей угрозой в течение всего года. Мы внимательно следим за развитием актера», — сказал он.

Ранее компания сообщала о самом большом количестве случаев программ-вымогателей в январе и феврале, чем за последние 3 года.

Как защититься от ускоряющихся угроз программ-вымогателей

NCC Group предполагает, что в этом году число атак увеличится:

Знайте, затронет ли недавно объявленная уязвимость вашу организацию, а также свои системы и конфигурации.

Патч часто. Тот факт, что Log4j все еще активен, показывает, что неисправленные CVE открывают двери.

Блокируйте распространенные формы входа: создайте план, как быстро отключить подверженные риску системы, такие как VPN или RDP.

Изучите пакеты безопасности конечных точек, чтобы обнаружить эксплойты и вредоносное ПО.

Создавайте резервные копии в автономном режиме и вне офиса, вне досягаемости злоумышленников.

Будьте бдительны: Злоумышленники возвращаются к той же жертве, когда знают, что дыра не закрыта.

В случае атаки, когда вспышка изолирована и остановлена, все следы их вторжения, вредоносное ПО, инструменты и методы проникновения должны быть удалены, оценены и приняты меры, чтобы избежать повторной атаки». ***(Karl Greenberg. Ransomware attacks increased 91% in March, as threat actors find new vulnerabilities // TechnologyAdvice (https://www.techrepublic.com/article/ransomware-attacks-increased-march/). 19.04.2023).***

***

«Число случаев использования программ-вымогателей в авиационной цепочке поставок выросло на 600% всего за один год — это показатель эскалации рисков кибербезопасности, с которыми сталкивается отрасль.

Статистические данные были приведены Boeing на конференции MRO Americas, проводимой Aviation Week, в Атланте.

«Увеличивается количество интерфейсов с планером как в регулируемых, так и в нерегулируемых частях самолета», — сказал глава службы безопасности Boeing Ричард Пакетт. «Мы должны начать учитывать расширенную экосистему подключения... Увеличение запросов на датчики почти на каждой рабочей части самолета делает его более эффективным, но также делает его более уязвимым, потому что все, что отправляет или получает сигнал, может быть взломано. Любой, кто говорит иначе, на самом деле не обращает внимания».

По словам United Airlines, помимо развития цифровой связи, решение правительства о признании аэрокосмической и авиационной инфраструктуры критической инфраструктурой также повышает риск.

«Это почти рисует цель на спине воздушного пространства для злоумышленников, которые хотят воспользоваться этой критически важной инфраструктурой», — сказал директор по безопасности United Airlines Джен Миози. «Из-за этого он растет. С точки зрения ландшафта угроз мы наблюдаем все больше и больше кибератак, пытающихся проникнуть в эту критически важную инфраструктуру, которую мы называем авиацией».

Aviation ISAC, некоммерческая организация по сбору информации о кибербезопасности, также указала на геополитические мотивы.

«В мире много вещей, которые мотивируют людей нападать на авиационную отрасль, — сказал генеральный директор Aviation ISAC Джеффри Трой. «Мы должны быть обеспокоены этим. Мы даже видели «хактивистов», людей, которые, по сути, занимаются какой-то кибердеятельностью, чтобы поддержать определенную политическую повестку дня».

Отметив эскалацию беспокойства по поводу этого сценария, он добавил: «Без сомнения, угроза в этом уравнении возрастает».

С точки зрения того, где находится самая большая угроза, отраслевая группа больше смотрела на поддерживающую экосистему, а не на сам планер. Группа отметила, что ключевое значение имеет приоритизация рисков, наряду с обеспечением того, чтобы поставщики думали о кибербезопасности. Для некоторых авиакомпаний с контрактами, заключенными более десяти лет, положений о кибербезопасности может не быть. Это то, над чем работает United с более чем 30 000 поставщиков.

«Мы оцениваем всех наших третьих лиц, — сказал Миози. «Мы также работаем над улучшением наших контрактов со всеми нашими третьими сторонами… добавляя условия, связанные с необходимостью внедрения кибербезопасности в базу поставок».

Чтобы повысить устойчивость отрасли к угрозе, слишком динамичной, чтобы полагаться только на правила, участники дискуссии заявили, что необходимо более добровольное сотрудничество, а также признание того, что риск реален и растет.

Они подчеркнули, что бросить вызов прошлым предположениям и двигаться вперед, говоря на одном языке в понимании угроз, является ключевым.

«Это все еще закулисный разговор, потому что я думаю, что люди боятся выставлять напоказ свои слабости, которые у них могут быть», — сказал Пакетт. «Вы видите, как ватерлиния опускается вокруг экосистемы планера. Это на самом деле все больше и больше подвергается воздействию сообщества, которое очень, очень хорошо делится информацией. Одна из вещей, которую злоумышленники делают намного лучше, чем сегодня, я думаю, это то, что они делятся друг с другом». ***(Christine Boynton. Cybersecurity Threats To Aviation Bolstered By Efficiency, Geopolitics // Informa Markets (https://aviationweek.com/air-transport/airlines-lessors/cybersecurity-threats-aviation-bolstered-efficiency-geopolitics). 20.04.2023).***

***

«Поскольку программы-вымогатели продолжают поражать организации по всему миру, лидеры кибербезопасности все больше осознают важность инвестирования ресурсов в улучшение своих программ и процессов безопасности. Более 90 процентов опрошенных лидеров кибербезопасности и лиц, принимающих решения в различных отраслях, сообщили о планах увеличить бюджеты на безопасность в следующем году, говорится в отчете Fortinet Global Ransomware Report за 2023 год.

Лидеры сообщили о приоритетных инвестициях в искусственный интеллект (ИИ) и машинное обучение (МО) для улучшения обнаружения угроз, а также в инструменты безопасности Интернета вещей (IoT), межсетевые экраны нового поколения (NGFW) и обнаружение и реагирование конечных точек (EDR).) и шлюз безопасности электронной почты (SEG).

Увеличение бюджетов показывает, что руководители высшего звена все больше осознают важность кибербезопасности. Однако выделение бюджетных ресурсов исключительно на инструменты и технологии может не устранить ключевые недостатки безопасности.

«Интересно, что, хотя многие лидеры в области безопасности традиционно считали, что покупка лучшего отдельного продукта для проекта обеспечит наилучшую кибербезопасность, данные опроса этого года показывают, что те организации, которые сообщили о применении точечного подхода к продукту, с наибольшей вероятностью стали жертвой кибербезопасности. программы-вымогатели», — отмечается в отчете.

«Однако технологии — это только часть решения. Опрос показал, что четыре из пяти главных проблем в предотвращении программ-вымогателей связаны с людьми и процессами».

Несмотря на то, что 78% опрошенных руководителей охарактеризовали свои организации как «очень» или «чрезвычайно» подготовленные к борьбе с утечкой данных, половина опрошенных организаций все еще подвергалась атакам программ-вымогателей в прошлом году. Более того, 71 процент респондентов заявили, что они заплатили по крайней мере часть спроса на программы-вымогатели.

Из всех опрошенных организаций, ставших жертвами программ-вымогателей в прошлом году, фишинг оставался наиболее распространенной тактикой. Фишинговые атаки обычно используются против организаций здравоохранения и других организаций, чтобы обмануть сотрудников вредоносными ссылками и получить доступ к сети.

«Один из самых неожиданных выводов предыдущего опроса Fortinet заключался в том, что основным способом входа в 2021 году был фишинг по электронной почте, однако только треть организаций сообщили о планах по улучшению этой защиты», — отмечает Fortinet.

Тем не менее, результаты показали, что лидеры вкладывают средства в широкий спектр инструментов, нацеленных на различные потенциальные уязвимости. Но в отчете также подчеркивается важность инвестирования в технологии, которые оптимизируют и улучшают процессы, а не усложняют их.

В то время как 45 % респондентов заявили, что используют сочетание платформ безопасности и специализированных продуктов, 36 % заявили, что продолжают покупать только «лучшие в своем классе» точечные продукты.

«В результате многие группы безопасности в конечном итоге тратят много времени на управление отдельными продуктами, развертываемыми с течением времени, и изо всех сил пытаются заставить свою коллекцию технологий эффективно работать вместе», — говорится в отчете. «И такие ручные процессы могут помешать команде безопасности собрать правильные данные и быстро отреагировать на инцидент с программой-вымогателем».

Если организации придерживаются подхода «меньше значит больше» к инвестициям в безопасность, они могут сократить избыточность и неэффективность и посвятить больше времени совершенствованию своих программ в целом. Результаты показали, что обучение сотрудников безопасности и продуманные улучшения процессов будут иметь большое значение.

«Согласно исследованию Fortinet, опубликованному сегодня, хотя три из четырех организаций рано обнаружили атаки программ-вымогателей, половина все же стала их жертвой. Эти результаты демонстрируют необходимость перехода от простого обнаружения к реагированию в реальном времени», — заявил Джон Мэддисон, исполнительный вице-президент по продуктам и директор по маркетингу в Fortinet, в сопроводительном пресс-релизе…» ***(Jill McKeon. 91% of Orgs Expect to Increase Cybersecurity Budgets in Next Year // TechTarget, Inc. (https://healthitsecurity.com/news/91-of-orgs-expect-to-increase-cybersecurity-budgets-in-next-year). 26.04.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В ходе исторической операции правоохранительные органы из 18 стран, в том числе Федеральное бюро расследований США (ФБР) и

Национальная полиция Нидерландов (Politie), закрыли Genesis Market, один из крупнейших онлайн-рынков, где киберпреступники продавали украденные личные данные, сообщает The Guardian.

Операция рекламировалась как беспрецедентная по своим масштабам и успеху.

Европол объявил в сообщении, что на печально известном онлайн-рынке было продано более 1,5 миллиона списков ботов, содержащих личные учетные данные, для двух миллионов человек, при этом в общей сложности было продано 80 миллионов учетных данных.

С помощью этих учетных данных киберпреступники могут получить доступ к информации из таких учетных записей, как онлайн-банкинг, Facebook, Amazon, PayPal и Netflix, среди прочих.

Торговая площадка продавала цифровые отпечатки пальцев устройств жертв в дополнение к личным учетным данным, что позволяло киберпреступникам обходить онлайн-проверки безопасности, выдавая себя за жертву.

Что такое Genesis Market? Почему это опасно?

Воздействие преступной деятельности, организованной Genesis Market, было далеко идущим: информация о предприятиях также продавалась на платформе.

Торговая площадка допускала преступную деятельность, такую как мошенничество, атаки программ-вымогателей, подмену сим-карт и кражу исходного кода у компаний.

Покупатели ботов получали не только доступ к украденным данным, но и кастомные браузеры, имитирующие браузеры их жертв. Это позволило преступникам получить доступ к учетной записи жертвы в обход мер безопасности платформы.

Как пользователи получают доступ к нелегальному сайту

Genesis Market был доступен как в открытом, так и в даркнете, но был скрыт от правоохранительных органов за завесой, доступной только по приглашению.

Согласно сообщениям, пользователям были даны пошаговые инструкции по приобретению украденной информации и использованию ее для мошенничества. В зависимости от типа доступной информации цены варьировались от 70 центов США (56 пенсов) до нескольких сотен долларов.

Успешная охотничья операция

Операцию, в результате которой было произведено более 120 арестов и более 200 обысков по всему миру, возглавило Национальное агентство по борьбе с преступностью Великобритании (NCA), которое провело серию рейдов во вторник, 4 апреля. В Соединенном Королевстве были задержаны 19 подозреваемых пользователей сайта.

Агентство Reuters сообщает, что в расследовании участвовали Австралия, Канада, Дания, Эстония, Финляндия, Франция, США, Великобритания, Германия, Исландия, Италия, Новая Зеландия, Польша, Румыния, Испания, Швеция и Швейцария.

Уилл Лайн, глава отдела киберразведки Национального агентства по борьбе с преступностью Великобритании, прокомментировал, что Genesis Market был «огромным инструментом мошенничества и ряда других преступных действий в

Интернете, облегчая этот первоначальный доступ к жертвам, который является важной частью бизнес-модели. во всем диапазоне гнусной деятельности».

Роб Джонс, генеральный директор Национального центра экономических преступлений, подчеркнул легкость, с которой любой может получить доступ к рынку для совершения преступления.

Знайте, были ли вы жертвой

Глобальные правоохранительные органы продемонстрировали свою способность сотрудничать в борьбе с международным характером киберпреступности. Следователи уже создали поддельные распределенные сайты отказа в обслуживании для сбора криминальной информации, и они могут использовать аналогичную тактику с мошенническими сайтами.

Закрытие Genesis Market посылает киберпреступникам четкий сигнал о том, что их действия не останутся безнаказанными». ***(John Lopez. FBI, Dutch Police Crush Massive Online Identity Theft Ring: 80 Million 'Identities' Recovered // TECHTIMES.com (https://www.techtimes.com/articles/290044/20230405/fbi-dutch-police-crush-massive-online-identity-theft-ring.htm). 05.04.2023).***

***

«Международные правоохранительные органы захватили обширную торговую площадку даркнета, популярную среди киберпреступников, сообщило в среду Национальное агентство по борьбе с преступностью Великобритании (NCA) в ходе многонациональной операции, получившей название «Операция Cookie Monster».

Баннер, размещенный на сайте Genesis Market поздно вечером во вторник, сообщил, что домены, принадлежащие организации, были конфискованы ФБР. На сайте также красовались логотипы других европейских, канадских и австралийских полицейских организаций, а также логотип компании Qintel, занимающейся кибербезопасностью.

«По нашим оценкам, Genesis является одним из самых значительных рынков доступа в любой точке мира», — сказал Роб Джонс, генеральный директор NCA по управлению угрозами.

По оценкам NCA, на сервисе было размещено около 80 миллионов учетных данных и цифровых отпечатков пальцев, украденных у более чем 2 миллионов человек.

Заместитель генерального прокурора Министерства юстиции США Лиза Монако в своем заявлении сообщила, что многие пользователи форума были арестованы во вторник. Высокопоставленный чиновник ФБР сообщил, что аресты были произведены в Соединенных Штатах, но отказался сообщить подробности. Расследование Генезиса все еще продолжается.

Министерство финансов США в заявлении, объявляющем о санкциях против рынка, назвало его «одним из самых известных брокеров украденных учетных данных и другой конфиденциальной информации».

Британские власти заявили, что в операции, которую возглавляли ФБР и голландская национальная полиция, участвовали 17 стран, в результате которой

было проведено около 120 арестов, более 200 обысков и почти 100 единиц «профилактической деятельности».

Qintel не сразу ответила на сообщения с просьбой прокомментировать ситуацию, а Reuters не смогло сразу же найти контактную информацию администраторов Genesis Market, которые, по словам Минфина США, предположительно работали из России.

Genesis специализируется на продаже цифровых продуктов, особенно «отпечатков пальцев браузера», собранных с компьютеров, зараженных вредоносным ПО, говорит Луиза Ферретт, аналитик британской фирмы по кибербезопасности Searchlight Cyber.

По ее словам, поскольку эти отпечатки часто включают в себя учетные данные, файлы cookie, адреса интернет-протокола и другие сведения о браузере или операционной системе, преступники могут использовать их для обхода решений по борьбе с мошенничеством, таких как многофакторная аутентификация или снятие отпечатков пальцев устройства.

Сайт работает с 2018 года.

NCA заявило, что Genesis продавал учетные данные от 70 центов до сотен долларов в зависимости от доступных украденных данных.

«Чтобы приступить к работе, вам просто нужно знать о сайте, потенциально быть в состоянии получить себе приглашение, что, учитывая количество пользователей, вероятно, не будет особенно сложным», — сказал Уилл Лайн, глава отдела киберразведки NCA. «Как только вы становитесь пользователем, очень легко… совершать преступные действия».

По данным NCA, в расследовании участвовали Австралия, Канада, Дания, Эстония, Финляндия, Франция, США, Великобритания, Германия, Исландия, Италия, Новая Зеландия, Польша, Румыния, Испания, Швеция и Швейцария.

«Рынок Genesis снизил входной барьер для групп вымогателей и позволил многим киберпреступникам быстро масштабировать свои операции и проводить целевые атаки для получения немедленной финансовой выгоды», — сказал Джон Фоккер, глава отдела анализа угроз американской фирмы по кибербезопасности Trellix. «Даже не принимая во внимание аресты членов Genesis Market, простое удаление этого огромного киберпреступного рынка из сети значительно замедлит активность киберпреступников». ***(Michael Holden, James Pearson, Christopher Bing. 'Operation Cookie Monster': International police action seizes dark web market // Reuters (https://www.reuters.com/world/uk/operation-cookie-monster-international-police-action-seizes-dark-web-market-2023-04-05/). 05.04.2023).***

***

Технічні аспекти кібербезпеки

«По мере развития цифровой эпохи частота и изощренность кибератак угрожают нашей личной конфиденциальности, финансовым системам и критической инфраструктуре. Среди этого хаоса появилась одна технологическая инновация, которая может изменить правила игры: блокчейн

технология. От защиты конфиденциальных данных до аутентификации онлайн-идентификаций технология блокчейн предлагает множество приложений, которые могут сильно повлиять на наш цифровой ландшафт…

Технология блокчейн получила широкое признание в качестве основы Биткойн около десяти лет назад и с тех пор в общественном понимании в основном ассоциируется с криптовалютами. Децентрализованный, основанный на консенсусе и ненадежный характер блокчейна делает его естественно устойчивым к атакам.

Например, в методах подтверждения работы, таких как биткойн, хакеры должны получить контроль над большинством узлов, чтобы скомпрометировать транзакции бухгалтерской книги, что требует больших вычислительных ресурсов и требует больших затрат, что затрудняет компрометацию системы. Распространяя эти вычислительные затраты на другие операции в рамках схемы безопасности, становится менее необходимым полагаться на доверенный центральный орган.

Атаки распределенного отказа в обслуживании (DDoS) часто используют серверы доменных имен в Интернете (DNS), которые сопоставляют IP-адреса с удобочитаемыми именами веб-сайтов. Переместив DNS в блокчейн, ресурсы могут быть распределены между несколькими узлами, что делает непрактичным контроль над базой данных для злоумышленников.

Однако простого создания баз данных или приложений на блокчейне недостаточно для обеспечения неуязвимости, учитывая настойчивость хакеров и растущую тенденцию к кибервойне между правительствами. Один из подходов к укреплению технологии блокчейна включает использование искусственного интеллекта (ИИ) для выявления и предотвращения злонамеренных манипуляций с данными. Кроме того, специально созданный ИИ может защитить систему или базу данных и быть реализован в более распределенной модели как приложение блокчейна, которому не требуются доверенные узлы для поддержания целостности.

Замена паролей аутентификацией блокчейна

Пароли, несомненно, являются самым слабым звеном в современных инфраструктурах кибербезопасности. Около 80% всех кибератак в 2022 году были вызваны взломом пароля. Различные источники предлагают различный процент слабых и уязвимых паролей, но широко распространено мнение, что пароли являются неадекватной мерой безопасности для любого устройства или программного обеспечения. Хакеры могут получить конфиденциальные личные данные 1,5 миллиарда пользователей Facebook с помощью простых фишинговых и парольных атак.

Понимание проблемы пароля в кибербезопасности

Проблема с паролями заключается в том, что они требуют частых обновлений и изменений, что приводит к чрезмерно сложным комбинациям, которые трудно запомнить, в результате чего пользователи часто повторно используют одни и те же пароли. Кроме того, многие пользователи игнорируют основные правила безопасности и игнорируют предупреждения о ненадежных паролях от поставщиков программного обеспечения. Даже специалисты по безопасности не застрахованы: только 50% из них меняли пароли в социальных сетях за последний год, а 20% никогда их не меняли. Несмотря на регулярную смену пароля, решительный хакер в конечном итоге может взломать любой пароль.

По данным Ponemon Institute, более половины обычных пользователей и ИТ-специалистов хотят иметь альтернативный метод защиты своих учетных записей, более простой, но безопасный. Блокчейн-аутентификация может стать такой альтернативой. Некоторые проекты позволяют пользователям создавать учетную запись в своей системе и использовать этот ключ доступа для других систем и программного обеспечения, аналогично использованию учетных записей Facebook или Google для входа в Spotify или Netflix.

Признание блокчейн-решения

В отличие от Facebook или Google, аутентификация на блокчейне не требует паролей, поскольку использует закрытые ключи, многоэтапную аутентификацию и биометрические данные для проверки личности пользователя, что делает ее более безопасной и удобной для пользователя.

Системы на основе блокчейна присваивают каждому пользователю открытый ключ и закрытый ключ, необходимые для прямой аутентификации. Блокчейн хранит открытый ключ, а пользователь сохраняет закрытый ключ.

Открытые ключи служат для идентификации пользователя, позволяя прозрачно отслеживать его действия в блокчейне. Между тем, соответствующие закрытые ключи, которые должны быть защищены на аппаратных устройствах, аутентифицируют действия, выполняемые в цепочке.

Встраивая закрытый ключ в аппаратные устройства, он больше не хранится в базе данных приложения, которая часто становится целью утечек данных. Эта настройка повышает безопасность и обеспечивает полный контроль пользователей над своими учетными данными, а также дополнительное преимущество, заключающееся в том, что пользователю не обязательно знать свой закрытый ключ.

Фактически, несколько технологических гигантов, таких как Civic, IBM и Microsoft, уже работают над решениями для идентификации на основе блокчейна. Microsoft уже запустила децентрализованную систему идентификации, основанную на сети блокчейн.

Остановка автоматических атак бокового движения

Появление интеллектуальных устройств и автономных технологий увеличило мобильность и автоматизировало рутинные задачи. Однако потери, понесенные из-за хакерских атак и утечек данных, сейчас беспрецедентны, и такие примеры, как взлом Amazon Alexa или захват беспилотников в Украине, выявляют значительные пробелы в безопасности.

Наличие нескольких интеллектуальных устройств увеличивает вероятность того, что хакеры взломают систему безопасности, поскольку они могут выбирать свои цели, а большинство целей не защищены от киберугроз. Это продемонстрировала компания Senrio Security, которая взломала квартиру или офис, получив доступ к сети смартфона или камеры видеонаблюдения. Кроме того, даже конфиденциальность в сети не вызывает особого беспокойства, поскольку для доступа к локальной сети можно использовать обычный дрон.

Однако внедрение системы на основе блокчейна может защитить интеллектуальные устройства. Такие системы трудно взломать, поскольку хакерам потребуется взять под контроль 51% устройств в системе. Более того, технология блокчейна может эффективно выявлять недостоверные или потенциально опасные

команды и входные данные, которые представляют собой серьезные пробелы в безопасности систем интеллектуальных устройств.

Поддержание целостности данных с помощью блокчейна

В современном мире безопасность данных стала серьезной проблемой для отдельных лиц, учреждений и правительств. Появление технологии блокчейна предоставило решение, обеспечивающее высокий уровень безопасности и надежности для хранения данных и управления ими.

В отличие от традиционных баз данных, данные в блокчейнах неизменяемы и защищены от несанкционированного доступа, поскольку сетевые узлы ссылаются друг на друга и опираются друг на друга, что требует консенсуса для проверки транзакций. Тем не менее, данные вне сети уязвимы для повреждения, что подчеркивает важность подписей в сети для обеспечения новых вариантов использования блокчейна, где безопасность данных имеет первостепенное значение.

Три ключевые области, в которых технология блокчейна используется для обеспечения целостности данных, включают децентрализованное голосование, совместную работу медицинских и научных данных между учреждениями и децентрализованные метаданные. Благодаря децентрализованной архитектуре блокчейна и способности поддерживать защищенную от несанкционированного доступа запись данных, он может сыграть решающую роль в обеспечении целостности и подлинности записей о голосовании, медицинских карт пациентов и данных научных исследований.

Кроме того, технология блокчейна может сыграть ключевую роль в оптимизации ИИ в сфере кибербезопасности, предоставляя децентрализованный уровень метаданных для анализа угроз кибербезопасности. Способность блокчейна обеспечивать целостность и подлинность данных станет важным инструментом предотвращения угроз кибербезопасности и защиты от утечек данных.

Защита DNS с децентрализацией

DNS (система доменных имен) функционирует как телефонная книга, связывая имена веб-сайтов с IP-адресами, чтобы пользователи могли посещать веб-сайты. К сожалению, DNS лишь частично децентрализован, что делает его уязвимым для атак, которые могут отключить веб-сайты. В результате многие интернет-продавцы и интернет-магазины потеряли клиентов из-за временной деактивации, вызванной DNS-атаками.

Согласно исследованию Международного совета безопасности Neustar, проведенному в сентябре 2021 года, 72% участников исследования пострадали от DNS-атак за последние 12 месяцев. Распространенные типы DNS-атак включают отравление кэша DNS для перенаправления пользователей на мошеннические веб-сайты, атаки с усилением DNS, которые используют уязвимости в системах DNS для усиления DDoS-атак, и DDoS-атаки, которые перегружают серверы, что приводит к полной деактивации веб-сайта.

Децентрализованные блокчейны, на которых размещаются системы DNS, могут защитить от этих типов атак DNS, устраняя уязвимости, существующие в централизованных системах. Взломать центральный сервер, даже самый защищенный, проще, чем взломать блокчейн с тысячами P2P-узлов.

Будущее блокчейна в кибербезопасности

Будущий потенциал блокчейна в области кибербезопасности огромен, и эта технология призвана сыграть решающую роль в обеспечении безопасности нашего цифрового мира. Децентрализация и неизменность блокчейна может устранить необходимость в посредниках, снизить риск утечки данных и повысить целостность данных.

Кроме того, системы управления идентификацией на основе блокчейна могут обеспечить более безопасный и прозрачный способ проверки и аутентификации пользователей, а использование смарт-контрактов может обеспечить безопасное и автоматическое выполнение протоколов кибербезопасности. Поскольку технология блокчейна продолжает развиваться, мы можем ожидать появления еще большего количества инновационных приложений и вариантов использования, революционизирующих наш подход к кибербезопасности и защищающих нас от постоянно растущей угрозы киберпреступности.

Невозможно считать любую киберзащиту или информационную систему защищенной на 100%. То, что считается безопасным сегодня, может оказаться небезопасным завтра из-за прибыльного характера киберпреступности и способности преступников изобретать новые методы атак. Хотя технология блокчейна предлагает такие возможности, как конфиденциальность, целостность и доступность данных кибербезопасности для защиты организаций, которые включают блокчейн в свою техническую инфраструктуру, от внешних атак, как и в случае любой другой системы., необходимо принять средства контроля и стандарты

Заключение

Блокчейн уже становится неотъемлемой практикой безопасности для корпораций в различных отраслях, выступая в качестве базовой технологии для защиты данных. Блокчейн может выходить за рамки корпоративного и государственного управления данными и снижения ответственности, возвращая право собственности на данные пользователям. Эта технология поднимает планку безопасности данных и готова оставаться ведущим решением для защиты конфиденциальной информации в Интернете. Пользователи получат более простую и безопасную цифровую жизнь на блокчейне, уменьшая мошенничество и восстанавливая доверие к онлайн-транзакциям». ***(Damilola Lawrence. How is Blockchain Re-inventing Cybersecurity and Profoundly Protecting the Digital Landscape? // Cryptopolitan (https://www.cryptopolitan.com/blockchain-reinvent-cybersecurity-protect/). 05.04.2023).***

***

«Сетевое оборудование корпоративного уровня на вторичном рынке скрывает конфиденциальные данные, которые хакеры могут использовать для проникновения в корпоративную среду или для получения информации о клиентах.

Изучив несколько бывших в употреблении маршрутизаторов корпоративного класса, исследователи обнаружили, что большинство из них были ненадлежащим

образом очищены в процессе вывода из эксплуатации, а затем проданы через Интернет.

Основные маршрутизаторы для продажи

Исследователи из компании ESET, занимающейся кибербезопасностью, приобрели 18 бывших в употреблении основных маршрутизаторов и обнаружили, что полные данные конфигурации по-прежнему доступны более чем на половине из них, которые работали должным образом.

Основные маршрутизаторы являются основой большой сети, поскольку они соединяют все остальные сетевые устройства. Они поддерживают несколько интерфейсов передачи данных и предназначены для пересылки IP-пакетов на самых высоких скоростях.

Первоначально исследовательская группа ESET купила несколько бывших в употреблении маршрутизаторов для настройки тестовой среды и обнаружила, что они не были должным образом стерты и содержали данные о конфигурации сети, а также информацию, которая помогла идентифицировать предыдущих владельцев.

Приобретенное оборудование включало четыре устройства Cisco (ASA 5500), три устройства Fortinet (серия Fortigate) и 11 устройств Juniper Networks (Сервисный шлюз серии SRX).

В отчете, опубликованном ранее на этой неделе, Кэмерон Кэмп и Тони Анскомб говорят, что одно устройство было неисправно по прибытии и исключено из испытаний, а два из них были зеркалами друг друга и считались одним в результатах оценки.

Из оставшихся 16 устройств только пять были очищены должным образом и только два были защищены, что затруднило доступ к некоторым данным.

Однако для большинства из них можно было получить доступ к полным данным конфигурации, которые представляют собой кладезь подробностей о владельце, о том, как он настроил сеть, и о соединениях между другими системами.

В случае с корпоративными сетевыми устройствами администратору необходимо выполнить несколько команд, чтобы безопасно стереть конфигурацию и сбросить ее. Без этого маршрутизаторы могут быть загружены в режим восстановления, который позволяет проверить, как он был настроен.

Секреты в сети

Исследователи говорят, что некоторые из маршрутизаторов сохраняли информацию о клиентах, данные, которые позволяли третьим сторонам подключаться к сети, и даже «учетные данные для подключения к другим сетям в качестве доверенной стороны».

Кроме того, восемь из девяти маршрутизаторов, предоставивших полные данные конфигурации, также содержали ключи и хэши аутентификации между маршрутизаторами.

Список корпоративных секретов расширен за счет полных карт конфиденциальных приложений, размещенных локально или в облаке. Некоторые примеры включают Microsoft Exchange, Salesforce, SharePoint, Spiceworks, VMware Horizon и SQL…

Исследователи объясняют, что такие обширные инсайдерские данные обычно зарезервированы для «высококвалифицированного персонала», такого как сетевые администраторы и их менеджеры.

Злоумышленник, имеющий доступ к информации такого типа, может легко разработать план атаки, который позволит ему пройти вглубь сети незамеченным…

Судя по деталям, обнаруженным в маршрутизаторах, некоторые из них находились в среде управляемых ИТ-провайдеров, которые управляют сетями крупных компаний.

Одно устройство даже принадлежало поставщику управляемых услуг безопасности (MSSP), который обслуживал сети для сотен клиентов в различных секторах (например, в образовании, финансах, здравоохранении, производстве).

Следуя своим выводам, исследователи подчеркивают важность правильной очистки сетевых устройств, прежде чем избавляться от них. Компании должны иметь процедуры безопасного уничтожения и утилизации своего цифрового оборудования.

Исследователи также предупреждают, что использование стороннего сервиса для этой деятельности не всегда может быть хорошей идеей. Сообщив о своей находке владельцу роутера, они узнали, что компания воспользовалась такой услугой. «Это явно пошло не так, как планировалось».

Совет здесь состоит в том, чтобы следовать рекомендациям производителя устройства по очистке оборудования от потенциально конфиденциальных данных и доведению его до заводского состояния по умолчанию». ***(Ionut Ilascu. Hackers can breach networks using data on resold corporate routers // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/hackers-can-breach-networks-using-data-on-resold-corporate-routers/). 23.04.2023).***

***

«Угрозы кибербезопасности для организаций увеличиваются с каждым годом. Тем не менее, используя многоуровневый подход к кибербезопасности, компании могут бороться с современными угрозами.

Многоуровневая стратегия кибербезопасности — это стратегия, в которой используются преимущества различных технологий и протоколов для настройки защиты в различных частях сети. Каждый из этих семи слоев работает в тандеме с другими, чтобы обеспечить надежную защиту окружающей среды.

Такая комплексная стратегия гарантирует, что каждый участок сети защищен и проактивно отслеживается для предотвращения всех типов угроз.

Какие решения есть в программе многоуровневой безопасности?

1. Безопасность периметра. Решения по обеспечению безопасности периметра защищают данные, проходящие через внешний край сети или барьер между внутренней и внешней сетью. Он действует как защитный щит для бизнеса.

Этого можно добиться несколькими решениями, такими как унифицированное управление угрозами (UTM) и брандмауэры веб-приложений.

UTM — это комплексное решение, включающее в себя такие технологии, как антивирус нового поколения, брандмауэры, защищающие безопасность всей сети,

обнаружение вторжений, фильтрацию спама и контента и даже VPN — зашифрованное онлайн-соединение, соединяющее ваши устройства и сети.

В то время как безопасность периметра блокирует угрозы, проникающие в сеть, другие уровни защиты действуют для обнаружения любых угроз, которые активны внутри сети.

2. Мониторинг сетевой безопасности: инструменты сетевого мониторинга позволяют бизнесу просматривать активность в системе и получать полную информацию для обнаружения подозрительных действий.

Инструменты, составляющие этот уровень, включают в себя информацию о безопасности и управление событиями (SIEM), а также сетевое обнаружение и реагирование (NDR).

SIEM — это решение для мониторинга и управления событиями, которое может предупреждать заинтересованные стороны о любых нерегулярных попытках входа в систему. Эти оповещения также могут быть переданы ИТ-команде для немедленного исправления.

Сетевое обнаружение и ответ (NDR) аналогичны, но сосредоточены на обнаружении аномальной активности в сетевом трафике.

Помимо этих инструментов, сотрудники организации также составляют уровень безопасности.

3. Осведомленность о безопасности. Осведомленность о безопасности может показаться простой, но на самом деле это один из самых мощных инструментов, которые организация может использовать в многоуровневой стратегии. Поскольку человеческая ошибка является основной причиной утечек данных и других успешных кибератак, компаниям следует вкладывать средства в обучение кибербезопасности, чтобы их сотрудники были готовы обнаруживать угрозы и сообщать о них.

В то время, когда атаки с использованием социальной инженерии стали обычным явлением, программа повышения осведомленности о кибербезопасности — отличный способ защитить компанию. Такая программа обучает сотрудников передовым методам кибербезопасности, гигиене паролей, осведомленности о фишинге и многому другому.

4. Защита конечных точек. Распространенность Интернета вещей (IoT) — взаимосвязанной сети вычислительных и цифровых устройств — поддерживает связь между предприятиями, но также создает большую поверхность для атак. Чтобы защитить эту поверхность, организации могут использовать защиту конечных точек.

Конечные точки в современной бизнес-среде повсюду: смарт-телевизоры, мобильные устройства, принтеры, торговые автоматы и т. д. Система доменных имен (DNS) и управляемая защита обнаружения и реагирования (MDR) могут помочь защитить эти конечные точки.

Защита DNS блокирует доступ устройств к вредоносным сайтам, а защита MDR отслеживает процессы каждого устройства, чтобы распознавать отклонения и быстро реагировать.

Кроме того, постоянное обнаружение предотвращает доступ киберпреступников к вашей сети с помощью передовой технологии, которая

собирает активность, связанную с атаками, которые ускользают, а затем остаются в системе в течение длительного периода времени, просто собирая информацию.

Эти инструменты эффективны для предприятий с удаленной рабочей силой, поскольку угрозы могут непреднамеренно попасть через незащищенное сетевое соединение или вредоносный веб-сайт.

5. Информационная безопасность. Этот уровень защищает доступность, конфиденциальность и целостность данных. Это позволяет бизнесу защищать свою собственную и личную информацию своих клиентов.

В рамках этого уровня предотвращение потери данных (DLP) предотвращает несанкционированную передачу информации внутри организации наружу. DLP устанавливает стандарты безопасного хранения данных и доступа к ним.

Кроме того, решение для защиты электронной почты помогает предотвратить распространенные угрозы, такие как попытки фишинга, спам и распространение вирусов среди конечных пользователей через серверы электронной почты.

6. Протоколы аутентификации. Как следует из названия, решения для аутентификации гарантируют, что люди, получающие доступ к бизнес-данным организации, являются теми, кем они себя называют.

Аутентификация — это простой и невероятно эффективный способ предотвратить проникновение внешних субъектов в вашу сеть или доступ к вашим данным.

Предприятиям следует применять MFA (многофакторную аутентификацию), которая требует от пользователя подтверждения своей личности с помощью дополнительного метода подтверждения, такого как приложение, биометрическое сканирование или код, отправленный на устройство.

Еще один инструмент на этом уровне — автоматизированное решение для управления паролями. Эта технология может автоматически уведомлять пользователей о смене паролей, сохранять полную историю паролей и шифровать всю отслеживаемую информацию.

7. Безопасность критически важных активов. Организации также должны быть готовы к успешной атаке или взлому. В конечном счете, независимо от того, насколько хороша защита, всегда существует вероятность того, что новый эксплойт проскользнет сквозь щели, и каждая организация должна иметь план на случай непредвиденных обстоятельств.

Службы резервного копирования и аварийного восстановления (BDR) обеспечивают резервное копирование важных данных организации, независимо от того, хранятся ли они на внутренних серверах или в облаке.

В рамках этого уровня резервное копирование «программное обеспечение как услуга» защищает данные, хранящиеся в облачных приложениях пользователей, а резервное копирование веб-сайтов восстанавливает данные онлайн в случае взлома.

Все эти уровни составляют комплексную и надежную стратегию кибербезопасности, которая защищает каждую часть корпоративной сети. Лидеры службы безопасности должны изучить свои собственные и исправить любые уязвимые слои, чтобы их организация могла продолжать работать без перебоев». ***(Jeff Leder. The 7 layers of a strong cybersecurity strategy // BNP Media***

(https://www.securitymagazine.com/articles/99253-the-7-layers-of-a-strong-cybersecurity-strategy). 25.04.2023).

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Компания HP выпустила предупреждение (opens in new tab) для бизнес-клиентов, использующих определенные модели принтеров LaserJet, о том, что они должны сохранять бдительность и предпринимать шаги для устранения уязвимости, которая может привести к раскрытию нежелательной информации.

CVE-2023-1707 получила оценку 9,1, что делает ее критической. Его описание гласит: «Некоторые принтеры HP Enterprise LaserJet и HP LaserJet Managed Printers потенциально уязвимы для раскрытия информации, если IPsec включен в FutureSmart версии 5.6».

Гигант аппаратного и инфраструктурного оборудования объявил о планах выпустить обновление прошивки в течение 90 дней, рекомендуя клиентам тем временем понизить версию прошивки, чтобы предотвратить нежелательные атаки.

Компания подтвердила, что затронутые клиенты используют FutureSmart 5.6, программное обеспечение, предназначенное для настройки принтера с панели управления или специальной веб-страницы. У затронутых пользователей также будет включен IPsec.

Полный список затронутых моделей HP Enterprise LaserJet и управляемых принтеров HP LaserJet можно найти в уведомлении о безопасности (откроется в новой вкладке), в котором предлагается временно перейти на версию микропрограммы 5.5.0.3 на период до трех месяцев. пока HP работает над исправлением.

Поскольку лазерная печать находится под пристальным вниманием из-за ее воздействия на окружающую среду, такого как высокое энергопотребление, недовольные клиенты, не желающие ждать 90 дней, могут испытать соблазн рассмотреть новое оборудование.

Недавно компания анонсировала новые принтеры Color LaserJet, которые обещают снизить энергопотребление на 27%. ITDM, менее лояльные к HP, возможно, также захотят рассмотреть возможность перехода к конкурирующим брендам, таким как Epson, которая ранее в этом году объявила о выпуске новых струйных принтеров, которые потребляют четверть энергии обычного лазерного принтера при одинаковой скорости печати.

Несмотря на это, рекомендации производителя по безопасности следует всегда соблюдать, а переход на более раннюю версию прошивки является обязательным для любого бизнеса, который ценит безопасность, а не исправление». ***(Craig Hale. HP LaserJet printers have a critical security bug - and there's nothing you can do for now // Future US, Inc. (https://www.techradar.com/news/hp-laserjet-***

printers-have-a-critical-security-bug-and-theres-nothing-you-can-do-for-now). 05.04.2023).

***

«Существует серьезная уязвимость, затрагивающая все поддерживаемые версии сервера и клиента Windows, которую активно используют хакеры, предупреждают исследователи. Поэтому, по их словам, ИТ-команды должны немедленно применить исправление.

Рассматриваемая уязвимость отслеживается как CVE-2023-28252, уязвимость нулевого дня в общей файловой системе журналов Windows (CLFS). Уязвимость, обнаруженная исследователями из Mandiant и WeBin Lab, может использоваться в атаках низкой сложности. Он не требует взаимодействия с пользователем, но требует локального доступа, сообщает BleepingComputer.

Было сказано, что злоумышленники, успешно использующие уязвимость, могут получить привилегии SYSTEM и полностью скомпрометировать целевую конечную точку. Nokoyawa В то же время исследователи из «Лаборатории Касперского» также видели, как его использовали, по-видимому, для развертывания вируса-вымогателя (opens in new tab).

«Исследователи Kaspersky обнаружили уязвимость в феврале в результате дополнительных проверок ряда попыток выполнения аналогичных эксплойтов повышения привилегий на серверах Microsoft Windows, принадлежащих различным предприятиям малого и среднего бизнеса в ближневосточном и североамериканском регионах», — говорится в сообщении. говорится в сообщении компании.

«CVE-2023-28252 впервые была обнаружена «Лабораторией Касперского» в ходе атаки, в ходе которой киберпреступники пытались развернуть более новую версию программы-вымогателя Nokoyawa».

Исследователи утверждают, что один и тот же злоумышленник использовал эту уязвимость, а также ряд других подобных уязвимостей с начала лета 2022 года. Они использовали их для атак на оптовую торговлю, энергетику, производство, здравоохранение и фирмы по разработке программного обеспечения.

Теперь Microsoft устранила проблему в своем накопительном обновлении за апрельское исправление вторника, и исследователи призывают всех пользователей немедленно установить исправление. Накопительное обновление устраняет еще 96 недостатков, в том числе 45 недостатков удаленного выполнения кода (RCE).

Кроме того, Агентство по кибербезопасности и безопасности инфраструктуры (CISA) добавило этот нулевой день в свой каталог известных эксплуатируемых уязвимостей и приказало организациям Федеральной гражданской исполнительной власти (FCEB) применить исправление к 2 мая». ***(Sead Fadilpašić. Critical Windows flaw has been exploited in ransomware attacks, so patch now // Future US, Inc. (https://www.techradar.com/news/critical-windows-flaw-has-been-exploited-in-ransomware-attacks-so-patch-now). 12.04.2023).***

***

«Познакомьтесь с Bastion, французским стартапом, созданным в октябре 2022 года, чтобы помочь небольшим компаниям справиться с рисками кибербезопасности без особых сложностей. Созданная бывшими сотрудниками Palantir компания уже привлекла 2,8 миллиона долларов.

Что отличает Bastion от других стартапов в области кибербезопасности, так это то, что он хочет стать вашей первой и последней подпиской на кибербезопасность. Он объединяет несколько различных продуктов, связанных с рисками кибербезопасности, с подходом «программное обеспечение как услуга»…

Сейчас в Bastion есть четыре разных модуля. Во-первых, стартап проводит тесты с имитацией фишинга, потому что многие проблемы с безопасностью возникают из-за того, что сотрудники раздают учетные данные. С этим учебным модулем Bastion конкурирует с Riot.

Во-вторых, Bastion сканирует вашу инфраструктуру и веб-приложения, чтобы свести к минимуму поверхность атаки. Компания предоставляет вам список исправлений для улучшения вашей конфигурации.

В-третьих, Bastion сканирует и защищает конечные точки, например ноутбуки сотрудников. «Мы предоставляем решение EDR, которое представляет собой своего рода улучшенный антивирусный инструмент с командой, которая следит за тем, что происходит в режиме реального времени», — сказал Фурнье. EDR означает «обнаружение и ответ конечной точки». Для этого продукта Bastion сотрудничает с поставщиком EDR с белой этикеткой.

И, наконец, Bastion хочет помочь компаниям отслеживать входящие электронные письма с помощью своего четвертого модуля. Прямо сейчас клиенты могут пересылать подозрительные электронные письма, чтобы точно знать, законное это письмо или нет. В какой-то момент стартап также хочет помочь вам настроить фильтры на входящие электронные письма, чтобы они даже никогда не появлялись в почтовых ящиках ваших сотрудников…

Bastion предлагает весь пакет всего за 10 евро на сотрудника в месяц. Это недешево, но некоторые компании могут подписаться на часть того, что может предложить Bastion.

Интересно, что компания не планирует продавать свой продукт напрямую небольшим компаниям. Вместо этого компания сотрудничает с аутсорсинговыми поставщиками услуг безопасности, банками, страховыми компаниями и т. д.

В ближайшие месяцы Bastion планирует создать сеть партнеров, которые уже помогают малому и среднему бизнесу, а также могут начать продавать Bastion своим клиентам. И, конечно же, будут новые функции и улучшения продукта». ***(Romain Dillet. Bastion is an all-in-one cybersecurity solution for small businesses // Yahoo (https://techcrunch.com/2023/04/26/bastion-is-an-all-in-one-cybersecurity-solution-for-small-businesses/?guccounter=1&guce_referrer=aHR0cHM6Ly9yLnNlYXJjaC55YWhvby5jb20vX3lsdD1Bd3JFb2ZGalprcGtRMlVEQVZEUXRETUQ7X3lsdT1ZMjlzYndOaVpqR***

UVjRzl6QXpJRWRuUnBaQU1FYzJWakEzTnkvUlY9Mi9SRT0xNjgyNjI2Mjc2L1JPPTEwL1JVPWh0dHBzJTNhJTJmJTJmdGVjaGNydW5jaC5jb20lMmYyMDIzJTJmMDQlMmYyNiUyZmJhc3Rpb24taXMtYW4tYWxsLWluLW9uZS1jeWJlcnNlY3VyaXR5LXNvbHV0aW9uLWZvci1zbWFsbC1idXNpbmVzc2VzJTJmL1JLPTIvUlM9cXlaTktjWWxoZlBhbDhWOXFERldXMXF2NjJRLQ&guce_referrer_sig=AQAAAKKIv0WAF-qnEdUJBcfgQ3FexhfayMgSq2ZTmtbLuFAeTSDyLwoLIU56-knFvU4_XYQCSn0UHQX-3NSEXFz_ntz8VqS6xUAdCRCF55WAmRwiYXB_Tw43RFBUY2mE-liDed1VMpFwO6QDrXyQfYUUgJfrvfgQEZPEohDlFxemsZkd). 27.04.2023).

***

«Поскольку хакерство стало более разрушительным и всепроникающим, мощные инструменты таких компаний, как CrowdStrike Holdings Inc. и Corp. Microsoft стал благом для индустрии кибербезопасности.

Программное обеспечение для обнаружения конечных точек и реагирования на них предназначено для обнаружения ранних признаков вредоносной активности на ноутбуках, серверах и других устройствах — «конечных точках» в компьютерной сети — и блокирования их до того, как злоумышленники смогут украсть данные или заблокировать машины.

Но эксперты говорят, что хакеры разработали обходные пути для некоторых форм технологии, что позволило им обойти продукты, которые стали золотым стандартом для защиты критически важных систем.

Например, за последние два года компания Mandiant, входящая в подразделение Alphabet Inc. Google Cloud, расследовала 84 нарушения, когда EDR или другое программное обеспечение для защиты конечных точек было взломано или отключено, сказал Тайлер Маклеллан, главный аналитик угроз с компания.

Полученные данные представляют собой последнюю эволюцию игры в кошки-мышки, которая разыгрывалась десятилетиями, поскольку хакеры адаптируют свои методы для преодоления новейших средств защиты от кибербезопасности, по словам Марка Керфи, который занимал руководящие должности в McAfee и Microsoft, а теперь является специалистом по кибербезопасности. предприниматель в Великобритании.

«Во взломе средств защиты безопасности нет ничего нового», — сказал он, добавив, что «призом в случае успеха является доступ ко всем системам, использующим их, которые по определению достойны защиты».

Исследователи из нескольких фирм, занимающихся кибербезопасностью, заявили, что количество атак, в которых EDR отключается или обходится, невелико, но растет, и что хакеры становятся все более изобретательными в поиске способов обойти более надежную защиту, которую он обеспечивает.

Microsoft в декабре раскрывается в сообщение в блоге о том, что хакеры обманом заставили компанию применить печать подлинности к вредоносному ПО, которое затем использовалось для отключения EDR компании и других инструментов безопасности в сетях жертв. Microsoft заблокировала учетные записи сторонних разработчиков, причастных к уловке, и заявила, что компания «работает

над долгосрочными решениями для устранения этих обманных практик и предотвращения будущих последствий для клиентов».

В феврале Arctic Wolf Networks подробно описал случай, который он расследовал в конце прошлого года, когда хакеры из группы вымогателей Lorenz были первоначально загнаны в угол EDR жертвы. По словам компании, хакеры перегруппировались и развернули бесплатный инструмент цифровой криминалистики, который позволил им получить прямой доступ к памяти компьютеров и успешно развернуть свою программу-вымогатель, минуя EDR. Arctic Wolf не опознал жертву или затронутый EDR.

А в апреле Sophos Group раскрыла новое вредоносное ПО, обнаруженное британской фирмой, которое использовалось для отключения инструментов EDR от Microsoft, самой Sophos и нескольких других компаний перед развертыванием программ-вымогателей Lockbit и Medusa Locker. «Обход EDR и отключение программного обеспечения для обеспечения безопасности явно набирает обороты, — сказал Кристофер Бадд, старший менеджер по исследованию угроз. «Из-за характера такого рода атак их особенно трудно обнаружить, поскольку они нацелены на те самые инструменты, которые обнаруживают и предотвращают кибератаки».

По данным IDC, рынок EDR и других новых технологий безопасности конечных точек вырос на 27% и достиг 8,6 млрд долларов в мире в прошлом году, во главе с CrowdStrike и Microsoft.

Адам Мейерс, старший вице-президент CrowdStrike по разведке, сказал, что растущее число атак на программное обеспечение EDR показывает, что хакеры «развиваются». По его словам, многие из атак, которые отслеживала CrowdStrike, — против ее продуктов и продуктов, предлагаемых конкурентами, — связаны с неправильными конфигурациями клиентских систем или уязвимостями глубоко в программном обеспечении или прошивке, что является признаком того, что хакерам приходится прилагать больше усилий, чтобы проникнуть в целевые сети.

«Это гонка в конец стека», — сказал Мейерс. «Мы пытаемся спускаться все ниже и ниже, все ближе и ближе к оборудованию, и чем ближе вы подходите к оборудованию, тем сложнее остановить атаку».

Представитель Microsoft отказался комментировать эту историю.

Десять лет назад производители антивирусного программного обеспечения были доминирующими поставщиками продуктов для обеспечения безопасности ПК и других конечных устройств. Их популярность снизилась по мере того, как все более совершенные атаки обнажали слабые стороны технологий, которые полагались на то, что аналитики вручную создавали цифровые «подписи» новых штаммов вредоносных программ, чтобы блокировать их. по мнению экспертов по кибербезопасности.

Распространение программ-вымогателей и других разрушительных атак подстегнуло спрос на EDR и аналогичные технологии, которые нацелены на более раннее обнаружение и блокировку заражений. Эти инструменты выявляют дополнительные признаки вредоносной активности и автоматизируют многие трудоемкие задачи по расследованию и устранению нарушений.

Один ранее не сообщавшийся инцидент, раскрытый Bloomberg News, произошел в октябре, когда копенгагенская, датская группа безопасности CSIS расследовала взлом европейской производственной компании». ***(Jordan Robertson. Hackers Are Finding Ways to Evade Latest Cybersecurity Tools // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2023-04-27/hackers-are-finding-ways-to-evade-latest-cybersecurity-tools). 27.04.2023).***

***

Нові надходження до Національної бібліотеки України імені В.І. Вернадського

Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України / Ю. В. Завгородня // Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право. - 2021. - № 4. - С.33-38.

Проаналізовано сучасні наукові підходи до розуміння поняття кіберзахисту та кібербезпеки, надано узагальнену характеристику цих понять. Виокремлено сучасні форми безпеки в кіберпросторі. Проаналізовано стан кібербезпеки в українському інформаційному просторі та визначено її статус як суб'єкта глобальної взаємодії в інформаційному просторі.

Шифр зберігання НБУВ: Ж29126/псп

***

Койбічук В. Ефективність національної кібербезпеки: DEA-аналітика / В. Койбічук, В. Герасименко // Вісник економіки. - 2022. - Вип. 3. - С. 8-21.

Визначено ефективність національної кібербезпеки 97 країн світу у 2021 р., виявлено еталонні країни, які мають високоякісну систему національної кібербезпеки, а також визначено потенційні резерви для збільшення таргетованого значення індексу національної кібербезпеки.

Шифр зберігання НБУВ: Ж69632

***

Леган І. М. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму / І. М. Леган // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. - 2021. - Вип. 50. - С. 118-121.

Розкрито сутність понять «кіберзлочинність» і «кібертероризм», здійснено класифікацію найбільш популярних кіберзлочинів в сучасних умовах. Досліджено характерні риси кіберзлочинності та визначено критерії, за якими вона відмежовується від інших видів злочинності, зокрема кібертероризму. Доведено всю нинішню глобальність проблеми кіберзлочинності, адже сучасні кібератаки паралізують роботу не тільки приватних структур, а й державних органів влади. Розглянуто міжнародно-правову систему норм, спрямованих на створення правових засад співробітництва держав у сфері боротьби з кіберзлочинами.

Проаналізовано основні нормативно-правові акти та міжнародні документи у цій сфері, визначено шляхи удосконалення її правового регулювання на майбутнє.

Шифр зберігання НБУВ: Ж74042/Юр.

***

Лєонов С. В. Компаративний аналіз наглядово-регуляторного забезпечення процедур фінансового моніторингу та кібербезпеки / Лєонов С. В., Кузьменко О. В., Койбічук В. В., Горай Д. С. // Вісник Сумського державного університету. Серія : Економіка. - 2021. - № 3. - С. 162−169.

Проведено компаративний аналіз правого забезпечення кіберзахисту та кібербезпеки фінансової системи та інформаційно-комунікаційних технологій Німеччини, Польщі, України, Сполучених Штатів Америки, Швейцарії, Європейського Союзу. Узагальнюючий алгоритм фінансового моніторингу розглянуто в розрізі країн-членів Євросоюзу, що ґрунтується на діючих положеннях Директиви 2018/843/EU Європейського Парламенту та Ради Європейського про запобігання використанню фінансової системи з метою відмивання коштів та фінансування тероризму.

Шифр зберігання НБУВ: Ж69231/ек

***

Макух-Федоркова І. Нормативно-правові основи формування політики кібербезпеки Канади / І. Макух-Федоркова // Історико-політичні проблеми сучасного світу. - 2022. - Т. 45. - С. 29-40.

Досліджено питання нормативно-правового регулювання політики кібербезпеки Канади. Подно оцінку основним етапам формування кібернетичного законодавства.

Характеризуються програмні документи, спрямовані на удосконалення кібербезпеки Канади та опрацьовано директиви, які позитивно впливають на розвиток системи національної безпеки. Зосереджено увагу на міжнародній інтеграції Канади в сфері кібербезпеки та співпраці в плані захисту національного простору з країнами-партнерами в сучасних умовах.

Шифр зберігання НБУВ: Ж71049

***

Матеріали V Міжнародної науково-практичної конференції «Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід» : тези наук. доп. (16-17 квіт. 2021 р.). - Тернопіль : Західноукр. нац. ун-т, 2021. - 268 с.

Зі змісту:

- Грубінко А.В. Правове забезпечення політики кібербезпеки Європейського Союзу.

Шифр зберігання НБУВ: ВА859276

***

Матеріали XXVII науково-практичної конференції «Теорія та практика сучасної юриспруденції», 30 квітня 2021 року. - Харків, 2021. - 241 с.

Зі змісту:

- Трусов Я. І. Інформаційна безпека та кібербезпека: порівняння і актуальність;
- Бутко Д.В. Актуальні проблеми кібербезпеки та захисту інформації в Україні.

Шифр зберігання НБУВ: ВА859278

***

Федонюк С. Протистояння між США й Китаєм у сфері кібербезпеки / Сергій Федонюк, Сергій Магдисюк // Історико-політичні проблеми сучасного світу. - 2022. - Т. 45. - С. 113-127.

Досліджено глобальну конкуренцію США і Китаю в сфері кібербезпеки. Встановлено характер і тенденції протистояння між країнами в сфері кібербезпеки, досліджено цілі, засоби кібернетичних впливів у протистоянні США й Китаю в цій сфері. Встановлено напрями їх розвитку. Проаналізовано характер і напрями розвитку негативних кібернетичних впливів з точки зору кожної зі сторін. Розглянуто основні приклади кібернетичних впливів і позиції США й Китаю щодо взаємних кібернетичних загроз.

Шифр зберігання НБУВ: Ж71049

***

«Цифрова Україна»: конституційно-правова модель : матеріали всеукр. наук.-практ. конф. - Київ, 2020. - 344 с.

Зі змісту:

- Баранов О.А. Конституціно правова-парадигма цифрової трансформації та кібербезпеки.

Шифр зберігання НБУВ: ВА857302

***

Яровенко Г. М. Аналіз та моделювання соціально-економічного розвитку країн з урахуванням рівня їх кібербезпеки / Яровенко Г. М., Кочережченко Р. Д. // Вісник Сумського державного університету. Серія : Економіка. - 2022. - № 1. - С. 53−62.

Рівень кіберзлочинів, які набувають глобальних масштабів та їх наслідки призводять до дестабілізації економічних, соціальних та політичних процесів у суспільстві, досліджувався на основі статистичних даних 141 країни світу за 2019 рік за допомогою мови програмування Python. Національний індекс кібербезпеки було обрано як індикатор, що характеризує рівень країн протидіяти різного роду кіберзагрозам. Виявлено, що масив даних не містить пропущених значень, але за рядом показників, таких як рівень інфляції, рівень безробіття, витрати уряду на освіту, дохід за винятком грантів, експорт високих технологій, витрати на кінцеве споживання державного бюджету, ВВП, спостерігаються викиди. Проведений кореляційний аналіз виявив існування помітної та високої кореляції між факторами: національний індекс кібербезпеки, загальна очікувана тривалість життя

при народженні, легкість ведення бізнесу, ВВП на душу населення, наймані працівники та вразлива зайнятість.

Шифр зберігання НБУВ: Ж69231/ек

***

Prykaziuk N. Pandemic COVID-19 as a key factor in the development of DDos-attacks insurance / N. Prykaziuk, L. Gumenyuk // Вісник Київського національного університету імені Тараса Шевченка. Економіка. - 2022. - Вип. 1 (218). - С. 39-44.

Досліджено трансформацію ринку кіберстрахування у світі до та після початку пандемії COVID-19, оскільки пандемія стала переломним моментом для усіх учасників економічних відносин. Розглянуто стан і перспективи страхування від DDoS-атак та доведено необхідність розвитку зазначеного виду страхування в Україні. Надано рекомендації з уведення продуктів кіберстрахування від DDoS-атак у портфель українських страхових компаній у контексті Цифрової стратегії України 2030.

Шифр зберігання НБУВ: Ж28079/ек

***