**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

№ 3 (березень)

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.– №3 (березень) . – 267 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

Стан кібербезпеки в Україні 4
Кібервійна проти України 9
Боротьба з кіберзлочинністю в Україні 30
Світові тенденції в галузі кібербезпеки 32
Сполучені Штати Америки та Канада 90
Країни ЄС та Великобританія 99
Австралія та Нова Зеландія 108
Індія 111
Інші країни 112
Питання кіберстрахування 116
Кібервійни та протидія зовнішній кібернетичній агресії 118
Створення та функціонування кібервійськ 119
Кіберзахист критичної інфраструктури 121
Кіберзахист закладів охорони здоров'я 131
Захист персональних даних та соціальні мережі 131
Кібербезпека та хмарні технології 152
Кібербезпека Інтернету речей. Штучний інтелект 153
Кіберзлочинність та кібертероризм 162
Вірусне та інше шкідливе програмне забезпечення 198
Фішингові атаки 236
Операції правоохоронних органів та судові справи проти кіберзлочинців . 240
Технічні аспекти кібербезпеки 248
Виявлені вразливості технічних засобів та програмного забезпечення 248
Технічні та програмні рішення для протидії кібернетичним загрозам 267

«Держспецзв'язку провела змагання з кібербезпеки UA30CTF для студентів за підтримки ЄС. Держспецзв'язку за підтримки проекту EU4DigitalUA, що фінансується ЄС, провела змагання з кібербезпеки UA30CTF. У змаганні взяли участь 156 студентів III-VI курсів із 22 закладів вищої освіти України. Про це інформує Експерт із посиланням на Урядовий портал.

Перше місце здобула команда 4n0M4lY (Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»), друге та третє – Ghost of Sheva («Київський Національний університет ім. Тараса Шевченка») та Silent Sparrow («Київський національний економічний університет ім. Вадима Гетьмана», Університет «Україна», Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського») відповідно.

Змагання проходили у форматі гри #Jeopardy CTF. Протягом шести годин команди вирішували 25 завдань як на логіку, так і на пошук та експлуатацію вразливостей, у поєднанні з вирішенням цікавих логічних завдань.

«Одним із пріоритетів Держспецзв'язку в напрямку реформування сфери кіберзахисту є розбудова кадрового потенціалу. Зокрема, підвищення рівня підготовки майбутніх фахівців. Задля цього Держспецзв'язку не тільки розпочала реформування формальної освіти, а й проводить практичні заходи на зразок цього, де студенти матимуть можливість використати свої знання у форматі змагань. Сподіваюсь, що в майбутньому в Україні буде ще більше таких заходів», – зазначив заступник Голови Держспецзв'язку Віктор Жора.

Марія Гастон Бетран, технічна інституційна координаторка FIIAPP проекту EU4DigitalUA, який підтримав змагання, зазначила: «З кожним днем кіберзагрози стають все більш складними. Якісна освіта та практичні навички є ключем до формування майбутнього кожної людини. У EU4DigitalUA, що фінансується ЄС, ми розуміємо важливість розвитку експертної IT-спільноти в Україні. Потрібні яскраві, амбітні та віддані своїй справі експерти, які долучаться до боротьби з кіберзагрозами. Тому ми раді підтримати цей хакатон, який дозволив студентам

застосувати знання на практиці та дізнатися більше про можливості у сфері кібербезпеки».

Окрім участі у змаганнях, студенти мали можливість відвідати лекції з кібербезпеки провідних українських фахівців у цій галузі. Зокрема, від CISSP CISA OSCP – Володимира Стирана, CEO агенції «Мольфар» – Артема Старосєка та керівниці Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA – Євгенії Волівник». ***(Держспецзв'язку провела змагання з кібербезпеки для студентів // Expert (https://expert.in.ua/novosti/02032023-derzhspeczzvyazku-provela-zmagannya-z-kiberbezpeki-dlya-studentiv/). 02.03.2023).***

***

«У Державній службі спеціального зв'язку та захисту інформації розповіли, як компаніям, зокрема, медіа, захиститися від кібератак.

Про це повідомив кореспонденту Укрінформ голова Держспецзв'язку Юрій Щиголь.

«Щоб зменшити ризики, радимо усім компаніям, і учасникам медіаспільноти, зокрема, постійно проводити аудит кібербезпеки власних систем для вчасного виявлення ймовірних прогалин у захисті та визначення кроків для їх ліквідації. Сформуйте надійну команду: без професіоналів, які опікуватимуться питаннями кіберзахисту, буде важко підтримувати задовільний рівень кіберстійкості. Однією із невід'ємних умов підвищення рівня безпеки є навчання співробітників, адже, за статистикою, 9 із 10 кібератак відбуваються саме через необережність, неуважність чи відсутність знань персоналу», - зазначив він.

Водночас Щиголь наголосив, що у другому півріччі минулого року фахівці Держспецзв'язку зіткнулися з понад десятком серйозних кібератак на медіа, метою яких, зазвичай, було стирання даних. Підкреслюється, що хибним варіантом дій в умовахї кібервійни є сподівання, що кіберзловмисники можуть обійти увагою певні компанії.

Відтак зв'язківець рекомендує не нехтувати стандартними способами захисту: встановлювати складні паролі з різним регістром літер і спеціальними

символами. Водночас не варто зберігати паролі у доступних місцях. Також рекомендується використовувати двофакторну автентифікацію в усіх сервісах, де є така функція.

«Підходи до захисту власних акаунтів у різних соціальних мережах мають багато спільного. Головне завдання – не дати зловмисникам доступу до акаунту. Для цього варто не ігнорувати наявних у застосунках систем захисту й бути обачним самому», - підкреслив голова відомства.

Щиголь наголосив, що керівники компаній і кожен окремий громадянин несуть пряму відповідальність за інформаційні ресурси, які перебувають у їхній власності чи користуванні.

«Якщо ж ви помітили якусь незвичну активність у власній мережі чи маєте підозри, що ваші ресурси були атаковані, варто одразу звертатися до фахівців. Також допомогу за вашим зверненням готова надати наша Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA)», - зауважив голова Держспецзв'язку.

Як повідомлялося, за даними Інституту масової інформації, за 11 місяців війни на медіа було здійснено 42 кібератаки…» ***(Дев'ять із десяти кібератак відбуваються через необережність чи відсутність знань у персоналу // Укрінформ (https://www.ukrinform.ua/rubric-technology/3679866-devat-iz-desati-kiberatak-vidbuvautsa-cerez-neobereznist-ci-vidsutnist-znan-u-personalu.html). 08.03.2023).***

***

«Опитування про кіберстійкість провели CISO Ukraine спільно з Octava Defence, Accord Group, Cisco, Мегатрейд та «iForum.Кіберсцена».

Воно допомогло проаналізувати стратегії та системи й порівняти глобальні та локальні тренди. Опитування проводили протягом майже двох місяців узимку, у ньому взяли участь 150 українських підприємств. CIO та CISO українських підприємств відповіли на 15 питань з кібербезпеки: про прогрес компанії в окремих сферах кібербезпеки, використання технологій тощо.

Найбільше було компаній зі сфер ритейлу (23%), IT (14%), державного сектора (14%). Також в опитуванні взяли участь середній бізнес, фінансові, страхові компанії та інші.

Опитування показало, що існує розрив між тим, як компанії сприймають власну кіберстійкість, і реальним станом речей. Наприклад, 91% організацій вважають, що мають повний або достатньо повний набір технологій. 52% зазначили, що можуть бачити стан речей в IT-інфраструктурі.

Але дані про 10 ключових технологій, які забезпечують захист, надають дані для аналізу та визначають надійність системи, свідчать про інше.

Від 50% до 60% респондентів розповіли, що взагалі не використовують такі технології, як оркестрування систем безпеки, кіберрозвідка, захист із використанням методів обману тощо.

Що із цим робити?

Рішення з кібербезпеки дають не тільки автоматизований захист і протидію в моменті, а й багато інформації, яка дозволяє розслідувати всі випадки і правильно реагувати на них потім.

Для цього в Octava Defence супроводжують впровадження будь-яких рішень з кібербезпеки: детально аналізують інфраструктуру, критичні бізнес-сервіси, проводять аналіз ризиків і допомагають з тюнінгом і налаштуванням відповідних систем…

Опитування показало, що перші особи компаній стали більше долучатися до питань кібербезпеки. Так, 85% учасників розповіли, що топменеджмент бере в них участь. А рекордні 45% кажуть, що процесом Business Continuity and Disaster Recovery опікується наглядова рада або CEO.

Проте лише 41% компаній зазначили, що мають виокремленого CISO.

Що із цим робити?

З досвіду Octava Defence, відсутність CISO зазвичай каже про поверхневе ставлення до кібербезпеки, адже ця функція вимагає певної організаційно-технічної кваліфікації…

В Україні функції кібербезпеки стали зрілішими, тобто збільшується частка респондентів, які створюють політики і процедури в цьому напрямі.

Керівники вже починають сприймати організацію кібербезпеки не тільки як суто технічне завдання, а й як організаційне. При цьому ринок усе ще приділяє недостатньо уваги аварійному відновленню. 31% компаній зазначають, що цей процес покриває менше ніж 50% систем. 32% зазначили, що взагалі не перевіряють аварійне відновлення.

Що із цим робити?

Аварійне відновлення дозволяє програмам працювати ще декілька хвилин після збою. Загалом воно включає три компоненти:

Запобігання. Ви маєте створити правильні інструменти, щоб запобігти форс-мажору. Наприклад, софт для тестування системи, який автоматично перевіряє нові файли конфігурації перед їх застосуванням.

Передбачення. Важко передбачити, що може статися, але ви можете вигадати рішення для відновлення, використовуючи знання попередніх ситуацій та аналіз. Наприклад, зробити резервне копіювання всіх критично важливих бізнес-даних у хмару.

Пом’якшення наслідків. Це те, як підприємство реагує після лиха. Стратегія може знизити поганий вплив на звичайні бізнес-процеси. Вона включає такі кроки:

оновлення документації;

регулярне тестування системи аварійного відновлення;

робочі процедури, що виконують вручну в разі відключення електроенергії;

координація стратегії аварійного відновлення з відповідним персоналом.

Компанії розуміють кібербезпеку не тільки як впровадження технічних засобів захисту та переходять до більш зрілого операційного підходу й більш стратегічних завдань.

Але авторів опитування здивувало, що на фоні багатьох кібератак керівники не проводять розслідування таких подій.

«Спираючись на наш досвід, можемо розцінювати таку “самовпевненість” як тенденцію до надто поверхневого аналізу сповіщень та інцидентів, використання

стратегії “затикання дір”», – кажуть в Octava Defence. Можливі дві причини цього: відсутні професійні кібераналітики чи немає потрібних технічних засобів, які б могли надати дані для якісного розслідування». ***(Лише 41% компаній мають директора з IT-безпеки, третина не перевіряє аварійне відновлення – дослідження з кібербезпеки // ITC.ua (https://itc.ua/ua/articles/lyshe-41-kompanij-mayut-dyrektora-z-it-bezpeky-tretyna-ne-pereviryaye-avarijne-vidnovlennya-doslidzhennya-z-kiberbezpeky/). 20.03.2023).***

***

Кібервійна проти України

«В ноябре прошлого года несколько украинских организаций стали жертвами нового типа программ-вымогателей под названием RansomBoggs. Его операторы отправили зараженным компьютерам записку с требованием выкупа, написанную от имени Джеймса П. Салливана — главного героя мультфильма «Корпорация монстров».

В записке Салливан, чья работа в фильме заключалась в том, чтобы пугать детей, просил финансовой помощи в обмен на расшифровку документов организаций.

Предполагается, что хакеры, стоящие за этой атакой, связаны с Песчаным червем, российским действующим лицом, представляющим угрозу национальному государству, работающим от имени военной разведки ГРУ. Но, несмотря на то, что атака носила все атрибуты программы-вымогателя, Sandworm не собиралась зарабатывать деньги — ее основной целью было либо уничтожить украинские сети, либо украсть ценные данные, как утверждают исследователи из словацкой компании по кибербезопасности ESET, которая первой обнаружила атаку RansomBoggs.

Хотя Sandworm не является самой важной хакерской группой Кремля, она, пожалуй, стала самой заметной из них, уделяя особое внимание разрушительным кибератакам. А его послужной список успешных атак с глобальными

последствиями — в первую очередь вредоносное ПО NotPetya и несколько атак на электроснабжение Украины — вызывает серьезную озабоченность у исследователей.

В 2017 году группа использовала вредоносное ПО NotPetya Wiper, замаскированное под программу-вымогатель, чтобы вывести из строя сотни сетей в украинских государственных учреждениях, банках, больницах и аэропортах, нанеся глобальный ущерб примерно в 10 миллиардов долларов. Представляя разрушительные атаки как программы-вымогатели, хакеры Sandworm могут пытаться замести следы и затруднить для исследователей безопасности возможность приписать атаки группе, спонсируемой государством.

В случае атак RansomBoggs группа, вероятно, тестировала новые методы или обучала новых сотрудников тому, как использовать их программное обеспечение, сказал The Record старший исследователь вредоносного ПО ESET Антон Черепанов.

С самого начала войны Sandworm неустанно атакует Украину различными штаммами вредоносного ПО. Некоторые из них были очень сложными, в то время как другие содержали ошибки, которые облегчали их обнаружение и предотвращение распространения.

Исследователи полагают, что Sandworm решил экспериментировать с вредоносными программами, чтобы найти штаммы, способные обойти улучшенную защиту Украины.

По словам экспертов по кибербезопасности и правительственных чиновников, до сих пор он не оказал серьезного влияния на свои цели. Большая часть атак была нейтрализована на начальных этапах, а второго отключения электроэнергии, которого ожидали исследователи от Sandworm после того, как они атаковали украинскую энергосистему в 2015 и 2016 годах, так и не произошло.

ESET приписала Sandworm большинство подрывных атак Wiper против Украины в прошлом году. А поскольку Украина и Россия готовятся к крупному весеннему наступлению, ожидается, что число кибератак, в том числе со стороны Sandworm, возрастет.

«У России есть кибервозможности, и она будет продолжать использовать их, чтобы нанести любой ущерб Украине», — сказал Роберт Липовски, главный исследователь ESET в области разведки угроз.

Год дворников

За последний год группировка Sandworm осуществила не менее 30 кибератак на украинские системы, сообщили The Record в Госспецсвязи Украины. Большинство из этих инцидентов были атаками вайперов, такими как NotPetya, с использованием типа вредоносного ПО, предназначенного для удаления или уничтожения данных в целевой системе. Как только очиститель заражает компьютер, он может быстро и необратимо удалить файлы, перезаписать данные и вообще сделать систему непригодной для использования.

По данным ESET, ни одна страна еще не подвергалась атаке такого количества видов дворников за один год.

«Цель российских хакеров в Украине — вызвать сбои, а вайперы — инструмент для достижения этой цели», — сказал Липовский.

Sandworm и другие хакерские группы с первых дней войны размещают в Украине вайперы. За день до вторжения HermeticWiper, который также связан с группой Sandworm, атаковал сотни систем как минимум в пяти украинских организациях. На следующий день вайпер «Кислотный дождь» нацелился на спутниковые модемы Viasat, которые украинское правительство якобы использовало в качестве резервного канала связи. Исследователи также связывают эту кампанию с Sandworm.

По данным SSSCIP, Sandworm использовал не менее 20 штаммов вредоносных программ с тех пор, как Россия вторглась в Украину. В этом году коллекция вредоносных программ Sandworm значительно расширилась, и теперь группа может атаковать большинство операционных систем, используемых в Украине.

По данным ESET, во время атаки Sandworm на украинскую энергетическую компанию в апреле группа предприняла безуспешную попытку нарушить подачу

электроэнергии с помощью вредоносного ПО Industroyer2 и обычных очистителей дисков для операционных систем Windows, Linux и Solaris.

Хакеры также экспериментировали с различными языками программирования и методами разрушения сети.

Группа также продолжает полагаться на ранее успешные методы, такие как использование уязвимостей в групповой политике Active Directory — функции Microsoft Windows, которая позволяет администраторам настраивать параметры для пользователей и компьютеров в организации. Внедрив свой собственный вредоносный код в законные файлы, используемые этой функцией, они могут получить доступ к сети и перемещаться в боковом направлении для потенциального доступа к конфиденциальной информации или системам.

И тем не менее, большинство вайперов, обнаруженных во время войны в Украине, были «относительно простыми и плохо разработанными», без возможности автоматической репликации или бокового перемещения, что позволяло хакерам скомпрометировать другие части системы после получения первоначального доступа.

По словам Черепанова, пока новые атаки группировки не оправдали опасений, вызванных их предыдущей активностью в киберпространстве Украины. «Воздействие, вызванное атаками, могло быть намного хуже», — сказал он. «Украинские защитники очень хорошо работают над предотвращением этих атак на всех этапах».

Неудачные попытки

Предыдущие атаки Sandworm оказали глубокое влияние на индустрию кибербезопасности Украины. По данным SSSCIP, до первоначальных атак многие украинские организации не были готовы противостоять кибератакам любого масштаба, поэтому в ответ им пришлось усилить свою защиту.

Когда началась война, Украина и ее партнеры ожидали, что Sandworm и другие группировки попытаются повторить успешные атаки на украинские электростанции, чтобы погрузить города во тьму.

Однако в конечном итоге России было проще и эффективнее нанести ущерб энергосистеме Украины с помощью обычного оружия. По сообщениям, к ноябрю прошлого года Россия уничтожила 40 % энергосистемы Украины с помощью беспилотников и ракет, что привело к массовым отключениям электроэнергии по всей стране.

Украинское правительство заявило, что смогло отразить «самую масштабную» кибератаку Sandworm — апрельскую атаку на электрические подстанции страны с помощью Industroyer2, новой версии вредоносного ПО, впервые обнаруженного во время атаки группы на украинскую электросеть в 2016 году, которая покинула часть Киева. без электричества в течение часа.

ESET назвала первую атаку Industroyer «самой большой угрозой для промышленных систем управления со времен Stuxnet» — сложнейшего компьютерного червя, который, как считается, был разработан США и Израилем для борьбы с ядерной программой Ирана.

Новый вариант Industroyer имел сходство кода с исходной версией, но использовал один вместо четырех протоколов для связи с промышленным оборудованием, включая устройства, используемые для защиты систем электроснабжения от повреждений.

«Хакеры пытались адаптировать свое вредоносное ПО к новым условиям, — сказал Черепанов.

Атака должна была пройти в два этапа, но о возможном компрометации украинцы узнали за день до инцидента от неназванных «партнеров». «Нам удалось его идентифицировать, бороться с ним и уничтожить», — сказал тогда заместитель начальника ГСИН Виктор Жора.

В октябре ESET также обнаружила ранее неизвестную программу NikoWiper, связанную с Sandworm, которая использовалась против одной из компаний энергетического сектора Украины. Ни ESET, ни SSSCIP не согласились раскрыть более подробную информацию об этой атаке.

Приоритеты и цели

По данным SSSCIP, за год или два до полномасштабного вторжения Sandworm был активен, но в основном затаился. Его внимание было сосредоточено на «создании условий» для проведения будущих кибератак.

Например, хакеры проникли в украинские информационные системы и разработали инфраструктуру, которая поможет проводить будущие операции. В частности, они установили VPNFilter и Cyclops Blink — вредоносные программы, способные заражать широкий спектр маршрутизаторов и сетевых устройств.

Атаки группы направлены на продвижение целей России и адаптацию к изменяющимся потребностям разведки во время конфликта. Согласно недавнему отчету Google

Основными целями Sandworm в Украине являются государственные учреждения, предприятия энергетики, СМИ и логистики.

Но хакеры, поддерживаемые ГРУ, атакуют и союзников Украины. Они нацелились на турецкого производителя беспилотников, чьи системы использовались Украиной в первые недели войны, а в октябре Microsoft обнаружила программу-вымогатель Prestige, развернутую против логистических компаний как в Украине, так и в Польше.

Хакеры Sandworm также вносят свой вклад в информационные операции. Например, они распространяют конспирологию о западных лабораториях биологического оружия в Украине в собственном блоге Substack и через Telegram-канал, контролируемый ГРУ.

Пока неясно, координируют ли хакеры Sandworm свои кибератаки с российскими военными операциями.

Липовски из ESET сказал, что достижение этой координации может быть сложной задачей, поскольку цифровые и физические атаки различаются по своей природе: кибератаки осуществляются в несколько этапов, основаны на социальной инженерии и даже требуют некоторой удачи.

Как правило, корреляция между кибератаками и кинетическими атаками является просто вопросом времени, поскольку оба типа атак происходят постоянно, добавил он.

По данным ESET, например, атака NikoWiper произошла примерно в тот же период, когда российские вооруженные силы нанесли ракетные удары по украинской энергетической инфраструктуре.

«Это не доказывает прямую координацию, но предполагает, что у Sandworm и российских вооруженных сил одни и те же цели», — заявили исследователи». ***(Daryna Antoniuk. A year of wipers: How the Kremlin-backed Sandworm has attacked Ukraine during the war // Recorded Future News (https://therecord.media/a-year-of-wipers-how-the-kremlin-backed-sandworm-has-attacked-ukraine-during-the-war/). 04.03.2023).***

***

«Згідно з інформацією Telegram-каналу IT ARMY of Ukraine, українським хакерам вдалось здійснити DDoS-атаку на російську митницю.

Кібератака українців призвела до збоїв у системі електронного декларування та до блокування розмитнення вантажів країни-терориста. Про це розповіли і російські ЗМІ, уникаючи інформації про те, що атаку здійснили українці.

Представники системи електронного декларування товарів «Альфа-Софт» розіслали своїм клієнтам повідомлення про «потужну DDoS-атаку», яка почалася о 8:10 ранку 28 лютого і тривала декілька годин.

У той же день українські з угруповання NLB повідомили про злам найбільшого російського банку – Сбербанку. «Ми зламали Сбер і його проекти та готові поділитися з вами даними його клієнтів і співробітників», – написали представники NLB на своєму Telegram-каналі.

Як розповіли хакери, їм вдалось вивантажити безліч баз із сервісів, що входять в екосистему Сбербанку, а також внутрішні чати розробників. «Для початку надамо вам дані клієнтів і співробітників СберЛогістики», – написали NLB, прикріпивши посилання на файл…». ***(Українські хакери атакували систему***

російської митниці // No worries! (https://noworries.news/ukrayinski-hakery-atakuvaly-systemu-rosijskoyi-mytnyczi/#). 02.03.2023).

***

«Активісти українського ІТ-угруповування «Кібер Спротив» оголосили про «глобальний злам даних «уповноваженої при президенті рф з прав дитини» Марії Львової-Бєлової. Згідно з дослідженнями Conflict Observatory (американської неурядової організації, яка аналізує та оприлюднює докази російських воєнних злочинів та інших звірств під час повномасштабного вторгнення в Україну у 2022 році), чиновниця займає провідну роль в організації викрадення та «перевиховання» дітей з України.

На підтвердження зламу хактивісти виклали скани паспортів самої Марії Львової-Бєлової, її чоловіка та найближчого оточення. Також у розпорядженні програмістів, з'явилось численне листування, інформація про бізнес-інтереси Львової-Бєлової та інші приватні дані, які планують використати як важелі тиску на злочинницю.

«Маємо новий експонат в музеї – марія львова-бєлова», – зазначили у телеграм-каналі «Кібер Спротиву». – «Жінка творить геноцид цілого покоління українців, адже краде наших дітей. Ну, а ми крадемо її дані, які допоможуть притягнути окупантку до відповідальності та повернути дітей в Україну».

Батько російської чиновниці, Алєксєй Львов-Бєлов, заслужений діяч культури рф, високо відзначив роботу українських кіберактивістів і написав гнівний пост в російській соцмережі «ВКонтакте».

Щоправда, дуже швидко пост прибрали, а сторінка Львова-Бєлова зникла. «Ми зламали його доньку, а він зламався від перегляду російських змі», — кепкують у «Кібер Спротиві»…» ***(Хакери зламали базу даних російської чиновниці, яка викрадала українських дітей // No worries! (https://noworries.news/hakery-zlamaly-bazu-danyh-rosijskoyi-chynovnyczi-yaka-vykradala-ukrayinskyh-ditej/). 04.03.2023).***

***

«Технічні служби Inter Media Group вжили всіх необхідних заходів для ліквідації загрози зовнішнього втручання в роботу ефірних серверів. Про це у коментарі «Детектору медіа» розказали у пресслужбі групи.

У четвер, 23 лютого, відбулася кібератака на телеканал «Інтер», в етері якого ввімкнули гімн СРСР. Це сталось під час виступу в «Єдиному марафоні» секретаря РНБО Олексія Данілова. Також гімн, як повідомляли користувачі у соцмережах, звучав і на інших каналах групи: К2 та Zoom. Однак, за інформацією пресслужби медіагрупи, атака на К2 не здійснювалась.

За інформацією джерел «Детектора медіа», нібито атака сталась через те, що сервери «Інтера» мали доступ в інтернеті і через вірус на комп'ютері головного редактора випуску новин.

У пресслужбі каналу у відповідь на прохання прокоментувати цю інформацію повідомили, що необхідні заходи для ліквідації загроз вжиті і додали: «На цей момент правоохоронці проводять розслідування щодо втручання у ефір телеканалів «Інтер» та «Zoom», тому Inter Media Group не може оприлюднювати будь-яку додаткову інформацію щодо ситуації або давати більш детальні коментарі на цю тему»…». ***(Наталія Данькова. «Інтер» запевняє, що вжито всіх необхідних заходів проти хакерських атак // Інтернет-видання «Детектор медіа» (https://detector.media/rinok/article/208571/2023-03-03-inter-zapevnyaie-shcho-vzhyto-vsikh-neobkhidnykh-zakhodiv-proty-khakerskykh-atak/). 03.03.2023).***

***

«Хакери з Росії намагались здійснити кібератаку на ефір радіостанції FM «Галичина». Служба безпеки України завчасно повідомила керівництво медіа про напад. Про це написала пресслужба радіостанції.

Напередодні, 1 березня, у російських телеграм-каналах з'явилися заклики до кібернападу з посиланнями на IP-адреси стримінгових платформ та сайту радіо. За словами технічного директора FM «Галичина» Володимира Кушнірука, фахівці вчасно відреагували на дії ворога та ліквідували загрозу.

«Очевидно, що вони вирішили зламати наші засоби передачі даних або навіть мовити від нашого імені в ефірі. Технічний відділ радіостанції вжив додаткових заходів безпеки для унеможливлення такої ситуації», — сказав Володимир Кушнірук.

На радіостанції передбачають, що вороги й надалі намагатимуться захопити мовлення.

«Від початку свого існування радіостанція принципово не ротувала жодної російської пісні, а з вуст дикторів та ведучих не звучали проросійські наративи. Ми продовжимо правдиво висвітлювати події російсько-української війни і називати росіян ворогами, навіть якщо для них при цьому ми будемо кісткою в горлі. Думаємо, що ця кібератака — це тільки початок, окупанти не зупиняться у своїх спробах нашкодити ефіру FM «Галичина». Ми підвищили пильність та будемо стежити за тим, щоб вчасно відбивати кібератаки ворогів. Сайт радіостанції відновить свою роботу вже найближчим часом», — зазначила програмна директорка Юла Бєльська.

У медіа додали, що ефір радіо на FM-частоті та усіх онлайн-платформах наразі працює у звичному режимі…». ***(Валерія Буняк. Ефір радіостанції FM «Галичина» намагалися захопити російські хакери // Інтернет-видання «Детектор медіа» (https://detector.media/infospace/article/208554/2023-03-02-efir-radiostantsii-fm-galychyna-namagalysya-zakhopyty-rosiyski-khakery/). 02.03.2023).***

***

«Пророссийские хакерские группы продолжают нацеливаться на Украину, и в недавнем отчете говорится, что кибератаки на Украину за последний год утроились.

В то время как пророссийская хакерская группа KillNet планирует атаковать 18 различных организаций из Эстонии, Польши, Великобритании и Украины, хактивистская группа NoName якобы атаковала веб-сайт OGCC (Объединенной горно-химической компании), одной из крупнейших производителей титанового сырья в Украине.

Однако о предполагаемой кибератаке на OGCC известно немногое…

В прошлом киберпреступная группировка атаковала несколько проукраинских стран, чтобы продемонстрировать свою солидарность с Россией. NoName нацелен на организации, принадлежащие Украине, с июня 2022 года.

В марте NoName нацелился на европейские логистические и транспортные компании Vlantana и UAB RUSKO. Их веб-сайты были недоступны после атаки, что затруднило работу.

Коллектив хакеров также утверждал, что в декабре прошлого года атаковал итальянских военных. «Решил наказать итальянскую военную систему электронного обучения — довел до настоящего падения веб-сайт», — написал NoName в сообщении группы Telegram.

Более того, NoName также заявлял об атаках на японские организации после того, как страна ввела санкции против 48 российских граждан и 73 организаций.

Группа нацелилась на несколько японских организаций, включая Японскую нефтяную ассоциацию и Восточно-Японскую железнодорожную компанию, чтобы продемонстрировать поддержку России.

Сайт японских организаций был недоступен вскоре после кибератаки. Кроме того, группа сообщила, что активы Японии будут заморожены, а финансовые операции «ограничены»

Известно, что NoName использует фишинговые электронные письма и вредоносные программы для целевых пользователей. Они запустили DDoS-атаки на организации в датском, польском, норвежском, финском и чешском регионах.

Группа также нацелена на государственные учреждения и медиа-компании в Украине, Соединенных Штатах Америки и странах Европы.

В прошлом коллектив хакеров также рассылал письма с угрозами украинским журналистам.

Несколько пророссийских киберпреступных групп, таких как Killnet, Hive нападали на различные больницы и правительственные веб-сайты. и NoName, в прошлом

Президент США Джо Байден предсказал крупномасштабные кибератаки со стороны российских группировок в заявлении, опубликованном Белым домом в марте прошлого года, в котором говорится: «Россия может вести злонамеренную киберактивность против Соединенных Штатов».

Несколько групп предприняли кибератаки на проукраинские организации, которые подчеркивают необходимость «усилить вашу киберзащиту», как говорится в заявлении президента США.

Все внимание приковано к бюджету, который будет опубликован в этот четверг и будет отражать, как будут финансироваться усилия по обеспечению кибербезопасности». ***(Vishwa Pandagle. Ukraine Cyberattacks: Pro-Russian Group NoName Strikes Again, Targets OGCC // cyber express (https://thecyberexpress.com/ukraine-cyberattack-pro-russia-noname-ogcc/). 13.03.2023).***

***

«Російські хакери можуть готувати нову хвилю кібератак проти України, включно з загрозою застосування програм-вимагачів проти організацій, які обслуговують українські лінії постачання, йдеться в звіті Microsoft від 15 березня.

Як інформує Reuters, у звіті дослідницької та аналітичної групи технологічного гіганта з питань кібербезпеки окреслюється серія нових відкриттів про те, як російські хакери діяли під час конфлікту в Україні та що може бути далі.

«З січня 2023 року Microsoft спостерігає, як активність Росії в кібернетичних загрозах пристосовується для посилення деструктивних можливостей і можливостей збору розвідувальних даних щодо цивільних і військових активів України та її партнерів», – ідеться у звіті.

У січні президент Microsoft Бред Сміт повідомляв, що кібератаки Росії проти українських цілей послабилися, але такі атаки можуть активізуватися навесні». ***(Російські хакери готують новий кібернапад на Україну – звіт Microsoft // Радіо***

Свобода (https://www.radiosvoboda.org/a/news-microsoft-rosijski-hakery-napad-na-ukrajinu/32320069.html). 16.03.2023).

***

«Ще до того, як Росія вторглася в Україну, її хакерська атака була в розпалу.

Підозрювані російські хакери атакували українські урядові та фінансові веб-сайти за допомогою так званих розподілених атак типу «відмова в обслуговуванні», спрямованих на створення хаосу; вони бомбардували державні, некомерційні та IT-організації шкідливим програмним забезпеченням, призначеним для виведення комп'ютерів з ладу; і, в основному звинувачуючи Росію, вони зосередилися на комерційній супутниковій мережі Viasat Inc., спричинивши серйозні збої в українському зв'язку, включно з військовими частинами, на вирішальному ранньому етапі війни.

Довгоочікувана кібервійна, здавалося, нарешті почалася. Але те, що почалося з вибухом, зупинилося в чомусь менш суттєвому — постійному потоці цифрових атак, але нічого близького до повномасштабних кібер-військ, які багато хто передбачав.

Представники служби кібербезпеки, знайомі з конфліктом, кажуть, що головною причиною є те, що Україна була готова до цього – і мала значну допомогу від технологічних компаній, що базуються в США та інших країнах, щоб зміцнити свій кіберзахист.

За словами експертів з кібербезпеки, російські хакери, спонсоровані державою, знущалися над українськими мережами протягом цілого покоління, націлюючись на підприємства та електричні служби, навіть відключивши електроенергію в 2015 році та знову в 2016 році. Атака Росії на фінансовий сектор України у 2017 році з використанням зловмисного програмного забезпечення NotPetya поширилася по всьому світу та завдала збитків у 10 мільярдів доларів. Знаючи про можливу атаку, українська влада почала готуватися до російських хакерів восени 2021 року. Окрім підтримки західних урядів, таких технологічних

компаній, як Microsoft, Google та інші надали підтримку українському уряду для посилення кіберзахисту. Крім надання безкоштовного програмного забезпечення, технологічні компанії поділилися аналізом російських хакерів, допомогли уряду дослідити вразливі місця в мережах і надали розвідувальні дані про кіберзагрози.

Експерти кажуть, що ще одним сприяючим фактором є те, що президент Росії Володимир Путін очікував, що війна швидко завершиться, накинувши на Україну війська та кібератаки, що призведе до швидкого падіння уряду країни. Поряд із численними невдачами російських військових, її план використання кібероперацій як частини гібридної війни постійно не виконувався «без суттєвого сприяння просуванню військ», згідно зі звітом фірми з кібербезпеки Recorded Future від 9 лютого.

«Щоб істотно вплинути на війну такого масштабу, кібероперації повинні проводитися в такому темпі, який Росія, очевидно, могла б підтримувати щонайбільше кілька тижнів», — сказав Джон Бейтман, старший науковий співробітник Програми технологій і міжнародних відносин Фонду Карнегі. Мир, у грудневій панельній дискусії.

У електронному листі Бейтман, який у грудні опублікував аналіз російських кібероперацій в Україні, додав: «Я не вважаю російські кіберневдачі головною проблемою планування. Швидше, кіберсилам Москви не вистачило потенціалу та витривалості, необхідних для війни такого масштабу».

Щодо того, чому Росія не критикувала США та інші країни, які підтримують Україну, принаймні не значною мірою, експерти вважають, що Путін просто не хотів розпочинати нові бої, враховуючи проблеми, з якими він зіткнувся на полі бою.

Еріка Лонерган, науковий співробітник Інституту вивчення війни та миру імені Зальцмана при Колумбійському університеті, сказала, що, хоча Росія не проявляла стриманості на полі бою в Україні, «здається, вона не хоче воювати як з Україною, так і з НАТО».

«Це хороша новина, — сказала вона. «Ви можете розглядати це як успішний приклад кіберстримування». Але вона попередила, що США та їх союзники повинні розглянути, які фактори можуть змусити Росію змінити свою думку.

Хоча це не була повномасштабна кібервійна, вторгнення в Україну знаменує собою перший випадок, коли кібероперації відіграють таку помітну роль у світовому конфлікті, згідно до Google. Компанія з кібербезпеки Mandiant, яка тепер є частиною Google Cloud, відстежила більше руйнівних кібератак в Україні протягом перших чотирьох місяців 2022 року, ніж за попередні вісім років.

Руйнівні кібератаки проти України досягли свого піку в першому кварталі 2022 року і знову зросли наприкінці року, тоді як розвідувальні операції досягли піку в першому кварталі, а потім стали рівними протягом решти року, повідомляє інша компанія з кібербезпеки, CrowdStrike Holdings Inc. Так зване зловмисне програмне забезпечення, наприклад, видаляло дані та виводило з ладу уражені пристрої. «Я думаю, що на початку вторгнення було дуже важко», — сказала Сандра Джойс, віце-президент розвідки Mandiant». ***(Дмитро Сизов. Блумберг: російська кібервійна в Україні спотикається // Internetua (https://internetua.com/blumberg-rosiiska-kiberviina-v-ukrayini-spotikayetsya). 10.03.2023).***

***

«Держспецзв'язку підготувала аналітичний звіт про кіберагресію росії проти України у 2022 році Russia's Cyber Tactics: Lessons Learned 2022. У звіті фахівці відомства дослідили основні угрупування, їхню мотивацію, методи та інструменти атак.

Отримана інформація допоможе фахівцям у побудові ефективних систем захисту як в українських установах, так і в організаціях по всьому світу. Звіт буде цікавий, в першу чергу, топменеджерам органів влади України, фахівцям з інформаційної безпеки операторів критичної та критичної інформаційної інфраструктури та компаніям, які надають їм послуги, вендорам, що створюють продукти з кібербезпеки, а також партнерам України по всьому світу.

На базі проведеного дослідження Держспецзв'язку може заявити про основні тенденції російської кіберзагрози. Фахівці впевнилися, що кібератаки – це повноцінна складова війни росії проти України. Цілі, які переслідують російські хакери, збігаються з загальними цілями російської воєнної агресії. російські кіберзлочинці обирають основною мішенню цивільну інфраструктуру, а пріоритети хакерів протягом повномасштабного вторгнення змінювалися, підлаштовуючись до воєнних потреб.

Державні структури постійно залишалися ключовими цілями кібератак, але на початку вторгнення у фокусі кіберзлочинців були також медіа та телеком. російська влада очікувала швидкої перемоги та сподівалась, що за допомогою ЗМІ впливатиме на українців та лякатиме населення. Згодом увага хакерів і російської армії змістилася на енергетичний сектор.

Також одним із домінантних і ефективних методів отримання доступу до організацій-жертв був таргетований фішинг, проте у Держспецзв'язку помітили, що у другій половині 2022 року російські хакери змінили тактику – вони почали зміщувати акцент на використання технічних вразливостей установ, які надають послуги операторам критичної інформаційної інфраструктури.

Характер атак російських хакерів вказує на те, що жодна установа не може бути в безпеці. Передусім у зоні ризику знаходяться компанії, які надають послуги та сервіси операторам критичної інформаційної інфраструктури: розробники, інтернет-провайдери тощо.

Також у Держспецзв'язку говорять, що російські хакери здійснюють кібератаки у тому числі з метою помсти або спроб інформаційно-психологічного впливу – щоб переконати населення в тому, що держава не здатна їх захистити. І такі атаки часто привертають до себе увагу ЗМІ та суспільства. Проте небезпечнішими є повільні та «тихі» атаки, спрямовані на шпигунство.

Зокрема, такі атаки здійснює угрупування InvisiMole (Служба зовнішньої розвідки рф). Його учасники атакують високопосадовців, дипломатів та інших фахівців, які мають доступ до найбільш чутливої інформації. Їх складніше виявити, а тому такі атаки можуть мати критичніші наслідки». ***(Svitlana Anisimova.***

Держспецзв'язку випустила звіт про рік повномасштабної кібервійни росії проти України // Root Nation (https://root-nation.com/ua/news-ua/it-news-ua/ua-derzhspetszv-yazku-vipustila-zvit-pro-rik-povnomasshtabnoi-kiberviyni-rosii-proti-ukraini/). 08.03.2023).

***

«Війна в Україні показала, що заподіяти ворогу значних збитків за допомогою масштабних кібератак набагато складніше, ніж здається. Про це заявив директор Агентства національної безпеки США генерал Пол Накасоне в коментарі The Wall Street Journal.

За його словами, США розглядають Росію як «досвідченого гравця», який має намір здійснити проти американської держави масштабні кібератаки. В першу чергу метою росіян можуть бути ділові та урядові мережі, бази даних і системи озброєнь.

Аналогічна небезпека виходить і з боку Китаю, який також може розгорнути масштабну кібервійну проти США в разі спроби вторгнення на Тайвань. Китайські хакери, швидше за все, націляться на енергосистему, транспортну мережу і телекомунікаційні системи Америки, щоб посіяти паніку і потенційно послабити американську допомогу Тайваню.

«Набагато легше сказати, ніж зробити», — коментує такі погрози генерал Накасоне і киває в бік України.

Він зазначив, що українські та західні офіційні особи побоювалися, що в рамках повномасштабного вторгнення одним з напрямків російських ударів стане кіберпростір. Руйнівні кібератаки проти України в теорії повинні були підтримати військове вторгнення, але через рік війни не відбулося нічого, що виходило б за рамки обмежених тактичних операцій для підтримки військових дій.

За словами Накасоне, великі кібератаки вимагають синхронізації, розвідки, інструментів і можливостей для їх здійснення.

«Якщо у вас немає хоча б одного з цих елементів, то я думаю, як ми бачили в лютому і пізніше, росіянам було набагато важче діяти в цій області кіберпростору», — сказав він.

Кібератаки як поле бою у війні РФ проти України

Росія за допомогою кібератак намагається тероризувати українців, оскільки на реальному полі бою успіхи росіян вкрай обмежені і чергуються з катастрофічними поразками. Кібератаки перенаправлені з військових цілей на комерційний, енергетичний, фінансовий, телекомунікаційний та державний сектори.

Водночас стає очевидним, що значні зусилля, які агресор докладає до атак у кіберпросторі, теж не приносять значущого ефекту. Кібератаки не порушили працездатність важливих систем і не вплинули на виконання державними органами своїх функцій.

При цьому Україна вважає російські кібератаки воєнними злочинами. Вони теж стануть доказами для подальшого трибуналу в Гаазі». ***(Юрий Кобзар. Війна в Україні показала неефективність масштабних кібератак – США // UNIAN. NET (https://www.unian.ua/techno/communications/masshtabna-kiberataka-viyavilasya-slabkoyu-zbroyeyu-u-viyni-specsluzhbi-ssha-12191496.html). 24.03.2023).***

***

«У лютому 2023 року ворог вчинив 16 539 759 ворожих кібератак на державний сектор України, водночас за цей період кіберфахівці зафіксували 179 814 фішингових атак.

Про це свідчать результати моніторингу подій, що відбувались у сфері цифрових прав, проведеного ГО «Платформа прав людини» (ППЛ).

Дані щодо атак зловмисників надав Держспецзв’язку на запит ППЛ.

У відкритих джерелах експерти зафіксували повідомлення про кібератаки на п’ять сайтів:

Міністерства культури та інформаційної політики України;

Міністерства захисту довкілля та природних ресурсів України;

Миколаївського інтернет-видання «Преступности.НЕТ»;

Миколаївського інтернет-видання «NikLife»;

Суспільно-культурний українознавчий проєкт Ukraïner.

У звітному періоді кіберфахівці виявили дев’ять шахрайських схем введення українців в оману. Зокрема, кіберзловмисники знову намагались атакувати українських користувачів, застосовуючи схему з електронними листами нібито від імені органів державної влади, відомих установ та організацій. Після успішного ураження комп’ютерів зловмисники викрадають автентифікаційні дані, а також використовують інфіковані пристрої для розвідки локальної обчислювальної мережі й для подальшого розвитку атаки на інформаційно-комунікаційну систему організації.

Водночас за даними ППЛ, здійснювалися та продовжували діяти позасудові блокування вебресурсів або інформації на вебресурсах, зокрема триває блокування 854 ресурсів за ініціативи Національного центру оперативно-технічного управління мережами телекомунікацій при Держспецзв’язку.

Також зафіксовано три повідомлення про блокування платформами спільного доступу до інформації…» ***(У лютому кіберзлочинці атакували держсектор України понад 16 мільйонів разів // ZMINA (https://zmina.info/news/u-lyutomu-kiberzlochynczi-atakuvaly-derzhsektor-ukrayiny-ponad-16-miljoniv-raziv/). 21.03.2023).***

***

«Служба Держспецзв'язку України опублікувала звіт, в якому наводяться докладні дані про кібератаки на Україну з моменту початку російської агресії. У звіті перераховано кількість атак і ту шкоду, яку було завдано інфраструктурі країни, а також наводяться прогнози на 2023 рік та аналізуються їхні можливі наслідки. Фокус уважно ознайомився зі звітом, щоб пояснити основні пункти.

Що відбувалося на кіберфронті у 2022 році

Метою російських кібератак було підірвати українську інфраструктуру, дезінформувати й деморалізувати населення. Серед атакованих цілей були урядові сайти, енергетичні компанії, банки, аеропорти й залізниці. Деякі з атак призводили до серйозних наслідків, таких як відключення електрики або блокування платіжних систем.

Найбільші атаки розпочалися ще до вторгнення 24 лютого 2022 року. Вони мали виконувати диверсійні завдання. Наприклад, 14 січня минулого року було атаковано понад 70 сайтів центральних та регіональних органів влади. Через 2 дні розпочалася DDoS-атака на державні сайти і сайти багатьох банків України, що тривала понад 5 годин, 23 лютого відбулася кібератака на сайт Національного банку України. А за минулий рік СБУ, а також кіберструктури України нейтралізували 4,5 тис. хакерських атак.

Але українські експерти з кібербезпеки оперативно відновлювали роботу пошкоджених систем, запобігали новим атакам і активно контратакували російські цілі в інтернеті. Україна також отримувала допомогу від своїх західних партнерів. Вони надавали українським спеціалістам обладнання, програмне забезпечення та проводили навчання.

У звіті Держспецзв'язку зазначається, що важливу роль у цій кібервійні відіграло українське суспільство. Українці активно поширювали правдиву інформацію про ситуацію в країні через свої особисті облікові записи в соцмережах, підтримували ЗСУ та волонтерів. Отже, українська кібероборона виявилася досить сильною та гнучкою, щоб упоратися з російською кіберагресією.

Хто з хакерів воює на боці Росії

Зі 100-відсотковою точністю ніхто не може підтвердити участь будь-якого угруповання в тій чи іншій кібератаці на Україну, проте фахівці з розвідслужб називають кілька найактивніших груп хакерів, підконтрольних спецслужбам РФ.

Серед них називають Sandworm, Fancy Bear та Cozy Bear. Ці групи пов'язані з російськими спецслужбами, такими як ГРУ та ФСБ. Однак найбільш небезпечним є

угруповання Killnet, яке з'явилося в результаті розколу своєрідного хакерського «братства», про яке Фокус писав раніше у великому матеріалі про кібервійни.

Кібератаки Killnet мали серйозні наслідки для безпеки: вони порушили роботу гуманітарної місії НАТО в Туреччині та Сирії після землетрусу, атакували уряд Молдови та погрожували відключити апарати ШВЛ у лікарнях Великобританії. Кремлівські хакери з Killnet використовували різні методи кібератак, такі як перехоплення даних і DDoS, вони також «оголосили війну» спільноті Anonymous, яка атакувала російські сайти, підтримуючи Україну.

Хто з хакерів воює на боці України

Кіберагресії росіян успішно протистоїть досить широка коаліція проукраїнських угруповань хакерів. Серед них: KelvinSecurity HackingTeam, GhostSec, "Білоруські кіберпартизани", AgainstTheWest і Anonymous. Вони проводять кібератаки на російські вебресурси та системи, а також захищають українські ресурси. Ці групи також використовують різні методи кібератак, такі як фішинг, зламування паролів і поширення шкідливого ПЗ.

Наприклад, хакери з Anonymous успішно атакували сайт телеканалу «Росія 24» та показали відео із закликом до миру та солідарності з Україною. Їхнім атакам піддавалися сайти і структури ФСБ. Хакери з KelvinSecurity HackingTeam відзначилися атакою на сайт Міністерства оборони РФ і опублікували персональні дані російських військових та урядовців. Хакери GhostSec виклали документи про російську підтримку сепаратистів на Донбасі, зламавши сайт Міністерства закордонних справ РФ, а також взяли на себе відповідальність за атаку на Гусинозерську гідроелектростанцію, яка призвела до аварійного відключення.

Хакери-одинаки та анонімні угруповання зливали журналістам бази даних «Роскомнагляду», включаючи листування й дані працівників. Ukrainian Cyber Alliance отримав секретні документи про морські дрони РФ, що включають технічні подробиці. Проукраїнські хакери зламували бази "Газпрому" та передавали розвідслужбам дані про найбільші родовища газу в Росії та понад 6 тис. секретних файлів про діяльність компанії.

Прогнози щодо кібератак на системи України

Фахівці з кібербезпеки зазначають, що кібератаки з двох сторін продовжуватимуться навіть із більшою регулярністю, ніж минулого року. До того ж, на думку експертів із Microsoft, російські хакери готують нову хвилю кібератак проти України, включаючи погрози у вигляді програм-шифрувальників для організацій, які обслуговують українські лінії постачання. Аналітики кажуть, що Росія готується до нового витку атак і поєднуватиме фізичні атаки з кібернападами, як це було в лютому 2022 року.

Зокрема, російські хакери можуть атакувати українські енергетичні системи, урядові вебресурси, сервіси відеоконференцій та інші цифрові платформи. Експерти попереджають, що у зв'язку з активним розвитком інструментів ШІ хакери можуть використовувати технології Deepfake для дискредитації українських політиків та внесення сум'яття в суспільстві.

На думку експертів, особливе значення кремлівські кіберзлочинці надаватимуть атакам на логістичні центри та ланцюжки постачання озброєння для ЗСУ від союзників. Кібератак зазнають різноманітні транспортні компанії в Україні та фірми, що надають логістичні послуги.

Але й українські хакери не розслаблюються. На думку російських експертів з ІТ-безпеки, Росію цього року атакуватимуть утричі частіше, ніж роком раніше…» ***(Пилип Бойко. Війни хакерів: хто за Україну, а хто за Росію? // ТОВ «ФОКУС МЕДІА» (https://focus.ua/uk/digital/555653-russkie-hakery-budut-snova-atakovat-pod-pricelom-postavki-vooruzheniy-dlya-vsu). 17.03.2023).***

***

Боротьба з кіберзлочинністю в Україні

«Служби поліції Німеччини та України провели спільну операцію проти хакерів із угрупування Double-Spider, відповідальних за проведення масштабних кібератак за допомогою програми-здирника DoppelPaymer.

Deutsche Welle передає, що 28 лютого Земельне відомство з кримінальних справ (LKA) Північного Рейну – Вестфалії та Національна поліція України за підтримки Європолу, Поліції Нідерландів та Федерального бюро розслідувань (ФБР) США провели масштабну операцію у двох країнах, інформують Економічні Новини.

Як заявили на прес-конференції представники LKA, цього дня в Німеччині та Україні було проведено обшуки, вилучено докази та допитано підозрюваних. Є ордери на арешт трьох осіб, але їх поки що не вдалося затримати, оскільки вони перебувають поза досяжністю європейських органів юстиції. Повідомляється, що у кількох злочинах брали участь 41-річний росіянин та 32-річний чоловік, громадянство якого невідоме. США оголосили нагороду у розмірі 5 млн. доларів за допомогу в затриманні росіянина, повідомили в LKA.

Крім того, видано ордер на арешт громадянки РФ, яка, ймовірно, працювала адміністратором злочинної мережі Double-Spider.

У свою чергу Європол повідомив про включення до списку людей, які особливо розшукуються в Європі, на запит Німеччини двох росіян – 31-річного Ігоря Гаршина і 41-річного Ігоря Турашова. За даними відомства, обидва можуть проживати у Йошкар-Олі. Як зазначається у картці Гаршина на сайті Європолу, він брав активну участь у кібератаках на німецькі компанії, займався стеженням, проникненням у системи та шифруванням даних постраждалих фірм. У свою чергу, Турашев був адміністратором мережі, що здійснювала атаки, і є ключовим підозрюваним у кібератаках на німецькі компанії, зазначається на сайті Європолу». ***(Німеччина та Україна провели спільну операцію проти кіберзлочинців // Экономические новости (https://enovosty.com/uk/news-ukr/news_technology-ukr/full/0603-nimechchina-ta-ukraina-proveli-spilnu-operaciyu-proti-kiberzlochinciv). 06.03.2023).***

***

Потенциал кибератак растет по мере расширения и изменения цифрового мира. В «эпоху пандемии» 2020-2021 годов количество атак программ-вымогателей увеличилось на 150%. Только в первой половине 2022 года было зарегистрировано в общей сложности 236,1 миллиона атак программ-вымогателей. Наиболее частыми кибератаками являются программы-вымогатели, которые захватывают и хранят важные данные бизнеса и раскрывают их только после того, как злоумышленник получит заранее определенную сумму денег. Несостоятельность традиционных методов обеспечения безопасности является существенным фактором, способствующим увеличению числа таких нападений.

Базовая кибербезопасность больше не поможет

Их неспособность адаптироваться к новым и более изощренным опасностям является единственным фактором, способствующим их краху. Текущие методы безопасности позволяют обнаружить брешь в среднем за 287 дней. Это дает взлому более чем достаточно времени, чтобы добиться успеха несколько раз. «Время ожидания» между «скрытными» нападениями и вторжениями выросло на 36% в 2022 году, что обеспечило небольшое окно для обнаружения и пресечения вторжений. Еще одна важная вещь, о которой следует помнить, это то, что современные киберпреступники пытаются скрыть свои следы, стирая свои журналы, чтобы их нельзя было найти. Необходимо внедрить новую стратегию для защиты онлайн-среды. Однако крайне важно точно определить опасность для сетевой безопасности, которую прозвали «темным пространством».

Темным пространством можно назвать любую сетевую инфраструктуру, которая не указана в «золотом хранилище» конфигурационных данных. Брандмауэры, маршрутизаторы, прокси, балансировщики нагрузки, конечные точки и хосты — все это часть этих данных. Возможно, более поразительным является тот факт, что 70% сетей — это темное пространство. Шифрование традиционно использовалось, чтобы скрыть конфиденциальные данные и затруднить кражу данных. В настоящее время киберпреступники скрывают свои

операции, используя зашифрованные технологии. На самом деле 91,5% вредоносных программ проходят через зашифрованные сети.

Насколько уверены ИТ-эксперты в выявлении зашифрованных кибератак?

59% из них признались, что не знают обо всех коммуникациях между устройствами в своей сети. Они также заявили, что им не хватает инструментов, необходимых для выявления, перехвата и оценки угроз, что затрудняет работу с зашифрованными сообщениями. К сожалению, они не одиноки в этом, поскольку 79% предприятий не могут найти опасности, скрытые в зашифрованных данных. Они не уверены, что полностью понимают, как выявлять и предотвращать цифровые атаки.

Платформы сетевого обнаружения и реагирования (NDR) — это технология кибербезопасности будущего. Отчет о недоставке выявляет необычную сетевую активность, чтобы техническая группа могла быстрее реагировать на скрытые угрозы. Ничего не расшифровывая, это программное обеспечение исследует зашифрованный трафик, чтобы найти вредоносное ПО во время защищенных сетевых подключений. Кроме того, он следит за движением всего сетевого трафика и ищет внешние угрозы. Кроме того, отчет о недоставке может связать любую вредоносную активность с определенным IP-адресом, что позволяет найти злоумышленников, даже если они удалят журналы. Наконец, отчет о недоставке предлагает немедленные уведомления для ускорения реакции на события.

В заключении

Однако это всего лишь базовый отчет о недоставке. Платформа NDR, которая будет поддерживаться искусственным интеллектом, будет находиться в разработке, чтобы перемещаться в темном пространстве с большим интеллектом и адаптивностью. Названный ThreatEye, он использует платформу NDR для создания отпечатков всех моделей активов и поведения и следит за необычной активностью». ***(Brian Wallace. NDR: The Next Generation of Cyber Security // iEntry Network (https://www.webpronews.com/ndr-cybersecurity/). 03.03.2023).***

***

«Начало пандемии COVID-19 и последующий рост удаленной работы вынудили ИТ-команды внедрить более надежные системы безопасности для устройств в разных местах. 41% директоров по информационной безопасности (CISO) сообщили, что трансформация и гибридные ИТ были самым сложным аспектом с начала пандемии.

Только в США, по сообщениям IBM, утечки данных обходятся компаниям в среднем в 9,4 миллиона долларов. Это изменение рабочей среды напомнило специалистам по кибербезопасности, что недостаточно просто сосредоточиться на защите: в уравнение также необходимо учитывать то, насколько быстро они могут восстановиться после кибератаки.

Кибербезопасность и киберустойчивость не исключают друг друга, а скорее дополняют друг друга. Кибербезопасность сосредоточена на защите от компьютерных хакеров, а компании обеспечивают киберустойчивость за счет дисциплины и небольших, но постоянных действий, которые минимизируют ущерб от кибератак. Оба одинаково важны в борьбе с киберпреступниками.

Но как вы можете стать более устойчивыми после того, как защитите свои системы?

Маленькие шаги: большое влияние

Киберустойчивая компания создает культуру безопасности систем и данных. Все в организации, даже за пределами ИТ-отдела, должны осознавать свои повседневные действия, чтобы обеспечить устойчивость. Это клише, но когда дело доходит до кибербезопасности, вы настолько сильны, насколько ваше самое слабое звено. И человеческий фактор является причиной почти всех уязвимостей кибербезопасности. Даже если вы предоставляете персоналу правильное программное обеспечение, необходима достаточная подготовка.

Выполните два небольших шага: обновите программное обеспечение и запустите резервное копирование данных. Это может звучать так, как будто обычный системный инженер говорит о священных обновлениях, но в этом есть смысл. 54% кибератак произошли на внешние приложения, такие как Microsoft Exchange, которые сообщили об уязвимостях и новых исправлениях в своем

последнем обновлении. Здесь люди из каждого отдела должны запускать эти обновления всякий раз, когда программа предложит им это сделать.

Автономные резервные копии данных также защитят ваши активы в случае повреждения файлов или дешифрования от атак программ-вымогателей. Следуя правилам и регулярно планируя резервное копирование данных, вы обеспечите бесперебойную работу вашей компании, несмотря на кибератаки.

Быстрые планы действий

Принятие менталитета «когда» вместо «если», как это делают 83% компаний в отчете IBM, имеет решающее значение. Это позволит вам вместе с ИТ-командой составить план немедленных действий после атаки. Ваш план должен сводиться к трем ключевым действиям: определение важных контактов на случай чрезвычайной ситуации, установление безопасного канала связи с этими контактами и информирование компании о чрезвычайной ситуации.

В ваш список контактов должны быть включены заинтересованные стороны, на которых может повлиять атака: поставщики программного обеспечения, партнеры, банки и службы реагирования на инциденты (компании, которые специализируются на таких ситуациях).

То, как вы сообщаете о нападении, также имеет первостепенное значение. Убедитесь, что вы настроили каналы, такие как определенные платформы чата, которые не связаны напрямую с ежедневным общением, чтобы минимизировать риск компрометации этой службы. Немедленно сообщите об этом нарушении остальным сотрудникам компании, независимо от того, являются ли они отделами, не относящимися к ИТ. Все должны быть в курсе таких ситуаций, чтобы избежать дезинформации и повысить активность вашего плана действий.

Кроме того, чтобы сохранить доверие потребителей и сократить финансовые потери, необходимо обеспечить, чтобы ключевые операции компании могли продолжаться даже в случае перерыва. Это может включать внедрение мер по резервному копированию и восстановлению, включая резервное копирование данных и стратегии аварийного восстановления.

Важность обучения кибербезопасности

Удивительно, но только 42% компаний привлекают своих сотрудников к обучению по вопросам кибербезопасности. Это число относительно мало по сравнению с большим количеством поверхностей атак, за которые отвечают сотрудники всех отделов. Обучение вашего персонала выявлению скомпрометированной системы, попытки фишинга и других потенциальных угроз имеет решающее значение для того, будут ли ваши операции продолжать обслуживать клиентов или нет.

Сотрудники с меньшей вероятностью станут жертвами ловушек, если они обучены распознавать типичные нападения и избегать общих угроз безопасности. Уроки по кибербезопасности также дадут сотрудникам четкое представление о стратегии безопасности данных компании, что позволит им быстро и решительно реагировать в случае возникновения чрезвычайных ситуаций. Организация будет лучше подготовлена к предотвращению кибератак, смягчению их последствий и быстрому реагированию на них, предлагая это важное обучение, повышая общую киберустойчивость предприятия.

Периодические тренинги по кибербезопасности будут информировать вашу компанию о новых модальностях кибератак и о том, как с ними справляться. Например, внезапное замедление работы компьютера может означать ошибку в системе. Если сотрудник замечает это, он может сообщить своей ИТ-группе, чтобы она проверила ситуацию и обнаружила проблему до того, как она разрастется как снежный ком.

Предприятия могут повысить доверие и уверенность потребителей, обеспечить непрерывность работы компании в случае киберкризиса и повысить общую производительность и эффективность, приняв меры киберустойчивости». ***(Taylor Hersom. Why You Should Give Cyber-Resilience a Starring Role in Your Company's Cybersecurity // THE FAST MODE (https://www.thefastmode.com/expert-opinion/30890-why-you-should-give-cyber-resilience-a-starring-role-in-your-company-s-cybersecurity). 03.03.2023).***

***

«Жизненный цикл инцидента безопасности данных начинается и заканчивается подготовкой.

К сожалению, не существует такой вещи, как сеть или система с «нулевыми уязвимостями». Ходят шутки об абсолютной сетевой безопасности, в том числе о том, что единственная безопасная сеть — это сеть без пользователей или без доступа. Не существует идеального кода, идеального программного обеспечения, идеального оборудования, и даже самый благонамеренный пользователь может быть подвергнут социальной инженерии. Следовательно, подготовка на всех уровнях информационной безопасности имеет решающее значение для защиты бизнеса от катастрофических атак.

По данным Национального института стандартов и технологий, существует четыре этапа инцидента, связанного с безопасностью данных: (1) подготовка до возникновения инцидента, (2) обнаружение и анализ, (3) сдерживание уничтожения и восстановление и (4) постинцидентная активность, которая по сути представляет собой шаги, предпринятые для того, чтобы, насколько это возможно, не допустить повторения подобного инцидента в будущем.

Другими словами, как на первом, так и на четвертом этапе необходимо предпринять шаги, чтобы избежать инцидента с безопасностью данных в будущем. Как бывший руководитель ФБР, отвечающий за представление и хранение данных для оперативных миссий агентства, я ежедневно задавался вопросом: насколько достаточно подготовки? Компании ежедневно сталкиваются с одним и тем же вопросом: какой уровень кибербезопасности достаточен, чтобы предотвратить или пресечь атаку на наши компьютерные системы? Я обнаружил, что лучше всего задать себе вопрос: что нужно сделать, чтобы предотвратить или пресечь наиболее вероятные атаки на наши компьютерные системы?

При подготовке к защите от сетевой атаки я обнаружил, что внешние источники опыта очень полезны. Вместо того чтобы искать ответы внутри себя, мы пригласили внешних специалистов тщательно оценить нашу позицию в области кибербезопасности, показав нам наши слабости и недостатки. Как опытные

эксперты, они смогли указать на многие области для улучшения, такие как аппаратное обеспечение, программное обеспечение, сети и обучение. По мере того как мы вносили изменения в нашу цифровую среду и режим обучения, мы также пересматривали, редактировали и составляли политики и протоколы для защиты наших данных. Затем мы проверили эти внутренние правила и руководства, участвуя в внутренних кабинетных упражнениях. Все это помогло подчеркнуть важность подготовки к защите от неизбежной кибератаки.

Многие предприятия изо всех сил пытаются определить лучшие средства подготовки к кибератакам. Некоторым предприятиям могут потребоваться упреждающие услуги технических экспертов, которые могут сканировать уязвимости, тестировать векторы вторжений, проводить кибер-обучение или разрабатывать и устанавливать новые системы, основанные на концепции безопасности как на опоре, а не как надстройке. Другим предприятиям могут потребоваться упреждающие услуги, ориентированные на новые политики и протоколы безопасности и обработки данных, а также кабинетные упражнения для руководства и персонала. Эти меры помогают предприятиям выявлять проблемы безопасности при сборе, обработке и управлении конфиденциальными данными, такими как личная информация и защищенная медицинская информация. Другие компании могут захотеть провести оценку своих внутренних систем в дополнение к политикам или протоколам, чтобы помочь им лучше подготовиться к инциденту, связанному с безопасностью данных.

Для каждого бизнеса потребность в профилактических услугах может варьироваться в зависимости от размера, отрасли, правил, уникальных рабочих процессов или целей, общих операций и других факторов. Каждый бизнес будет определять свой уровень подготовки по-разному. Профессионалы в области конфиденциальности данных и информационной безопасности знают, что, когда бизнес сомневается в достаточности своего положения в области кибербезопасности, ответ всегда должен быть адаптирован к конкретным потребностям клиента». ***(Jason Cherry. Cybersecurity: It begins and ends with preparation // Constangy, Brooks, Smith & Prophete, LLP***

(https://www.constangy.com/constangy-cyber-advisor/cybersecurity-it-begins-and-ends-with-preparation). 06.03.2023).

***

«Новое исследование Networks показало, что в среднем организации полагаются на более чем 30 инструментов для общей безопасности, и эта степень сложности приводит к снижению безопасности, а не к увеличению.

Согласно Отчету о состоянии облачной безопасности за 2023 год, более 60% организаций работают в облачной среде в течение трех и более лет, но технические сложности и обеспечение комплексной безопасности по-прежнему мешают их усилиям по миграции в облако.

Три четверти респондентов опроса Palo Alto Networks сообщили, что количество используемых ими инструментов облачной безопасности создает слепые зоны, которые влияют на их способность определять приоритеты рисков и предотвращать угрозы. Более трех четвертей заявили, что им сложно определить, какие инструменты безопасности необходимы для достижения их целей.

90 % респондентов из числа руководителей высшего звена заявили, что не могут обнаружить, локализовать и устранить киберугрозы в течение часа, и около половины признали, что большинство их сотрудников не понимают своих обязанностей по обеспечению безопасности.

Респонденты опроса Palo Alto Networks назвали основные проблемы, связанные с обеспечением комплексной безопасности, в том числе следующие:

Целостное управление безопасностью в командах

Недостаточно принять модель ответственности между поставщиками облачных услуг и пользователями; компаниям необходимо смотреть внутрь себя и устранять разрозненность, поскольку они препятствуют процессам безопасности, которые работают для разработки, эксплуатации и безопасности.

Внедрение безопасности на протяжении всего жизненного цикла облачной разработки

Внедрение правильных решений для облачной безопасности на каждом этапе процесса разработки приложения от кода до среды выполнения имеет решающее значение.

Обучение ИТ-специалистов, разработчиков и специалистов по безопасности использованию инструментов безопасности

Разработка облачных приложений требует защиты «экспоненциально большего количества облачных активов в коде, рабочих нагрузках, удостоверениях, данных и т. д., а также в нескольких средах выполнения, таких как контейнеры, бессерверные решения и платформы», — отметили в компании.

Отсутствие информации об уязвимостях безопасности в облачных ресурсах

Palo Alto Networks называет управление уязвимостями «Святым Граалем безопасности приложений». Но достижение этого означает возможность отразить масштаб, скорость и гибкость облака, по словам компании. При успешном выполнении это может наградить компании обнаружением угроз и уязвимостей практически в реальном времени.

Использование правильных инструментов

В отчете идеальное решение для облачной безопасности является масштабируемым и способным удовлетворить неотложные потребности в безопасности и дополнительные варианты использования по мере того, как компания расширяет облачные приложения и их использование.

Руководители C-Suites не уверены в безопасном развертывании облака

Отчет основан на опросе 2500 руководителей высшего звена по всему миру в ноябре и декабре 2022 года, в ходе которого отслеживался переход предприятий от локального программного обеспечения и услуг к облаку и был обнаружен в целом слабый уровень безопасности. Общей темой среди опрошенных руководителей было то, что их организациям необходимо улучшить видимость нескольких облаков, а также реагирование на инциденты и их расследование.

«Поскольку три из четырех организаций еженедельно развертывают новый или обновленный код в рабочей среде, а почти 40 % ежедневно вносят новый код, никто не может позволить себе игнорировать безопасность облачных рабочих

нагрузок, — сказал Анкур Шах, старший вице-президент Prisma Cloud, Пало. Альт Сети.

«По мере внедрения и расширения облачных технологий организациям необходимо применять платформенный подход, обеспечивающий защиту приложений от кода до облака в мультиоблачных средах».

5 ключей к лучшим в своем классе возможностям безопасности и простоте использования

Согласно опросу, основными факторами, которые компании учитывают при выборе решений безопасности для своих облачных приложений, были:

Простота использования.

Лучшие в своем классе возможности.

Возможное влияние на производительность предприятия.

Знакомство с поставщиком или инструментом.

Конкурентоспособные цены и/или стоимость.

Опрос показал, что предприятия делятся между подходом одного поставщика/инструмента безопасности и подходом нескольких поставщиков/инструментов безопасности для каждой из своих потребностей в безопасности.

Компании держат в своих колчанах слишком много стрел безопасности

Три четверти руководителей, опрошенных в Пало-Альто, заявили, что им трудно определить, какие инструменты безопасности необходимы для достижения их целей, что привело к развертыванию множества единых решений для обеспечения безопасности — из 30 с лишним инструментов безопасности, которые организации используют в среднем, от шести до десяти. посвящены облачной безопасности…

Исследование Palo Alto Networks показало, что только около 10% респондентов не смогли обнаружить, локализовать и устранить угрозы менее чем за час. Кроме того, 68% организаций не смогли даже обнаружить инцидент безопасности менее чем за час, а среди тех, кто это сделал, 69% не смогли отреагировать менее чем за час…

Рекомендации авторов исследования включают быстрое выявление аномального или подозрительного поведения, указывающего на компрометацию, и сосредоточение внимания на средствах повышения почти постоянной видимости облачных активов, отчасти за счет устранения слепых зон, вызванных отсутствием целостного подхода к развертыванию инструментов безопасности.. Авторы также предложили:

Обеспечение безопасности на всех этапах

Команды безопасности должны иметь полное представление о том, как их компания переходит от разработки к производству в облаке, чтобы найти наименее разрушительные точки внедрения инструментов безопасности.

«Начать с повышения видимости и рекомендаций по исправлению для программного обеспечения с известными уязвимостями и сканирования образов контейнеров — это отличный первый шаг к тому, чтобы получить раннюю поддержку от DevOps или команд платформы», — говорится в отчете.

Используйте методы предотвращения угроз

Тактика развертывания может активно блокировать атаки нулевого дня и сдерживать боковое движение в случае взлома. Кроме того, рассчитайте эффективные сетевые разрешения для облачных ресурсов, чтобы обеспечить лучшие практики для доступа с минимальными правами.

«По крайней мере, организациям следует подумать о применении решений по предотвращению угроз для своих критически важных приложений», — сказал Пало-Альто.

Согласуйте кибер-тактику с присутствием в облаке

Не останавливайтесь на десятках инструментов, разрозненных для конкретных случаев использования в облаке, что приводит к тому, что Palo Alto Networks называет «расползанием» инструментов, которые тормозят команды по безопасности в облаке и оставляют пробелы в видимости. Компания предлагает пересмотреть цели внедрения облачных технологий в течение двух-пяти лет.

По возможности объединяйте инструменты

Объедините данные и элементы управления безопасностью в платформенный подход, чтобы получить всестороннее представление о рисках по сравнению с детальными представлениями, предоставляемыми несколькими разрозненными инструментами.

«Объединяя инструменты, группы безопасности могут автоматизировать корреляцию и решать наиболее важные проблемы безопасности на протяжении всего жизненного цикла приложения», — отметили в компании.

Быстрое действие при возникновении инцидента зависит от сильной политики

Инциденты безопасности на компьютерах и других устройствах, в сетях, приложениях и платформах облачных сервисов требуют быстрого реагирования. Чем раньше вы сообщаете ИТ-специалистам и соответствующим группам безопасности, тем лучше при получении подозрительных сообщений, обнаружении необычных изменений в производительности системы или устройства, обнаружении неверной ссылки или любой другой предполагаемой атаке или проникновении. TechRepublic Premium Загрузите Политику реагирования на инциденты безопасности, чтобы узнать о передовых методах реагирования на инциденты». ***(Karl Greenberg. Cloud security, hampered by proliferation of tools, has a "forest for trees" problem // TechnologyAdvice (https://www.techrepublic.com/article/cloud-security-tools-trees-problem/). 10.03.2023).***

***

«…Несмотря на растущую потребность в достижениях в области кибербезопасности, во всем мире по-прежнему не хватает 3,4 миллиона работников в этой области. Поскольку 64% компаний во всем мире испытали хотя бы одну форму кибератаки, ландшафт угроз постоянно расширяется, и те, кто работает над борьбой с этими угрозами, никогда не были так важны. Наши специалисты по кибербезопасности — незамеченные герои нашего поколения,

заслуживающие большего признания, и чтобы опередить угрозы в 2023 году, нам нужно их больше.

К сожалению, мы начинаем воспринимать нехватку кадров в области кибербезопасности как постоянную проблему, и это будет продолжаться, поскольку мы изо всех сил пытаемся побудить молодое поколение выбрать профессию, связанную с кибербезопасностью. Образование в области кибербезопасности имеет ключевое значение, и хотя мы видим, что все больше университетов разрабатывают курсы по кибербезопасности, они по-прежнему остаются очень незначительными по сравнению с критическими проблемами, с которыми организации сталкиваются ежедневно.

Чтобы это новое поколение было успешным, университеты должны расширять киберобразование и предоставлять реальное практическое обучение кибербезопасности, а не только теоретическую подготовку.

Разумеется, компании тоже должны взять такое образование в свои руки. В 2023 году мы должны обучить всех сотрудников тому, как предотвращать и минимизировать киберриски, поскольку это действительно лучший способ борьбы с расширяющимся ландшафтом угроз. Каждый человек в организации играет свою роль, даже если это просто повышение осведомленности о фишинговых электронных письмах или избегание небезопасных ссылок.

Подчеркните работу в области кибербезопасности как разнообразную, увлекательную

Чтобы также свести к минимуму отток сотрудников в киберпространстве, как организации, так и университеты должны подчеркивать уникальность, влияние и преимущества работы в отрасли. Например, повседневные задачи по кибербезопасности разнообразны, что позволяет разным людям получать удовольствие от этой работы.

Задачи также почти не повторяются, и сотрудники никогда не должны скучать. Роль кибербезопасности постоянно меняется из-за постоянного творчества и растущей изощренности злоумышленников, и это интригующий фактор при поиске работы. Продвижение таких желательных рабочих качеств будет иметь

решающее значение, поскольку отрасль стремится эффективно расширить свою рабочую силу для защиты от угроз.

Что еще более важно, организации должны лучше поддерживать свои киберкоманды. Наличие правильно мотивированной команды помогает сотрудникам чувствовать себя уверенными, уверенными в своих силах и воодушевленными своей карьерой. Как компании и лидеры, мы обязаны создавать безопасную среду для наших сотрудников и сообщать об этом всем, кто интересуется этой областью.

Обращение к разным людям

Создание безопасной рабочей среды способствует более открытым разговорам во время эмоционального выгорания и улучшает командную работу. На самом деле, один из самых важных ключевых показателей эффективности, который следует искать в опросах вовлеченности сотрудников, заключается в том, чувствуют ли сотрудники себя комфортно, разговаривая с руководством: это лучший способ избежать выгорания и убедиться, что сотрудники получают удовольствие от своей работы, поскольку этот увеличивающийся разрыв в талантах продолжается.

Будь то организованный, творческий или аналитический человек, кибериндустрия может понравиться самым разным людям. каждый день — важная работа Защита и реагирование на постоянно меняющиеся вопросы кибербезопасности, и эту истину необходимо подчеркивать на протяжении всей учебы и даже после нее.

Стратегическое привлечение новых кибер-специалистов и обеспечение того, чтобы кибер-команды выполняли свою работу на рабочем месте, помогут сократить дефицит кадров в области кибербезопасности и, в идеале, оттеснить злоумышленников на второй план». ***(Caroline Vignollet. The challenges of attracting cybersecurity talent and how to address them // VentureBeat (https://venturebeat.com/security/the-challenges-of-attracting-cybersecurity-talent-and-how-to-address-them/). 11.03.2023).***

***

«Владельцу малого бизнеса очень важно защитить данные и системы вашей компании от киберугроз. В условиях растущей зависимости от технологий и Интернета для общения и ведения бизнеса как никогда важно иметь надежный план кибербезопасности.

Вот несколько шагов, которые вы можете выполнить, чтобы создать план кибербезопасности для вашего малого бизнеса:

Определите свои активы

Первым шагом в создании плана кибербезопасности является определение активов, которые необходимо защитить. Эти активы могут включать данные, сети и системы вашей компании, а также любые устройства, которые подключаются к вашей сети. Важно понимать, что нужно защищать, чтобы вы могли расставить приоритеты в своих мерах безопасности.

Оцените свои уязвимые места

После того, как вы определили свои активы, следующим шагом будет оценка ваших уязвимостей. Это означает анализ того, как ваши активы могут быть скомпрометированы киберугрозами. Некоторые распространенные уязвимости включают слабые пароли, незащищенные сети и устаревшее программное обеспечение. Выявив эти уязвимости, вы можете предпринять шаги для защиты своих активов и снизить риск нарушения кибербезопасности.

Внедрить меры безопасности

Следующим шагом после определения ваших активов и уязвимостей является внедрение мер безопасности для защиты данных и систем вашей компании. Некоторые основные меры безопасности, которые вы должны учитывать, включают:

Использование надежных паролей. Очень важно использовать надежные уникальные пароли для всех ваших учетных записей и устройств. Избегайте использования легко угадываемых паролей, таких как «пароль» или «123456», и рассмотрите возможность использования диспетчера паролей для создания и хранения безопасных паролей.

Установка антивирусного программного обеспечения. Антивирусное программное обеспечение может помочь защитить ваши системы и устройства от вредоносных программ и других киберугроз. Обязательно обновляйте антивирусное программное обеспечение, чтобы оно эффективно защищало ваши системы.

Защита вашей сети. Чтобы защитить данные и системы вашей компании, вы должны защитить свою сеть с помощью брандмауэров и других мер безопасности. Это может помочь предотвратить несанкционированный доступ к вашей сети и снизить риск кибератаки.

Включение двухфакторной аутентификации. Двухфакторная аутентификация (2FA) добавляет дополнительный уровень безопасности вашим учетным записям, требуя второй формы аутентификации, например кода, отправленного на ваш телефон, перед входом в систему. Включение 2FA может помочь предотвратить несанкционированный доступ к вашим учетным записям.

Создайте план реагирования:

Несмотря на все ваши усилия, ваша компания все еще может столкнуться с нарушением кибербезопасности. Вот почему так важно иметь план реагирования, чтобы свести к минимуму последствия взлома и восстановить работоспособность вашего бизнеса как можно быстрее. Ваш план реагирования должен включать шаги по выявлению нарушения, сдерживанию ущерба и восстановлению после атаки.

Обучите своих сотрудников:

Ваши сотрудники — это первая линия защиты от киберугроз, поэтому важно научить их тому, как защитить данные и системы вашей компании. Это может включать обучение созданию надежных паролей, распознаванию фишинговых атак и выявлению подозрительных действий. Обучая своих сотрудников, вы можете помочь предотвратить нарушения кибербезопасности и обеспечить безопасность данных и систем вашей компании.

Используйте безопасное облачное хранилище:

В дополнение к традиционным мерам безопасности также важно использовать безопасное облачное хранилище для защиты данных вашей

компании. Облачное хранилище позволяет вам хранить и получать доступ к своим данным из любого места, где есть подключение к Интернету, но важно выбрать поставщика, который предлагает надежные меры безопасности. Ищите поставщика, который шифрует ваши данные, предлагает двухфакторную аутентификацию и имеет проверенную репутацию в области безопасности…» ***(How to Create a Cybersecurity Plan for Your Small Business // Cryptopolitan (https://www.cryptopolitan.com/how-to-create-a-cybersecurity-plan-for-your-small-business/). 10.03.2023).***

***

«Опрос, проведенный компанией-разработчиком программного обеспечения Ivanti, показывает, что сочетание работы на дому и в офисе повышает уязвимость ИТ-сетей государственных учреждений к кибератакам.

В отчете Ivanti о состоянии кибербезопасности правительства, который был опубликован в четверг, подчеркивается, что риски технической безопасности растут отчасти из-за отношения государственных служащих «не к моей работе».

Среди более чем 800 государственных служащих, участвовавших в исследовании, 70 процентов заявили, что они работали практически некоторое время. Результаты показали, что 5% респондентов не смогли распознать фишинговые атаки, а 36% не сообщали о таких электронных письмах, если они получали их на работе.

Опрос также отметил отсутствие беспокойства среди сотрудников, когда речь заходит об онлайн-безопасности агентств. 34% заявили, что не думают, что их действия повлияют на информационную безопасность правительства, а 21% признали, что им все равно, взломают ли их офис…» ***(Jamie Bennet. Ivanti Cybersecurity Report Cites Risks in Hybrid Government Work Set-up // Executive Mosaic (https://executivegov.com/2023/03/ivanti-cybersecurity-report-cites-risks-in-hybrid-government-work-set-up/). 13.03.2023).***

***

«Согласно последним данным CyberSeek, несмотря на недавние громкие увольнения в технологической отрасли, спрос на специалистов по кибербезопасности остается высоким.

Согласно новым данным с сайта Cybersecurity Workforce Analytics, разработанного в сотрудничестве с Национальной инициативой NIST по образованию в области кибербезопасности, CompTIA и Lightcast, общее количество занятых в сфере кибербезопасности в 2022 году остается довольно стабильным и составляет около 1,1 миллиона человек, в то время как количество онлайн-работ количество сообщений немного снизилось до 755 743 с 769 736 за 12 месяцев до декабря 2022 года.

«Несмотря на опасения по поводу замедления экономики, спрос на специалистов по кибербезопасности остается исторически высоким. Компании знают, что киберпреступность не остановится во время экономического спада, поэтому работодатели не могут позволить себе отложить набор сотрудников в области кибербезопасности», — сказал Уилл Маркоу, вице-президент Lightcast., Прикладные исследования-талант.

Спрос устанавливал рекорды на протяжении большей части 2022 года

Согласно данным Lightcast, каждый из первых девяти месяцев 2022 года устанавливал рекорды по самому высокому месячному спросу на кибербезопасность с 2012 года, но в ноябре и декабре он снизился.

Работников по кибербезопасности по-прежнему недостаточно, чтобы удовлетворить спрос

Ключевым индикатором является соотношение числа занятых в сфере кибербезопасности в настоящее время и новых вакансий, что дает представление о масштабах нехватки работников. Соотношение спроса и предложения в настоящее время составляет 68 рабочих на 100 вакансий, что немного выше, чем в предыдущий период, когда оно составляло 65 рабочих на 100 вакансий. Исходя из этих цифр, нам нужно около 530 000 дополнительных специалистов по кибербезопасности в Соединенных Штатах, чтобы восполнить текущие пробелы в поставках.

Спрос на специалистов по кибербезопасности увеличился в государственном и частном секторах

В период с 2021 по 2022 год спрос на кибербезопасность в государственном секторе вырос на 25% до 45 708 вакансий, а спрос в частном секторе вырос на 21% до 710 035 вакансий. Данные Lightcast показывают еще большее несоответствие в темпах роста при сравнении роста с 2019 года. За последние три года спрос на кибербезопасность в частном секторе увеличился на 36%, а отраслевой спрос на аудиторию увеличился на 58%.

Только на район Вашингтона, округ Колумбия, приходилось 19% (8 686) всего национального спроса на кибербезопасность государственного сектора в 2022 году. Ожидается, что району округа Колумбия потребуется 52 634 новых сотрудника по кибербезопасности, чтобы восполнить текущий дефицит предложения.

«Полезной функцией CyberSeek является разграничение данных государственного сектора для федерального правительства и правительств штатов и данных частного сектора, которые далее сегментируются по секторам экономики», — сказал Родни Петерсен, директор Национальной инициативы. образования в области кибербезопасности (NICE). «Методология определения рабочих мест и нанятой рабочей силы в государственном секторе использует структуру рабочей силы NICE для кибербезопасности и соответствует требованиям федерального закона об оценке рабочей силы в области кибербезопасности 2015 года, который предписывает федеральным агентствам определять должности, требующие работы с информационными технологиями, кибербезопасность или функции, связанные с кибербезопасностью.

«Каждое новое раскрытие информации об утечке данных увеличивает острую потребность в большем количестве профессионалов в области кибербезопасности», — сказала Нэнси Хаммервик, директор по решениям CompTIA. «Разнообразие и объем карьерных возможностей в области кибербезопасности, доступных по всей стране, четко и всесторонне иллюстрирует CyberSeek. Независимо от того, являетесь ли вы опытным специалистом в области кибербезопасности,

заинтересованным в новых задачах, или тем, кто хочет начать карьеру в области кибербезопасности, CyberSeek предоставит подробную информацию о возможностях карьерного роста, заработной плате, степенях и навыках, связанных с конкретными должностями». ***(Cybersecurity jobs abound despite surge in tech layoffs, report says // RushHourTimes.com (https://rushhourtimes.com/cybersecurity-jobs-abound-despite-surge-in-tech-layoffs-report-says-2/). 14.03.2023).***

***

«…Ниже приведены некоторые ключевые идеи, противоречия и компромиссы, которые, вероятно, сформируют будущее кибербезопасности и могут помочь организации лучше подготовиться к столкновению с киберугрозами.

1. Прогресс в кибербезопасности, но доступ должен быть расширен

Государственные и частные инвестиции в технологии безопасности, а также более широкие усилия по борьбе с киберпреступностью, защите критической инфраструктуры и повышению осведомленности общественности о кибербезопасности, скорее всего, принесут ощутимую отдачу к 2030 году. Кибербезопасность будет заключаться не столько в «защите крепостей», сколько в движении к принятию текущих кибер-рисков, уделяя особое внимание повышению устойчивости и способности к восстановлению. В качестве индикаторов этой тенденции к 2030 году пароли могут быть почти устаревшими, кибербезопасность будет широко преподаваться в начальных школах, а криптовалюты будут более эффективно регулироваться. Тем не менее, несмотря на то, что инвестиции в более безопасные системы и базовую кибергигиену поднимут многих людей выше «цифровой черты бедности», прогресс, вероятно, будет неравномерно распределен между сообществами и географическими регионами.

2. Обострение кризиса доверия в Интернете

Подрыв доверия в сети может усугубиться и продолжать подрывать офлайн-отношения и институты. Достижения в области искусственного интеллекта (ИИ) и машинного обучения (МО) сделают все более трудным различение людей и машин

в сети, что может привести к тому, что многие люди переведут свою деятельность в автономный режим и даже вернутся к использованию аналоговых устройств. В мире все более изощренных синтетических носителей и кибератак на основе ИИ кибербезопасность будет заключаться не столько в защите конфиденциальности, сколько в защите целостности и происхождения информации. К сожалению, в тот момент, когда обществам больше всего необходимо объединиться для решения серьезных проблем, таких как изменение климата, недоверие может привести к отступлению от регионального и глобального сотрудничества. Нам нужно работать, чтобы избежать такого исхода.

3. Обоюдоострый меч технологий искусственного интеллекта и машинного обучения

Есть как оптимизм, так и беспокойство по поводу быстрых темпов научного прогресса и коммерческого внедрения технологий искусственного интеллекта и машинного обучения. С другой стороны, мы увидим обширные инновации в таких секторах, как медицина и транспорт, а также улучшения в области кибербезопасности. С другой стороны, ИИ также приведет к инновациям в области киберпреступности, а модели ОД могут обучаться для достижения незаконных или коварных целей. Отсутствует ясность в отношении того, как правительства, компании или сообщества будут обеспечивать безопасное и этичное создание, развертывание и мониторинг систем на основе ИИ и других технологий, а также нет четкого форума, на котором будут исходить такие рекомендации.

4. Недостатки (и ограниченные преимущества) фрагментации интернета

Тенденция к «цифровому суверенитету» и фрагментации интернета будет продолжаться, поскольку усилия по обеспечению функциональной совместимости интернета и трансграничной передачи данных будут конкурировать с усилиями правительств по установлению локального или регионального контроля над онлайн-пространствами. Это может быть возможностью для местных сообществ иметь больше возможностей для определения цифровой безопасности, но мы также можем увидеть «Дикий Запад» дезинформации, слежки и более мощных кибератак, исходящих от государств-изгоев, которые изолировали себя от глобального

Интернета. Тенденция к деглобализации может также привести к более выраженным «региональным очагам правды» с различиями в информации, определяемыми географическими или другими границами, а правительства смогут осуществлять больший контроль с помощью технологий.

5. Тяни и толкай между нормативными экспериментами и будущим конфиденциальности

К 2030 году мы будем знать, достигают ли ранние усилия по кибербезопасности в законодательстве о конфиденциальности (такие как европейский GDPR) цели своей политики, но остается неясным, будем ли мы иметь улучшенные методы управления персональными данными к 2030 году или будем жить в мире в мы отказались от современных представлений о частной жизни.

6. Метавселенная неопределенность

Участники разделились на тех, кто считает, что метавселенная (или метавселенная) не материализуется и к 2030 году будет считаться неудачным экспериментом, и тех, кто считает, что нам необходимо ускорить инновации в политике, чтобы не отставать от новых проблем конфиденциальности и безопасности, которые полностью реализованная метавселенная поставит. Однако самые антиутопические видения будущего, появившиеся на семинарах, были основаны на пассивном потребителе (то есть на жизни в метавселенной, чтобы избежать проблем в реальном мире). Противоядие от этой антиутопии и ключевой аспект будущего зависят от нашей способности научить граждан принимать критическое мышление.

7. Суверенитет и смена власти

На семинарах, проводимых в Европе, мы слышали опасения по поводу стирания границ между правительствами и частными корпорациями (например, несколько участников рассуждали о будущем, в котором крупнейшие технологические компании будут занимать места в Совете Безопасности ООН). От участников из США мы услышали больше опасений по поводу тенденции к цифровому суверенитету, проблем безопасности, с которыми сталкиваются компании при выполнении все более расходящихся нормативных требований по

всему миру, и отсутствия практической основы прав человека для определения компромиссов соответствия. Большинство согласилось с тем, что государственный сектор будет играть важную роль как в качестве покупателя, так и инвестора в технологии, а также в создании барьеров для обеспечения кибербезопасности.

Планирование будущих рисков кибербезопасности

Специалистам по безопасности крайне важно иметь целостный взгляд на развитие цифровых технологий, чтобы оставаться на шаг впереди. Согласно Глобальному отчету о перспективах кибербезопасности, организации внедряют широкий спектр новых технологий, что значительно повышает сложность защиты цифровой экосистемы и расширяет поверхность атаки для злоумышленников. Поэтому крайне важно следить за тем, как эти технологии развиваются вместе с их социальным, экономическим и политическим контекстом, чтобы принимать обоснованные бизнес-решения в отношении организационной устойчивости…» ***(7 trends that could shape the future of cybersecurity in 2030 // World Economic Forum (https://www.weforum.org/agenda/2023/03/trends-for-future-of-cybersecurity/).03.03.2023).***

***

«Кибербезопасность поднялась на первое место в корпоративных программах, поскольку предприятия продолжают бороться с киберугрозами, связанными с ростом удаленной работы и ростом онлайн-торговли, вызванными пандемией COVID-19. Согласно исследованию Gartner, 88% советов директоров рассматривают кибербезопасность как бизнес-риск, а не просто как техническую проблему для ИТ.

По прогнозам Gartner, усиление опасений по поводу кибербезопасности в сочетании с продолжающейся нехваткой специалистов по кибербезопасности также приведет к изменениям в стратегиях кибербезопасности и политике на рабочем месте в ближайшие годы, в том числе в следующем:

К 2025 году 60 % организаций будут использовать риск кибербезопасности в качестве основного фактора, определяющего проведение транзакций и деловых контактов с третьими сторонами.

К 2025 году 80% предприятий примут стратегию объединения веб-сервисов, облачных сервисов и доступа к частным приложениям с пограничной платформы сервисов безопасности одного поставщика.

К 2026 году 50% руководителей высшего звена будут иметь в трудовых договорах требования к производительности, связанные с рисками.

Ниже приведены пять тенденций в области кибербезопасности, которые предприятия должны принять во время преодоления пандемии.

Тенденции кибербезопасности

Тренд 1: Работа из любого места становится постоянной

Пандемия COVID-19 коренным образом изменила общепринятую культуру во многих организациях. Первоначальное ожидание, что люди будут работать дома несколько недель, для многих превратилось в месяц за месяцем. Некоторые организации отказались от аренды офисов и выбрали для сотрудников постоянную работу из любого места, чтобы сэкономить деньги. В других организациях рабочая сила требовала продолжать работать из любого места неполный рабочий день или полный рабочий день.

Когда разразился COVID-19, большинству организаций пришлось быстро перенести свои службы и приложения из локальной среды в облако, и эта новая архитектура с облачными ресурсами и рабочей силой, работающей из любого места, должна была быть временной. Функциональность, естественно, ценилась больше, чем безопасность, потому что главной целью было поддержание работы организаций.

Но поскольку организации вынуждены работать из любого места в долгосрочной или постоянной перспективе, группам безопасности необходимо переосмыслить «временные» меры и сделать все необходимое для обновления политик, процессов и технологий безопасности. Почти наверняка возникнут проблемы с внедрением средств контроля безопасности, обеспечением

прозрачности событий безопасности и демонстрацией соответствия требованиям безопасности.

Последний элемент перекалибровки ваших стратегий кибербезопасности для удаленной работы: не забудьте потратить некоторое время на то, чтобы члены вашей команды безопасности могли хорошо работать вместе в этой новой среде, а также взаимодействовать и общаться с другими технологиями и бизнесом. команды.

Тенденция 2: автоматизировать, автоматизировать, автоматизировать

Службы безопасности уже много лет находятся в безвыходной ситуации. Они не могут справиться со всеми угрозами, с которыми сталкивается их все более большая и сложная сеть вычислительных ресурсов. Спрос на специалистов по кибербезопасности продолжает расти, и организациям пора признать, что в ближайшее время это не исправить.

Вместо того, чтобы пытаться увеличить свои человеческие ресурсы, чтобы компенсировать недостатки инструментов и технологий, организации должны больше полагаться на автоматизацию. Технологии безопасности, использующие искусственный интеллект и машинное обучение, а также выполняющие постоянный анализ данных об отслеживаемых событиях безопасности, могут обнаруживать новые угрозы намного быстрее, чем люди. Они могут находить тонкие закономерности злонамеренной деятельности, невидимые для человека. Точно так же автоматизация безопасности может постоянно выявлять наличие новых уязвимостей программного обеспечения, ошибок конфигурации и других проблем и обеспечивать быстрое устранение каждой проблемы.

Увеличение объема автоматизации и повышение качества технологий автоматизации снижает повседневную нагрузку на дефицитных специалистов по кибербезопасности. Затем эти эксперты могут потратить свое время, сосредоточившись на более стратегических вопросах, которые могут принести большую пользу организации в долгосрочной перспективе.

Тенденция 3: Внедрение принципов нулевого доверия

Нулевое доверие — это новое название старой концепции: не думайте, что чему-либо или кому-либо следует доверять. Проверяйте надежность каждого устройства, пользователя, службы или другого объекта, прежде чем предоставлять ему доступ, и часто проверяйте надежность во время доступа, чтобы гарантировать, что объект не был скомпрометирован. Предоставьте каждому объекту доступ только к тем ресурсам, которые ему необходимы, чтобы свести к минимуму последствия любого нарушения доверия. Принципы нулевого доверия могут снизить частоту инцидентов и их серьезность.

Нулевое доверие — это принцип, а не средство обеспечения безопасности или технология. Он опирается на всю технологическую инфраструктуру, предназначенную для проверки и повторной проверки личности и состояния безопасности каждого объекта, а также для постоянного мониторинга действий, связанных с каждым объектом. Для достижения этого требуется широкое сотрудничество между архитекторами и инженерами по безопасности, системными и сетевыми администраторами, разработчиками программного обеспечения и другими специалистами в области технологий. Внедрение почти всегда представляет собой поэтапную многолетнюю работу, и поэтому возрастает давление, чтобы как можно скорее начать внедрять принципы нулевого доверия. Это тот случай, когда вы должны подчиниться давлению.

Тенденция 4: улучшить возможности реагирования

Стало до боли очевидным, что большинству организаций необходимо улучшить свои возможности реагирования. Атаки на организации с помощью программ-вымогателей превратились в реальный бизнес: злоумышленники эффективно блокируют доступ пользователей к их системам и данным, а затем требуют и получают большие суммы выкупа за восстановление доступа. В то же время эти злоумышленники совершают крупные утечки данных, собирая огромное количество конфиденциальных данных и требуя выкуп, чтобы предотвратить их публикацию или продажу.

Организации должны быть готовы реагировать на крупномасштабные инциденты с программами-вымогателями, а это означает, что специалисты по

реагированию на инциденты тесно сотрудничают не только с экспертами по безопасности, но и с системными администраторами, юрисконсультами, связями с общественностью и другими, чтобы обеспечить бесперебойное реагирование и быстрое восстановление услуг. Приготовьтесь обрабатывать требования о выкупе до того, как они будут сделаны.

Тенденция 5: Признавайте риски, связанные с цепочками поставок

Обычно мы доверяем тому, что дают нам наши поставщики и поставщики услуг. Инцидент с SolarWinds показал, насколько рискованным является доверие к нашим цепочкам поставок. В одну компанию может успешно проникнуть национальное государство, и эта компания может предоставлять скомпрометированные технологические продукты или услуги тысячам других компаний. Эти компании, в свою очередь, не только сами будут скомпрометированы, но и могут раскрыть данные своих клиентов первоначальным злоумышленникам или предоставить скомпрометированные услуги своим клиентам. То, что началось с одной внедрившейся компании, может привести к компрометации миллионов организаций и отдельных лиц.

Нет простого ответа на этот вопрос. Многие аспекты нашей стратегии и технологии безопасности нуждаются в улучшении. В настоящее время наиболее важно, чтобы организации признавали и признавали риски, связанные с нашими цепочками поставок, и требовали, чтобы мы все работали лучше. Будь то привлечение поставщиков к ответственности за плохие методы обеспечения безопасности, которые приводят к компрометации, требование большей прозрачности методов обеспечения безопасности поставщиков перед продлением контрактов или добавление требований к новым закупкам, отдельные организации могут повышать осведомленность об этих проблемах и оказывать давление на поставщиков и поставщиков услуг, чтобы они сделать лучше». ***(Karen Scarfone. What is the future of cybersecurity? // TechTarget (https://www.techtarget.com/searchsecurity/feature/What-is-the-future-of-cybersecurity). 03.2023).***

***

«Кибератаки заняли пятое место в рейтинге рисков в 2020 году и стали новой нормой в государственном и частном секторах. Эта рискованная отрасль продолжит расти в 2023 году, поскольку ожидается, что к 2025 году количество кибератак, связанных с Интернетом вещей, удвоится. Кроме того, в Отчете о глобальных рисках Всемирного экономического форума за 2020 год говорится, что уровень обнаружения (или судебного преследования) составляет всего 0,05 процента в США.

Если вы один из многих, кто управляет растущим стартапом, вы знаете, что ситуация постоянно меняется, и 2020 год принес, по меньшей мере, несколько изменений. Пандемия коснулась всех видов бизнеса — большого и малого. Во всяком случае, пандемия усилила киберпреступность из-за неопределенности в отношении удаленной работы и способов защиты вашего бизнеса.

Киберпреступность, которая включает в себя все, от кражи или растраты до взлома и уничтожения данных, выросла на 600% в результате пандемии COVID-19. Почти в каждой отрасли приходилось использовать новые решения, и это вынуждало компании быстро адаптироваться.

Как вы можете подготовить свой стартап к обеспечению безопасности данных в 2023 году и далее? В этом руководстве мы анализируем наиболее важные статистические данные, факты, цифры и тенденции в области кибербезопасности, связанные с вашим стартапом.

К 2025 году киберпреступность будет стоить компаниям во всем мире примерно 10,5 трлн долларов в год по сравнению с 3 трлн долларов в 2015 году. При темпах роста в 15 процентов в годовом исчислении Cybersecurity Ventures также сообщает, что киберпреступность представляет собой крупнейшую передачу экономического богатства в истории.

Кибератаки на все предприятия, но особенно на предприятия малого и среднего бизнеса, становятся все более частыми, целенаправленными и сложными. Согласно исследованию Accenture Cost of Cybercrime Study, 43% кибератак нацелены на малый бизнес, но только 14% готовы защищаться.

Кибератака не только нарушает нормальную работу, но и может нанести ущерб важным ИТ-активам и инфраструктуре, который невозможно восстановить без бюджета или ресурсов.

Малый бизнес изо всех сил пытается защитить себя из-за этого. Согласно отчету о состоянии кибербезопасности Института Ponemon, предприятия малого и среднего бизнеса во всем мире сообщают о недавнем опыте кибератак:

Недостаточные меры безопасности: 45 % говорят, что их процессы неэффективны для отражения атак.

Частота атак: 66% подверглись кибератакам за последние 12 месяцев.

Предыстория атак: 69% говорят, что кибератаки становятся все более целенаправленными.

К наиболее распространенным типам атак на малый бизнес относятся:

Фишинг/социальная инженерия: 57%

Скомпрометированные/украденные устройства: 33%

Кража учетных данных: 30%

Понимая цели атак и их последствия, вы как бизнес-лидер можете свести к минимуму потенциал, повысить ценность своих усилий по кибербезопасности и даже предотвратить будущие атаки.

Цена длиннохвостых кибератак

Длинные затраты на утечку данных могут растянуться на месяцы или годы и включать в себя значительные расходы, о которых компании не знают или не планируют.

Эти затраты включают потерю данных, сбои в бизнесе, потерю доходов из-за простоя системы, расходы на уведомление или даже ущерб репутации бренда. На изображении ниже мы описываем влияние, с которым может столкнуться бизнес с первого по третий год.

Кибератаки могут повлиять на организацию по-разному — от незначительных сбоев в работе до крупных финансовых потерь. Независимо от типа кибератаки, каждое последствие имеет определенную стоимость, будь то денежная или иная.

Последствия инцидента кибербезопасности все еще могут повлиять на ваш бизнес спустя недели, если не месяцы. Ниже приведены пять областей, в которых может пострадать ваш бизнес:

Финансовые потери

Потеря производительности

Ущерб репутации

Ответственность, установленная законом

Проблемы с непрерывностью бизнеса

Атаки программ-вымогателей становятся все более распространенными. В конце 2016 года бизнес становился жертвой атаки программ-вымогателей каждые 40 секунд. Ожидается, что к 2021 году этот показатель возрастет до 11 секунд, согласно отчету Cybersecurity Ventures. Эта кибератака происходит, когда вредоносное программное обеспечение используется для ограничения доступа к компьютерной системе или данным до тех пор, пока жертва не заплатит выкуп, запрошенный преступником.

Некоторые отрасли более уязвимы для кибератак, чем другие, просто из-за характера их бизнеса. В то время как любая отрасль может подвергнуться утечке данных, наибольшему риску подвержены предприятия, которые тесно связаны с повседневной жизнью людей.

Компании, хранящие конфиденциальные данные или информацию, позволяющую установить личность, часто становятся мишенью для хакеров. Типы предприятий или организаций, которые наиболее уязвимы для кибератак, включают:

Банки и финансовые учреждения: содержат информацию о кредитной карте, информацию о банковском счете и личные данные клиента или клиента.

Медицинские учреждения: репозитории медицинских карт, данных клинических исследований и записей пациентов, таких как номера социального страхования, платежная информация и страховые претензии.

Корпорации: содержит всеобъемлющие данные, такие как концепции продуктов, интеллектуальная собственность, маркетинговые стратегии, базы

данных клиентов и сотрудников, контрактные сделки, предложения клиентов и многое другое.

Высшее образование: Храните информацию о данных о зачислении, академических исследованиях, финансовых отчетах и личной информации, такой как имена, адреса и платежные данные…

Обнаружение нарушения — это когда компания или бизнес узнают о том, что инцидент произошел. По данным IBM, компании требуется 197 дней, чтобы обнаружить брешь, и до 69 дней, чтобы ее локализовать.

Компании, устранившие нарушение менее чем за 30 дней, сэкономили более 1 миллиона долларов по сравнению с теми, которые заняли более 30 дней. Медленная реакция на утечку данных может создать еще больше проблем для вашей компании. Это может привести к потере доверия клиентов, снижению производительности или крупным штрафам.

План реагирования на утечку данных — это упреждающий способ подготовиться на случай, если утечка все же произойдет. Наличие стратегии управления рисками для борьбы с такими инцидентами, как взлом, может свести к минимуму влияние на вашу компанию и прибыль. План реагирования на инциденты, например, предоставляет руководство для вашей команды на этапах обнаружения, сдерживания, расследования, исправления и восстановления.

Прогнозируется, что глобальные расходы на продукты и услуги в области кибербезопасности в совокупности превысят 1 триллион долларов США за пятилетний период с 2017 по 2021 год. Это означает рост рынка кибербезопасности на 12-15% в годовом исчислении с 2021 года…

В связи с растущими угрозами хакеров, неправильно обращающихся с вашими данными, внедрение процессов для предотвращения нарушений безопасности данных является наиболее ответственным направлением действий после наличия надлежащей профессиональной страховки от взлома данных.

Законы об утечке данных различаются в зависимости от штата, поэтому в зависимости от того, где находится ваш бизнес, необходимо учитывать разные факторы. Уведомления о нарушении, о том, что покрывается, и о штрафах будут

выглядеть по-разному в зависимости от инцидента и штата, в котором вы находитесь.

1. Сокращение передачи данных

Передача данных между рабочими и личными устройствами часто неизбежна из-за увеличения числа сотрудников, работающих удаленно. Хранение конфиденциальных данных на личных устройствах значительно повышает уязвимость к кибератакам.

2. Загрузите внимательно

Загрузка файлов из непроверенных источников может подвергнуть ваши системы и устройства угрозам безопасности. Важно загружать файлы только из источников и избегать ненужных загрузок, чтобы снизить восприимчивость вашего устройства к вредоносным программам.

3. Улучшите безопасность паролей

Надежность пароля — это первая линия защиты от различных атак. Использование строк символов, которые не имеют смысла, регулярная смена паролей, никогда не записывайте их и не делитесь ими — это важный шаг к защите ваших конфиденциальных данных.

4. Обновите программное обеспечение устройства

Поставщики программного обеспечения постоянно работают над повышением безопасности своего программного обеспечения, а регулярная установка последних обновлений сделает ваши устройства менее уязвимыми для атак.

5. Отслеживайте утечки данных

Регулярный мониторинг ваших данных и выявление существующих утечек поможет смягчить потенциальные последствия долгосрочной утечки данных. Инструменты мониторинга утечки данных активно отслеживают и предупреждают вас о подозрительной активности.

6. Разработайте план реагирования на нарушения

Утечки данных могут случиться даже с самыми осторожными и дисциплинированными компаниями. Разработка формального плана управления

потенциальными случаями утечки данных, основного плана реагирования на кибератаки и плана восстановления после кибератак поможет организациям любого размера реагировать на фактические атаки и сдерживать их потенциальный ущерб.

Понятно, что предприятия находятся под постоянной угрозой киберпреступности и должны принимать меры для защиты своих данных. Не ждите, пока не станет слишком поздно, примите меры сегодня, чтобы предотвратить утечку данных в будущем и последующие последствия. Подобно необходимости иметь надлежащее страхование кибер-ответственности, необходима адекватная защита данных». ***(Mike Mclean. 2023 Must-Know Cyber Attack Statistics and Trends // Embroker Insurance Services, LLC. (https://www.embroker.com/blog/cyber-attack-statistics/). 06.03.2023).***

***

«Кибератаки продолжают атаковать финансовый сектор. Что произойдет, если в результате атаки банк или другая важная платформа выйдет из строя, и пользователи не смогут получить доступ к своим учетным записям?

Тесная финансовая и технологическая взаимосвязь в финансовом секторе может способствовать быстрому распространению атак по всей системе, потенциально вызывая широкомасштабные сбои и потерю доверия. Кибербезопасность представляет собой явную угрозу финансовой стабильности.

Согласно недавнему опросу МВФ, проведенному в 51 стране, в странах с формирующимся рынком и развивающихся странах большинство органов финансового надзора не ввели правила кибербезопасности и не накопили ресурсов для их обеспечения.

56% центральных банков или надзорных органов не имеют национальной киберстратегии для финансового сектора.

42% не имеют специального регламента по управлению кибербезопасностью или технологическими рисками, а 68% не имеют специализированного подразделения по управлению рисками в составе своего надзорного отдела.

64% не предписывают тестирование и применение мер кибербезопасности и не дают дополнительных указаний.

54% не имеют специального режима отчетности о киберинцидентах.

48% не имеют положений о киберпреступности.

Между тем, оценка Банком международных расчетов 29 юрисдикций выявила недостатки в надзоре за инфраструктурой финансовых рынков.

Однако существуют средства защиты от этих рисков, включая подготовку и согласованные регулирующие действия. Однако это будет нелегко, и срочно необходимы всесторонние и коллективные ответы.

Распространение угроз

Точно так же, как быстрый технологический прогресс предлагает злоумышленникам более дешевые и простые в использовании инструменты, точно так же эти изменения дают финансовым учреждениям больше возможностей для их противодействия.

Тем не менее, следует ожидать большей уязвимости во все более цифровизированном мире. Количество целей увеличивается по мере того, как подключается все больше систем и устройств. Фирмы Fintech, которые в значительной степени полагаются на новые цифровые технологии, могут сделать финансовую отрасль более эффективной и инклюзивной, но при этом более уязвимой для киберрисков.

Эскалация геополитической напряженности также усилила кибератаки. Виновные и их мотивы часто неясны, а риски не ограничиваются регионами конфликта. История показывает, что распространение вредоносного вредоносного ПО может нанести глобальный ущерб. Например, атака вредоносного ПО NotPetya, которая впервые захлестнула ИТ-системы украинских организаций в 2017 году, быстро распространилась на несколько других стран и нанесла ущерб, оцениваемый более чем в 10 миллиардов долларов.

Наконец, опора на общих поставщиков услуг означает, что атаки имеют более высокую вероятность системных последствий. Концентрация рисков для широко используемых сервисов, включая облачные вычисления, управляемые сервисы безопасности и сетевых операторов, может повлиять на целые секторы. Потери могут быть высокими и стать макрокритическими.

В то время как финансовые компании и регулирующие органы все больше осознают атаки и готовятся к ним, пробелы в пруденциальной системе остаются существенными.

Нейтрализация угрозы

Финансовые учреждения и регулирующие органы должны подготовиться к повышенным киберугрозам и потенциальным успешным взломам, расставив приоритеты по пяти вещам:

Центральные банки, регулирующие органы и финансовые компании должны разработать стратегию кибербезопасности. Киберриск — это многоаспектная проблема, требующая надежной защиты со стороны органов власти; надежный надзор посредством регулирования и надзора; коллективные действия на рынке; и усилия по наращиванию потенциала и опыта.

Финансовые регуляторы и фирмы должны переключить свое внимание с классического планирования непрерывности бизнеса и аварийного восстановления на предоставление критически важных услуг, даже когда атаки нарушают нормальную работу. Устойчивость требует поддержки со стороны высших руководителей компаний и финансовых регуляторов, а также членов их советов директоров. Фирмы должны быть готовы к серьезным, но вероятным инцидентам, которые могут иметь системные последствия. Надзорные органы должны требовать от отрасли рассмотрения таких неблагоприятных сценариев и проверки своих планов на случай непредвиденных обстоятельств как индивидуально, так и коллективно.

Финансовые надзорные органы должны обеспечить, чтобы киберрегулирование и надзор могли эффективно способствовать устойчивости. Не существует универсального подхода, но многие элементы являются общими.

Эффективный подход к надзору уравновешивает локальную и внешнюю деятельность, выполняемую экспертами по безопасности и универсальными супервайзерами, которые обеспечивают пропорциональное регулирование.

Финансовые компании должны усилить кибергигиену, безопасные системы, а также стратегии реагирования и восстановления. Хотя многие из современных атак становятся все более изощренными и основаны на социальной инженерии, чтобы заставить жертву предоставить конфиденциальную информацию, большинство успешных атак являются результатом рутинных ошибок, таких как невозможность развертывания обновлений исправлений или неправильной настройки безопасности. В этом контексте привычные методы обеспечения безопасного обращения с критически важными данными и защиты сетей имеют большое значение.

Международное сообщество должно согласовать отчетность о киберинцидентах и эффективный обмен информацией, чтобы власти во всем мире могли эффективно справляться с инцидентами.

Сила киберзащиты зависит от самого слабого звена. С ростом взаимосвязей по всему миру ограничение риска требует международных усилий». ***(Tobias Adrian, Caio Ferreira. Mounting cyber threats mean financial firms urgently need better safeguards // thedailystar.net (https://www.thedailystar.net/business/news/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards-3265941). 08.03.2023).***

***

«Integrity360, крупнейший специалист по услугам кибербезопасности в Великобритании и Ирландии, сегодня объявил результаты опроса Twitter, чтобы получить представление о бюджетах кибербезопасности и излишних решениях в компаниях. Опрос, проведенный с 8 по 10 марта, показал, что более 30% предприятий считают, что 30% их бюджета тратится на инструменты и решения, которые не используются в полной мере.

Кроме того, почти 30% опрошенных согласны с тем, что в их техническом стеке имеется более 31-40 инструментов и решений, которые можно было бы удалить из-за дублирования и неиспользуемых функций. Тревожная цифра, когда число нарушений кибербезопасности продолжает расти, а в компаниях остаются бреши, которые могут дать путь кибер-злоумышленникам.

Ричард Форд, технический директор Integrity360, прокомментировал: «Хотя предприятия признают необходимость выделения большего бюджета на кибербезопасность, сложность заключается в том, чтобы знать, куда распределять расходы. Легко вкладывать деньги во все блестящие новые технологии и решения, представленные на рынке, но это приводит к разрозненным системам со слишком большим количеством инструментов, развернутых для конкретных целей, которые в конечном итоге остаются неуправляемыми и недоиспользуемыми».

Более того, 46% опрошенных респондентов считают, что наиболее разрушительным последствием нарушения кибербезопасности являются финансовые потери. Неудивительно, учитывая огромные финансовые последствия, которые понесли предприятия в результате инцидента с безопасностью и роста числа атак программ-вымогателей.

«Компаниям нужна стратегия кибербезопасности, обеспечивающая полную видимость их технологического стека и решений, которые у них есть, тех, которые им нужны, и тех, без которых они могут обойтись. Переизбыток решений с перекрывающимися или ненужными функциями — это катастрофа, ожидающая своего часа, истощающая бюджет и снижающая эффективность», — продолжил Форд.

«Эти результаты вызывают тревогу, особенно во время экономического спада, когда бюджеты на кибербезопасность ограничены, а риски возрастают. При этом бюджет тратится на ненужные и неиспользуемые решения. Консолидация платформ и конвергенция технологий могут быть полезным способом оптимизации расходов в дополнение к улучшению общего состояния безопасности», — добавил он…» ***(Cyber security budgets being misspent on tools and solutions not meeting***

expectations // OnDot® Media (https://itsecuritywire.com/news/cyber-security-budgets-being-misspent-on-tools-and-solutions-not-meeting-expectations/). 14.03.2023).

***

«Кибербезопасность будет по-прежнему оставаться постоянной проблемой для организаций, особенно с учетом того, что киберугрозы продолжают становиться все более интенсивными, наряду с нашей растущей зависимостью от программного обеспечения для бизнес-функций. Аналитики Gartner прогнозируют рост SaaS-сервисов на 16,8% в этом году, поскольку инфляция заставляет компании сокращать штат сотрудников. Согласно дальнейшим прогнозам, к концу 2023 года мировая индустрия SaaS будет стоить 195 миллиардов долларов.

Готовы ли вы принять на себя новые угрозы безопасности, которые совпадают с этой растущей зависимостью от технологий?

Для поддержки различных рабочих сред в разных географических точках многие организации полагаются на платформы SaaS. С платформами SaaS организации могут реализовать удаленную работу, цифровое сотрудничество или несколько полевых офисов. Хотя оцифровка ручных процессов может улучшить взаимодействие с пользователем, вероятность раскрытия данных возрастает.

Ответственность за кибербезопасность лежит исключительно на компании, которая хранит и использует данные клиентов. Пользователи доверяют своей информации компаниям и полагаются на них в создании необходимых протоколов для ее защиты. Ситуация с кибербезопасностью постоянно меняется, поэтому ваша стратегия защиты данных также должна постоянно развиваться для решения новых задач.

Часть этого заключается в том, чтобы быть в курсе самых насущных угроз вашей конфиденциальной информации. Вот пять главных проблем кибербезопасности и то, что вы можете сделать, чтобы решить их сегодня.

1. Атаки программ-вымогателей/фишинг

Программы-вымогатели и фишинг, конечно, не новые тактики, но они становятся все более распространенными и сложными. Например, хакеры взломали систему государственного подрядчика и с помощью программы-вымогателя получили контроль над данными нескольких энергетических компаний. в конце 2022 года

Целями этих атак являются компании во всех отраслях. Достаточно простой ошибки члена вашей команды, чтобы открыть заднюю дверь для киберпреступников. Это может стать невероятно дорогим — в прошлом году средняя стоимость утечки данных достигла 4,35 миллиона долларов. Лучший способ избежать этих угроз — обучить свою команду тому, как обнаруживать фальшивые электронные письма, в которых им предлагается щелкнуть ссылку или загрузить вложение.

2. Расширенные постоянные угрозы

Усовершенствованные постоянные угрозы (APT) — это сложный тип киберугроз, предназначенный для кражи конфиденциальной информации и возникающий в течение длительного периода времени. Они часто связаны с организованными преступными группировками или национальными государственными деятелями, имеющими доступ к огромному количеству ресурсов, таких как Lazarus Group в Северной Корее и Stone Panda в Китае.

От APT сложно защититься, потому что их изощренная тактика позволяет им избегать обнаружения в течение более длительных периодов времени. Чтобы снизить риски ADT, организациям следует внедрить комплексную стратегию безопасности, включающую регулярные обновления безопасности, сегментацию сети, обнаружение вторжений и обучение сотрудников.

3. Неправильная безопасность на уровне полей

Безопасность на уровне полей (FLS) настолько надежна, насколько сильны меры безопасности, используемые для контроля доступа к системе. Внутренние угрозы, такие как мошеннические сотрудники или подрядчики, потенциально могут обойти FLS и получить доступ к конфиденциальным данным.

Неправильно настроенный FLS может привести к уязвимости данных и другим уязвимостям безопасности, которые приводят к несанкционированному доступу к системным данным. Обновления и миграции в системы баз данных могут повлиять на конфигурацию FLS, что может привести к раскрытию конфиденциальных данных при неправильном управлении. Необходимо обеспечить строгий контроль за этими настройками с помощью диспетчера встреч или автоматизированного сканера, чтобы избежать создания ненужных уязвимостей в системе безопасности данных.

4. Устаревшие средства контроля доступа к системе

Контроль доступа — это ваша первая линия защиты от киберпреступников. Он позволяет отслеживать доступность к компьютерным системам, сетям и приложениям. Однако эти процессы ненадежны, если не введены обновленные меры безопасности.

Пароли являются основной точкой уязвимости. Слабые пароли легко взламываются с помощью автоматизированных инструментов и предоставляют доступ ко всем сетям, к которым подключена учетная запись. Включение надежных паролей, которые регулярно обновляются, помогает защитить вас от утечки данных.

Многофакторная проверка подлинности обеспечивает еще один уровень безопасности, даже если пароль пользователя будет скомпрометирован. Этот простой шаг может принести пользу, помогая избежать кибератаки.

5. Данные общего доступа

Данные общедоступного доступа находятся в свободном доступе для широкой публики без каких-либо ограничений или необходимости аутентификации. Этот тип данных можно получить через веб-сайты, базы данных, API или другие источники и использовать для различных целей, таких как исследования, бизнес-аналитика или разработка политики.

Однако эти данные не всегда достоверны. Это также может создавать риски кибербезопасности, такие как раскрытие конфиденциальной информации,

несанкционированный доступ или манипулирование или несанкционированное использование личных данных.

Важно ответственно и безопасно использовать общедоступные данные на платформе вашей организации. Объясните его потенциальные риски для вашей команды и включите соответствующие меры безопасности, чтобы помочь защитить конфиденциальную информацию и предотвратить несанкционированный доступ или использование…» ***(Meredith Bell. The Top Five Cybersecurity Concerns // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/03/20/the-top-five-cybersecurity-concerns/amp/). 20.03.2023).***

***

«…Реагирование на кибер-инциденты — это формализованный процесс реагирования на события, инциденты, нарушения и угрозы кибербезопасности. Хороший план реагирования на кибер-инциденты разработан специально для вашей организации и позволяет вам быстро выявлять такие инциденты, реагировать на них и минимизировать их последствия.

Путем определения конкретных групповых и индивидуальных обязанностей до инцидента сводится к минимуму путаница, которая часто сопровождает сразу после кибер-события. Сотрудники должны знать, на что обращать внимание и к кому обращаться, если они подозревают, что произошел кибер-инцидент. Первые несколько часов (и минут) после обнаружения предполагаемого инцидента могут повлиять на эффективность вашего реагирования и решить, будете ли вы подвергать себя ненужным юридическим рискам и/или сохраните привилегию доступа к важным сообщениям и материалам расследования. Поэтому мы настоятельно рекомендуем обращаться в суд как можно раньше.

Кроме того, создание четкого протокола реагирования с конкретными контрольными показателями и целями помогает сосредоточить усилия группы реагирования на инциденты. Кроме того, планы реагирования на киберинциденты должны постоянно обновляться, чтобы оставаться актуальными и полезными. После того, как кибер-инцидент был разрешен, сбор членов вашей группы

реагирования на кибер-инциденты для проведения «горячей промывки» помогает собрать ценную информацию, сделанную во время реагирования, и определить возможности для минимизации или предотвращения подобных инцидентов в будущем. Обновите свой план реагирования на кибер-инциденты, чтобы отразить эти извлеченные уроки.

Но план реагирования на кибер-инциденты полезен только тогда, когда он используется. С этой целью ваша организация не должна ждать, пока произойдет кибер-инцидент, прежде чем снять его с полки (надеюсь, не придется счищать пыль). Рассмотрите возможность проведения кабинетных учений по реагированию на кибер-инциденты или Legal Pre-Mortem, чтобы оценить реакцию вашей организации на воображаемый кибер-инцидент. Поначалу будьте проще — нет необходимости разрабатывать слишком сложные сценарии. Цель состоит в том, чтобы участники ознакомились со своими ролями и обязанностями сразу после киберинцидента, а также с тем, как они должны координировать свои усилия по реагированию как с внутренними, так и с внешними партнерами.

Информация, полученная во время кабинетных учений по реагированию на кибер-инциденты и юридических пре-мортемов, часто включает:

Отдельные лица и группы не имеют четкого представления о своих конкретных ролях, обязанностях и полномочиях.

Ключевые заинтересованные стороны исключены из Плана реагирования на киберинциденты.

Линии связи неясны — люди не знают, кому им нужно отчитываться и быть в курсе.

Кадровые изменения и реорганизация отделов не отражаются в Плане реагирования на киберинциденты.

Новые законы и требования к отчетности не включены в План реагирования на киберинциденты.

Эффективное реагирование на инциденты является обязательным для организаций в 2023 году. Компании должны стремиться развивать культуру, которая поощряет внутреннюю отчетность и понимание методов, используемых

при распространенных кибератаках, чтобы такие происшествия можно было обнаружить и устранить как можно раньше. Члены группы реагирования на инциденты (включая юристов) должны быть гибкими и осведомленными о типах конфиденциальных данных, хранящихся в организации, которые будут использоваться для расследования и диктовать требования к отчетности. Также следует уделить внимание надлежащему времени для уведомления правоохранительных органов и/или клиентов в случае отсутствия строгих нормативных требований. По сути, хорошее реагирование на инциденты зависит от ваших людей — частое обучение и отработка потенциальных сценариев могут иметь большое значение для минимизации стресса и хаоса, которые часто могут сопровождать кибер-инцидент; и помогите свести к минимуму ваши расходы и потенциальную ответственность». ***(Townsend L. Bourne. Cybersecurity Incident Response // National Law Forum, LLC (https://www.natlawreview.com/article/cybersecurity-incident-response). 22.03.2023).***

***

«Несмотря на новости о разрушительных кибератаках, которые происходят почти ежедневно, многие бизнес-лидеры до сих пор не осознают всей ценности, которую строгие меры кибербезопасности приносят их организациям, как показало новое исследование.

Об этом говорится в новом отчете Risky Rewards, опубликованном экспертами по кибербезопасности Trend Micro. В ходе опроса более 2700 лиц, принимающих бизнес-решения, в компаниях с более чем 250 сотрудниками в 26 странах было обнаружено, что около половины (51%) считают кибербезопасность «необходимыми затратами, но не является источником дохода».

В то же время примерно такой же процент — 48% — утверждает, что ценность кибербезопасности «ограничена» предотвращением атак и угроз. Почти для двух пятых (38%) кибербезопасность является барьером, а не стимулом для бизнеса…

Далее в отчете Trend Micro утверждает, что 81% обеспокоены тем, что плохая система кибербезопасности может повредить их способности закрывать новых клиентов. Фактически для 19% это уже произошло. Более того, 71% лиц, принимающих бизнес-решения, спрашивают об их позиции в области кибербезопасности на переговорах с потенциальными клиентами и поставщиками, причем 78% признают, что такие вопросы становятся все чаще.

Кибербезопасность также стала ключевым фактором для привлечения талантов. Почти три четверти (71%) заявили, что предложения удаленной и гибридной работы теперь необходимы для привлечения талантов. Для 83% текущие политики безопасности влияют на возможность удаленных сотрудников выполнять свою работу, при этом 43% говорят, что текущие политики безопасности не позволяют сотрудникам работать удаленно. Кроме того, 54% заявили, что их политика ограничивает устройства и платформы, которые сотрудники могут использовать для работы.

Наконец, две трети (64%) лиц, принимающих бизнес-решения, подтвердили, что планируют увеличить свои бюджеты на безопасность в этом году». ***(Sead Fadilpašić. Many companies still don't see the full value of cybersecurity // Future US, Inc. (https://www.techradar.com/news/many-companies-still-dont-see-the-full-value-of-cybersecurity). 22.03.2023).***

***

«Согласно индексу готовности Cisco к кибербезопасности, опубликованному сегодня, организации в развитых странах не так подготовлены к инцидентам в области кибербезопасности, как в развивающихся странах.

Страны, которые оказались наиболее зрелыми в своей общей готовности к кибербезопасности, включали страны Азиатско-Тихоокеанского региона, такие как Индонезия, где 39% организаций находятся на том, что Cisco считает «зрелой стадией» готовности к безопасности; Филиппины и Таиланд, где 27% организаций

находятся на стадии зрелости; и Индия, где 24% организаций находятся на стадии зрелости.

С другой стороны, организации в более богатых странах показали гораздо худшие результаты в опросе. Например, согласно отчету Cisco, только 5% организаций в Японии находятся на зрелой стадии готовности к кибербезопасности, в то время как 7% организаций в Южной Корее находятся на зрелой стадии.

Похожая тенденция наблюдалась в США: согласно отчету, только 13% организаций полностью готовы к устранению инцидентов кибербезопасности. Между тем, только 9% организаций в Канаде и 12% в Мексике оказались на стадии зрелости.

Технический долг вызывает отсутствие готовности к кибербезопасности

Резкая разница в готовности к кибербезопасности между развитыми и развивающимися странами, вероятно, связана с тем, что организации на развивающихся рынках начали внедрять цифровые технологии позже, чем их коллеги на развитых рынках. «Это означает, что многие из этих компаний не имеют устаревших систем, сдерживающих их, что упрощает развертывание и интеграцию решений безопасности во всей их ИТ-инфраструктуре», — говорится в отчете, добавляя, что технологический долг — предполагаемая стоимость или предполагаемое влияние обновления. системы — по-прежнему является основной причиной разрыва в готовности.

Индекс готовности Cisco к кибербезопасности классифицирует компании по четырем стадиям готовности — новичок, формирующийся, прогрессирующий и зрелый. Отчет основан на опросе 6700 лидеров кибербезопасности на 27 мировых рынках.

Опрос показал, что 47% организаций попадают в категорию формирующихся, когда они предприняли некоторые из основных шагов для своей защиты, 30% находятся на прогрессивной стадии, 8% — на начальном этапе и только 15% — на зрелом этапе.

Около 82% лидеров в области безопасности во всем мире заявили, что инциденты кибербезопасности могут нарушить их бизнес в течение следующих 12–24 месяцев.

Почти 60% руководителей служб безопасности заявили, что за последние 12 месяцев сталкивались с какими-либо инцидентами кибербезопасности. В отчете Cisco говорится, что инциденты обошлись 71% затронутых организаций не менее чем в 100 000 долларов, при этом 41% понесли общие расходы в размере 500 000 долларов и более.

«У нас есть тревожный разрыв в готовности к кибербезопасности, и он будет только увеличиваться, если глобальные лидеры бизнеса и безопасности не изменятся быстро», — говорится в отчете Cisco.

5 столпов готовности Cisco к кибербезопасности

Cisco классифицировала организации на основе пяти столпов готовности к кибербезопасности: идентификационные данные, устройства, сеть, рабочие нагрузки приложений и данные.

Управление идентификацией было признано наиболее важной областью для беспокойства. Почти трое из пяти респондентов, или 58% организаций, относились либо к формирующейся, либо к начинающей категории в области управления идентификацией. Однако в отчете говорится, что 95% из них находились как минимум на каком-то этапе развертывания с соответствующим приложением для управления идентификаторами.

Что касается защиты сети, то 56 % организаций оказались в нижней части спектра готовности. «Это указывает на то, что многие из них находятся на ранних стадиях развертывания решений, хотя хорошая новость заключается в том, что половина наших респондентов (50%) планируют завершить развертывание в течение следующих 12 месяцев», — говорится в отчете Cisco.

Почти треть организаций, или 31 %, относятся к категории готовности, и около 97% организаций развернули систему для защиты рабочих нагрузок приложений.

Что касается защиты данных, то 98% респондентов установили приложения, а 67% выбрали шифрование данных или обеспечение возможности резервного копирования и восстановления потерянных данных. Почти 94% частично или полностью развернули эти системы.

«Развертывание некоторых решений, особенно для идентификации, устройств и сетей, разворачивается не так быстро, как могло бы, что делает некоторые организации уязвимыми для атак», — говорится в отчете Cisco.

Организации увеличивают бюджеты на кибербезопасность

Хотя было обнаружено, что многие глобальные организации имеют низкий уровень готовности к кибератакам, большинство из них заявили, что планируют увеличить инвестиции в кибербезопасность в ближайшие месяцы.

В отчете говорится, что почти 86% организаций заявили, что планируют увеличить свои бюджеты на кибербезопасность как минимум на 10% в течение следующих 12 месяцев.

Большинство организаций уже думают об устойчивости своих финансовых, операционных, организационных функций и функций цепочки поставок. «Организациям нужна устойчивость к внешним воздействиям, когда безопасность является основой бизнес-стратегии и является коллективным приоритетом во всей организации, что позволяет компаниям лучше предвидеть угрозы и быстрее восстанавливаться, когда угроза становится реальной», — говорится в отчете.

Почти 53% организаций, отнесенных к категории зрелых, заявили, что они очень уверены в своей способности оставаться устойчивыми к потенциальным кибератакам в течение следующих 12-24 месяцев. Только 30% компаний на начальной стадии и 34% на стадии становления чувствовали то же самое». ***(Apurva Venkat. Developed countries lag emerging markets in cybersecurity readiness // IDG Communications, Inc. (https://www.csoonline.com/article/3691294/developed-countries-lag-emerging-markets-in-cybersecurity-readiness.html). 21.03.2023).***

***

«…Усталость от кибербезопасности относится к усталости, незаинтересованности или нежеланию сотрудников заниматься компьютерной безопасностью. Это коррелирует с повышенным риском поведения, которое ставит под угрозу безопасность компании или даже личную безопасность.

Когда сотрудников постоянно бомбардируют уведомлениями безопасности или им приходится иметь дело с большим объемом информации и процессов безопасности, они могут устать и перестать обращать внимание.

Иногда ложные представления о рисках также могут способствовать усталости от безопасности. Некоторые сотрудники, например, могут подумать, что хакеры не будут нападать на них, поскольку они не обрабатывают важные данные.

Если не проверить, усталость от кибербезопасности может привести к тому, что сотрудники будут игнорировать даже обычные методы обеспечения безопасности, основанные на поведении, чтобы оставаться в безопасности в Интернете.

Например, при усталостной атаке с многофакторной аутентификацией (MFA) сотрудник, постоянно получающий push-уведомления MFA, через некоторое время может сдаться.

Усталость от кибербезопасности представляет собой серьезный риск, поскольку может привести к утечке данных, заражению вредоносным ПО и атакам социальной инженерии. Поэтому вам необходимо заранее выявлять симптомы усталости от кибербезопасности, чтобы эффективно защитить свою ИТ-инфраструктуру.

Вот некоторые признаки усталости от безопасности, на которые следует обратить внимание.

1. После плохого управления паролями

Создание плохих паролей и их использование для нескольких учетных записей может быть признаком усталости от кибербезопасности. Но как вы можете это распознать? Такие подробности они должны держать при себе. Но в том-то и дело. Сотрудники, страдающие от усталости от безопасности, могут отправлять

пароли членам своей команды по электронной почте, текстовым сообщениям, в мессенджерах или другими незащищенными способами.

2. Небезопасный доступ к ИТ-ресурсам

Если некоторые из ваших сотрудников часто небезопасно получают доступ к ИТ-ресурсам или серверам компании, это признак усталости от кибербезопасности. Например, если они подключаются к вашему серверу, не включив свой VPN или брандмауэр, или подключаются к общедоступной сети Wi-Fi, не имея надлежащей защиты.

3. Игнорирование обновлений и программных исправлений

Своевременные обновления и исправления программного обеспечения не позволяют хакерам использовать известные уязвимости. Таким образом, ваша политика безопасности должна обеспечивать своевременное обновление используемых операционных систем и программ.

Если несколько сотрудников не хотят обновлять свои системы и программы, возможно, они устали от кибербезопасности.

4. Демонстрация рискованного поведения в сети

Открытие фишинговых сообщений электронной почты, переход по ссылкам, упомянутым в спам-сообщениях, и загрузка пиратских программ являются признаками усталости от системы безопасности.

Вам также не обязательно быть на работе, чтобы стать жертвой усталости от кибербезопасности. Если вы подключаетесь к общедоступной сети Wi-Fi без надлежащей защиты, используете свой основной адрес электронной почты для всех своих учетных записей в Интернете и открываете фишинговые электронные письма, не задумываясь, вы можете страдать от усталости от кибербезопасности.

Чем опасна усталость от кибербезопасности?

Люди — самое слабое звено в кибербезопасности. Сотрудники, страдающие от усталости от безопасности, могут нанести непоправимый ущерб вашей компании.

Если некоторые из ваших сотрудников обычно используют общедоступную сеть Wi-Fi без надлежащей защиты, они подвержены атакам злобных близнецов,

заражению вредоносным ПО, атакам Man-in-the-Middle (MitM), прослушиванию Wi-Fi и многому другому.

Плохое управление паролями представляет собой серьезную угрозу и может привести к захвату учетных записей, утечке данных и другим нарушениям безопасности. Более того, безрассудное поведение ваших сотрудников в сети может привести к установке вредоносных программ на ваши системы, заражению устройств троянами удаленного доступа, утечке данных и многим другим типам кибератак.

Как вы можете защититься от усталости от кибербезопасности?

Усталость от кибербезопасности ослабляет кибербезопасность вашей компании. Примите необходимые меры, чтобы пресечь это в зародыше.

Ниже приведены несколько эффективных способов борьбы с усталостью от безопасности в вашей компании.

Ограничьте количество решений по безопасности, которые должны принимать пользователи

Принятие множества решений в области безопасности каждый день может привести к перегрузке ваших сотрудников. В результате они чувствуют себя выгоревшими. Вы должны свести к минимуму решения, которые ваши сотрудники должны принимать ежедневно. И использование правильной техники может помочь вам в этом.

Автоматизируйте установку исправлений для программного обеспечения и операционных систем, удаленно управляйте ноутбуками и устройствами ваших сотрудников и внедряйте решения для обеспечения безопасности, способные автоматизировать реакцию на угрозы.

Кроме того, используйте хороший менеджер паролей, чтобы избавиться от усталости паролей. И позаботьтесь о том, чтобы вашим сотрудникам не приходилось иметь дело с сотнями сообщений системы безопасности, чтобы избежать усталости от предупреждений.

Упростите для пользователей принятие правильных решений по обеспечению безопасности

Сложность — враг обеспечения хорошей безопасности. Если вашим сотрудникам трудно принимать правильные решения по обеспечению безопасности, они, скорее всего, будут чувствовать себя утомленными.

Четкая политика кибербезопасности поможет сотрудникам сделать правильный выбор.

Убедитесь, что в вашей политике кибербезопасности есть четкие инструкции о том, что сотрудники должны делать при выполнении своей повседневной работы и в случае инцидента безопасности.

Проведите тренировки по безопасности

Проведение учений по безопасности — один из лучших способов оценить, насколько ваши сотрудники готовы к борьбе с кибератаками. Поэтому вам следует регулярно проводить такие мероприятия, как фишинговые тесты или учения по реагированию на инциденты. Это поможет сотрудникам сосредоточиться на защите своих систем и серверов.

Сделайте безопасность частью культуры вашей компании

Когда дело доходит до кибербезопасности, лучше быть активным, чем реагировать. Встраивание безопасности в культуру вашей компании может помочь вам создать атмосферу доверия, осведомленности и знаний, сводя к минимуму случаи усталости от кибербезопасности.

Содействие гигиене безопасности сверху вниз, постоянное информирование о важности безопасности, выделение того, что поставлено на карту, и принятие политики нулевого доверия могут помочь вам создать сильную культуру кибербезопасности.

Сделайте обучение безопасности интерактивным

Если вы сделаете свои учебные занятия по кибербезопасности более интерактивными, это повысит вовлеченность сотрудников. Следовательно, ваши сотрудники будут чувствовать себя более мотивированными для защиты ИТ-ресурсов в вашей компании.

Используйте моделирование реального мира и геймификацию на своих учебных занятиях, чтобы заинтересовать сотрудников. Учебные занятия по

вопросам безопасности должны длиться от 20 до 25 минут каждое, чтобы никого не перегружать.

Ваше обучение безопасности должно дать сотрудникам возможность выразить свое отношение к различным средствам контроля безопасности. Это поможет вам выяснить, есть ли что-то конкретное в кибербезопасности, что вызывает стресс у ваших сотрудников.

Боритесь с усталостью от кибербезопасности, чтобы оставаться в безопасности

Усталость от безопасности — это реальная вещь. Если вы не будете бороться с этим, вы можете легко стать жертвой хакеров. Вот почему вам необходимо предотвратить усталость от кибербезопасности в вашей компании.

Поскольку пароли играют решающую роль в защите учетных записей и данных, вы также должны следить за любыми признаками усталости паролей в вашей организации». ***(Sandeep Babu. What Is Cybersecurity Fatigue and How Can You Overcome It? // www.makeuseof.com (https://www.makeuseof.com/what-is-cybersecurity-fatigue/). 23.03.2023).***

***

«…В глобальном масштабе (ISC)² предполагает, что штат сотрудников в области кибербезопасности значительно расширится за счет добавления 464 000 новых специалистов в 2022 году, что означает резкое увеличение числа сотрудников на 11,1% в 2021 году.

Это, без сомнения, позитивная новость, однако рост далеко не соответствует требуемому уровню. Интересно, что нехватка кадров в области кибербезопасности увеличилась более чем в два раза по сравнению с численностью рабочей силы, увеличившись на 26,2% по сравнению с прошлым годом.

Эти цифры напоминают о том, как быстро растут требования к кибербезопасности. К сожалению, в 2023 году организациям, стремящимся привлечь и удержать специалистов по кибербезопасности, предстоит тяжелая битва.

Действительно, по оценкам (ISC)², глобальный пул профессионалов в области безопасности должен вырасти на 65%, чтобы эффективно защищать критически важные активы организаций. Напротив, по оценкам Департамента цифровых технологий, культуры, СМИ и спорта (DCMS), почти 700 000 предприятий (51%) не имеют базовых навыков.

Государственный сектор не является исключением. От школ до больниц и многих министерских ведомств между ними, центральные общественные столпы нашего общества хранят огромные объемы крайне конфиденциальных данных, таких как личная информация (PII) и секретные документы — данные, которые очень привлекательны для злоумышленников.

Вызывает тревогу (но совершенно неудивительно), что любая организация, столкнувшаяся с недостатком навыков в области кибербезопасности, гораздо более подвержена взлому. Действительно, отраслевая организация ISACA обнаружила, что 69% организаций, подвергшихся кибератакам в прошлом году, в той или иной степени или значительно недоукомплектованы персоналом.

Однако что действительно усугубляет эти опасения, так это потенциальное влияние, которое могут иметь нарушения. Согласно отчету IBM о стоимости утечки данных за 2022 год, средняя общая стоимость утечки данных в настоящее время составляет 4,35 миллиона долларов.

Эта комбинация статистических данных, несомненно, вызывает беспокойство. Однако атаки не являются безнадежным делом или неизбежностью, которую просто нельзя предотвратить. Сегодня существует множество вспомогательных технологий, которые можно использовать, чтобы помочь организациям всех форм и размеров — как государственным, так и частным — переломить ситуацию в борьбе с угрозами, с которыми они сталкиваются.

Понимание ценности автоматизации

Исследование (ISC)² показывает, что более половины (57%) организаций в настоящее время автоматизируют аспекты своей безопасности, а еще четверть (26%) намерены сделать это в ближайшем будущем. Следует отметить, что, по крайней мере, в большинстве случаев организации

делают это не для того, чтобы полностью устранить потребность в специалистах по кибербезопасности. Искусственный интеллект и близко не соответствует уровню сложности, необходимому для достижения этого в контексте безопасности. И действительно, маловероятно, что человеческий вклад когда-либо не потребуется, по крайней мере, в каком-то качестве.

Сегодня мы наблюдаем, как организации используют технологии для автоматизации повторяющихся процессов и освобождения специалистов по безопасности, позволяя им сосредоточиться на более важных задачах.

Идея сосредоточена на расширении возможностей ограниченного числа профессионалов, которые организации могут получить в свои руки с помощью наилучших возможных наборов инструментов для оптимизации их опыта и вклада. Такой подход не только позволяет профессионалам работать эффективно и результативно, но и повышает опыт сотрудников, упрощая удержание талантов и смягчая проблемы, связанные с нехваткой кадров.

Итак, как именно организациям следует автоматизировать свои процессы безопасности, чтобы уменьшить нагрузку на свои группы безопасности? Здесь мы опишем три ключевых инструмента для рассмотрения.

UEBA работает, создавая базовые параметры нормального поведения для каждого пользователя.

Во-первых, у нас есть аналитика поведения пользователей и объектов (UEBA), которая работает путем создания базовых показателей нормального поведения для каждого пользователя, группы одноранговых узлов и объекта в корпоративной сети; Затем технология автоматически идентифицирует, помечает и оценивает любые потенциально опасные действия, выходящие за рамки этих «нормальных» параметров.

В конечном итоге это помогает аналитикам выполнять большую часть тяжелой работы по поиску угроз, указывая им непосредственно на те угрозы, которые действительно требуют устранения.

Автоматический опрос событий

Успешная безопасность зависит от способности организаций понимать свои уязвимости и смягчать соответствующие угрозы. Хотя индикаторы риска бывает трудно определить, а подготовка к каждой новой угрозе невозможна, использование разнообразных данных аналитики угроз может помочь специалистам по безопасности лучше определять приоритеты угроз и соответствующим образом защищать себя. Будь то поставщики средств обеспечения безопасности, аналитические группы или другие связи, сбор информации из различных источников может помочь в упреждающем выявлении тенденций.

Конечно, ручной просмотр больших потоков данных в поисках новых угроз может показаться поиском иголки в стоге сена. Поэтому автоматизация имеет ключевое значение.

В частности, мы рекомендуем аналитикам автоматизировать опрос событий, проверяя различные признаки компрометации (IOC) в различных внутренних и внешних аналитических каналах, чтобы сопоставить ключевые индикаторы угроз.

SOAR — технология обнаружения инцидентов и реагирования на них

В-третьих, у нас есть управление безопасностью, автоматизация и реагирование (SOAR) — технология обнаружения инцидентов и реагирования, ориентированная на агрегирование предупреждений и установление приоритетов. Специально разработанное, чтобы помочь специалистам по безопасности найти последовательные и оптимальные ответы, оно ускоряет расследование и устранение угроз за счет автоматической корреляции и анализа данных.

При этом вся контекстуальная информация и аналитические данные могут быть представлены прозрачно, что позволяет службам безопасности реагировать эффективно и обоснованно. Важно отметить, что это значительно сокращает время отклика, помогая командам SOC быстро выявлять и устранять инциденты.

Использование конвергентного решения для обеспечения безопасности

Действительно, для создания эффективной, высокоавтоматизированной стратегии безопасности потребуется сочетание правильных технологий. Однако следует тщательно взвешивать степень использования решений.

Может возникнуть соблазн приобрести каждую блестящую новую технологию на рынке. Тем не менее, такой подход может фактически подорвать любые усилия по поддержке и без того ограниченных и находящихся под давлением специалистов по безопасности. Если организация настаивает на использовании 20 или 30 инструментов, специалистам по безопасности придется потратить значительное количество времени на изучение и навигацию по каждой платформе.

Точно так же приобретение широкого спектра автоматизированных решений будет дорогостоящим, и это не привлекательно и не осуществимо, учитывая текущую экономическую ситуацию, особенно для многих отделов государственного сектора, испытывающих нехватку денежных средств.

По этой причине мы рекомендуем государственным организациям использовать конвергентное решение для обеспечения безопасности, отвечающее их конкретным потребностям.

В конвергентном решении несколько инструментов объединены в единую платформу. Учитывая, что сложность ИТ-операций и операций по обеспечению безопасности часто может быть связана с интеграцией, развитием технологий и изменением масштаба, это является ключевым моментом. Действительно, использование единой платформы, включающей широкий набор функций, уменьшит сложность, стоимость и трения.

Не только это, но и производительность может также улучшиться в таких настройках. Действительно, сочетание централизованного мониторинга SIEM с автоматизацией, рабочими процессами и системой управления делами предоставит группам безопасности данные, которые они должны предоставлять прозрачно.

Точно так же общая стоимость владения становится намного яснее. Как правило, решения для конвергентной безопасности строятся на предсказуемых

моделях лицензирования, которые гарантируют, что клиенты точно знают, за что они платят.

Для организаций государственного сектора это может изменить правила игры. Конвергентная система безопасности не только аккуратно впишется в ограниченный бюджет, но и улучшит производительность, облегчив жизнь специалистам по безопасности — качества, которые никогда не были так важны, учитывая пробел в навыках, который необходимо заполнить». ***(Plugging the cybersecurity skills gap to retain security professionals // Adjacent Digital Politics Ltd (https://www.openaccessgovernment.org/plugging-cybersecurity-skills-gap-security-professionals/155418/). 23.03.2023).***

***

«…Одним из наиболее значительных преимуществ регулярных оценок кибербезопасности является возможность выявления уязвимостей в системах и сетях компании. Оценки кибербезопасности могут предоставить ценную информацию о любых слабых местах в мерах безопасности компании и помочь определить потенциальные точки входа для хакеров или киберпреступников. Выявив эти уязвимости, предприятия могут принять упреждающие меры для повышения уровня безопасности и снижения вероятности кибератаки.

Идти в ногу с растущими угрозами

Еще одна важная причина для проведения регулярных оценок кибербезопасности — быть в курсе меняющихся угроз. По мере развития технологий совершенствуются и тактики, используемые киберпреступниками. Регулярные оценки могут помочь компаниям быть в курсе новых и возникающих угроз и принимать меры для их смягчения. Идя в ногу с новыми угрозами, предприятия могут гарантировать, что их меры безопасности остаются эффективными и актуальными.

Обеспечение соответствия

Во многих отраслях соблюдение правил и стандартов имеет важное значение. Регулярные оценки кибербезопасности могут помочь компаниям убедиться, что

они соответствуют необходимым требованиям соответствия. Например, предприятия, которые обрабатывают конфиденциальную информацию о клиентах, должны соблюдать Общие правила защиты данных (GDPR) в Европейском Союзе. Проводя регулярные оценки, компании могут убедиться, что они соблюдают требования GDPR, и избежать дорогостоящих штрафов и санкций.

Снижение рисков

Риски кибербезопасности могут представлять серьезную угрозу для деятельности, репутации и финансовой стабильности компании. Регулярные оценки могут помочь предприятиям выявлять и снижать потенциальные риски до того, как они станут серьезными проблемами. Заблаговременно устраняя риски, компании могут свести к минимуму последствия любых нарушений безопасности и обеспечить непрерывность бизнеса.

Усиление мер безопасности

Регулярные оценки кибербезопасности также могут помочь предприятиям укрепить свои меры безопасности. Оценки могут дать ценную информацию о том, как работают меры безопасности компании, и определить области для улучшения. Усиливая меры безопасности, предприятия могут повысить свою устойчивость к кибератакам и снизить вероятность успешного взлома.

Укрепление доверия с клиентами

Наконец, регулярные оценки кибербезопасности могут помочь компаниям укрепить доверие своих клиентов. Клиенты все больше осознают риски кибербезопасности и ожидают, что компании будут принимать упреждающие меры для защиты своих данных. Проводя регулярные оценки и внедряя строгие меры безопасности, компании могут продемонстрировать свою приверженность защите информации о клиентах и укреплению доверия со своей аудиторией.

В заключение следует отметить, что регулярные оценки кибербезопасности имеют решающее значение для предприятий любого размера. Они могут помочь выявлять уязвимости, не отставать от развивающихся угроз, обеспечивать соответствие требованиям, снижать риски, усиливать меры безопасности и укреплять доверие клиентов. Инвестируя в регулярные оценки, предприятия могут

гарантировать, что их меры безопасности остаются эффективными и актуальными, снижая вероятность успешной кибератаки и защищая свою деятельность, репутацию и финансовую стабильность». ***(Jerry Balworth. Why Regular Cybersecurity Assessments Are Critical // Talk Business (https://www.talk-business.co.uk/2023/03/23/why-regular-cybersecurity-assessments-are-critical/). 23.03.2023).***

***

Сполучені Штати Америки та Канада

«Эксперт по кибербезопасности из Нью-Брансуика говорит, что громкие утечки данных в Sobeys и Indigo указывают на слабость канадских законов, поскольку уязвимости критически важной инфраструктуры растут.

«Наша текущая национальная стратегия кибербезопасности безнадежно устарела, — говорит Дэвид Шипли, генеральный директор компании Beauceron Security Inc. из Фредериктона. — Мы сильно отстаем от наших коллег в США и Европе».

Федеральное законодательство ожидает второго чтения для обновления канадских законов о кибербезопасности.

«Потенциально у нас есть два-три года до того, как эти законы будут приняты, а правила введены в действие», — говорит Шипли. «Между тем, в Интернете никогда не было так плохо».

Шипли указывает на Общий регламент ЕС по защите данных как на строгую политику, которой должны следовать канадские законодатели.

«Это дало регулятивным органам настоящие, значимые зубы, чтобы обуздать технологических гигантов и другие компании, которые либо собирали информацию о людях без их согласия, либо взламывали ее из-за отсутствия безопасности», — говорит Шипли.

Некоторые штрафы могут составлять до 20 миллионов евро, или четыре процента от глобального дохода компании.

«Это заставило компании гораздо серьезнее относиться к конфиденциальности», — говорит Шипли. «Наш закон о земле на федеральном уровне в Канаде абсолютно беззуб. Реальных последствий не будет». Шипли говорит, что критическая инфраструктура в Канаде также находится под угрозой из-за слабых законов о кибербезопасности, включая энергосистемы, телекоммуникации, транспорт и ИТ-системы здравоохранения.

«Пока это не происходит, для многих организаций это нереально», — говорит Шипли.

В Ньюфаундленде и Лабрадоре в результате кибератаки на систему здравоохранения провинции в 2021 году были взломаны тысячи записей личных данных.

В Сент-Джоне, штат Нью-Брансуик, город отказался выплатить почти 17 миллионов долларов в биткойнах после атаки программы-вымогателя в 2020 году. В результате городу пришлось перестраивать свою ИТ-систему с нуля.

В Национальной оценке киберугроз федерального правительства на 2023-2024 годы говорится, что программы-вымогатели и спонсируемые государством киберугрозы являются одними из главных проблем Канады.

«Это всего лишь превью довольно мрачной оставшейся части года и довольно мрачной оставшейся части десятилетия», — говорит Шипли. «Это не веселое заявление. И так быть не должно». ***(Nick Moore. Cyberattacks put spotlight on weak Canadian laws, says cybersecurity expert // Bell Media (https://atlantic.ctvnews.ca/cyberattacks-put-spotlight-on-weak-canadian-laws-says-cybersecurity-expert-1.6299535). 05.03.2023).***

***

«Агентство по охране окружающей среды США в пятницу объявило о новых требованиях к общественным объектам водоснабжения для повышения их кибербезопасности, выразив при этом обеспокоенность тем, что многие объекты не предприняли элементарных шагов для защиты от хакеров.

Новый меморандум Агентства по охране окружающей среды требует от правительств штатов проводить аудит практики кибербезопасности общественных систем водоснабжения, а затем использовать государственные регулирующие органы, чтобы заставить системы водоснабжения добавить меры безопасности, если существующие будут сочтены недостаточными.

«Кибератаки, нацеленные на системы водоснабжения, представляют собой реальную и серьезную угрозу нашей безопасности», — заявила в четверг журналистам помощник администратора Агентства по охране окружающей среды Радхика Фокс.

Это последний шаг администрации Байдена в судебной прессе, направленный на использование своих регулирующих и политических полномочий, чтобы попытаться усилить киберзащиту критически важной инфраструктуры США, которая часто становится мишенью для киберпреступников и хакеров, поддерживаемых иностранным правительством.

Меморандум EPA появился через день после того, как Белый дом опубликовал национальную стратегию кибербезопасности, которая призывает производителей программного обеспечения нести ответственность, когда их продукты оставляют зияющие дыры для использования хакерами.

Тревожный сигнал для кибербезопасности в водном секторе прозвучал в администрации Байдена всего через несколько недель, в феврале 2021 года, когда хакер проник на водоочистное сооружение во Флориде и попытался увеличить количество гидроксида натрия до потенциально опасного уровня, по словам местных властей.

Объект остановил атаку до того, как можно было причинить вред, но этот эпизод встревожил официальных лиц в Вашингтоне и привел к усилению федерального контроля за методами обеспечения безопасности в водном секторе.

ФБР и Агентство США по кибербезопасности и безопасности инфраструктуры предупредили о многочисленных атаках программ-вымогателей на компьютерные сети объектов водоснабжения и водоотведения от Калифорнии до штата Мэн.

То, что большее внимание общественности к этому вопросу принесло улучшения; Центр обмена и анализа информации о воде (WaterISAC), отраслевой центр данных о киберугрозах и передового опыта, сообщает, что в его состав теперь входят объекты, которые обеспечивают водой большую часть США.

«Множество ассоциаций водного сектора осознают необходимость помочь водным системам повысить устойчивость к киберугрозам», — сказала CNN Дженнифер Лин Уокер, директор WaterISAC по защите инфраструктуры от киберугроз. «Большие системы лидируют в течение многих лет, поэтому я думаю, что мы можем адаптировать эти усилия к средним и меньшим системам для большего блага сектора».

Но разросшийся сектор водоснабжения США, который включает более 148 000 общественных систем водоснабжения, иногда испытывает трудности с финансированием и персоналом для защиты систем.

В системах общественного водоснабжения «авторизация сверху вниз для крупных проектов кибербезопасности, к сожалению, обычно происходит только после инцидента», — сказал CNN Крис Гроув, директор по стратегии кибербезопасности в фирме промышленной безопасности Nozomi Networks.

«В муниципалитетах, которые управляют общественными системами водоснабжения, они выбирают между расширением библиотек, камерами для полиции или кибербезопасностью систем водоснабжения и очистки сточных вод», — сказал Гроув». ***(Sean Lyngaas. US introduces new rules to protect water systems from hackers // Cable News Network (https://edition.cnn.com/2023/03/03/politics/epa-water-cybersecurity-rules/). 03.03.2023).***

***

«Правительство Соединенных Штатов недавно обнародовало свою Национальную стратегию кибербезопасности, в которой излагаются планы администрации Байдена по обеспечению безопасного и надежного киберпространства для американцев перед лицом растущих опасений в Интернете.

В документе описывается, как Китай, Россия, Иран и Северная Корея используют технологии для угрозы национальной безопасности США сверх международно признанных норм.

Учитывая угрозу, которую представляют злоумышленники, 39-страничная стратегия утверждает необходимость более «преднамеренного, скоординированного и хорошо обеспеченного ресурсами подхода» к кибербезопасности.

В соответствии с последней стратегией правительство хочет, чтобы малые предприятия, частные лица и местные органы власти не беспокоились о том, что они являются самым слабым звеном в цепочке кибербезопасности.

Стратегия направлена на значительное перераспределение ответственности в пользу организаций, которые лучше подготовлены к управлению рисками и их минимизации.

Gizmodo сообщает нам, что новая киберстратегия направлена на то, чтобы заставить компании Силиконовой долины уделять первостепенное внимание безопасности при разработке своих продуктов.

Кроме того, перераспределяя роли, обязанности и ресурсы в киберпространстве, Соединенные Штаты совершают гигантский скачок к более безопасному и устойчивому цифровому будущему благодаря коллективным усилиям в области кибербезопасности.

Правительство США также занимается действиями, которые уравновешивают защиту от непосредственных угроз и позиционирование на долгосрочную перспективу.

Что касается кибербезопасности, правительство применяет комплексный и скоординированный подход к защите национальной безопасности, общественной безопасности и экономического процветания, стимулируя долгосрочные инвестиции в кибербезопасность, а также устраняя неотложные угрозы настоящего.

Защита критически важных инфраструктур

Министерство внутренней безопасности выпустило предупреждение о том, что в январе 2022 года Россия может предпринять кибератаки против Соединенных

Штатов, если посчитает, что действия НАТО поставят под угрозу их долгосрочную безопасность.

Возможными целями могут стать государственные и местные органы власти, а также операторы критической инфраструктуры.

В ответ на подобные угрозы правительство расширяет использование минимальных требований к кибербезопасности в критически важных секторах, поощряет государственно-частное партнерство для защиты основных услуг и модернизирует федеральные сети для повышения их устойчивости.

Эти меры направлены на то, чтобы вселить уверенность в критически важную инфраструктуру страны и основные услуги, которые имеют жизненно важное значение для ее безопасности и экономической стабильности.

Препятствование действиям злоумышленников в киберпространстве

Соединенные Штаты продолжают сталкиваться с серьезной проблемой взлома и киберпреступности в своем киберпространстве. Атаки программ-вымогателей стали повседневным явлением, нацеленным на известные общедоступные платформы.

В ответ правительство использует все инструменты национальной власти, чтобы нейтрализовать злоумышленников в киберпространстве.

Он стремится вовлечь частный сектор в масштабные действия по разрушению и всесторонне бороться с угрозой программ-вымогателей с международными партнерами.

Усилия правительства демонстрируют его решимость защитить национальную киберинфраструктуру от растущей угрозы киберпреступности и конфиденциальную информацию своих граждан от злоумышленников.

Инвестиции в кибербезопасность

В марте 2022 года президент Джо Байден призвал американский бизнес укрепить свою киберзащиту из-за надвигающейся угрозы российских кибератак.

Однако заполнение вакансий в области кибербезопасности становится все более трудным из-за острой конкуренции на более широком рынке труда: почти 600 000 должностей из миллиона остаются незаполненными.

Правительство намерено уделять приоритетное внимание исследованиям и разработкам в области кибербезопасности и уменьшать технические уязвимости для решения этой проблемы. Кроме того, основное внимание будет уделено развитию разнообразной и надежной национальной рабочей силы в области кибербезопасности и превращению Соединенных Штатов в мирового лидера в области безопасных и устойчивых технологий и инфраструктуры следующего поколения.

Разрабатывая технологии следующего поколения, Соединенные Штаты намерены опережать киберугрозы и обеспечить, чтобы их сотрудники в области кибербезопасности были хорошо оснащены для борьбы с постоянно меняющимся ландшафтом угроз.

Наконец, США активно поощряют ответственное поведение государства в киберпространстве.

Чтобы противостоять угрозам цифровой экосистеме страны, правительство пытается изолировать и наказывать за безответственное поведение, используя международные партнерства и коалиции.

Соединенные Штаты надеются содействовать глобальному сотрудничеству и сделать киберпространство более безопасным посредством партнерства и коалиций». ***(John Lopez. US Government Releases National Cybersecurity Strategy—Here's Why It Matters // TECHTIMES.com (https://www.techtimes.com/articles/288541/20230304/us-government-biden-national-cybersecurity-strategy-heres-why-matters.htm). 04.03.2023).***

***

«Пара двухпартийных депутатов Сената представила закон, устанавливающий основанный на оценке риска подход к устранению угроз, исходящих от иностранных технологий, включая приложения для социальных сетей, телекоммуникационные платформы и программное обеспечение для обеспечения безопасности.

Сенаторы Джон Тьюн, RS.D., высокопоставленный член Подкомитета по коммуникациям, средствам массовой информации и широкополосной связи, и Марк Уорнер, D-Va, председатель Специального комитета по разведке, стремятся дать указание Министерству торговли создать риск. Об этом во вторник заявил офис Thune, основанный на технологии идентификации и смягчения угроз со стороны иностранных технологий.

Закон об ограничении возникновения угроз безопасности, связанных с информационными и коммуникационными технологиями, будет отдавать приоритет продуктам ИКТ, используемым в критической инфраструктуре и миссиях национальной безопасности.

«Нам нужен комплексный, основанный на оценке риска подход, который активно устраняет источники потенциально опасных технологий до того, как они закрепятся в Америке, поэтому мы не играем в Whac-A-Mole и не пытаемся наверстать упущенное, когда они уже повсеместно распространены». — сказал Уорнер, трехкратный лауреат премии Wash100.

Тьюн сказал, что необходим «целостный, методичный подход» для устранения угроз, создаваемых продуктами, произведенными иностранными противниками, и обеспечения безопасности продуктов ИКТ, используемых потребителями.

Сенатор также подчеркнул проблемы национальной безопасности с приложениями, созданными китайскими разработчиками, включая TikTok от ByteDance…» ***(Naomi Cooper. Senate Bill to Develop Risk-Based Approach to Addressing Foreign Technology Threats // Executive Mosaic (https://executivegov.com/2023/03/senate-bill-to-develop-risk-based-approach-to-addressing-foreign-technology-thre/). 08.03.2023).***

***

«В своем последнем бюджетном отчете Белый дом выделил в общей сложности 3,1 миллиарда долларов на инфраструктуру кибербезопасности.

Опубликованный в четверг документ показывает, что 145 миллионов долларов из этой суммы пойдут на то, чтобы сделать Агентство кибербезопасности и безопасности инфраструктуры (CISA) «более устойчивым и защищенным».

Из оставшихся средств 98 млн долларов будут инвестированы в реализацию Закона об отчетности о кибер-инцидентах для критически важной инфраструктуры от 2021 года и 425 млн долларов в улучшение внутренней кибербезопасности и аналитических возможностей CISA.

«Для защиты от иностранных противников и защиты федеральных систем, на которые опирается американский народ, бюджет укрепляет кибербезопасность, гарантируя, что каждое агентство повышает безопасность государственных услуг», — говорится в документе.

По словам Илоны Коэн, директора по политике платформы безопасности HackerOne, средства будут необходимы для создания более квалифицированной и разнообразной рабочей силы в области кибербезопасности, поддержки перехода от устаревших систем к современной инфраструктуре и содействия внедрению агентствами архитектур с нулевым доверием.

«Я считаю, что законодатели могут выполнить все вышеперечисленное и поощрять внедрение передового опыта в отношении раскрытия информации об уязвимостях», — добавил Коэн. «Запуск программ раскрытия уязвимостей и доверие к этическим хакерам имеет решающее значение для выявления наиболее критических уязвимостей в нашей цифровой инфраструктуре и создания более устойчивых систем».

Тем не менее, Ричард Берд, директор по безопасности компании Traceable AI, занимающейся безопасностью API, сказал, что, хотя новые инвестиции в кибербезопасность приветствуются, разочаровывает тот факт, что акцент делается на устаревшие способы мышления.

«Быстрая отчетность об инцидентах — это не улучшение безопасности, так же, как система сигнализации, которая срабатывает через два дня после того, как вас ограбили, — это улучшение безопасности», — пояснил Бёрд. «Правительству США пора серьезно заняться законодательной законодательной защитой граждан и

потребителей в нашей стране от киберугроз вместо того, чтобы предпринимать такие полумеры и полушаги».

Объявление о бюджете появилось через несколько дней после того, как администрация Байдена-Харриса опубликовала свою Национальную стратегию кибербезопасности». ***(Alessandro Mascellino. White House Allocates $3.1bn to Cybersecurity in New Budget // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/white-house-allocates-dollar31bn/). 10.03.2023).***

***

Країни ЄС та Великобританія

«Промышленный комитет Европейского парламента в четверг (9 марта) проголосовал за проект отчета депутата Европарламента Хенны Вирккунен, в котором предлагается ввести общие стандарты кибербезопасности в учреждениях ЕС, что прокладывает путь к началу трехсторонних переговоров.

Законопроект представляет собой версию ЕС пересмотренной Директивы о сетях и информационной безопасности (NIS2), которая ввела требования кибербезопасности на национальном уровне для организаций, играющих важную роль в функционировании общества.

Он направлен на установление «высокого общего уровня кибербезопасности в учреждениях, органах, офисах и агентствах Союза».

Это законодательство отвечает растущим проблемам кибербезопасности, вызванным в основном растущей цифровизацией государственных органов, административных процедур и недостаточной готовностью органов ЕС к борьбе с потенциальными атаками.

«Высокий уровень готовности к кибербезопасности должен быть нормой в организациях ЕС», — сказал Вирккунен. «Мы должны обеспечить достаточные технические возможности, знания и ресурсы для эффективного противодействия все более изощренным угрозам кибербезопасности».

Европейская комиссия предложила закон в марте 2022 года, в том же месяце, когда Европейская аудиторская палата опубликовала исследование, в котором подчеркивается настоятельная необходимость повышения потенциала кибербезопасности институтов ЕС в условиях ухудшающейся картины угроз.

По мнению аудиторов, органы ЕС становились все более привлекательными целями для кибератак: в период с 2018 по 2021 год количество серьезных инцидентов увеличилось более чем в 10 раз. Эта тенденция отчасти была вызвана пандемией COVID-19, когда все больше людей работают из дома.

Аудиторы также обнаружили, что возможности ЕС по обеспечению киберустойчивости значительно недостаточны и что целевые атаки представляют собой широко распространенный риск, учитывая взаимосвязь институтов ЕС.

В отчете содержится призыв к модернизации инфраструктуры кибербезопасности блока, в котором говорится, что «ЕС должен сделать больше для защиты своих собственных властей».

Предложение Комиссии вводит общие стандарты кибербезопасности, такие как структуры управления, оценки рисков и планы улучшения кибербезопасности.

Регламент также расширит возможности и финансирование Группы реагирования на инциденты компьютерной безопасности ЕС (CERT-EU), которая осуществляет надзор за безопасностью ИКТ в учреждениях и организациях Союза.

Парламентский проект отчета ввел дополнительные обязанности для CERT-EU, такие как выполнение координирующей роли в раскрытии уязвимостей и возложение на него задачи по предложению критериев и шкалы для рамок кибербезопасности, принятых организациями ЕС.

В поправки также включено положение о создании CERT-EU в качестве «автономного межведомственного поставщика услуг для всех субъектов Союза», интегрированного в отдел Комиссии, с регулярными оценками его функционирования.

Это позволит внести изменения в его структуру, включая его возможное восстановление в качестве офиса Союза в ответ на то, что в проекте отчета

определяется как «растущая важность кибербезопасности и постоянно возникающий уровень угроз».

В отчете также реорганизованы временные рамки для сообщения о значительных кибер-инцидентах, приведенные в соответствие требования по срокам уведомления с требованиями Директивы NIS2.

В соответствии с поправками к отчету организации должны представить раннее предупреждение об инциденте в течение 24 часов после того, как ему стало известно, и официальное уведомление об инциденте с указанием первоначальной оценки его серьезности и воздействия в течение 72 часов.

«Общая структура мер кибербезопасности для организаций ЕС необходима для повышения их устойчивости и возможностей реагирования на инциденты», — заявил докладчик Вирккунен после единогласного одобрения проекта отчета отраслевым комитетом.

«Все структуры ЕС взаимосвязаны, и в цепи не должно быть слабых звеньев. Межведомственный подход позволит субъектам ЕС разрабатывать свои меры кибербезопасности и реагировать на киберугрозы и потенциальные атаки».

Парламентский отчет должен быть принят без пленарного голосования. Поскольку Совет министров ЕС согласился со своей позицией по делу в ноябре, межведомственные переговоры, так называемые трилоги, начнутся в ближайшие недели.

В своем подходе Совет определил элементы для укрепления CERT-EU, в частности, его возможностей по обмену информацией и укрепления координации при реагировании на серьезные киберинциденты». ***(Molly Killeen. European Parliament agrees cybersecurity requirements for EU bodies // EURACTIV (https://www.euractiv.com/section/cybersecurity/news/european-parliament-agrees-cybersecurity-requirements-for-eu-bodies/). 09.03.2023).***

***

«В следующем году европейские порты готовятся к серьезным нормативным изменениям в том, как сотни компаний в их глобальных

цепочках поставок решают вопросы кибербезопасности, поскольку порты стали мишенью для преступных хакерских групп и атак, спонсируемых государством.

Правила кибербезопасности, утвержденные Европейским союзом для фармацевтических, транспортных, энергетических и других компаний, представляющих критическую инфраструктуру, вступят в силу в 2024 году и потребуют от сотен фирм, работающих за пределами крупных портов Европы, соблюдения основных мер безопасности и сообщения о взломе в органы кибербезопасности. Регламент станет первым таким требованием кибербезопасности для многих компаний, предоставляющих услуги критически важным секторам. Нарушителям грозит штраф в размере до 10 миллионов евро, что эквивалентно примерно 10,7 миллиона долларов, или до 2% от мирового дохода, в зависимости от того, что больше.

Война в Украине, рост цен на энергоносители и сбои в цепочке поставок во время пандемии заставили портовые власти быть в состоянии повышенной готовности в связи с растущим числом кибератак. Порты в таких городах, как Роттердам в Нидерландах и Антверпен в Бельгии, два крупнейших порта Европы по объему грузов, являются узлами энергетической инфраструктуры и других важнейших секторов. Кибератака за три недели до того, как Россия вторглась в Украину в феврале 2022 года, нарушила работу компаний по хранению и распределению энергии, а также крупного оператора терминалов в Антверпене и других бельгийских и голландских портах.

Для портовых властей, которые обеспечивают безопасное перемещение грузов через порты, будущие правила могут упростить их работу, потому что может быть трудно подтолкнуть портовые компании, такие как поставщики хранилищ нефти и товаров, операторы терминалов или логистические фирмы, к добровольному принятию средств защиты от кибербезопасности., — сказал Афанасиос Другкас, эксперт по безопасности Enisa, европейского агентства по кибербезопасности. «Это облегчит их жизнь», — сказал он.

Правила будут применяться к операторам критической инфраструктуры и компаниям в их цепочках поставок, включая поставщиков технологических услуг. Растущее число киберугроз было направлено на компании критической инфраструктуры во время войны в Украине, что подчеркивает уязвимость цепочек поставок. «Мы чувствовали, что компания попала в яблочко», — сказал Янник Эрребаут, директор по информационной безопасности бельгийского порта Антверпен-Брюгге NV, имея в виду администрацию порта.

Компании, базирующиеся в порту Антверпен-Брюгге, пострадали от программ-вымогателей в феврале 2022 года, в то время как кибератаки нарушили работу немецких компаний по хранению энергии и фирм в голландских портах. Пострадавшие приостановили некоторые операции, и танкеры столпились у порта Антверпен-Брюгге в ожидании разгрузки.

«Становится все более и более важным, чтобы вы имели контроль над этой цепочкой поставок», — сказал он.

Со временем грядущий европейский закон о кибербезопасности для критической инфраструктуры, вероятно, будет иметь такой же эффект, как и общие правила конфиденциальности Европейского союза, известные как Общий регламент защиты данных, сказал Дипак Мехта, разработчик экосистемы в Морском кампусе Антверпена, который работает над технологическими инновациями. с морскими компаниями, включая порты и судовладельцев.

Предыдущая версия будущего закона ЕС о кибербезопасности предусматривала меньше мер безопасности, чем окончательный вариант, и применялась только к крупным компаниям в нескольких критически важных секторах. Со следующего года расширенные киберправила будут применяться к более широкому кругу компаний, включая многие фирмы среднего размера, а также к секторам, включая управление отходами, поставщиков космических и технологических услуг, которые ранее не подпадали под действие закона 2018 года. У стран ЕС есть время до октября 2024 года, чтобы приступить к выполнению требований и обеспечить соблюдение правил национальными регулирующими органами.

Около пяти компаний в порту Роттердама подпадают под юрисдикцию предыдущего закона, сказал Марин ван Шут, глава отдела кибербезопасности в порту Роттердама. По его словам, это число увеличится примерно до 200, когда вступит в силу обновленная версия.

Новый закон требует от компаний критической инфраструктуры убедиться, что они проводят оценку киберрисков, используют технические средства защиты, такие как шифрование, и меры по предотвращению кибератак и реагированию на них, а также проявляют должную осмотрительность в отношении средств защиты кибербезопасности, которые имеют поставщики услуг.

«В ближайшие годы предстоит проделать большую работу, — сказал г-н ван Шут.

Расширение заставит компании улучшать меры кибербезопасности, которыми они пренебрегали, сказал Роб Ниджман, представитель FERM, группы, которая обменивается информацией о кибербезопасности от государственных органов среди примерно 50 компаний-членов в порту Роттердама. «Конечно, у компаний есть возможности привести свои вещи в порядок, потому что они должны это делать», — сказал он.

По словам г-на ван Шота, порт Роттердама оценивает возможность создания центра операций по обеспечению безопасности по образцу аналогичной инициативы в порту Лос-Анджелеса. Его офис решит до лета, стоит ли идти вперед.

Порт Лос-Анджелеса обменивается информацией об угрозах через центр киберзащиты с примерно 20 членами, включая компании и группы, такие как докеры порта. Отдельный оперативный центр безопасности в порту работает круглосуточно и ежемесячно останавливает около 40 миллионов попыток кибератак. Гена Серока, исполнительный директор порта.

Ежегодно порт Лос-Анджелеса используют более 200 000 компаний, с помощью судоходных линий, грузовиков и железных дорог, доставляющих туда грузы. «Это действительно сложный набор участников, — сказал он». ***(Catherine Stupp. European Ports Brace for Cybersecurity Regulation // Dow Jones & Company,***

Inc (https://www.wsj.com/articles/european-ports-brace-for-cybersecurity-regulation-ece61a30?mod=flipboard). 21.03.2023).

***

«Нынешнее председательство Швеции в Совете ЕС недавно распространило новые компромиссные тексты по некоторым положениям предложения о новом Европейском законе о киберустойчивости («Закон о киберустойчивости»), между Законом и другим законодательством включая, среди прочего, серьезные изменения в классификации цифровых продуктов и разъяснение взаимодействия.

Напомним, что предложение о Законе о киберустойчивости, представленное Комиссией 15 сентября 2022 года, вводит горизонтальные обязательные требования кибербезопасности для продуктов с цифровыми элементами, которые не являются специфическими для секторов, на протяжении всего их жизненного цикла. Целью Закона о киберустойчивости является защита потребителей и предприятий от продуктов с неадекватными функциями безопасности. Предложение дополняет требования директивы NIS2, целью которой является обеспечение высокого уровня кибербезопасности услуг, предоставляемых важными и важными организациями.

Закон будет применяться к так называемым экономическим операторам, таким как производители, импортеры и дистрибьюторы. В сферу действия этого нового проекта регламента входят все продукты, которые прямо или косвенно подключены к другому устройству или сети, такие как интеллектуальные устройства Интернета вещей (IoT), компьютеры, мобильные устройства, операционные системы и приложения, а также критически важные для безопасности компоненты, которые устанавливаются в сетях или на промышленных объектах. Есть некоторые исключения для продуктов, для которых требования кибербезопасности уже изложены в существующих правилах ЕС, например, в области медицинских устройств, авиации или автомобилей.

Каковы основные элементы новых компромиссных текстов?

Ключевые элементы, внесенные в компромиссные тексты шведского председательства, заключаются в следующем:

Более подробно описана классификация критичных продуктов с цифровыми элементами и особо критичных продуктов с цифровыми элементами. Кроме того, в контексте критически важных продуктов ряд категорий цифровых продуктов был перемещен из класса I в класс II (например, программное обеспечение систем управления идентификацией и программное обеспечение управления привилегированным доступом; продукты с цифровыми элементами с функцией виртуальной частной сети).), а некоторые теперь относятся к классу I (например, инфраструктура открытых ключей и программное обеспечение для выдачи цифровых сертификатов), а не к классу II. Продукты для умного дома с функциями безопасности, такие как дверные замки и системы сигнализации, были недавно включены в текст. Это повлияет на тип необходимой процедуры оценки соответствия;

Чтобы продемонстрировать соответствие основным требованиям, изложенным в Законе, Европейская комиссия будет уполномочена принимать делегированные акты в дополнение к Закону о киберустойчивости. Эти делегированные акты могут указывать категории особо важных продуктов с цифровыми элементами, для которых производители должны получить европейский сертификат кибербезопасности с уровнем гарантии «значительный» или «высокий» в соответствии с европейской схемой сертификации кибербезопасности в соответствии с Законом о кибербезопасности;

Образец упрощенной Декларации о соответствии ЕС со ссылкой на адрес в Интернете, где доступен полный текст Декларации, был включен в качестве дополнительного приложения;

Орган по надзору за рынком государства-члена потребует от экономического оператора принятия соответствующих мер, если, выполнив оценку, он обнаружит, что, несмотря на то, что продукт с цифровыми элементами и процессы, внедренные производителем, соответствуют Закону о киберустойчивости., это представляет

значительный риск для кибербезопасности, а также риск для здоровья или безопасности людей или других аспектов защиты общественных интересов;

Упомянутые выше меры могут включать меры по обеспечению того, чтобы продукт с соответствующими цифровыми элементами и процессы, внедренные изготовителем, больше не представляли соответствующих рисков при появлении на рынке, изъятие с рынка продукта с соответствующими цифровыми элементами, или отзыв о нем, и должны быть соразмерны характеру этих рисков;

Уточнено взаимодействие с Общим регламентом безопасности продукции, Регламентом AI, а также Регламентом по машинному оборудованию; и

По сравнению с первоначальным предложением Комиссии новый компромиссный текст теперь ограничивает виды обязательств, которые могут подлежать административным штрафам в размере до 10 миллионов евро в случае несоблюдения или, если правонарушителем является предприятие, до 2% общий годовой оборот по всему миру за предыдущий финансовый год, в зависимости от того, что больше. В этом контексте обязательства, на которые ссылается текст, включают, среди прочего, положения о технической документации и процедурах оценки соответствия для продуктов с цифровыми элементами.

Следующие шаги

Европейский парламент начал работу над Законом о киберустойчивости. Рассмотрение проекта Отчета в ведущем Комитете по промышленности, исследованиям и энергетике (ITRE) в настоящее время запланировано на 24-25 апреля 2023 г., а крайний срок внесения поправок установлен на 27 апреля 2023 г.

После принятия у экономических операторов и государств-членов будет два года, чтобы адаптироваться к новым требованиям. Исключением из этого правила является обязательство производителей сообщать об активно эксплуатируемых уязвимостях и инцидентах. Это обязательство будет применяться уже через год после вступления в силу, учитывая меньшее количество организационных корректировок, чем другие новые обязательства». ***(Natallia Karniyevich. Cybersecurity: Swedish Presidency proposes major changes to the European Cyber Resilience Act // Bird & Bird***

(https://www.twobirds.com/en/insights/2023/sweden/cybersecurity-swedish-presidency-proposes-major-changes-to-the-european-cyber-resilience-act). 17.03.2023).

***

Австралія та Нова Зеландія

«Австралия переживает революцию в области кибербезопасности. 8 декабря 2022 года министр кибербезопасности достопочтенный. Член парламента Клэр О'Нил объявила о разработке Австралийской стратегии кибербезопасности на 2023-2030 годы (Стратегия). Министр назначил Экспертный консультативный совет (под председательством бывшего генерального директора Telstra Эндрю Пенна) для консультирования по вопросам разработки Стратегии, и 27 февраля 2023 года Экспертный консультативный совет опубликовал дискуссионный документ (дискуссионный документ), сделать предложения о том, как правительство может реализовать свое видение превращения Австралии в самую кибербезопасную страну к 2030 году. И Стратегия, и дискуссионный документ подкрепляют идею о том, что Австралия лидирует в повышении кибербезопасности, факт, который получил международное признание от MIT Technology Review Индекс киберзащиты (Обзор), согласно которому Австралия занимает первое место в мире по показателю наибольшего прогресса и приверженности делу повышения кибербезопасности…

Сам дискуссионный документ не описывает каких-либо реформ, которые будут проводиться в области кибербезопасности, вместо этого ставит ряд вопросов, касающихся состояния кибербезопасности, и предлагает отрасли представить ответы на эти вопросы. В дискуссионном документе подчеркивается, что Стратегия сформирует основу для развивающегося подхода к кибербезопасности в будущем, и что ее реализация потребует надежного управления и прозрачной, значимой системы оценки, чтобы гарантировать, что Стратегия соответствует цели сейчас и в будущем. будущее. В нем указывается, что Стратегия будет разрабатываться в сотрудничестве с отраслевыми академическими кругами, правительствами штатов и территорий, а также австралийским и международным сообществом. Министр

внутренних дел и кибербезопасности и Экспертный консультативный совет также консультируются по передовым мировым практикам со стороны Глобальной консультативной группы, в которую входят лучшие умы из ближайших союзников Австралии. Глобальную консультативную группу возглавляет Киаран Мартин СВ, бывший генеральный директор Национального центра кибербезопасности Соединенного Королевства.

В Дискуссионном документе признается, что австралийские предприятия и неправительственные организации несут ряд неявных обязательств в области кибербезопасности, в том числе через корпорации, потребителей, критически важную инфраструктуру, а также законодательные и нормативные рамки конфиденциальности. В нем подчеркивается, что из-за серьезности крупных киберинцидентов во всей отрасли требуется более четкое указание обязательств, включая некоторые формы передовых стандартов кибербезопасности, для повышения нашей национальной киберустойчивости и обеспечения безопасности австралийцев и их данных. Хотя в нем не приводится пример того, как могут выглядеть эти прямо выраженные обязательства, в нем содержится призыв к отрасли прокомментировать потенциальное рассмотрение нового Закона о кибербезопасности, который объединит законодательные обязательства и стандарты, относящиеся к кибербезопасности, для отрасли и правительства.

В нем также подчеркивается, что также могут быть возможности для упрощения и рационализации существующей нормативно-правовой базы. Например, заинтересованные стороны призвали правительство упорядочить обязательства по отчетности и требования к реагированию после крупного кибер-инцидента. Это было бы долгожданной реформой, учитывая текущее состояние обязательств по отчетности, разбросанных по нескольким законодательным актам и отраслевым стандартам.

В документе для обсуждения также предлагается рассмотреть вопрос о том, оправданы ли дальнейшие изменения в Законе о безопасности критически важной инфраструктуры 2018 года (Cth) (Закон SOCI), например, включение данных клиентов и «систем» в определение критических активов для обеспечения

полномочий, предоставляемых Правительство в соответствии с Законом о SOCI распространяется на серьезные утечки данных, такие как те, с которыми столкнулись Medibank и Optus, а не только на сбои в работе. В соответствии с Законом о SOCI правительство имеет полномочия «последней инстанции» для реагирования на серьезные инциденты кибербезопасности, связанные с критически важными инфраструктурными активами в критически важных секторах инфраструктуры. Если данные о клиентах и «системы» будут добавлены к определению критически важных активов в соответствии с Законом о SOCI, это фактически предоставит министру полномочия:

давать указания определенному субъекту в целях сбора информации об инциденте кибербезопасности;

давать указание указанному объекту, требуя от объекта предпринять определенные действия или выполнить определенные действия в ответ на инцидент кибербезопасности; и

запросить у уполномоченного государственного органа помощь в реагировании на инцидент кибербезопасности.

Если бы это изменение имело место во время взлома Medibank или Optus, правительство имело бы возможность эффективно управлять реагированием этих предприятий на кибер-инциденты, если бы оно того пожелало. В то время как Закон SOCI уже содержит права правительства на «вмешательство» после серьезного киберинцидента, министр О'Нил предположил, что эти полномочия в настоящее время слишком ограничены и «очень, очень узко определены» и практически не помогают правительству. Однако определение «актива» в соответствии с Законом о SOCI уже очень широкое (включая систему, устройство, компьютерную программу, данные и «любую другую вещь»), что поднимает вопрос о том, как повлияет расширение определения актива. практически имел бы…

В Документе для обсуждения выдвинуто это предложение с целью разъяснения того, что сообщество и жертвы кибератаки могут ожидать от правительства после инцидента. В нем четко указано, что правительство должно

обеспечить соответствие рамок управления инцидентами и координации поставленным целям, а также что правительство должно проводить анализ после инцидентов и управление последствиями после крупных киберинцидентов. Кроме того, в нем утверждается, что правительство должно делиться выводами об основных причинах расследований крупных кибер-инцидентов, чтобы каждый мог извлечь пользу из этих знаний…» ***(Michael Caplan, Astan Ure. 2023-2030 Australian Cyber Security Strategy: Leading the Charge // Gilbert + Tobin (https://www.gtlaw.com.au/knowledge/2023-2030-australian-cyber-security-strategy-leading-charge). 17.03.2023).***

***

Індія

«Только 24% индийских организаций имеют «зрелый» уровень готовности, необходимый для устойчивости к современным угрозам кибербезопасности, говорится в новом отчете, опубликованном во вторник.

Согласно Индексу готовности к кибербезопасности Cisco, Индия заняла высокие места в мировом рейтинге с точки зрения зрелости, показывая показатели готовности к кибербезопасности выше среднемирового показателя в 15%.

«Индекс был построен с акцентом на пять основных столпов идентификации, устройств, сети, приложений и данных, а также анализирует организационные подходы к их защите», — сказал Виш Айер, вице-президент по архитектуре, Cisco APJC.

«Эти пять столпов необходимо защитить с помощью сочетания точечных инструментов и интегрированных платформ, чтобы обеспечить устойчивость безопасности при одновременном снижении сложности. Только тогда предприятия смогут закрыть пробел в готовности к кибербезопасности», — добавил он.

В то время как организации в Индии чувствуют себя лучше, чем в среднем по миру, их число все еще очень мало, учитывая риски, говорится в отчете.

Несмотря на этот пробел в готовности, около 90% респондентов заявили, что ожидают, что инцидент кибербезопасности нарушит их бизнес в ближайшие 12–24 месяца.

Цена неподготовленности может быть значительной, так как 80% респондентов заявили, что за последние 12 месяцев сталкивались с инцидентом кибербезопасности, а 53% пострадавших заявили, что это стоило им не менее 5 000 000 долларов.

Более того, около 95% респондентов заявили, что их организации планируют увеличить свой бюджет на кибербезопасность как минимум на 10 % в течение следующих 12 месяцев…» ***(Only 24% of Indian firms are ready to defend against cybersecurity threats // bhaskar live (https://bhaskarlive.in/only-24-of-indian-firms-are-ready-to-defend-against-cybersecurity-threats/). 21.03.2023).***

***

Інші країни

«Комплексное решение по кибербезопасности не гарантирует наилучшую защиту без компетентного специалиста, управляющего им. Поиск компанией таких квалифицированных работников осложняется глобальной нехваткой специалистов в этой области. Этот факт был проиллюстрирован (ISC)² — международной некоммерческой ассоциацией лидеров информационной безопасности, которая в своем исследовании рабочей силы по кибербезопасности за 2022 год сообщила о нехватке навыков у 3,4 миллиона работников на профессиональном рынке. Эта ситуация вынудила предприятия передать определенные ИТ-функции поставщикам управляемых услуг (MSP) или поставщикам управляемых услуг безопасности (MSSP), чтобы получить соответствующий опыт и группы повышения квалификации.

Исследование «Лаборатории Касперского», проведенное в Саудовской Аравии среди лиц, принимающих решения в области ИТ, показало, что 60% малых и средних предприятий и корпораций заявили, что наиболее распространенной причиной передачи определенных обязанностей по обеспечению ИТ-безопасности

MSP/MSSP в 2022 году была нехватка ИТ-сотрудников. Среди других наиболее часто упоминаемых причин компании также назвали эффективность предоставления решений по кибербезопасности (57,1%), потребность в специальных знаниях (57%), масштабируемость (48,6%) и сложность бизнес-процессов (42,9%).

Что касается сотрудничества с MSP/MSSP, 77,1% компаний в Саудовской Аравии заявили, что обычно работают с двумя или тремя поставщиками, а 17,1% имеют дело с более чем четырьмя поставщиками услуг ИТ-безопасности в год.

«Внешние специалисты могут как управлять всеми процессами кибербезопасности в компании, так и заниматься отдельными задачами. Обычно это зависит от размера организации, ее зрелости и желания руководства участвовать в решении задач информационной безопасности. Для некоторых малых и средних компаний может быть разумным не нанимать штатного специалиста, а передать часть его функций МСП или МСП, так как это будет выгоднее с точки зрения затрат и эффективности. Для крупных корпораций сторонние специалисты обычно означают дополнительные руки, помогающие собственным командам по кибербезопасности справляться с большим объемом работы. Однако важно понимать, что в любом случае компания должна иметь базовые знания в области информационной безопасности, чтобы правильно оценивать работу аутсорсеров», — комментирует Константин Сапронов, руководитель группы глобального реагирования на чрезвычайные ситуации «Лаборатории Касперского».

Чтобы защитить вашу компанию от изощренных кибератак, даже если ей не хватает сотрудников службы безопасности или внутренних специалистов, «Лаборатория Касперского» рекомендует использовать услуги управляемой защиты. Комплексные тренинги для экспертов также помогают специалистам по ИТ-безопасности поддерживать соответствующие навыки и лучше подготовиться к ландшафту киберугроз…» ***(Companies in Saudi Arabia named the reasons to outsource cybersecurity functions // Zawya (https://www.zawya.com/en/press-***

release/research-and-studies/companies-in-saudi-arabia-named-the-reasons-to-outsource-cybersecurity-functions-lxum6axe). 12.03.2023).

***

«…Согласно опросу, проведенному Cisco, большинство компаний в Сингапуре не готовы защищаться от угроз кибербезопасности.

Согласно Индексу готовности к кибербезопасности Cisco, только 14% компаний находятся на «зрелом» уровне готовности к безопасности. В соответствии с индексом компании делятся на четыре.

Компании, находящиеся на зрелом этапе, достигли продвинутых этапов развертывания и почти готовы устранить риски безопасности.

Cisco считает компании «новичками», если они находятся «на начальных этапах развертывания решений»; «Формативный»: если у них есть определенный уровень развертывания, но показатели готовности к кибербезопасности ниже среднего; и «Прогрессивный», если у них значительный уровень развертывания и показатели готовности к кибербезопасности выше среднего.

В Сингапуре 7% компаний относятся к категории «Начинающие», а 42% находятся на стадиях «Формирование», демонстрируя уровень готовности к кибербезопасности ниже среднего.

«Этот пробел в готовности говорит не в последнюю очередь потому, что 85% респондентов заявили, что ожидают, что инцидент кибербезопасности нарушит их бизнес в ближайшие 12-24 месяца», — заявили в Cisco.

Cisco добавила, что цена неподготовленности может быть значительной, учитывая, что инциденты кибербезопасности обходятся 58% компаний не менее чем в 500 000 долларов США». ***(Only 1 in 10 companies in Singapore are prepared to address cybersecurity risks // Microsoft (Only 1 in 10 companies in Singapore are prepared to address cybersecurity risks). 23.03.2023).***

***

«Технический гигант Cisco Systems Inc. предупредил, что только 27 процентов или одна из четырех филиппинских фирм готовы к утечке данных, что свидетельствует о необходимости для местных организаций инвестировать в защиту кибербезопасности.

Cisco в своем Индексе готовности к кибербезопасности сообщает, что индонезийские фирмы лидируют в мире по готовности к кибербезопасности, причем 39% из них готовы защищаться от будущих рисков.

С другой стороны, Cisco сообщила, что 27% предприятий на Филиппинах и в Таиланде имеют все необходимое для отражения потенциальных атак на свои цифровые системы.

Бразилия лидирует среди всех стран Америки: 26% респондентов считают, что они готовы к угрозам кибербезопасности. Удивительно, но Cisco обнаружила, что развитые страны, такие как США (13 процентов), Канада (девять процентов), Южная Корея (семь процентов) и Япония (пять процентов), практически не инвестируют в защиту своих баз данных.

«Эта разница может быть в значительной степени объяснена тем, что компании на развивающихся рынках начали свой путь к оцифровке позже, чем их коллеги на развитых рынках. Это означает, что многие из этих компаний не имеют устаревших систем, которые их сдерживают», — заявили в Cisco.

Что касается Филиппин, Cisco сообщила, что 85% фирм здесь признают, что кибератаки могут нарушить их работу в ближайшие 24 месяца.

Кроме того, исследование показало, что по крайней мере три из каждых четырех филиппинских предприятий подвергались цифровым рискам за последние 12 месяцев, что превышает среднемировой показатель в 57 процентов.

Копнув глубже, Cisco обнаружила, что инциденты кибербезопасности в стране обошлись 38 процентам жертв примерно в 500 000 долларов, или более 27 миллионов песо.

В дальнейшем 87% филиппинских фирм увеличат свой бюджет на кибербезопасность более чем на 10% в течение следующих 12 месяцев. Cisco, однако, заявила, что это увеличение бюджета должно быть произведено раньше,

чем позже, предупредив, что 12-месячное ожидание усугубляет подверженность цифровым угрозам…» ***(Elijah Felice Rosale. Only 27% of Philippines firms ready vs cybersecurity risks – Cisco // Microsoft (https://www.msn.com/en-ph/news/other/only-27-of-philippines-firms-ready-vs-cybersecurity-risks-cisco/ar-AA18WLFS). 24.03.2023).***

***

Питання кіберстрахування

«Coalition Inc., поставщик киберстрахования, который пытается обуздать цифровые риски, разработал технологию, имитирующую крупномасштабные атаки, чтобы помочь страховщикам выявить потенциальные недостатки в своих портфелях и предотвратить широкомасштабные убытки.

Модель компании из Сан-Франциско измеряет киберриски в случае катастрофических потерь, например, если бы все компьютеры в мире были отключены одновременно. «Модель активного киберриска», о которой компания планирует объявить во вторник, предоставит страховщикам обзор их потенциальных убытков как способ более целенаправленно продавать свои полисы.

«Страховая отрасль слишком упрощенно относится к агрегированию киберрисков, — сказал главный исполнительный директор Coalition Джошуа Мотта. «Наша технология обеспечивает как основу для размышлений о риске, так и технологию для его реальной оценки и измерения».

Коалиция, основанная в 2017 году Моттой и Джоном Херингом, имеет около 175 000 клиентов для своей киберполитики, включая публичные компании, правительства и команды Национальной футбольной лиги. Закрытая страховая компания расширилась за пределы США в прошлом году, поскольку ее выручка выросла почти на 200% по сравнению с предыдущим годом. сказал. Коалиция в настоящее время оценивается в 5 миллиардов долларов, сказал Мотта.

Компания предоставляет то, что она называет «активной страховкой», имея в виду инструмент, который постоянно отслеживает цифровую инфраструктуру клиента для обнаружения вредоносных программ и проверяет наличие уязвимого программного обеспечения.

Например, модель активного киберриска, построенная на данных из портфеля компаний Coalition, смоделировала, что произойдет, если катастрофическая кибератака поразит 5000 компаний США. Коалиция определила, что такое событие может стоить всей экономике США примерно 29,8 миллиарда долларов.

«Мы считаем, что это уровень убытков, который можно застраховать», — сказал Мотта. «Мы пытаемся создать для отрасли путь вперед, чтобы попытаться застраховать эти системные кибер-события».

Структура, лежащая в основе модели активных киберрисков, будет общедоступна на веб-сайте Coalition для использования другими страховщиками, в то время как технология сканирования, которую компания использует для обнаружения киберрисков, является запатентованной.

Потребность в большей киберустойчивости стала более острой в связи с всплеском атак программ-вымогателей в эпоху пандемии. industrial supply chains, hospital systems and софтверные компании.

«Сегодня все больше людей осознают, что кибербезопасность может быть системным риском», — сказала Хайди Шей, аналитик по безопасности данных и конфиденциальности в Forrester, исследовательская организация. «Страховщики, предлагающие полисы, должны делать это осторожно — они не хотят быть уничтоженными». ***(Lucy Papachristou. Insurer Spots Cybersecurity Weakness With Model Simulating Catastrophic Attacks // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2023-03-20/cyber-insurer-unveils-model-to-simulate-worst-case-cyberattack). 20.03.2023).***

***

«Польща знову стала об'єктом кібератак із боку росії. Як повідомив уповноважений уряду Польщі з питань безпеки у кіберпросторі Януш Цешинський, 28 лютого російські хакери атакували сайт податкової адміністрації Польщі Podatki.gov.pl. Цешинський наголосив, що хакери не змогли викрасти дані платників податків.

Кібератака полягала у генеруванні значного штучного трафіку на сайті, що призвело до блокування його роботи. Цешинський також зазначив, що Польща є одним із об'єктів росії, що часто атакуються, і кількість кібератак на Польщу зросла в п'ять разів з початку повномасштабного вторгнення росії в Україну.

Цешинський заявив, що росія несе відповідальність за цю атаку, і Польща має інформацію, яка вказує на причетність російських хакерів до неї. Водночас він наголосив, що блокування сайту не означає загрози безпеці даних платників податків.

Цей випадок є черговим нагадуванням про необхідність підвищення кібербезпеки та пильності в Інтернеті. Організації та держави повинні бути готові до можливих кібератак та вживати відповідних заходів для захисту своїх систем та даних». ***(TATIANA TKACHENKO. Російські хакери атакували сайт податкової адміністрації Польщі // myc.news (https://myc.news/ua/proishestvie/rossijskie_hakery_atakovali_sajt_nalogovoj_administracii_polshi). 01.03.2023).***

***

«Немецкий производитель оружия Rheinmetall, базирующаяся в Дюссельдорфе, только что была включена в ведущий немецкий фондовый индекс Dax, а через несколько дней стала целью российской кибератаки.

Отмечается, что атака имела лишь незначительные последствия: веб-сайт группы, управляемый внешним поставщиком услуг, был временно недоступен, сообщил представитель концерна.

Нет никаких указаний на то, что утечка могла повлиять на внутреннюю IT-инфраструктуру Rheinmetall, и, вероятно, не было никакого финансового ущерба.

Ответственность за атаку взяла на себя кремлевская группировка Killnet.

Отметим, что кибератака была совершена на фоне сообщений о планах концерна построить танковый завод в Украине…». ***(Хакеры из РФ атаковали немецкого производителя оружия Rheinmetall // Информационное агентство GuildHall (https://ghall.com.ua/2023/03/07/hakery-iz-rf-atakovali-nemetskogo-proizvoditelya-oruzhiya-rheinmetall/).07.03.2023).***

***

Створення та функціонування кібервійськ

«На прошлой неделе два тревожных инцидента всколыхнули киберморе, один иностранный и один внутренний. Оба они подкрепляют доводы — которые уже были убедительными и которые я приводил уже почти десятилетие — в пользу создания Киберсилы США.

Первым инцидентом стала очередная кибератака Ирана на члена НАТО Албанию. Это было частью продолжающейся иранской кампании по нападению на Албанию, небольшую мусульманскую страну с населением всего около трех миллионов человек на Балканах. Атаки включали в себя обнуление личных банковских счетов, разоблачение правительственных и полицейских осведомителей и деградацию командно-контрольных сетей. Иран совершает нападения, потому что Албания не преследует антииранскую группировку моджахедов Халек, которая широко представлена в Албании.

Это нападение подняло вопрос о том, следует ли ссылаться на Статью 5 НАТО, в которой говорится, что нападение на одну страну будет рассматриваться как нападение на все. Поскольку договор НАТО был составлен много десятилетий назад, в нем не говорится, приводит ли кибератака в действие статью 5. Но, учитывая эволюцию ведения войны и расширение кибероперацій, такие атаки теперь должны подпадать под эту категорию.

Второй инцидент связан с атакой программы-вымогателя на Службу маршалов США. Было скомпрометировано огромное количество конфиденциальных данных, в том числе информация о беглецах, лицах с высоким уровнем безопасности и операциях правоохранительных органов. Атака была признана «крупным инцидентом», требующим серьезного межведомственного расследования и устранения последствий.

По иронии судьбы, на прошлой неделе Джен Истерли, директор Агентства кибербезопасности и безопасности инфраструктуры США, опубликовала Национальную стратегию кибербезопасности, над которой работали уже много месяцев.

Когда я был главнокомандующим ОВС НАТО в НАТО, альянс создал небольшой центр передового опыта в Таллине, Эстония, для координации кибервозможностей НАТО. С тех пор его значение возросло. Поскольку я наблюдаю, как уровень киберугроз продолжает расти в геометрической прогрессии — в соответствии с огромным всплеском устройств, подключенных к «интернету вещей», число которых превышает 50 миллиардов, — я беспокоюсь о том, как защитить кибератривы Америки и американцев.

У США есть очень компетентные вооруженные силы, которые защищают нас круглосуточно и без выходных: армия, флот, корпус морской пехоты, военно-воздушные и космические силы в составе Министерства обороны, а также Береговая охрана в составе Министерства внутренней безопасности. Киберсила США теперь также необходима.

Успешное создание Космических сил США три года назад дает хороший план для кибервойск США. В то время как силы составляют крошечную часть остальной части Министерства обороны, имея менее 10 000 военнослужащих, они управляют почти 100 космическими кораблями и сложной глобальной сетью, которая поддерживает спутниковые системы США.

Что наиболее важно, создание Кибервойска США выведет Америку за рамки нынешнего подхода к кибербезопасности в виде «группы захвата», при котором в

каждой вооруженной силе имеется небольшое количество киберэкспертов (большинство из рабочих мест).

Создание чуть более десяти лет назад Киберкомандования США значительно улучшило национальную безопасность Америки. Расположенный в Форт-Мид, штат Мэриленд, с Агентством национальной безопасности, его возглавляет четырехзвездочный офицер в форме. Многие из ветеранов Киберкомандования США составят ядро новой Киберсилы США. Киберсила также позволила бы иметь независимый голос в советах Объединенного комитета начальников штабов, как это обеспечивает начальник космических операций Космических сил США.

Поскольку США смотрят в будущее, которое включает в себя не только киберконкуренцию великих держав со стороны России и Китая, но и кибератаки среднего уровня со стороны таких стран, как Иран и Северная Корея, время близко. Нация должна двигаться вперед с помощью специальных киберсил США». ***(James Stavridis. U.S. military needs to create a dedicated cyber force // MediaNews Group (https://www.greeleytribune.com/2023/03/11/opinion-u-s-military-needs-to-create-a-dedicated-cyber-force/). 11.03.2023).***

***

Кіберзахист критичної інфраструктури

«7 марта 2023 года Управление транспортной безопасности (TSA) объявило о выпуске в экстренном порядке поправки о кибербезопасности к программам безопасности некоторых аэропортов и операторов самолетов, регулируемых TSA, в рамках инициатив Министерства внутренней безопасности США. для повышения кибербезопасности критической инфраструктуры США.

Поправка требует, чтобы затронутые организации, регулируемые TSA, разработали утвержденный план реализации, в котором описаны меры, которые организации принимают для повышения своей устойчивости к кибербезопасности и предотвращения возможных сбоев или деградации своей инфраструктуры. Эти

организации, регулируемые TSA, также должны активно оценивать эффективность этих мер путем:

Разработка политик сегментации сети и средств контроля для обеспечения того, чтобы системы операционных технологий могли продолжать безопасно работать в случае компрометации системы информационных технологий, и наоборот;

Создание мер контроля доступа для защиты и предотвращения несанкционированного доступа к критически важным киберсистемам;

Внедрение политик и процедур непрерывного мониторинга и обнаружения для защиты, обнаружения и реагирования на угрозы и аномалии кибербезопасности, которые влияют на критически важные операции киберсистемы; и

Снижение риска эксплуатации незащищенных систем за счет своевременного применения исправлений и обновлений безопасности для операционных систем, приложений, драйверов и микропрограмм на критически важных киберсистемах с использованием методологии, основанной на оценке рисков.

Поправка последовала за объявлением Белым домом Национальной стратегии кибербезопасности от 2 марта 2023 года и директивой TSA от октября 2022 года о повышении кибербезопасности для пассажирских и грузовых железнодорожных перевозчиков». ***(TSA Announces New Cybersecurity Requirements for Airport and Aircraft Operators // National Law Forum, LLC (https://www.natlawreview.com/article/tsa-announces-new-cybersecurity-requirements-airport-and-aircraft-operators). 09.03.2023).***

***

«…Для критически важных инфраструктурных организаций создание стратегии безопасности, которая работает как с точки зрения операционных технологий (OT), так и с точки зрения потребительских данных, не так проста, как во многих других отраслях. Безопасное хранение этих данных при внедрении

новейших технологий оказалось серьезной проблемой во всем секторе, а это означает, что услуги, предоставляемые этими компаниями, затруднены.

Эти опасения не позволили ряд технологий быстро или вообще интегрировать. Эти технологии включают в себя проекты по возобновляемым источникам энергии, технологии электромобилей, непредвиденные обстоятельства, связанные со стихийными бедствиями, и переход к более интеллектуальным сетевым решениям для замены устаревшей инфраструктуры.

Старые операционные технологии становится трудно обновлять и достаточно защищать, а использование стороннего программного обеспечения также снижает уровень контроля организаций над своими данными. В дополнение к этому отсутствие автоматизации увеличивает вероятность человеческой ошибки, что может открыть возможности для киберпреступников. Это серьезная проблема, в частности, в финансовой отрасли, где обычные потребители в настоящее время очень подвержены банковскому мошенничеству.

Строгие правила также создают множество препятствий для соблюдения требований, которые необходимо преодолеть компаниям инфраструктуры коммунальных услуг. Это означает, что они должны посвящать много времени и ресурсов тому, чтобы обеспечивать и поддерживать соответствие требованиям, а также соблюдать и отчитываться по всем аспектам своей деятельности. Эти требования теперь включают отчеты, связанные с кибербезопасностью, такие как Закон об отчетах о кибер-инцидентах для критически важной инфраструктуры от 2022 года (CIRCIA).

Три способа, которыми поставщики критически важной инфраструктуры могут защитить данные

К счастью, существуют решения проблем, с которыми сталкивается сектор критической инфраструктуры, с тремя ключевыми мерами, которые могут помочь защитить данные компаний и потребителей. Эти шаги обеспечивают комплексное решение, охватывающее операционные технологии и хранилище данных, с использованием аналитики в реальном времени, чтобы помочь организациям принять современный подход.

1. Демилитаризованные зоны (ДМЗ)

Создание демилитаризованных зон (DMZ) может способствовать лучшей сегментации сети, обеспечивая более надежную работу и создавая дополнительный уровень безопасности. Для коммунальных предприятий это означает разделение ИТ-среды и среды ОТ, что усложняет жизнь киберпреступникам.

Эта сегментация означает, что многие традиционные методы атак не смогут взломать ИТ-систему, а злоумышленник не сможет получить доступ к оперативным данным. Еще одним преимуществом разделения систем ИТ и ОТ является создание более управляемой и упрощенной сети. Беспорядочные и сложные сети увеличивают поверхность атаки и могут привести к появлению большего количества уязвимостей, которые может быть трудно обнаружить внутри.

Однако даже при наличии демилитаризованной зоны сеть все еще может подвергаться риску более изощренных кибератак. Вот почему необходимы регулярное тестирование и постоянный мониторинг, а также стратегия реагирования на инциденты в случае атаки. Наличие тщательных процедур может помочь свести к минимуму время простоя и остановить злоумышленника, прежде чем он сможет нанести какой-либо долгосрочный ущерб.

2. Уменьшите вероятность человеческой ошибки

Защита от киберпреступности — это не просто внедрение передовых систем и использование современных инструментов. Это может быть так же просто, как обеспечить лучшее образование для сотрудников и потребителей. Сведение к минимуму вероятности человеческой ошибки — один из наиболее эффективных способов защиты операций и данных критически важных инфраструктурных организаций.

Продвижение культуры кибербезопасности является основной целью во всех отраслях в ближайшие годы, повышая осведомленность о выявлении мошенничества и потенциальных угроз и обеспечивая соблюдение сотрудниками передовых методов для обеспечения безопасности данных.

Наряду с лучшим обучением и документацией для сотрудников, эффективными маркетинговыми материалами и легкодоступными ресурсами для потребителей, необходимо также эффективно управлять доступом пользователей. Также рекомендуются такие меры, как многофакторная аутентификация и ограничение доступа к системе на основе ролей пользователей.

Также необходимо внедрить процедуры внутреннего аудита для регистрации всех пользователей, подключенных устройств, систем, установленного программного обеспечения и многого другого, помогая группам безопасности отслеживать сетевую архитектуру для проверки на наличие уязвимостей. Это должно сочетаться с обнаружением конечных точек и реагированием, брандмауэром, VPN, антивирусным и антивредоносным программным обеспечением и фильтрами спама.

3. Настройте дополнительные уровни безопасности

Многие крупные организации в настоящее время перешли к политике нулевого доверия, которая реализует дополнительные меры безопасности и дополнительную проверку для повышения безопасности сетей. Нулевое доверие работает, предполагая, что никаким пользователям, внутренним или внешним, нельзя доверять доступ к сети без проверки. Таким образом, пользователи могут получить доступ только к тем областям сети, которые им необходимы для выполнения их роли.

Протоколы проверки также могут управлять тем, какие пользователи, устройства и приложения могут получить доступ к сети и конкретным системам. Этот уровень контроля может значительно уменьшить уязвимость сети, предотвращая доступ злоумышленников к областям сети, где хранятся ценные данные. Пользователи высокого уровня с полным доступом также должны соблюдать рекомендации по безопасности, чтобы их учетные данные для входа не попали в чужие руки.

Настоятельно рекомендуется стороннее тестирование на проникновение, чтобы взять на себя роль потенциального злоумышленника, выявляя уязвимости, которые могут быть пропущены внутренней командой по кибербезопасности. В то

же время данные и активы, которые считаются вероятными целями для киберпреступников, должны быть зашифрованы и снабжены дополнительными уровнями защиты, такими как двухфакторная аутентификация.

Кибербезопасность и критическая инфраструктура – Заключение

Отрасль критической инфраструктуры страдает от слишком многих проблем с кибербезопасностью, в первую очередь от того, как внедрение современных инструментов может поставить под угрозу данные. Из-за этого многие крупные организации в США продолжали использовать устаревшие системы, откладывая модернизацию своей деятельности.

К счастью, лучшая кибербезопасность может позволить организациям внедрять новые технологии и системы для предоставления более качественных и устойчивых услуг. Конечно, это, вероятно, потребует значительных инвестиций, но долгосрочная отдача и снижение затрат для потребителя окупятся.

Аналитика данных в режиме реального времени является одной из ключевых проблем, связанных с конфиденциальностью данных, но при наличии эффективных мер критически важная инфраструктура станет более надежной и надежной, обеспечивая удовлетворение спроса на услуги, электроэнергию и воду». ***(Nahla Davies. How Cybersecurity Delays Critical Infrastructure Modernization // Techstrong Group (https://securityboulevard.com/2023/03/how-cybersecurity-delays-critical-infrastructure-modernization/amp/). 14.03.2023).***

***

«Проблемы кибербезопасности, безусловно, находятся в центре внимания судовладельцев и операторов. Нарушения кибербезопасности могут проникать в системы на борту и на берегу и могут поставить под угрозу безопасность и негативно повлиять на морские операции, а также нарушить распределение товаров на борту. В этом свете крайне важно, чтобы судовладельцы и операторы разработали жесткие планы смягчения последствий, обнаружения и реагирования.

По мере оцифровки судов и модернизации автономных систем кибератаки и попытки программ-вымогателей становятся все более распространенными. Программа-вымогатель определяется как тип вредоносного программного обеспечения, предназначенного для блокировки доступа к компьютерной системе до тех пор, пока атакуемая сторона не заплатит определенную сумму денег. Киберпреступники монетизируют свои операции, вымогая деньги у своих жертв, и могут в дальнейшем продавать извлеченные данные. Кибер-злоумышленники обычно ищут максимально возможную выплату и нацелены на компании и отрасли, включая морской сектор, которые полагаются на срочные данные для работы. Такие атаки могут иметь разрушительные одновременные последствия для нескольких игроков.

Во время инцидента с вредоносным ПО NotPetya в 2017 году злоумышленники зашифровали системы Maersk и потребовали оплаты. «Не имея доступа к данным, хранящимся в его разрушенной компьютерной системе, Maersk буквально не знал, что находится в его контейнерах. Персоналу на местах приходилось проверять вручную, а срочные лекарства вызывали особую озабоченность в цепочке поставок». Злоумышленники отключили системы за семь минут, но реакция и осознание отраслью необходимости защиты длились гораздо дольше. «Ключевой урок, который Maersk извлекла из борьбы с атакой NotPetya: защита важна, но не менее важно обеспечить надежный процесс восстановления».

Примечательно, что 6 мая 2021 года инцидент с Colonial Pipeline попал в заголовки газет, когда эта компания заплатила 4,4 миллиона долларов в качестве выкупа после того, как крупный поставщик нефти не смог получить доступ или контролировать свои ИТ-системы, которые повлияли на 45 процентов топлива, поставляемого на Восточное побережье. Кроме того, в 2021 году южноафриканский портовый оператор Transnet объявил о форс-мажорных обстоятельствах после того, как атака программы-вымогателя остановила его ИТ-системы и нарушила контейнерные операции в ряде его портов, включая Дурбан, Кейптаун и Порт-Элизабет. В феврале 2022 года порты в Германии, Бельгии и Нидерландах пострадали от атаки программы-вымогателя, которая задержала

работу нефтяных терминалов и нанесла ущерб портовым системам. Паромный оператор в штате Массачусетс, Управление пароходства, также стал мишенью изнурительной атаки программ-вымогателей, которая отразилась на его операциях, обеспечивающих транспортную линию на острова Нантакет и Мартас-Винъярд, сбое веб-сайта компании, остановке бронирования транспортных средств и отключении системы внутренних коммуникаций. Совсем недавно, 7 января 2023 года, серверы DNV ShipManager стали жертвами кибератаки программы-вымогателя. Пострадали около 70 клиентов, эксплуатирующих около 1000 судов.

Есть множество других примеров атак программ-вымогателей; однако не все случаи предаются гласности. В некоторых случаях об атаках программ-вымогателей не сообщается, и компании предпочитают платить злоумышленникам деньги, не обращаясь за помощью к правительству. По оценкам Министерства финансов США, в 2021 году злоумышленникам-вымогателям было выплачено 1,2 миллиарда долларов. К сожалению, более чем в 35% случаев, когда деньги были выплачены, злоумышленники не восстанавливали данные или воздерживались от повторной атаки в будущем. Управление по контролю за иностранными активами («OFAC») предупредило, что выплата выкупа может представлять собой нарушение законов об экономических санкциях, представлять угрозу национальной безопасности и способствовать будущим нападениям. Правительство США продолжает обращать внимание на требование сообщать об атаках программ-вымогателей. В марте 2022 года президент Байден подписал Закон об отчетности о кибер-инцидентах в отношении критически важной инфраструктуры. Закон требует от компаний, обеспечивающих работу критической инфраструктуры страны, сообщать CISA о «существенных» кибер-инцидентах в течение семидесяти двух (72) часов и сообщать о платежах, произведенных за атаки программ-вымогателей, в течение 24 часов. Инциденты также могут быть добровольными. Об этом сообщили в Агентстве кибербезопасности и безопасности инфраструктуры (CISA). Это американское агентство работает с партнерами для защиты от киберугроз и сотрудничает с партнерами для создания более безопасной и отказоустойчивой инфраструктуры.

В июле 2021 года президент Байден подписал Меморандум о национальной безопасности о повышении кибербезопасности для систем управления критически важной инфраструктурой. Этот меморандум требовал от Агентства по кибербезопасности и безопасности инфраструктуры в сотрудничестве с Национальным институтом стандартов и технологий и межведомственным сообществом разработки базовых показателей эффективности кибербезопасности, которые были бы согласованными во всех критических секторах инфраструктуры. Эти цели включают рекомендуемые действия по обеспечению безопасности учетных записей и устройств, безопасности данных, управлению и обучению, управлению уязвимостями, цепочке поставок/третьим сторонам, а также реагированию и восстановлению. Правительство также запустило StopRansomware.gov, чтобы предоставить ресурсы для более эффективной борьбы с программами-вымогателями.

Портовые агентства еще больше подчеркивают важность кибербезопасности. В январе 2022 года в порту Лос-Анджелеса дебютировал Центр киберустойчивости, решение для киберзащиты, созданное для повышения готовности порта к кибербезопасности, позволяющее заинтересованным сторонам автоматически обмениваться индикаторами киберугроз и потенциальными мерами защиты друг с другом.

Судовладельцы и операторы должны, выявлять их и реагировать готовиться к киберинцидентам на них. Согласно данным анализа IBM Security Cost of a Data Breach Report 2022, составленного Ponemon Institute, средняя стоимость атаки программы-вымогателя без учета самого выкупа составляет 4,54 миллиона долларов. Кроме того, в отчете указано, что средняя экономия, связанная с группой реагирования на инциденты и регулярно тестируемыми планами реагирования на инциденты, составляет 2,66 миллиона долларов.

Важно не только разработать планы кибербезопасности, но и получить консультации на протяжении всего периода реагирования на инциденты и восстановления, включая, помимо прочего, помощь во внедрении и поддержании необходимых мер безопасности данных, таких как письменные программы

информационной безопасности для соблюдения законов о безопасности данных и консультирование. об уведомлениях об утечке данных затронутым лицам и соответствующему государственному/регулирующему органу. Компании могут снизить киберриски, проводя ежегодную оценку рисков и обучение по повышению осведомленности, внедряя стратегические инвестиции в ИТ, анализируя обязательства руководства поставщиков по обеспечению безопасности и оценивая страховое покрытие. Если кибер-инцидент действительно произошел, первые 24 часа имеют решающее значение для расследования нарушения, включая определение характера нарушения, категорий скомпрометированной информации, количества затронутых лиц, причины взлома и вероятных последствий. нарушение и риски для затронутых лиц, а также немедленно приступить к исправлению. Следует следовать плану реагирования компании на инциденты и уведомлять соответствующие заинтересованные стороны внутри и за пределами компании (например, главный юрисконсульт, совет директоров компании, отдел внутренних коммуникаций, страховые брокеры, государственные регулирующие органы и затронутые лица). Опытный консультант также может помочь с уведомлениями, которые требуются в соответствии с нормативными требованиями и контрактами, а также помочь составить проекты положений о безопасности, конфиденциальности и возмещении убытков в контрактах с поставщиками и при приобретениях, чтобы гарантировать, что все стороны сотрудничают в снижении рисков кибербезопасности. В этой сфере заблаговременное планирование и надлежащее выполнение этих планов является ключом к преодолению шторма кибербезопасности». ***(Vanessa C. DiDomenico, Sharon R. Klein, Karen H. Shin. Maritime Ransomware // Blank Rome LLP (https://www.blankrome.com/publications/maritime-ransomware). 03.2023).***

***

«Згідно зі звітом дослідників кібербезпеки з Microsoft, найбільше російське хакерське угруповування KillNet з листопада 2022 року збільшило кількість своїх DDoS-атак на організації охорони здоров'я втричі. Учасники групи мережевої безпеки Microsoft Azure Амір Дахан та Сайєд Паша опублікували аналіз DDoS-атак, відстеживши їх з 18 листопада 2022 по 17 лютого 2023.

За словами спеціалістів Microsoft Azure, кількість атак збільшилась з 10−20 в день у листопаді до 40-60 атак щодня в лютому. Типи організацій охорони здоров'я, які атакують хакери:

фармацевтичні компанії - 31% усіх атак;

лікарні - 26%;

медичне страхування — 16%;

медичні послуги — 16%;

громадська охорона здоров'я — 8%;

біотехнології - 3%.

Дослідники заявили, що KillNet і пов'язані з нею кіберзлочинці використовують DDoS-атаки як найпоширенішу тактику. Використовуючи DDoS-скрипти, ботнети та підроблені джерела атак, KillNet може легко атакувати практично будь-який сайт…» ***(Microsoft: найбільше російське хакерське угруповування збільшило кількість кібератак втричі // No worries! (https://noworries.news/microsoft-najbilshe-rosijske-hakerske-ugrupovuvannya-zbilshylo-kilkist-kiberatak-vtrychi/). 20.03.2023).***

***

Захист персональних даних та соціальні мережі

«Американский телекоммуникационный гигант AT&T предупредил миллионы своих пользователей, что некоторые из их конфиденциальных

данных (opens in new tab) были раскрыты в результате киберинцидента в цепочке поставок.

Согласно отчету BleepingComputer, утечка данных является результатом инцидента со взломом поставщика маркетинговых услуг AT&T, который произошел в январе 2023 года.

Теперь компания разослала предупреждения примерно девяти миллионам своих клиентов о том, что некоторые из их конфиденциальных данных были получены несанкционированным третьим лицом.

«Была раскрыта информация о частной сети клиента из некоторых учетных записей беспроводной связи, например, количество линий в учетной записи или тарифный план беспроводной связи», — сообщила изданию AT&T. «Информация не содержала данные кредитной карты, номера социального страхования, пароли учетных записей или другую конфиденциальную личную информацию. Мы уведомляем пострадавших клиентов».

В уведомлении не указывалось, сколько именно людей пострадало от взлома, но компания сообщила СМИ, что «9 миллионов беспроводных учетных записей» были скомпрометированы.

Компания добавила, что были раскрыты имена клиентов, номера учетных записей беспроводных сетей, номера беспроводных телефонов, а также адреса электронной почты.

«Небольшой процент пострадавших клиентов также имел доступ к названию тарифного плана, просроченной сумме, сумме ежемесячного платежа, различным ежемесячным платежам и / или использованным минутам. Информация была старой несколько лет», — далее заявила AT&T.

Компания подтвердила, что это была атака на цепочку поставок и что ее системы остаются нескомпрометированными. Кроме того, Ти добавил, что полученные данные в основном связаны с правом на обновление устройства. Как бы то ни было, компания уведомила полицию о случившемся.

«Мы уведомили федеральные правоохранительные органы о несанкционированном доступе к вашему CPNI в соответствии с требованиями

Федеральной комиссии по связи», — сообщила компания своим клиентам. «Наш отчет правоохранительным органам не содержит конкретной информации о вашей учетной записи, только то, что произошел несанкционированный доступ». ***(Sead Fadilpašić. AT&T alerts millions of customers following major data breach // Future US, Inc (https://www.techradar.com/news/atandt-alerts-millions-of-customers-that-it-suffered-a-data-breach). 10.03.2023).***

***

«Образец личной информации, относящейся к ряду членов Палаты представителей США, украденной в результате недавней утечки данных, был выставлен на продажу в Интернете.

Данные, взятые из систем поставщика медицинских услуг в Вашингтоне, округ Колумбия, который обслуживает федеральных законодателей и их семьи, как сообщается, уже были приобретены по крайней мере одним покупателем.

Огромный объем данных, которые были украдены и впоследствии просочились в сеть за последние несколько лет, побудил компаний-разработчиков программного обеспечения для кибербезопасности, таких как Surfshark, добавить в свои продукты инструменты мониторинга даркнета, чтобы пользователи могли сами проверить, была ли их информация раскрыта после атак.

Утечка данных попала в Конгресс

Ранее на этой неделе главный административный директор Палаты представителей США Кэтрин Л. Шпиндор подтвердила, что в DC HealthLink произошла «значительная утечка данных», в результате которой могла быть раскрыта «личная идентифицируемая информация» (PII) членов Конгресса, их семей и их сотрудников.

Шпиндор сказал, что истинные масштабы нарушения еще не раскрыты, и было мало дополнительной информации о характере PII. Всего от взлома может быть затронуто до 170 000 человек.

Хотя в настоящее время нет доказательств того, что какие-либо учетные записи были скомпрометированы, законодателям была предоставлена информация,

необходимая для замораживания семейного кредита в Equifax, Experian и Transunion.

Какие данные выставлены на продажу в Интернете?

Согласно Bleeping Computer, злоумышленник, известный как IntelBroker, пытался продать данные членов Палаты представителей на хакерском форуме в обмен на криптовалюту.

Наиболее конфиденциальная информация, выставленная на продажу, включает (но не ограничивается) рабочую и домашнюю электронную почту, домашние адреса, почтовые адреса, номера телефонов, номера социального страхования и информацию о плане медицинского обслуживания.

Злоумышленник утверждает, что им удалось получить эту информацию от Управления биржи медицинских пособий DC.gov. Они также опубликовали сообщения, которые предполагают, что у данных был по крайней мере один покупатель с тех пор, как они были выставлены на продажу.

Купило ли ФБР просочившиеся данные?

В совместном письме, написанном лидером Палаты представителей Кевином Маккарти и лидером меньшинства Хакимом Джеффрисом и адресованном Управлению биржи медицинских пособий округа Колумбия, они подтвердили, что ФБР успешно приобрело информацию в рамках операции.

Однако это только даст им лучшее представление о том, какая именно информация была утекла, поскольку у продавца будут копии наборов данных для продажи нескольким сторонам. В настоящее время остается неясным, было ли ФБР покупателем, на которого ссылался злоумышленник.

Также в письме Маккарти и Джеффрис говорят, что последствия взлома «могут быть экстраординарными» из-за огромного количества американских политиков, сотрудников и семей, которые пользовались услугами здравоохранения за последние 7 лет.

Зачем вам нужны инструменты для мониторинга даркнета

В 2023 году, когда методы взлома стали более изощренными, чем когда-либо прежде, даже самые безопасные и авторитетные организации рискуют столкнуться с утечкой данных.

Такие технологии, как менеджеры паролей, могут значительно снизить риск того, что ваши личные данные будут скомпрометированы в первую очередь, но если компания, в которой вы создали учетную запись или поделились личной информацией, пострадала от утечки данных, вы ничего не можете сделать, чтобы обратить это вспять.

Однако вы можете изменить свою информацию, и чем быстрее вы это сделаете, тем лучше. Вот почему такие инструменты, как Dark Web Monitor от Surfshark, который является частью их пакета Surfshark One, становятся все более популярными. Активно сканируя темную сеть на наличие ссылок на вашу личную информацию, вы сможете быстро отреагировать и сбросить все учетные данные своей учетной записи.

Если вы предпочитаете искать себя, такие веб-сайты, как haveibeenpwned.com, предоставляют вам возможность вручную искать любую вашу личную информацию. Любой из этих методов работает, но в 2023 году крайне важно, чтобы вы не отставали от него». ***(Aaron Drapkin. US House Members' Personal Information Is Up for Sale Online // Tech.co (https://tech.co/news/us-politician-data-for-sale). 10.03.2023).***

***

«Google One добавляет новую функцию кибер-наблюдения, которая позволит пользователям отслеживать темную сеть, чтобы увидеть, были ли их личные данные включены в утечку данных.

Новая функция, запущенная на этой неделе, будет доступна всем подписчикам Google One в США без дополнительной платы в рамках виртуальной персональной сети Google — VPN от Google One.

Google One VPN был запущен в конце 2020 года, но был ограничен подписчиками из США на Android с минимальным хранилищем 2 ТБ. С сегодняшнего дня виртуальная частная сеть будет доступна всем подписчикам Google One, а также пяти другим пользователям вашего плана Google One в 22 странах на Android, iOS, Windows и Mac.

Google One VPN, известная как «VPN от Google One», — это первая виртуальная частная сеть Google — мера безопасности, предназначенная для сокрытия IP-адреса пользователя, чтобы веб-сайты не собирали их данные, не отслеживали их местоположение и не контролировали их интернет-активность.

До вчерашнего объявления Google VPN был доступен только в планах Google One Premium 2 ТБ по годовой цене 99,99 долларов США. С сегодняшнего дня VPN будет доступен на всех тарифных планах Google One со 100 ГБ Basic по цене от 1,99 доллара США в месяц.

С ростом утечек данных и высокой конкуренцией на рынке VPN Google необходимо было расширить свое предложение, чтобы извлечь выгоду из растущего спроса. Поскольку 90% компаний обеспокоены устойчивостью к кибербезопасности, наблюдение в темной сети может быть функцией, которая нужна пользователям Google One, чтобы чувствовать себя более защищенными.

Как работает функция отчетов Google One VPN Dark Web?

Отчет о даркнете Google One VPN — это новая функция, которая позволит всем подходящим пользователям сканировать даркнет в поисках личных данных, чтобы проверить, не была ли их информация включена в утечку данных. Эта функция работает путем поиска личных данных в Интернете, таких как номера социального страхования, имя, адрес, адрес электронной почты и номера телефонов, и уведомления пользователя, если его данные были найдены.

По данным Google, когда пользователи впервые включают отчет темной сети, им необходимо будет выбрать и предоставить информацию, которую они хотели бы отслеживать, в своем «профиле мониторинга». Если какая-либо информация будет найдена в даркнете, пользователь будет уведомлен и получит рекомендации о том, как реагировать и наилучшим образом защитить свою информацию.

В дополнение к пометке личной информации даркнета, в отчете также будет показана связанная информация, которая может быть найдена при утечке данных. Хотя некоторые пользователи могут быть осторожны, Google гарантирует, что вся информация, введенная в профиль мониторинга, будет обрабатываться в соответствии с политикой конфиденциальности Google, что дает пользователям возможность удалить или прекратить мониторинг информации в своем профиле в любое время.

Стоит ли использовать Google One VPN?

Если вы являетесь подписчиком Google One в США, обновленная VPN станет долгожданным дополнением к вашему набору инструментов, но что касается VPN, Google One заслуживает такого же доверия, как и любая другая VPN на рынке. Тем не менее, теперь, когда VPN доступен с планами от 1,99 доллара в месяц, он, безусловно, будет одним из самых дешевых VPN.

Существует множество вариантов VPN. Согласно нашему исследованию, самым безопасным является NordVPN, но вы можете увидеть, как он сравнивается с другими ведущими провайдерами, в нашем руководстве по самым безопасным VPN в 2023 году, чтобы принять собственное решение». ***(Jade Artry. Google One VPN Scans Dark Web For Data Breaches // Tech.co (https://tech.co/news/google-one-dark-web-vpn-scan). 09.03.2023).***

***

«Бельгия запрещает использование TikTok на правительственных телефонах из-за опасений по поводу кибербезопасности, конфиденциальности и дезинформации, заявил в пятницу премьер-министр страны, отражая недавние действия других властей в Европе и США.

Согласно сообщению на веб-сайте Александра де Кроо, китайское приложение для обмена видео будет временно запрещено на устройствах, принадлежащих или оплачиваемых федеральным правительством Бельгии, в течение как минимум шести месяцев.

TikTok заявил, что «разочарован этой приостановкой, основанной на базовой дезинформации о нашей компании». Компания заявила, что «готова встретиться с официальными лицами для решения любых проблем и устранения неправильных представлений».

TikTok принадлежит китайской компании ByteDance, которая в 2020 году перенесла свою штаб-квартиру в Сингапур. Компания стремилась дистанцироваться от своих китайских корней, заявив, что ее материнская компания зарегистрирована за пределами Китая, и ее контрольный пакет принадлежит глобальным институциональным инвесторам.

Но Европейского союза три основных учреждения и министерство обороны Дании уже приказали сотрудникам удалить приложение с устройств, используемых в служебных целях. Подобные запреты были введены в Канаде и США.

Борьба за TikTok является частью более широкого глобального соперничества между Китаем и США и их западными союзниками за технологическое и экономическое превосходство.

Де Кроо сказал, что запрет Бельгии был основан на предупреждениях службы государственной безопасности и ее центра кибербезопасности, в которых говорилось, что приложение может собирать пользовательские данные и настраивать алгоритмы для манипулирования новостной лентой и контентом.

Они также предупредили, что TikTok может быть принужден к шпионажу в пользу Пекина, сказал он, не вдаваясь в подробности.

«Мы находимся в новом геополитическом контексте, когда влияние и слежка между государствами сместились в цифровой мир, — сказал де Кроо в онлайн-заявлении. — Мы не должны быть наивными: TikTok — китайская компания, которая сегодня обязана сотрудничать с спецслужбы. Это реальность. Запретить его использование на устройствах федеральных служб — это здравый смысл».

TikTok заявил, что пользовательские данные хранятся в США и Сингапуре, и указал на новые меры, призванные облегчить европейские опасения, путем хранения пользовательских данных в европейских центрах обработки данных.

«Правительство Китая не может заставить другую суверенную страну предоставлять данные, хранящиеся на территории этой страны», — говорится в заявлении компании». ***(Belgium Bans TikTok From Government Phones After US, EU // The Associated Press (https://www.usnews.com/news/business/articles/2023-03-10/belgium-bans-tiktok-from-government-phones-after-us-eu). 10.03.2023).***

***

«Ferrari стала жертвой кибератаки, когда хакер потребовал выкуп за данные клиентов итальянской фирмы.

Sky Sport Italy подтвердила новость о взломе в Ferrari, в ходе которого были украдены данные некоторых их клиентов, что служит координационным центром для этих требований о выкупе.

Ferrari проинформировала этих клиентов об атаке, но будет твердо противостоять хакеру и откажется платить какую-либо плату.

Говорят, что атака не оказала никакого влияния на повседневную работу Ferrari, поскольку их системы все еще работают в обычном режиме, системы, над которыми, по словам Ferrari, они работали с «экспертами», чтобы укрепить их в будущем.

На данный момент расследование начато совместно с «ведущей мировой компанией в области кибербезопасности», в котором также участвуют власти.

«В соответствии со своей корпоративной политикой Ferrari не примет никаких требований о выкупе, поскольку согласие на такие требования приведет к финансированию преступной деятельности и позволит исполнителям угроз увековечить свои атаки», — говорится в заявлении Ferrari, согласно Sky Sport Italy.

«Полагая, что лучший способ действий — проинформировать наших клиентов, мы уведомили наших клиентов о потенциальном раскрытии их данных и о характере события.

«Ferrari очень серьезно относится к вопросу конфиденциальности своих клиентов и понимает важность того, что произошло. Мы работали с экспертами для дальнейшего укрепления наших систем, в надежности которых мы уверены. Мы

также можем подтвердить, что нарушение не повлияло на деятельность нашей компании». ***(Jamie Woodhouse. Ferrari targeted by hackers with ransom demand for customer data // Planet Sport Limited (https://www.planetf1.com/news/ferrari-hacked-ransom-demand-customer-data/). 21.03.2023).***

***

«Злоумышленники наносят удары по предприятиям, главной целью которых является кража личных данных. Директора по информационной безопасности и директора по информационным технологиям сообщили VentureBeat, что в первые три месяца 2023 года они наблюдали всплеск атак с использованием личных данных.

Правильная идентификация является основой надежной системы нулевого доверия. Для этого требуется отказоустойчивость конечных точек, усовершенствованные методы сбора данных и анализа данных телеметрии, а также более быстрые инновации для защиты идентификационных данных.

Используя пробелы в облачной инфраструктуре для поиска слабых или незащищенных конечных точек, неудивительно, что количество атак на облачную инфраструктуру увеличилось на 95%, а количество попыток вторжения с участием облачных злоумышленников утроилось из года в год. Злоумышленники, от банд киберпреступников до финансируемых государством групп продвинутых постоянных угроз (APT), знают, что поражение только одной конечной точки открывает инфраструктуру организации для кражи учетных данных, личных данных и данных.

В отчете CrowdStrike о глобальных угрозах за 2023 год указано, почему личные данные находятся в осаде. Они являются одними из самых ценных активов организации, богатыми личными данными, которые имеют высокую цену в даркнете. Группа разведки CrowdStrike обнаружила тревожную тенденцию, когда злоумышленники становятся брокерами доступа, продавая украденные удостоверения оптом по высоким ценам в даркнете.

Используя пробелы в облачной инфраструктуре для поиска слабых или незащищенных конечных точек, неудивительно, что количество атак на облачную инфраструктуру увеличилось на 95%, а количество попыток вторжения с участием облачных злоумышленников утроилось из года в год. Злоумышленники, от банд киберпреступников до финансируемых государством групп продвинутых постоянных угроз (APT), знают, что поражение только одной конечной точки открывает инфраструктуру организации для кражи учетных данных, личных данных и данных.

В отчете CrowdStrike о глобальных угрозах за 2023 год указано, почему личные данные находятся в осаде. Они являются одними из самых ценных активов организации, богатыми личными данными, которые имеют высокую цену в даркнете. Группа разведки CrowdStrike обнаружила тревожную тенденцию, когда злоумышленники становятся брокерами доступа, продавая украденные удостоверения оптом по высоким ценам в даркнете.

Определение безопасности конечных точек в мире с нулевым доверием должно начинаться с понимания того, насколько быстро происходит сближение платформ защиты конечных точек и систем управления идентификацией. Конечные точки сети каждого предприятия имеют несколько цифровых удостоверений, начиная с тех, которые назначаются приложениями, платформами и внутренними системами, доступ к которым осуществляется с конечной точки, до удостоверения устройства.

Облачные сервисы вынуждают совмещать платформы защиты конечных точек и управление идентификацией. Например, служба приложений Microsoft Azure поддерживает назначение нескольких назначенных пользователем удостоверений конкретному приложению, что усложняет диапазон удостоверений, поддерживаемых конечными точками. То же самое относится и к устройствам. Cisco Identity Services Engine (ISE) может определять группы идентификации конечных точек по их авторизации. Эти сервисы отражают то, что быстро происходит на рынке — удостоверения быстро становятся основой конечных точек.

Директорам по информационной безопасности необходимо лучше видеть каждую идентификацию конечной точки. Необходимы фреймворки с нулевым доверием и установка на доступ с минимальными привилегиями…

Это важно для создания надежной и масштабируемой инфраструктуры с нулевым доверием, а данные телеметрии бесценны для выявления потенциальных попыток вторжения и взлома. Цель состоит в том, чтобы контролировать, проверять и отслеживать транзакции данных каждой конечной точки в режиме реального времени, чтобы помочь идентифицировать и реагировать на потенциальные угрозы. Ведущие поставщики, предоставляющие эту возможность, включают Cisco SecureX, Duo и Identity Services Engine (ISE); а также Microsoft Azure Active Directory и Defender. Платформа Falcon от CrowdStrike, Identity Cloud от Okta и решение Prisma Access от Palo Alto Networks также сегодня являются поставщиками, обеспечивающими непрерывный мониторинг для корпоративных клиентов.

Общеизвестно, что злоумышленники сканируют каждый потенциально открытый порт и конечную точку предприятия, надеясь, что хотя бы одна из них окажется незащищенной или неправильно настроенной. Отчет Absolute Software о рисках конечных точек за 2021 год показал, что чрезмерно настроенные конечные точки так же уязвимы, как и отсутствие какой-либо защиты конечных точек. Исследование Absolute выявило 11,7 элементов управления безопасностью на устройство, причем большинство из них содержит несколько элементов управления для одной и той же функции.

Самовосстанавливающиеся конечные точки помогают уменьшить разрастание программных агентов, обеспечивая большую отказоустойчивость. Самовосстанавливающаяся конечная точка по определению отключится и проверит свои основные компоненты, начиная с ОС. Затем конечная точка выполнит исправление версий, а затем сбросит себя до оптимизированной конфигурации без вмешательства человека.

Absolute Software, Akamai, Ivanti, Malwarebytes, Microsoft, SentinelOne, Tanium, Trend Micro и многие другие имеют конечные точки, способные к

автономному самовосстановлению. Программное обеспечение Absolute заслуживает внимания тем, что обеспечивает неразрывную цифровую привязку к каждой конечной точке на базе ПК, которая постоянно отслеживает и проверяет запросы данных и транзакции каждой конечной точки в режиме реального времени.

Платформа Absolute Resilience примечательна тем, что обеспечивает видимость и контроль любого устройства в режиме реального времени, независимо от того, подключено оно к сети или нет, а также предоставляет подробные данные об управлении активами. Компания Absolute также изобрела и запустила первую в отрасли самовосстанавливающуюся платформу с нулевым доверием, предназначенную для управления активами, контроля устройств и приложений, аналитики конечных точек, отчетности об инцидентах, отказоустойчивости и соответствия требованиям.

Защищенные, самовосстанавливающиеся конечные точки становятся незаменимыми для ИТ, ITSM и специалистов по безопасности, которые сегодня сталкиваются с хронической нехваткой времени. «Возможности управления конечными точками и самовосстановления позволяют ИТ-командам обнаруживать каждое устройство в своей сети, а затем управлять каждым устройством и обеспечивать его безопасность с использованием передовых современных методов, обеспечивающих продуктивность работы конечных пользователей и безопасность ресурсов компании», — сказал Сринивас Муккамала, директор по продукту Ivanti, во время недавнего интервью VentureBeat.

Он продолжил, сказав: «Автоматизация и самовосстановление повышают производительность сотрудников, упрощают управление устройствами и улучшают состояние безопасности, обеспечивая полную видимость всего имущества организации и обеспечивая автоматизацию для широкого спектра устройств».

Директора по информационной безопасности говорят, что их команды настолько перегружены рабочими нагрузками, направленными на защиту сотрудников, систем, а на производстве и целых заводов, что не хватает времени на управление исправлениями. Опрос Ivanti по управлению исправлениями показал,

что 71% ИТ-специалистов и специалистов по безопасности считают, что установка исправлений слишком сложна и требует много времени, а 53% заявили, что организация и приоритизация критических уязвимостей занимает большую часть их времени.

Учитывая важность правильного управления исправлениями, может помочь подход, основанный на данных. Еще одна инновация, которую несколько поставщиков используют для решения этой проблемы, — это искусственный интеллект (ИИ) и машинное обучение (МО).

Платформа Ivanti Neurons 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 заслуживает внимания тем, что их платформа 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.

Дополнительные поставщики, предлагающие автоматизированные решения для управления исправлениями, включают Broadcom, CrowdStrike, SentinelOne, McAfee, Sophos, Trend Micro, VMWare Carbon Black и Cybereason.

Наличие бреши в мышлении является ключом к тому, чтобы стать сильнее при нулевом доверии. Предположение о том, что попытки вторжений и взломов неизбежны, является сильным мотиватором для ИТ-специалистов и специалистов по кибербезопасности оттачивать свои стратегии, навыки и знания в области безопасности с нулевым доверием. Цель состоит в том, чтобы сделать нулевое доверие неотъемлемой частью мышечной памяти организации.

Лучший способ добиться этого — принять решение привести в форму инициативы и стратегии нулевого доверия. Это включает в себя внедрение микросегментации — важнейшего компонента нулевого доверия, как указано в

структуре нулевого доверия NIST. Микросегментация делит сети на более мелкие изолированные сегменты, уменьшая поверхность атаки сети и повышая безопасность данных и ресурсов.

Некоторые поставщики микросегментации также могут быстро выявлять и изолировать подозрительную активность в своих сетях. Из множества провайдеров микросегментации сегодня самыми инновационными являются Airgap, AlgoSec, ColorTokens, Illumio, Prisma Cloud и Zscaler Cloud Platform.

Из них платформа изоляции с нулевым доверием Airgap использует подход микросегментации, который рассматривает каждую конечную точку удостоверения как отдельный объект и применяет детализированные политики на основе контекстной информации, эффективно предотвращая любые боковые перемещения. Архитектура AirGap включает в себя автономную сеть политик, которая мгновенно масштабирует политики микросегментации по всей сети.

2023 год становится гораздо более сложным, чем ожидали директора по информационной безопасности и их команды. Пиковые атаки и более сложные попытки фишинга и социальной инженерии, созданные с помощью ChatGPT, создают нагрузку на и без того перегруженные ИТ-отделы и службы безопасности. В то же время директора по информационной безопасности сталкиваются с бюджетными ограничениями и заказами на консолидацию своих технологических стеков. На этом фоне более жестких бюджетов и большего количества нарушений многие начинают с повышения отказоустойчивости конечных точек…» ***(Louis Columbus. Defining endpoint security in a zero-trust world // VentureBeat (https://venturebeat.com/security/defining-endpoint-security-in-a-zero-trust-world/). 20.03.2023).***

***

«Согласно сообщениям, парламент Великобритании последовал примеру правительства, запретив TikTok на официальных устройствах, и пошел еще дальше, запретив пользователям доступ к приложению социальной сети из своей сети.

Эта новость последовала за аналогичными решениями правительств США, Канады, Бельгии и Европейской комиссии.

«После решения правительства запретить TikTok на правительственных устройствах комиссии Палаты общин и лордов решили, что TikTok будет заблокирован на всех парламентских устройствах и в более широкой парламентской сети», — сообщил представитель парламента.

«Кибербезопасность является главным приоритетом для парламента. Однако мы не комментируем конкретные детали наших средств контроля кибер- или физической безопасности, политик или инцидентов».

Тем не менее, члены по-прежнему смогут получить доступ к приложению для социальных сетей на своих личных устройствах, используя мобильное подключение к Интернету в Палате общин и лордов.

Сообщается, что представитель TikTok назвал это решение «ошибочным и основанным на фундаментальных заблуждениях о нашей компании».

Это нанесло еще один удар по репутации приложения после того, как на этой неделе его генеральный директор Шоу Зи Чу предстал перед комитетом Конгресса, чтобы встретиться с законодателями США.

В основе их беспокойства лежат две основные проблемы: любые данные, собранные приложением, в конечном итоге могут быть доступны китайскому государству; и что Пекин может оказать неправомерное влияние на алгоритм TikTok, чтобы использовать его в качестве инструмента пропаганды де-факто.

В прошлом году Ofcom заявил, что это приложение стало самым быстрорастущим источником новостей для взрослых в Великобритании.

TikTok заявил, что пытается развеять опасения по поводу безопасности данных, «храня данные пользователей из Великобритании в наших европейских центрах обработки данных и ужесточая контроль доступа к данным, включая независимый надзор третьих сторон за нашим подходом».

Однако еще в ноябре прошлого года TikTok признал, что сотрудники в Китае могут получать доступ к данным европейских пользователей для определенных целей.

Фирма также была отмечена регуляторами. Управление комиссара по информации (ICO) в сентябре прошлого года объявило о своем намерении оштрафовать TikTok на 27 миллионов фунтов стерлингов (33 миллиона долларов США) за нарушение законов о защите данных, включая обработку данных детей в возрасте до 13 лет без «надлежащего» согласия родителей». ***(Phil Muncaster. UK Parliament Bans TikTok from its Network and Devices // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/parliament-bans-tiktok-network/). 24.03.2023).***

***

«…Недавнее исследование взглядов потребителей на конфиденциальность и безопасность данных показало, что потребители более осторожно относятся к обмену данными. Большинство респондентов (87%) заявили, что не будут иметь дело с компаниями, у которых слабая безопасность. Участники исследования также оценили надежность в различных отраслях. Здравоохранение и финансовые услуги заняли более высокие места, чем другие отрасли, но ни одна из них не получила особенно высоких оценок. Надлежащая защита этих конфиденциальных данных имеет смысл для бизнеса. Именно здесь финансовый отдел организации может вмешаться, чтобы защитить данные и укрепить доверие.

Связь между финансами и кибербезопасностью

Финансовый отдел компании владеет жемчужиной компании: он обеспечивает безопасность финансовых транзакций и систем. Финансовый отдел является ключевым компонентом общей безопасности компании.

Несмотря на то, что финансовый отдел не занимается исключительно кибербезопасностью, он ежедневно обеспечивает безопасность жизненно важных операций. Эти команды хорошо знакомы с финансовой нормативной отчетностью и соблюдением требований. Цифровые транзакции составляют большую часть большинства бизнес-транзакций, и каждая из них должна быть безопасной. Природа современного бизнеса требует, чтобы этот отдел работал в тандеме с ИТ и

службами безопасности, чтобы обеспечить соответствие нормативным требованиям. Правила конфиденциальности и защиты данных различны, особенно для компаний, ведущих международную деятельность. Сложность соблюдения нормативных требований растет с каждым новым нормативным актом.

Финансы необходимы для оценки рисков и планирования непрерывности бизнеса. Финансовый отдел знаком со всеми финансовыми активами компании и с тем, как они организованы. Они могут быть полезны при оценке риска для этих активов. Финансовый отдел понимает риски, особенно риски третьих лиц и то, как партнер партнера становится риском. Финансовый отдел может количественно оценить потенциальные риски, такие как репутационный или экономический ущерб, в различных сценариях. Они понимают, что тоже могут стать источником риска без соответствующей подготовки и процедур.

Финансовые департаменты ставят привлекательные цели

Финансовый отдел является постоянной мишенью для киберпреступников. В результате этот отдел должен сохранять бдительность на всех фронтах, поскольку нападения могут принимать самые разные формы. Социальная инженерия и фишинг являются особенно популярными кибератаками, поскольку компрометация корпоративной электронной почты через этот отдел может привести к раскрытию банковских реквизитов или прямых денежных переводов. Фишинговые электронные письма обычно используют приманку неоплаченного счета или аналогичный подход для получения кликов по своим вредоносным ссылкам.

Система банковских переводов Общества всемирных межбанковских финансовых телекоммуникаций (SWIFT) была использована для кражи 81 миллиона долларов со счета в Федеральном резервном банке Нью-Йорка в 2016 году. Муниципалитет небольшого городка в Вашингтоне потерял 50 000 долларов, когда сотрудник в ответ перевел средства мошеннику. к серии поддельных электронных писем, которые, по-видимому, пришли от начальника отдела.

Эти риски представляют собой реальные проблемы для финансовых отделов, которые, прежде всего, не занимаются кибербезопасностью. Но этим отделам не нужно самим становиться экспертами по кибербезопасности, чтобы работать с ИТ-

директором, чтобы помочь создать и поддерживать культуру осведомленности о рисках во всей организации. Сочетание опыта отдела в качестве цели и защитника дает им уникальное представление о ценности обучения по вопросам безопасности и о том, насколько хорошо оно готовит нынешних сотрудников к потенциальным угрозам. Финансовый отдел может предложить ценные отзывы о текущем подходе.

Управление рисками укрепляет доверие

Являясь частью группы управления рисками, руководство финансового отдела обладает навыками экспертной оценки рисков, чтобы задавать правильные вопросы во время планирования. В состав групп быстрого реагирования на киберинциденты должен входить знающий руководитель из финансового отдела, который будет анализировать потенциальные финансовые последствия атаки. Важно включить этого человека в качестве основного контактного лица в официальную политику реагирования на инциденты и документацию по планированию. Назначенное контактное лицо по финансовым вопросам также должно по возможности участвовать в учениях или симуляциях по реагированию на кибер-инциденты.

Восприятие потребителями конфиденциальности данных компании и мер защиты безопасности влияет на их решения о покупке. Финансовый отдел помогает защитить данные клиентов и компании, снижая вероятность компрометации. Обеспечивая безопасность финансовых транзакций и систем, эти отделы способствуют общей операционной безопасности компании. Финансы приносят глубокие знания о соблюдении нормативных требований, которые могут помочь компании ориентироваться в национальных и международных правилах конфиденциальности и безопасности, которые регулируют использование, хранение и передачу данных. В целом, поддержание финансового отдела в курсе кибербезопасности помогает организациям снизить риски и быстро реагировать на угрозы». ***(Michelle Greenlee. The Role of Finance Departments in Cybersecurity // Security Intelligence (https://securityintelligence.com/articles/role-finance-departments-cybersecurity/). 20.03.2023).***

***

«…За останні кілька місяців багато країн наклали обмеження на TikTok, побоюючись, що він може бути використаний для отримання доступу до даних їхніх громадян або для поширення китайської пропаганди.

Однак такі заборони наштовхнулися на опір прихильників свободи слова, а також опозицію з боку китайського уряду. ByteDance заперечує твердження, що вона контролюється державною організацією, вказуючи на те, що її заснували підприємці та фінансували міжнародні інституційні інвестори.

Низка країн світу вже заборонили застосунок TikTok. Серед них:

Індія.TikTok в Індії спершу заборонили у 2020 році. Вже у січні 2021 року заборона стала постійною.

Цей крок був зроблений після того, як 20 індійських солдатів було вбито під час прикордонного зіткнення з китайськими військами у Гімалаях у червні 2020 року. Між двома країнами зросла напруженість, і Індія наклала заборону на понад 50 китайських застосунків, включаючи TikTok і застосунок для обміну повідомленнями WeChat.

У той час Forbes підрахував, що TikTok може зазнати збитків у розмірі до 6 мільярдів доларів через заборону свого найбільшого ринку за межами Китаю.

Сполучені Штати Америки. Ще під час президентства Дональда Трампа спалахнула напруженість між TikTok і США. Трамп погрожував заблокувати нові завантаження TikTok у Сполучених Штатах у 2020 році. Ця заборона так і не набула чинності після провалу в судах.

Однак напруженість не зникла і за президента Джо Байдена, і минулого місяця адміністрація дала державним установам 30 днів на видалення TikTok з державних пристроїв. Десятки штатів видали директиви, які забороняють додаток на пристроях, а Конгрес наполягав на повній забороні.

Канада. У Канаді заборонили TikTok на державних телефонах минулого місяця, невдовзі після США.

Уряд Канади заявив, що провів перевірку TikTok і “визначив, що він представляє неприйнятний рівень ризику для конфіденційності та безпеки”.

Прем’єр-міністр Канади Джастін Трюдо сказав, що цей крок “може бути першим кроком, можливо, це єдиний крок”, який повинен зробити уряд.

Тайвань. У Тайвані заборонили TikTok на урядових пристроях у грудні. Зараз уряд розглядає заборону застосунку по всій країні на тлі зростання напруженості з Китаєм.

Європейський Союз. Європейський парламент, Європейська комісія та Рада Європейського Союзу запровадили заборону на TikTok на пристроях персоналу.

«Цей захід має на меті захистити Комісію від загроз кібербезпеці та дій, які можуть бути використані для кібератак на корпоративне середовище Комісії», – заявила Європейська комісія, оголосивши про заборону в лютому.

Країни-члени ЄС, такі як Бельгія та Данія, заборонили TikTok на урядових телефонах.

Велика Британія. Британський уряд оголосив про заборону TikTok на державних пристроях у березні.

Міністр кабінету міністрів Олівер Доуден заявив парламенту Великої Британії, що це був запобіжний, але «обачливий» крок після перевірки Національним центром кібербезпеки.

Австралія. Структури австралійського уряду ввели аналогічні заборони на пристрої персоналу.

Зокрема міністерство зміни клімату, енергетики, навколишнього середовища та водних ресурсів, міністерство сільського господарства, рибальства та лісового господарства та міністерство оборони та внутрішніх справ заявили, що співробітники не можуть завантажити програму на свої робочі телефони.

Індонезія. Конфіденційність і геополітична напруженість у відносинах з Китаєм – не єдині причини, через які TikTok потрапив під пильну увагу уряду. Індонезія тимчасово заборонила додаток ще у 2018 році, посилаючись на «порнографію, неприйнятний контент і богохульство». Заборону було знято менше ніж через тиждень після того, як додаток погодився цензурувати частину свого вмісту.

Пакистан. Уряд Пакистану принаймні двічі тимчасово забороняв додаток через, на його думку, неприйнятний вміст. Це не є незвичним для уряду країни – цензурувати Інтернет вдома. Раніше цього місяця він заблокував Вікіпедію через «блюзнірський» вміст. Через кілька годин сайт було відновлено.

Афганістан. Таліби оголосили про заборону TikTok у 2021 році, щоб «запобігти введенню молодого покоління в оману». Заборона набула чинності, але Wired повідомляє, що користувачі знайшли способи обійти обмеження через VPN.

Нова Зеландія. Законодавці Веллінгтона також погодилися заборонити додаток на мобільних пристроях з доступом до парламентської мережі країни, посилаючись на проблеми кібербезпеки. Деякі винятки будуть зроблені для тих, кому потрібен доступ до TikTok для робочих цілей, повідомили чиновники. Заборона набуде чинності до кінця березня.

Міністерство закордонних справ Нової Зеландії та сили оборони також заявили, що ввели заборону на робочі пристрої як "запобіжний підхід»…» ***(Низка урядів світу заборонили або обмежили користування TikTok через побоювання щодо безпеки // Букви (https://bykvu.com/ua/bukvy/nyzka-uriadiv-svitu-zaboronyly-abo-obmezhyly-korystuvannia-tiktok-cherez-poboiuvannia-shchodo-bezpeky/). 17.03.2023).***

***

Кібербезпека та хмарні технології

«Израильский поставщик решений для кибербезопасности и доставки приложений Radware запустил центр безопасности облачных приложений нового поколения в Тель-Авиве. Новый центр является частью стратегической инициативы Radware по расширению услуг облачной безопасности, целью которой является предоставление клиентам инновационных и масштабируемых решений. Новый центр безопасности будет работать вместе с существующим облачным центром компании по защите от DDoS-атак в Израиле.

Добавление нового центра в Израиле последовало за недавним развертыванием объектов в других крупных странах, включая Австралию, Канаду, Чили, Италию, Новую Зеландию, Тайвань и Объединенные Арабские Эмираты, что указывает на растущий спрос на услуги облачной безопасности во всем мире…

Согласно отчету Radware Global Threat Analysis Report за 2022 год, количество DDoS-атак выросло на 150 % по сравнению с 2021 годом, в то время как количество атак на веб-приложения и API увеличилось на 128 % по сравнению с прошлым годом, что значительно опережает рост атак на 88 % в период с 2020 по 2021 год. Цифры подчеркивают необходимость принятия предприятиями упреждающих мер для защиты своих цифровых активов…

В бизнес-секторе наблюдается растущая зависимость от облачных сервисов, чему способствует неуклонный рост удаленной работы.

Согласно исследованию McKinsey, 98 миллионов работников в США в настоящее время работают удаленно, а исследование Deloitte показало, что 77% респондентов заявили, что их решение сменить работу было вызвано стремлением к большей гибкости рабочего места.

Кроме того, недавний опрос Fiverr, посвященный настроениям поколения Z, показал, что удаленная работа остается приоритетом, поскольку молодое поколение выходит на рынок труда…» ***(ZACHY HENNESSEY. Radware launches next-gen cloud security center in Tel Aviv // Jpost Inc. (https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-734290). 14.03.2023).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«За словами дослідників кібербезпеки компанії NordVPN, все більше кіберзлочинців шукають способи використовувати ChatGPT у своїй діяльності. Кількість нових повідомлень на форумах даркнету про ChatGPT зросла на 625%.

У дослідженні аналізували як кількість коментарів, так і кількість новостворених тем. Використання технологій штучного інтелекту у хакерській діяльності стало найпопулярнішою темою у даркнеті. Серед найпоширеніших запитань:

як змусити ChatGPT створювати шкідливе програмне забезпечення;

як зламати ChatGPT;

як використовувати ChatGPT для проведення кібератак.

За словами експертів, здатність чат-бота складати тексти, які не відрізняються від «людського» написання, потенційно може призвести до фішингових атак. На форумах зловмисники шукають способи змусити ChatGPT проводити такі атаки, долаючи контентні обмеження чат-бота…» ***(Популярність ChatGPT серед кіберзлочинців зросла на 625% // No worries! (https://noworries.news/populyarnist-chatgpt-sered-kiberzlochyncziv-zrosla-na-625/). 06.03.2023).***

***

«…Согласно недавнему отчету Cynerio и Ponemon Institute, 56% организаций подверглись одной или нескольким кибератакам в течение 24 месяцев с устройств IoMT/IoT. В отчете также упоминается тот факт, что 89% организаций каждую неделю сталкиваются с эквивалентом атаки, что обычно влияет на уход за пациентами. Сегодняшние больничные сети состоят из тысяч подключенных медицинских устройств, которые обеспечивают спасательную помощь, что создает среду с высоким риском кибератак. Согласно недавнему отчету ФБР, 53% подключенных медицинских устройств в больницах имеют критические уязвимости. Больницы подталкивают производителей устройств к большей прозрачности конструкции устройств, процессов кибербезопасности и управления сторонними программными компонентами.

Регуляторные органы также предъявляют все более высокие требования к безопасным конструкциям продуктов и возможностям подключения устройств. В недавно обновленном предварительном руководстве по кибербезопасности FDA

(апрель 2022 г.) производителям устройств конкретно предлагается продемонстрировать архитектуру кибербезопасности во всей экосистеме устройств. Оценки угроз должны учитывать безопасный поток данных в различных операционных состояниях, вариантах использования и пользователях, чтобы смягчить преднамеренные и непреднамеренные эксплойты. Проекты также должны включать оценку рисков для всех каналов связи, чтобы обеспечить безопасные потоки данных через внутренние и внешние интерфейсы.

Для производителей устройств недостаточный контроль кибербезопасности создает значительные риски с точки зрения одобрения регулирующих органов, доходов, репутации и раскрытия интеллектуальной собственности. Архитектуру кибербезопасности необходимо учитывать на ранней стадии проектирования, чтобы обеспечить эффективный и надежный контроль. Архитектуры безопасности также должны быть масштабируемыми по мере развития функций и поддерживаться в течение многих лет. Дальнейший анализ в отчете ФБР показал, что многие устройства «изначально не разрабатывались с учетом требований безопасности — из-за предположения, что они не подвергаются угрозам безопасности». По мере того, как медицинские устройства превращаются из исторически автономных устройств в компоненты распределенных и интеллектуальных систем, создание безопасных, надежных и гибких архитектур является серьезной задачей для производителей.

Подход с нулевым доверием

Как производители устройств могут использовать передовой опыт для разработки безопасных коммуникаций и совместимых систем? Одним из подходов, который обсуждается в разных отраслях, является концепция «нулевого доверия». Этот подход подчеркивает необходимость защиты сетевого трафика независимо от сетевого расположения. Ориентированные на данные программные коммуникационные платформы, такие как стандарт Data Distribution Service (DDS), могут реализовать принципы нулевого доверия, позволяя производителям устройств защищать фактические передаваемые данные, а не сообщения или сетевые периметры. Основанная на открытых стандартах, DDS абстрагирует обмен

сообщениями между приложениями и обеспечивает изоляцию данных и детальное управление доступом к данным в движении. Поскольку коммуникационная структура по своей природе «осведомлена о данных», известные структуры данных используются только авторизованными приложениями, которым нужны данные. Это мощная парадигма, которая позволяет использовать принцип «запретить по умолчанию», настроенный в соответствии с потребностями приложений и вариантами использования. Структура DDS является модульной и децентрализованной, без центрального сервера. DDS был разработан для безопасного, надежного обмена данными в режиме реального времени и используется в различных отраслях в распределенных и критически важных для безопасности системах.

Отрасль здравоохранения будущего будет определяться интероперабельными системами, которым необходимо безопасно обмениваться критически важными данными между устройствами, распределенными приложениями и сетями. Производители устройств играют ключевую роль в предоставлении этих безопасных и подключенных решений, и поэтому им необходимо использовать стандарты и современные коммуникационные платформы для обеспечения безопасной совместимости при проектировании устройств». ***(Darren Porras. Cybersecurity in the Connected Medical Future // Breaking Media, Inc. (https://medcitynews.com/2023/03/cybersecurity-in-the-connected-medical-future/). 10.03.2023).***

***

«Искусственный интеллект (ИИ) рекламируется как будущее кибербезопасности, и это правильно. В связи с растущим объемом и изощренностью киберугроз кибераналитикам все труднее уследить за ними. В результате ИИ стал неотъемлемой частью операций по кибербезопасности, обеспечивая более быстрый и точный анализ угроз. Однако распространение «теневого ИИ» в кибербезопасности может вызвать проблемы для организаций.

Что такое теневой ИИ?

Теневой ИИ относится к использованию инструментов ИИ сотрудниками компании, особенно в сфере кибербезопасности, такой как поиск угроз, без ведома или согласия их организации. Он возникает, когда сотрудники считают, что инструменты кибербезопасности их организаций неадекватны или что им не разрешено использовать ИИ в своей работе, и поэтому они обращаются к личным инструментам ИИ, чтобы помочь им выполнять свою работу более эффективно.

Теневой ИИ в кибербезопасности

Аналитики по кибербезопасности, в частности, используют инструменты искусственного интеллекта, чтобы помочь им выполнять свою работу более эффективно. Вот три способа использования теневого ИИ в кибербезопасности:

Деобфускация кода с помощью Shadow AI

Одной из наиболее серьезных проблем, с которыми сталкиваются аналитики кибербезопасности, является обфускация кода, особенно кода PowerShell. PowerShell — это язык сценариев, используемый Microsoft Windows, и кибер-злоумышленники часто используют методы запутывания, чтобы скрыть свой вредоносный код. Аналитики по кибербезопасности могут использовать инструменты искусственного интеллекта для деобфускации кода и понимания его основной функции, что может помочь им более эффективно выявлять и устранять угрозы.

Анализ вредоносного кода

Еще один способ использования теневого ИИ в кибербезопасности — это анализ вредоносного кода. Аналитики по кибербезопасности могут использовать инструменты ИИ для анализа кода и лучшего понимания того, как он работает. Это может помочь им определить шаблоны и модели поведения, которые можно использовать для создания более надежной защиты от кибербезопасности.

Узнайте больше об уязвимостях и форматах атак

Аналитики по кибербезопасности могут использовать ИИ для имитации атак и получения дополнительной информации о конкретных уязвимостях или

форматах атак. Моделируя атаки, аналитики могут понять шаги, предпринятые кибер-злоумышленниками, и определить наилучшие способы защиты от них.

Опасности теневого ИИ

Хотя теневой ИИ может предоставить аналитикам кибербезопасности ценный инструмент, помогающий в их работе, он также может вызвать проблемы для организаций. Вот некоторые из опасностей Shadow AI:

Возможные неправильные ответы

Когда аналитики по кибербезопасности полагаются на инструменты ИИ без надлежащей подготовки, они могут не полностью понимать, как работают алгоритмы ИИ. В результате они могут слишком сильно полагаться на ИИ при принятии решений, что может привести к неправильным ответам.

Использование ИИ в качестве опоры

Аналитики по кибербезопасности могут начать слишком сильно полагаться на инструменты ИИ, используя их как опору вместо того, чтобы полагаться на свои собственные навыки и опыт. Это может привести к снижению качества их работы и потере ценных навыков.

Осложняющие факторы

Использование теневого ИИ может ввести дополнительные факторы, усложняющие стратегию кибербезопасности организации. Например, использование персональных инструментов ИИ может привести к отсутствию стандартизации в организации, что затруднит координацию усилий и понимание состояния безопасности организации в целом.

Несанкционированное раскрытие информации

Одной из основных проблем является возможность раскрытия конфиденциальной информации программам ИИ, что может поставить под угрозу конфиденциальные данные. Это может произойти либо в одном запросе к ИИ, либо в совокупности многих запросов от одного или нескольких лиц, предоставляющих информацию в нескольких вопросах и ответах в течение длительного периода времени.

Заключение

Хотя теневой ИИ в кибербезопасности может предоставить ценные инструменты для аналитиков кибербезопасности, помогающие в их работе, он также может вызвать проблемы для организаций. Для организаций важно знать об использовании теневого ИИ в своей организации и обеспечить адекватное обучение сотрудников, которые хотят использовать инструменты ИИ. Таким образом, организации могут использовать возможности ИИ, избегая при этом потенциальных ловушек теневого ИИ». ***(Unveiling the Shadow AI: The Rise of AI Reliance in Cybersecurity // Techstrong Group (https://securityboulevard.com/2023/03/unveiling-the-shadow-ai-the-rise-of-ai-reliance-in-cybersecurity/amp/). 12.03.2023).***

***

«Доступ к искусственному интеллекту и машинному обучению быстро меняет технологии и разработку продуктов, что приводит к созданию более совершенных, эффективных и персонализированных приложений за счет использования огромного объема данных.

Однако те же самые возможности есть и у злоумышленников, которые используют ИИ для создания вредоносного ПО, не обнаруживаемого алгоритмами, широко используемыми средствами сетевой безопасности. Правительственные учреждения, банковские учреждения, критическая инфраструктура, а также крупнейшие мировые компании и их наиболее используемые продукты все чаще подвергаются угрозе со стороны вредоносных программ, которые могут обходить антивирусные системы, захватывать сети, останавливать операции и раскрывать конфиденциальную и личную информацию.

Технология, разработанная в Национальной лаборатории Ок-Риджа Министерства энергетики и используемая Командованием систем информационной войны ВМС США, или NAVWAR, для проверки возможностей коммерческих инструментов безопасности, была лицензирована фирмой по кибербезопасности Penguin Mustache для создания своей платформы Evasive.ai. Компания была

основана создателем технологии, бывшим ученым ORNL Джаредом М. Смитом, и его деловым партнером, предпринимателем Брэндоном Брюсом.

«Одна из основных задач ORNL — продвигать науку, стоящую за национальной безопасностью», — сказала Сьюзен Хаббард, заместитель ORNL по науке и технологиям. «Эта технология является результатом нашего глубокого опыта в области искусственного интеллекта, примененного к большой задаче — защите национальной кибер- и экономической безопасности».

Смит, проработавший в ORNL в течение шести лет в отделе киберустойчивости и разведки, создал технологию — генератор входных данных состязательного вредоносного ПО, или AMIGO, — по запросу Министерства обороны. AMIGO был создан в качестве инструмента оценки для задачи, выданной NAVWAR для приложений ИИ, которые автономно обнаруживают и изолируют угрозы кибербезопасности. NAVWAR — это оперативное подразделение ВМФ, занимающееся безопасными коммуникациями и сетями.

«Подразделение киберустойчивости и разведки ORNL является мировым лидером в области технологий кибербезопасности», — сказал Мо Халил, заместитель директора лаборатории Управления национальной безопасности лаборатории. «Выход AMIGO на рынок поможет защитить критически важную инфраструктуру нашей страны от атак».

«Мы испытали AMIGO в реальных условиях. Он прошел через отжим и был подтвержден на высоком уровне технической готовности», — сказал Смит. «Основная технология предназначена для создания уклоняющихся вредоносных программ, таких как вирусы, которые могут обойти существующие технологии обнаружения».

Опираясь на более чем 35 миллионов образцов вредоносных программ — некоторые из них общедоступны, а другие — никогда ранее не встречавшиеся, — AMIGO создает оптимально уклоняющееся вредоносное ПО в сочетании с обучающей информацией, необходимой системе безопасности для ее обнаружения в будущем.

Смит сравнивает этот процесс с разработкой вакцины. «Это как если бы мы создали миллион вариантов вируса и миллион вакцин для защиты от них — мы можем объединить это в одну вакцину и привить всех. Они защищены от угрозы, но также и от всех естественных эволюций угрозы в будущем».

Люк Кох, который в 2019 году работал в команде разработчиков AMIGO в рамках программы SULI Управления науки Министерства энергетики США, или программы стажировки в научной лаборатории бакалавриата, теперь является докторантом Бредесенского центра междисциплинарных исследований и последипломного образования, созданного в сотрудничестве между ORNL и университетом. штата Теннесси, а также дипломированный научный сотрудник исследовательской группы ORNL по кибербезопасности. Под руководством Смита Кох написал двоичный инструментальный код, используемый в AMIGO.

«Коммерциализация кибербезопасности важна, потому что наши противники всегда ищут слабые места во всей цепочке поставок», — сказал Кох. «Один единственный недостаток — это все, что нужно, чтобы сделать умную и дорогую защиту недействительной».

В условиях растущего понимания общественностью возможностей ИИ команда стремится к тому, чтобы AMIGO была интегрирована в Evasive.ai и внедрена агентствами национальной безопасности для защиты государственных активов и инфраструктуры.

«Злоумышленники уже используют искусственный интеллект для продвижения своих атак», — сказал Брюс. «По мере совершенствования открытых инструментов искусственного интеллекта попытки проникновения в системы безопасности будут увеличиваться в объеме и изощренности».

Кроме того, долгосрочное использование платформы Evasive.ai может дать более полное представление о механизмах, которые способствуют состязательным образцам. Это понимание сделает следующее поколение средств защиты на основе машинного обучения более надежным…» ***(Malware 'vaccine' generator licensed for cybersecurity platform // Tech Xplore (https://techxplore.com/news/2023-03-malware-vaccine-generator-cybersecurity-platform.html). 24.03.2023).***

***

Кіберзлочинність та кібертерроризм

«Кіберзлочинці винаходять все більш хитрі способи порушити роботу онлайн-служб, отримати доступ до конфіденційних даних або вивести з ладу пристрої користувачів Інтернету. Кібератака, яка стала дуже поширеною протягом останніх десятиліть, є так званою розподіленою відмовою в обслуговуванні (DDoS). Цей тип атаки включає низку пристроїв, підключених до Інтернету, які разом називаються «ботнет». Ця «група» підключених пристроїв потім використовується для заповнення цільового сервера або веб-сайту «фальшивим» трафіком, порушуючи його роботу та роблячи його недоступним для законних користувачів.

Щоб захистити свій веб-сайт або сервери від атак DDoS, компанії та інші користувачі зазвичай використовують брандмауери, програмне забезпечення для захисту від зловмисних програм або звичайні системи виявлення вторгнень. Однак виявлення цих атак сьогодні може бути дуже складним, оскільки вони часто здійснюються за допомогою генеративних змагальних мереж (GAN), методів машинного навчання, які можуть навчитися реалістично імітувати діяльність реальних користувачів і законні запити користувачів.

Як наслідок, багато що існує систем захисту від зловмисного програмного забезпечення зрештою не можуть захистити користувачів від них.

Дослідники з Паризького політехнічного інституту Telecom Paris (INFRES) нещодавно розробили новий обчислювальний метод, який може більш ефективно

та надійно виявляти DDoS-атаки. Цей метод, представлений у статті, опублікованій в Computers & Security, базується на моделі довготривалої короткочасної пам'яті (LSTM), типу рекурентної нейронної мережі (RNN), яка може навчитися виявляти довготривалі залежності в послідовностях подій.

«Наша дослідницька стаття базувалася на проблемі виявлення DDoS-атак, типу кібератак, які можуть завдати значної шкоди онлайн-сервісам і мережевим комунікаціям», — сказав Tech Xplore Алі Мустафа, один із дослідників, який проводив дослідження. «У той час, як попередні дослідження вивчали використання алгоритмів глибокого навчання для виявлення DDoS-атак, ці підходи все ще можуть бути вразливими для зловмисників, які використовують методи машинного та глибокого навчання для створення трафіку змагальної атаки, здатного обходити системи виявлення».

У рамках свого дослідження Мустафа та його колеги вирішили розробити абсолютно новий підхід на основі машинного навчання, який міг би підвищити стійкість систем виявлення DDoS. Запропонований ними метод базується на двох окремих моделях, які можна інтегрувати в єдину систему виявлення вторгнень.

«Перша модель розроблена для того, щоб визначити, чи є вхідний мережевий трафік конкурентним, і заблокувати його, якщо він вважається шахрайським», — пояснив Мустафа. «В іншому випадку він пересилається до другої моделі, яка відповідає за визначення того, чи є це DDoS-атака. Залежно від результату цього аналізу використовується відповідний набір правил і система сповіщень».

Інструмент виявлення DDoS, запропонований цією командою дослідників, має численні переваги перед іншими системами виявлення вторгнень, розробленими в минулому. Зокрема, він надійний і може виявляти DDoS-атаки з високим рівнем точності, його можна адаптувати, а також його можна адаптувати для задоволення унікальних потреб конкретних компаній або користувачів. Крім того, він може бути легко розгорнутий інтернет-провайдерами (ISP), захищаючи їх як від стандартних, так і від агресивних DDoS-атак.

«Наше дослідження дало кілька вагомих результатів і досягнень», — пояснив Мустафа. «Спочатку ми оцінювали високопродуктивні моделі, які навчені

ідентифікувати стандартні DDoS-атаки, перевіряючи їх проти змагальних DDoS-атак, згенерованих через Generative Adversarial Networks (GAN). Ми помітили, що моделі були відносно неефективними для виявлення таких типів атак; однак ми змогли удосконалити наш підхід і вдосконалити його, щоб виявляти ці атаки з точністю понад 91%».

Початкові тести, проведені Мустафою та його колегами, дали дуже багатообіцяючі результати, оскільки вони показали, що їхня система також може виявляти складніші атаки, спеціально розроблені для обману алгоритмів машинного навчання. Щоб ще більше продемонструвати потенціал свого інструменту, дослідники також провели серію тестів у режимі реального часу. Вони виявили, що система задовольняє вимоги щодо виявлення атак DDoS у реальному часі, витягуючи та аналізуючи мережеві пакети за обмежений проміжок часу та не викликаючи значних затримок мережевого трафіку.

Багатообіцяючий метод, представлений у цій статті, незабаром можна буде інтегрувати в існуючі та нові системи безпеки. Крім того, це може надихнути на розробку подібних методів машинного навчання для виявлення DDoS-атак.

«Оскільки ми дивимося вперед на майбутню роботу, дуже важливо оцінити ефективність нашої IDS, коли протистоїть ворожим атакам, створеним альтернативними моделями», — додав Мустафа. «Крім того, нам потрібно вивчити реалізацію алгоритмів онлайн-навчання, які дозволяють IDS постійно оновлювати свою модель у режимі реального часу під час аналізу нових даних. Завдяки інтеграції функції поступового оновлення IDS може зберегти свою ефективність у виявленні нових атак. техніки». ***(Володимир. Створено новий інструмент на основі ШІ для виявлення DDoS-атак // portaltele (https://portaltele.com.ua/news/cybersecurity/stvoreno-novyj-instrument-na-osnovi-shi-dlya-vyyavlennya-ddos-atak.html). 02.03.2023).***

***

«…В последнем отчете «Лаборатории Касперского» под названием «Темная сторона детских виртуальных игровых миров» раскрываются риски

для молодых игроков в онлайн-играх и то, что целенаправленные атаки на эту возрастную группу увеличились на 57% по сравнению с 2021 годом.

Фишинговые страницы, используемые киберпреступниками для нацеливания на молодых игроков, в основном имитировали глобальные игры, включая игры Roblox, Minecraft, Fortnite и Apex Legends.

Чтобы получить доступ к устройствам родителей, киберпреступники намеренно создают поддельные игровые сайты, вызывая у детей интерес к переходу на фишинговые страницы и загрузке вредоносных файлов, говорится в сообщении компании, занимающейся кибербезопасностью.

Эксперты «Лаборатории Касперского» проанализировали угрозы, связанные с самыми популярными онлайн-играми для детей от 3 до 16 лет. Защитные решения «Лаборатории Касперского» зафиксировали более семи миллионов атак с января по декабрь 2022 года.

В 2021 году киберпреступники предприняли 4,5 миллиона попыток атак, в результате чего количество попыток атак увеличилось на 57 процентов в 2022 году.

В 2022 году 232 735 геймеров столкнулись с почти 40 000 файлов, включая вредоносные программы и потенциально нежелательные приложения, которые были замаскированы под самые популярные детские игры.

Поскольку дети этого возраста часто не имеют собственных компьютеров и играют с устройств родителей, угрозы, распространяемые киберпреступниками, скорее всего, направлены на получение данных кредитных карт и учетных данных родителей.

За тот же период около 40 000 пользователей пытались загрузить вредоносный файл, имитирующий Roblox, популярную детскую игровую платформу. Это привело к увеличению числа жертв на 14 процентов по сравнению с 33 000 игроков, подвергшихся нападению в 2021 году.

Поскольку половина из 60 миллионов пользователей Roblox моложе 13 лет, большинство жертв атак этих киберпреступников потенциально являются детьми, которым не хватает знаний о кибербезопасности.

Согласно статистике «Лаборатории Касперского», фишинговые страницы, используемые киберпреступниками для таргетинга на молодых игроков, в основном имитировали игры Roblox, Minecraft, Fortnite и Apex Legends.

Всего для этих четырех игр в 2022 году было создано более 878 000 фишинговых страниц…

Одна из самых распространенных техник социальной инженерии, нацеленная на молодых игроков, — это предложения скачать популярные читы и моды для игр. На фишинговом сайте пользователь может получить целую инструкцию по правильной установке чита.

Касперский отметил, что особенно интересно то, что есть конкретные инструкции, в которых говорится о необходимости отключения антивируса перед установкой файла. Это может не насторожить юных игроков, но может быть специально создано, чтобы вредоносное ПО не обнаруживалось на зараженном устройстве. Чем дольше антивирус пользователя отключен, тем больше информации может быть собрано с компьютера жертвы.

Из-за этого, по словам Колесникова, родители должны быть особенно осторожны в отношении того, какие приложения загружают их дети, установлены ли на их устройствах надежные решения для обеспечения безопасности, и должны учить своих детей тому, как вести себя в Интернете». ***(Katlene O. Cacho. Cybercriminals attack young gamers // SunStar Publishing Inc. (https://www.sunstar.com.ph/article/1955832/cebu/business/cybercriminals-attack-young-gamers). 12.03.2023).***

***

«SonicWall — американская компания, которая продает интернет-устройства для сетевой безопасности и удаленного доступа, что делает ее потенциально очень привлекательной мишенью для киберпреступников, пытающихся развернуть постоянное присутствие в известных организациях по всему миру.

Исследователи безопасности из Mandiant обнаружили новую вредоносную кампанию против сетевых устройств, продаваемых SonicWall. Аналитики говорят, что неизвестные участники кампании, вероятно, китайцы и работают на благо коммунистической диктатуры, и в настоящее время эта группа отслеживается как UNC4540.

Атака нацелена на устройство Secure Mobile Access (SMA) 100, безопасное устройство удаленного доступа, используемое компаниями и организациями для развертывания и управления удаленными работниками. SMA 100 может обеспечивать контроль доступа для удаленных пользователей, VPN-подключения и уникальные профили для каждого пользователя. В 2021 году устройство стало мишенью хакеров, которые воспользовались уязвимостью нулевого дня.

Угроза, обнаруженная Mandiant, предназначена для того, чтобы выжить после последних обновлений прошивки, предоставляемых SonicWall. Чтобы добиться такого постоянства, вредоносное ПО удаленно проверяет наличие новых обновлений прошивки каждые 10 секунд. При наличии обновления вредонос скачивает архив, распаковывает и монтирует его, а затем копирует в него себя.

Вредоносная программа также добавляет в пакет пользователя root с бэкдором, прежде чем снова заархивировать файлы, чтобы вернуть его на место и подготовить к установке. Когда обновление будет выполнено, вредоносное ПО продолжит работать и в среде новой прошивки.

Мандиант сказал, что эта техника не особенно сложна, но она показывает значительные усилия, приложенные неизвестными киберпреступниками для изучения и понимания цикла обновления устройства.

«В последние годы, — констатируют аналитики, — китайские злоумышленники развернули несколько эксплойтов нулевого дня и вредоносное ПО для различных сетевых устройств, подключенных к Интернету», чтобы получить все возможности для вторжения в предприятие. Новый экземпляр UNC4540 — еще один эпизод в этом длинном списке изощренных атак, и Mandiant ожидает, что эта тенденция сохранится «в ближайшем будущем».

Проанализировав вредоносный пакет, исследователи Mandiant обнаружили набор сценариев Bash (Bash — это оболочка Unix, обычно используемая в качестве интерфейса входа в систему по умолчанию для операционных систем Linux) и один двоичный файл ELF (Linux), идентифицированный как вариант TinyShell.

Исследователи еще не определили первоначальный вектор заражения, но SonicWall (которая работала вместе с Mandiant над обнаружением угрозы) выпустила новое обновление прошивки (10.2.1.7) для SMA 100. Компания также рекомендует клиентам и администраторам регулярно просматривать журналы устройства для выявления любых признаков продолжающегося заражения». ***(Alfonso Maruccia. Hackers are targeting SonicWall devices with malware that can survive firmware updates // TechSpot, Inc. (https://www.techspot.com/news/97886-chinese-hackers-targeting-sonicwall-devices-persistent-malware.html). 10.03.2023).***

***

«Akamai только что отразила распределенную атаку типа «отказ в обслуживании» (DDoS) эпических масштабов. Хотя она была недолгим, но была очень интенсивной и, скорее всего, могла легко вывести целевой сервер из строя.

Это была крупнейшая в истории DDoS-атака на цель в Азиатско-Тихоокеанском регионе. Несмотря на масштаб атаки, Акамай смогла полностью ее заблокировать.

DDoS-атака состоит из сотен, если не тысяч компьютеров, которые используются для отправки поддельных запросов на целевой сервер. Когда такой большой объем запросов попадает на сервер из ниоткуда, в результате затронутые веб-сайты или приложения обычно отключаются. Даже если они останутся в сети, они, вероятно, будут очень медленно реагировать. Масштаб проблемы зависит от размера атаки. Совсем недавно произошла масштабная объемная атака, затронувшая более 30 000 компьютеров.

На этот раз мы не знаем, сколько разных IP-адресов было использовано для перегрузки целевого сервера, но мы знаем, что количество запросов в секунду было

рекордным. По данным Bleeping Computer, это была крупнейшая подобная DDoS-атака против клиента из Азиатско-Тихоокеанского региона.

Атака произошла 23 февраля 2023 года. Пиковые скорости составили 900,1 Гбит/с (гигабит в секунду) и 158,2 млн пакетов в секунду (миллион пакетов в секунду). Пик длился всего около минуты, а вся продолжительность, по-видимому, составила около часа.

Akamai сообщает, что ему удалось полностью смягчить атаку. Его клиент никак не пострадал. Чтобы заблокировать атаку, Akamai использовала чистящую сеть, представляющую собой защитную сеть, которая перехватывает входящий трафик для защиты цели от DDoS-атаки. Большая часть трафика оказалась в центрах Akamai, расположенных в Токио, Осаке, Гонконге, Сингапуре и Сан-Паулу. В конце концов, Akamai использовала все свои 26 центров, чтобы заблокировать эту беспрецедентную атаку.

Хотя это была крупнейшая атака на цель в регионе APAC, в последние месяцы было предпринято множество других попыток DDoS, которые были успешно подавлены. Самой Akamai удалось остановить массированную атаку на цель в Восточной Европе, скорость которой достигла 659,6 млн пакетов в секунду». ***(Monica J. White. Akamai foils massive DDoS attack in Asia that reached 900Gbps // Digital Trends Media Group (https://www.digitaltrends.com/computing/massive-ddos-attack-mitigated-by-akamai/). 10.03.2023).***

***

«Кибербезопасность является растущей глобальной проблемой. Новый отчет проливает свет на цифровые угрозы, с которыми сталкиваются многие организации и отдельные лица.

Trend Micro, мировой лидер в области кибербезопасности, обнаружил в 2022 году рекордные 146 миллиардов киберугроз, что на 55% больше, чем в предыдущем году. Компания также сообщила о росте заблокированных вредоносных файлов на 242%.

В отчете показано, что киберпреступники становятся все более изощренными в своей тактике, что затрудняет защиту от атак.

Джон Клэй, вице-президент Trend Micro по анализу угроз, сказал, что ежегодный отчет показывает, что киберпреступники пошли ва-банк, чтобы увеличить прибыль.

«Всплеск обнаружения бэкдоров особенно беспокоит, поскольку показывает нам их успехи в проникновении внутрь сетей», — сказал Клэй. «Чтобы эффективно управлять рисками в условиях быстро расширяющейся поверхности атак, растянутым командам по безопасности необходим более рациональный подход на основе платформы».

Еще одной тенденцией, отмеченной в отчете, является растущая угроза атак программ-вымогателей — типа вредоносного ПО, которое блокирует доступ к компьютеру до тех пор, пока не будет выплачена определенная сумма денег.

В отчете показано, что эти типы атак стали более изощренными и теперь нацелены на более крупные организации с более ценными данными.

В сентябре прошлого года объединенный школьный округ Лос-Анджелеса — второй по величине в стране — подвергся атаке программ-вымогателей на свои системы информационных технологий.

Этот инцидент произошел через несколько месяцев после того, как администрация Байдена предупредила американские компании об усилении защиты от кибербезопасности. Тем не менее, эксперты говорят, что некоторым фирмам очень дорого и сложно найти подходящих специалистов для заполнения должностей в сфере безопасности, что делает их уязвимыми.

Некоторые рекомендации для компаний и частных лиц по обеспечению безопасности и защиты своих данных от киберугроз включают:

- Поддержание программного обеспечения и операционных систем в актуальном состоянии.

- Включение многофакторной аутентификации

- Использование надежных паролей и менеджера паролей

- Распознавание фишинга и сообщение о нем

В целом, годовой отчет служит тревожным сигналом для компаний и частных лиц, чтобы они могли оставаться в курсе и предпринимать шаги для защиты своей конфиденциальной информации и данных от вредоносных атак». ***(Gage Jackson. Annual report shows a record 146B cyber-threats detected last year // Scripps News (https://scrippsnews.com/stories/report-shows-a-record-146b-cyber-threats-detected-in-2022/). 09.03.2023).***

***

«Понятие «безопасность по неизвестности» официально устарело. В последние годы кибератаки становятся все более изощренными, разрушительными и неизбирательными. В современных условиях киберугрозы могут исходить от внутренних сотрудников, групп хактивистов и даже от национальных государств. Но чаще всего за наиболее распространенными сегодня атаками стоят финансово мотивированные хакерские бригады. К сожалению, для большинства компаний бюджет безопасности и ресурсы, выделенные на защиту от атак, не увеличились, чтобы противостоять растущим угрозам.

Это особенно актуально для компаний среднего размера, которые часто сталкиваются с ограниченными ресурсами для инвестиций в кибербезопасность, несмотря на их растущее присутствие в сфере ИТ. Хакеры знают, что малые и средние компании с меньшей вероятностью будут иметь надежные средства контроля безопасности и средства обнаружения угроз, и поэтому их легче взломать. Кроме того, многие компании среднего размера менее способны выдержать перерыв в бизнес-операциях, чем более крупные организации, что делает их более уязвимыми для программ-вымогателей и других атак, направленных на нарушение «обычного бизнеса».

Средняя стоимость утечки данных в настоящее время оценивается в 4,35 миллиона долларов; для компаний, базирующихся в США, этот средний показатель почти в два раза выше и составляет 9,44 миллиона долларов. Что еще хуже, последствия кибератак не ограничиваются только финансовыми затратами; есть также репутационный ущерб, который может возникнуть в результате последствий.

Для многих компаний среднего размера потенциальные последствия серьезной утечки данных представляют собой экзистенциальную угрозу.

Кроме того, компании среднего размера чаще становятся мишенью злоумышленников и с большей вероятностью сталкиваются с нарушениями безопасности.

С 2019 года средний бизнес на 490 % чаще сталкивается с нарушениями безопасности, чем крупные корпорации.

73% компаний среднего размера ожидают кибератаки в ближайшем будущем.

В среднем на обнаружение нарушения уходит до 69 дней, а на его локализацию —197 дней.

Сейчас, как никогда ранее, в этой среде повышенных угроз для компаний среднего бизнеса крайне важно понимать различные типы кибератак и риски, которые они представляют. Сохранение бдительности и сокращение времени, необходимого для обнаружения, сдерживания и подавления угрозы, — это первый шаг в создании программы киберзащиты.

Итак, на что следует обращать внимание компаниям среднего размера?

В этой статье мы рассмотрим некоторые из наиболее распространенных и новых векторов кибератак, используемых против компаний среднего размера, а также некоторые новые тенденции, о которых следует знать.

Что такое вектор атаки?

Вектор атаки — это средство, с помощью которого злоумышленник может использовать уязвимость для доступа к системе или сети. Векторы атаки обычно рассматриваются как определенный путь или метод, который злоумышленник может использовать для достижения своей цели. Во многих случаях злоумышленник будет использовать несколько векторов, чтобы получить доступ к системе или сети, а затем перемещаться в пределах среды для достижения своих целей.

В целом существует два основных типа векторов атаки — пассивный и активный.

В чем разница между пассивным и активным векторами атаки?

ПАССИВНЫЕ ВЕКТОРЫ АТАКИ

Хакеры используют пассивные векторы атак для получения доступа к системам и сетям без ведома или согласия пользователя и без нарушения работы системы-жертвы. Хакеры часто используют первоначальное адресное фишинговое электронное письмо для установки вредоносного программного обеспечения на компьютер, которое позволяет им перехватывать и отслеживать трафик, проходящий через зараженную машину. Хакеры обычно стремятся получить учетные данные пользователя для входа в систему — имена пользователей и пароли — которые они затем могут использовать для получения первоначального доступа к сети и поддержания постоянного доступа. Часто пассивные атаки, используемые для получения начального доступа, трудно обнаружить, потому что поведение злоумышленника очень похоже на поведение удаленного пользователя. Получив доступ, хакер может использовать активные векторы атаки для дальнейшего использования системы. Некоторые из наиболее распространенных типов векторов пассивных атак включают слежку за сетевым трафиком, перехват паролей и фальсификацию данных.

ВЕКТОРЫ АКТИВНОЙ АТАКИ

Векторы активных атак используются хакерами для прямого взаимодействия с системами и сетями с целью получения привилегированного доступа, внесения изменений в систему или создания дополнительных лазеек, обеспечивающих постоянный доступ к сети жертвы. В отличие от пассивных векторов, активные векторы атаки требуют от хакера определенного уровня взаимодействия с системой или сетью в реальном времени. Это может быть связано с использованием известной уязвимости программного обеспечения или использованием неправильной конфигурации системы. Активные векторы атак, как правило, сложнее выполнить, чем пассивные, но они могут нанести больший ущерб, поскольку хакер может получить прямой контроль над системой или сетью. Атаки «человек посередине», когда злоумышленник может подслушивать или маскироваться под руководителя компании, поставщика или другую доверенную

сторону после компрометации учетной записи электронной почты, представляют собой растущий сегмент кибератак, наблюдаемых в последние годы.

Теперь, когда мы рассмотрели некоторые основы векторов атак, давайте рассмотрим некоторые из наиболее распространенных векторов кибератак, используемых против организаций среднего размера.

Семь распространенных векторов атак для компаний среднего размера и как их избежать

1 Скомпрометированные учетные данные

Одним из наиболее распространенных способов получения хакерами доступа к сети компании является компрометация, кража или иное получение учетных данных пользователя, то есть имени пользователя и пароля авторизованного пользователя. Получив эти учетные данные, хакер может войти в систему, как если бы он был законным пользователем, и получить доступ ко всем данным и ресурсам, на которые у пользователя есть разрешение. Есть несколько различных способов, которыми хакеры могут получить учетные данные пользователя, включая социальную инженерию, атаки грубой силы и инъекции языка структурированных запросов (SQL). А поскольку многие люди используют одну и ту же комбинацию имени пользователя и пароля для нескольких учетных записей, получение учетных данных с одной платформы может открыть доступ ко многим другим.

СОВЕТЫ ПО ПРЕДОТВРАЩЕНИЮ КИБЕРАТАКИ С ПОМОЩЬЮ УЧЕТНЫХ ДАННЫХ:

Внедрение двухфакторной аутентификации. Несмотря на то, что она не является надежной, требование, чтобы пользователи имели две разные формы идентификации, такие как пароль и код, отправляемый на их телефон, может значительно снизить угрозу компрометации учетных данных.

Установите надежные политики паролей для всей организации. Создание и применение политик паролей, требующих от сотрудников использования надежных, уникальных паролей, которые регулярно меняются, может помочь повысить общую безопасность.

#2 Фишинг

Социальная инженерия через электронную почту — один из самых распространенных способов, с помощью которых киберпреступники получают первоначальный доступ к сети компании. Это часто делается с помощью фишинга, когда злоумышленник отправляет электронное письмо, которое, как представляется, из законного источника, такого как банк или поставщик услуг. Электронное письмо обычно содержит ссылку или вложение, при нажатии на которое на компьютер жертвы будет установлено вредоносное программное обеспечение. Затем это программное обеспечение можно использовать для получения доступа к сети и данным компании.

СОВЕТЫ ПО ПРЕДОТВРАЩЕНИЮ ФИШИНГОВОЙ КИБЕРАТАКИ:

Проводите регулярные тренинги по повышению осведомленности пользователей. Убедитесь, что сотрудники знают и понимают опасности фишинговых атак, способы их предотвращения, распознания и сообщения о них. скомпрометировать учетные данные.

Внедряйте и регулярно обновляйте фильтры электронной почты. Нежелательные фильтры электронной почты могут помочь заблокировать попадание подозрительных электронных писем в почтовые ящики сотрудников. Важно следить за тем, чтобы эти фильтры регулярно обновлялись, чтобы гарантировать их эффективность против новейших киберугроз.

Implement advanced endpoint threat detection and response tools – Standard antivirus protection may not prevent malicious code delivered through a phishing email from executing on one of your endpoints. Deploying a threat detection advanced sensor on every endpoint that can detect unusual processes or suspicious files can make the difference between a successful attack and a close call.

3 Неправильная конфигурация

Хакеры также могут получить доступ к сети компании, скомпрометировав ее конфигурацию, воспользовавшись уязвимостями в системе, которые не защищены должным образом. Например, хакер может найти ошибку в том, как компания настроила среду облачного хранения, разрешая несанкционированный доступ к

среде без обнаружения. Или быстрорастущая компания может иметь краткосрочные пробелы в покрытии, что приводит к тому, что на устройствах, подключенных к Интернету, не включено базовое программное обеспечение для защиты конечных точек.

Гибкость растущих компаний среднего размера может увеличить вероятность развития уязвимостей, связанных с неправильной конфигурацией, поскольку они постоянно находятся в движении, перенося данные на новые платформы, системы и облачные среды. Добавьте к картине приобретения, и вероятность того, что даже временная проблема с неправильной конфигурацией может возникнуть, возрастет еще больше.

СОВЕТЫ ПО ПРЕДОТВРАЩЕНИЮ КИБЕРАТАКИ НЕПРАВИЛЬНОЙ НАСТРОЙКИ:

Проводите регулярные аудиты безопасности. Регулярные аудиты конфигурации вашей системы могут помочь выявить любые потенциальные уязвимости, которые могут быть использованы хакерами.

Внимательно отслеживайте сетевой трафик и модели доступа пользователей. Возможность быстро обнаруживать необычные входящие и исходящие соединения или распознавать необычный доступ к системе имеет решающее значение для защиты от эксплойтов неправильной конфигурации.

Убедитесь, что данные правильно зашифрованы. Шифрование данных может помочь предотвратить доступ к ним неавторизованных пользователей, даже если они могут обойти другие меры безопасности.

4 Уязвимости программного обеспечения

Злоумышленники часто узнают об уязвимости программного обеспечения так же, как и все мы: когда производитель выпускает патч. Как только становится известно о критической уязвимости, начинается гонка. Можете ли вы применить исправление быстрее, чем злоумышленник сможет определить и использовать вашу уязвимость? Надежная программа безопасности будет делать упор на своевременное применение критических исправлений, чтобы свести к минимуму этот риск.

Уязвимости нулевого дня — это несколько иная история. Уязвимость нулевого дня — это недостаток безопасности, который неизвестен разработчику программного обеспечения или сообществу пользователей, но может быть известен злоумышленнику. Эти типы уязвимостей могут быть чрезвычайно опасны в руках злоумышленника, потому что они обеспечивают информационное преимущество, которое может быть использовано хакерами до того, как разработчик успеет залатать дыру. Уязвимости нулевого дня часто встречаются в широко используемом программном обеспечении, таком как веб-браузеры и офисные пакеты. Не все уязвимости нулевого дня представляют высокий риск для компаний среднего размера, поскольку многие из них требуют значительного времени и опыта для эффективного использования. Но некоторые из них, такие как Log4J или SolarWinds, представляют реальную опасность для любой организации, которой не повезло использовать это программное обеспечение.

Еще одним известным случаем уязвимости нулевого дня является ошибка Heartbleed, о которой было объявлено в 2014 году и которая затронула библиотеку OpenSSL — широко используемый протокол безопасности, который в то время использовался большинством социальных сетей, включая Facebook и Twitter. Эта уязвимость позволяла хакерам получать доступ к личной информации пользователей, включая пароли и номера кредитных карт, более чем за два года до того, как она была обнаружена.

СОВЕТЫ ПО ПРЕДОТВРАЩЕНИЮ КИБЕРАТАКИ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ:

Устанавливайте обновления и исправления, как только они становятся доступны. Поддержание вашего программного обеспечения в актуальном состоянии с помощью последних исправлений безопасности — один из лучших способов защиты от уязвимостей нулевого дня.

Используйте надежное программное обеспечение для обеспечения безопасности. Программное обеспечение для обеспечения безопасности, такое как антивирусы и программы защиты от вредоносных программ, может помочь

защитить вашу систему от известных угроз, а также от новых, которые еще не обнаружены.

Следите за своей системой на предмет аномальной активности. Отслеживание признаков атаки, таких как необычная активность в вашей сети или странные сообщения от ваших контактов, может помочь вам определить проблему до того, как она станет серьезной.

5 Уязвимости браузера

Атаки на основе браузера — это тип кибератаки, в которой используются уязвимости браузера для получения доступа к системе. Эти типы атак часто осуществляются путем размещения вредоносного кода на веб-сайтах, которые посещает жертва. Когда жертва посещает зараженный веб-сайт, выполняется вредоносный код, который позволяет злоумышленнику получить контроль над зараженной системой. Атаки на основе браузера могут быть чрезвычайно опасны, поскольку они могут выполняться без ведома цели. В некоторых случаях единственный способ узнать, что вы подверглись нападению, — это заметить необычную активность в вашей системе.

СОВЕТЫ ПО ПРЕДОТВРАЩЕНИЮ КИБЕРАТАКИ БРАУЗЕРНОЙ УЯЗВИМОСТИ:

Используйте проверенный браузер. Некоторые браузеры более безопасны, чем другие. При выборе браузера обязательно изучите его, чтобы найти тот, который предлагает хорошие функции безопасности.

Поддерживайте актуальность своих браузеров. Разработчики браузеров регулярно выпускают обновления, включающие исправления безопасности для новых уязвимостей. Поэтому важно поддерживать ваш браузер в актуальном состоянии, чтобы защититься от подобных атак.

Внедрите расширенный мониторинг подключений к системе доменных имен (DNS). Ваши брандмауэры должны блокировать подключения к сайтам, которые, как известно, являются вредоносными. Злоумышленники знают об этом и попытаются использовать новые сайты, которых нет в списках блокировки

брандмауэра. Мониторинг и проверка новых или необычных подключений — эффективный способ обнаружения эксплойтов браузера.

6 Атаки на цепочку поставок

Еще один вектор кибератак, который часто упускается из виду, — это доверительные отношения со сторонними поставщиками. Во многих случаях кибератаки успешны, потому что хакеры могут использовать доверительные отношения между организациями. Например, если организация А имеет доверительные отношения с организацией Б, хакер может получить доступ к системам организации А, скомпрометировав системы организации Б. Поэтому для организаций важно тщательно проверять своих сторонних партнеров и убедиться, что у них есть строгие меры безопасности.

Один из самых известных случаев использования хакером доверительных отношений произошел в 2014 году, когда кибератака на Target привела к краже более 40 миллионов номеров кредитных карт. Хакеры получили доступ к системам Target, скомпрометировав системы компании, которая предоставляла услуги по отоплению, вентиляции и кондиционированию воздуха в магазинах Target. Эти доверительные отношения позволили хакерам обойти меры безопасности Target и получить доступ к конфиденциальным данным.

СОВЕТЫ ПО ПРЕДОТВРАЩЕНИЮ КИБЕРАТАКИ НА ЦЕПОЧКУ ПОСТАВОК:

Помните о доверительных отношениях. При настройке доверительных отношений между организациями обязательно тщательно учитывайте последствия этого для безопасности. Например, сторонний ИТ-поставщик имеет другие последствия для безопасности, чем поставщик, занимающийся доставкой.

Проверяйте сторонних партнеров. При работе со сторонними партнерами обязательно тщательно проверяйте их, чтобы убедиться, что у них есть строгие меры безопасности. Внедрение беспрепятственного процесса должной осмотрительности и проверки третьей стороной может помочь гарантировать, что только доверенные партнеры получат доступ к вашим системам и только к тем системам, к которым они должны иметь доступ.

Мониторинг сторонних подключений и элементов управления доступом. После установления доверительных отношений важно отслеживать их на предмет любых необычных действий. Например, если вы заметили, что сторонний партнер регулярно получает доступ к данным, к которым у него не должно быть доступа, это может быть признаком того, что его системы были взломаны.

7 Внутренние угрозы

Иногда злоумышленники могут также исходить из вашей организации. Люди, уже находящиеся за корпоративным брандмауэром, представляют собой повышенную угрозу, потому что они часто имеют авторизованный доступ к конфиденциальным системам и данным или даже имеют привилегированные права администратора для управления критически важными системами, отключения средств защиты и кражи данных. Кроме того, инсайдеры могут обладать обширными знаниями об архитектуре кибербезопасности и о том, как их компании реагируют на киберугрозы. Эти навыки полезны для получения доступа к местам с ограниченным доступом, изменения настроек безопасности или определения наилучшего времени для кибератак. Внутренние угрозы трудно идентифицировать, и обычно требуется всесторонний мониторинг активности, однако есть шаги, которые можно предпринять для смягчения этих угроз.

СОВЕТЫ ПО ПРЕДОТВРАЩЕНИЮ ВНУТРЕННЕЙ КИБЕРАТАКИ:

Ограничьте доступ к критически важным системам и данным. Ограничьте доступ к критически важным системам и данным в случае необходимости. Это поможет снизить вероятность того, что внутренняя угроза сможет скомпрометировать ваши системы.

Разработайте комплексные политики защиты и классификации данных. Классификация данных в соответствии с уровнем их конфиденциальности поможет обеспечить доступ к конфиденциальной информации только уполномоченным лицам. Кроме того, внедрение комплексных политик защиты данных поможет снизить вероятность того, что злоумышленник сможет украсть или удалить важные данные.

Включите ведение журналов и развертывание аналитики поведения пользователей и методов обнаружения угроз. Даже опытный субъект внутренней угрозы в конечном итоге создаст необычные модели действий, которые можно обнаружить, но только в том случае, если вы собираете и анализируете правильные журналы и используете правильные схемы обнаружения.

Партнер MDR может помочь вам защитить вашу организацию с помощью экспертного руководства, лучших в своем классе технологий, а также круглосуточного мониторинга и поддержки.

Нарушение данных может иметь разрушительные последствия для вашего бизнеса, включая потерю клиентов, ущерб репутации и огромные выкупы (и, возможно, штрафы). Знание множества способов, которыми киберпреступники используют уязвимости, имеет решающее значение для обеспечения безопасности ваших данных.

Как упоминалось в этой статье, привлечение пользователей в рамках вашей стратегии защиты путем проведения надлежащего обучения киберугрозам и передовым методам, проверки сторонних поставщиков, проведения регулярных аудитов безопасности, внедрения надежных протоколов безопасности и инвестирования в надежные решения для ведения журналов и мониторинга. укрепит вашу безопасность и защитит вас от нарушений.

Однако ресурсы, необходимые для всего этого (не говоря уже о том, чтобы сделать это хорошо), могут быть недостаточными. Именно здесь на помощь приходит решение MDR, поскольку оно может предоставить вашей организации как передовые инструменты, так и опыт и знания для обеспечения комплексной защиты, необходимой для защиты от киберугроз, без больших затрат. Это также может дать вам уверенность в том, что на вашей стороне всегда будет команда опытных экспертов по кибербезопасности, а в случае атаки вы сможете сэкономить. Например:

В среднем организации со специальной группой реагирования на инциденты, которые протестировали свои действия, могут сэкономить 2,66 миллиона долларов

при возникновении нарушений, часто потому, что они могут предотвратить расходы (платежи программ-вымогателей и т. д.) в первую очередь.

Организации, которые обнаруживают утечку данных в течение 200 дней или менее, экономят в среднем 1,12 миллиона долларов.

Организации, которые полностью развертывают программы искусственного интеллекта и автоматизации для выявления и пресечения нарушений, сокращают расходы на 3,05 миллиона долларов и обеспечивают более быстрое время отклика более чем на 28 дней». ***(Jason Straight. Emerging Middle Market Cyber Attack Vectors: Are You at Risk? // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102i9y7/emerging-middle-market-cyber-attack-vectors-are-you-at-risk). 10.03.2023).***

***

«Злоумышленник YoroTrooper взломал учетные записи важнейших учреждений здравоохранения ЕС, ряда посольств и Всемирной организации интеллектуальной собственности (ВОИС).

Отчет от Cisco Talos показал, что огромное количество данных, таких как учетные данные, файлы cookie и истории браузера, были украдены с ряда зараженных конечных точек

К ним относятся те, которые принадлежат государственным структурам и энергетическим компаниям стран, входящих в Евразийское Содружество Независимых Государств (СНГ).

…ранее было известно, что YoroTrooper распространяет известное вредоносное ПО, такое как PoetRAT и LodaRAT, Cisco считает, что перешла к разработке собственных троянов удаленного доступа (RAT), написанных на Python, чтобы выполнить эту работу.

Летом 2022 года белорусские организации пострадали от зараженных PDF-файлов, отправленных с почтовых доменов под видом организаций из Беларуси или России. В сентябре того же года YoroTrooper зарегистрировал домены для

опечаток, чтобы они были максимально похожи на российские государственные учреждения.

Эта стратегия коренится в том, что фишинговые электронные письма YoroTrooper должны выглядеть как можно более законными, особенно в связи с тем, что его последняя уловка включает в себя прикрепление зараженных вложений RAR и ZIP для получения доступа к информации о национальной безопасности по всему региону.

В 2023 году группа угроз двигалась быстро. В январе он начал выпускать скрипт для извлечения учетных данных из браузеров на основе Chromium, но в феврале уже перешел на новый модульный инструмент под названием «Воняет».

Новый инструмент, помимо проникновения в браузер Chromium и базовой системной информации, также крадет данные из FTP-клиента Filezilla и приложений для обмена сообщениями Discord и Telegram.

Мотивы, средства и сторонники YoroTrooper в настоящее время неизвестны, но переход на пользовательские инструменты может стать тревожным событием для корпоративного мира». ***(Luke Hughes. A cyberspy outfit is attacking high-level targets in the EU // Future US, Inc. (https://www.techradar.com/news/a-cyberspy-outfit-is-attacking-high-level-targets-in-the-eu). 15.03.2023).***

***

«Системы крупнейшей в Австралии группы фирм, предоставляющих услуги в области интеллектуальной собственности, некоторые из которых ранее работали с федеральным правительством, были взломаны в результате инцидента с кибербезопасностью.

IPH, котирующаяся на ASX, в четверг сообщила, что в начале недели произошел «несанкционированный доступ к части ее ИТ-среды», что привело к двухдневной остановке торгов.

В то время как расследование того, была ли информация украдена, продолжается, компания заявила, что «инцидент кибербезопасности» повлиял на системы управления делами двух ее австралийских фирм-членов.

Этими двумя фирмами являются Griffith Hack со штаб-квартирой в Мельбурне, которая претендует на звание «одного из крупнейших в Австралии регистраторов патентов и товарных знаков», а также расположенная в Сиднее и Spruson & Ferguson (Австралия).

В последние годы Гриффит Хак работал с несколькими федеральными правительственными ведомствами, включая министерства промышленности, обороны и образования, над Программой университетских исследований и коммерциализации, а также с университетами и другими исследовательскими учреждениями.

«Исходя из предварительного анализа, инцидент в первую очередь ограничивается системами управления документами (DMS) головного офиса IPH и двух фирм-членов IPH в Австралии… и системами управления практикой (PMS) этих двух фирм-членов», — IPH. говорится в заявлении.

«Информация, содержащаяся в системах управления документами, включает документы, касающиеся управления этими организациями, а в случае двух фирм-членов — клиентские документы и корреспонденцию.

«Системы управления практикой содержат информацию об управлении делами в области ИС (например, сроки подачи заявок), касающуюся практики двух фирм-членов IPH».

IPH заявила, что в настоящее время работает с внешними консультантами по кибербезопасности и судебным информационным технологиям, чтобы расследовать инцидент и определить, «была ли информация… доступна неуполномоченной третьей стороне».

Обнаружив инцидент, компания попыталась обезопасить свою ИТ-среду и уведомила об этом Австралийский центр кибербезопасности.

Компания заявила, что, хотя «функциональность некоторых систем была затронута», она «перешла на альтернативные процессы… чтобы позволить соответствующим фирмам продолжать работу, хотя и с некоторыми сбоями», в соответствии с планами обеспечения непрерывности бизнеса.

«Мы приносим извинения нашим клиентам и сообществу за любые опасения, которые может вызвать этот инцидент. Мы продолжим информировать наших клиентов, акционеров и ключевых заинтересованных лиц по мере того, как мы реагируем на это событие, и наше расследование продолжается, и устанавливаются дополнительные факты», — говорится в сообщении IPH.

IPH — крупнейшая группа IP-услуг в Азиатско-Тихоокеанском регионе, в которую входят AJ Park, Griffith Hack, Pizzeys, Smart & Biggar и Spruson & Ferguson. В фирмах работает 1200 сотрудников в 25 странах, включая Австралию, Канаду, Китай, Индонезию, Малайзию и Новую Зеландию.

Согласно последнему годовому отчету, доля компании на рынке патентов в Австралии составляет примерно 34% (без учета инновационных патентов). Только в период с 2018 по 2021 год Гриффит Хак подал более 64 000 патентов и управляет более чем 33 000 товарных знаков». ***(Justin Hendry. Australian IP firms hit by cyber breach // InnovationAus.com Pty Ltd. (https://www.innovationaus.com/australian-ip-firms-hit-by-cyber-breach/). 16.03.2023).***

***

«Злоумышленники нацелены на разработчиков NET и заражают их с помощью похитителей криптовалюты, доставляемых через репозиторий NuGet и выдающих себя за несколько законных пакетов с помощью опечаток.

По словам исследователей безопасности JFrog Натана Нехораи и Брайана Муссалли, которые заметили эту продолжающуюся кампанию, три из них были загружены более 150 000 раз в течение месяца.

Хотя огромное количество загрузок может указывать на большое количество разработчиков.NET, чьи системы были скомпрометированы, это также можно объяснить попытками злоумышленников узаконить свои вредоносные пакеты NuGet.

«Три верхних пакета были загружены невероятное количество раз — это может быть показателем того, что атака была очень успешной, заразив большое количество машин», — заявили исследователи безопасности JFrog.

«Однако это не совсем надежный показатель успеха атаки, поскольку злоумышленники могли автоматически увеличить количество загрузок (с помощью ботов), чтобы пакеты выглядели более законными».

Злоумышленники также использовали опечатку при создании своих профилей репозитория NuGet, чтобы выдать себя за учетные записи разработчиков программного обеспечения Microsoft, работающих над диспетчером пакетов NuGet.NET…

Вредоносные пакеты предназначены для загрузки и выполнения сценария дроппера на основе PowerShell (init.ps1), который настраивает зараженную машину на выполнение PowerShell без ограничений.

«Такое поведение крайне редко встречается за пределами вредоносных пакетов, особенно если принять во внимание политику «неограниченного» выполнения, которая должна немедленно вызвать тревожный сигнал», — пояснили исследователи.

На следующем этапе он загружает и запускает полезную нагрузку второго этапа, исполняемый файл Windows, описанный JFrog как «полностью настраиваемая исполняемая полезная нагрузка».

Это необычный подход по сравнению с другими злоумышленниками, которые в основном будут использовать хакерские инструменты с открытым исходным кодом и стандартные вредоносные программы вместо того, чтобы создавать свои собственные полезные нагрузки.

Вредоносное ПО, развернутое на скомпрометированных системах, может быть использовано для кражи криптовалюты путем эксфильтрации криптовалютных кошельков жертв с помощью веб-хуков Discord, извлечения и выполнения вредоносного кода из архивов Electron и автоматического обновления путем запроса командно-административного управления, контролируемого злоумышленником (C2). сервер.

«Некоторые пакеты не содержали прямой вредоносной полезной нагрузки. Вместо этого они определяли другие вредоносные пакеты как зависимости, которые затем содержали вредоносный скрипт», — добавили исследователи.

Полезные нагрузки, доставленные в ходе этой атаки, имеют очень низкий уровень обнаружения и не будут отмечены как вредоносные Защитником, встроенным компонентом защиты от вредоносных программ в операционной системе Microsoft Windows.

Эта атака является частью более широкой злонамеренной деятельности, когда другие злоумышленники загрузили более 144 000 пакетов, связанных с фишингом, в несколько репозиториев пакетов с открытым исходным кодом, включая NPM, PyPi и NuGet, в рамках широкомасштабной активной кампании. на протяжении 2022 года». ***(Sergiu Gatlan. Hackers target.NET developers with malicious NuGet packages // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/hackers-target-net-developers-with-malicious-nuget-packages/). 20.03.2023).***

***

«…поскольку злоумышленники находят новые и инновационные способы запуска кибератак, Саудовская Аравия остается одной из наиболее целевых стран в регионе Ближнего Востока и Африки (MEA), на которую приходится две трети случаев, согласно ежегодному отчету X IBM Security - Force Threat Intelligence Index.

В отчете за 2023 год подчеркивается, что в 40% случаев развертывание бэкдоров было наиболее распространенным действием злоумышленников в случаях, когда X-Force отреагировала в Саудовской Аравии. Другие наблюдаемые действия варьируются от спам-кампаний до программ-вымогателей и рекламного ПО.

Согласно индексу, на финансовые и страховые организации приходилось две трети случаев, а остальные распределялись между производственными и профессиональными, деловыми и потребительскими услугами.

В отчете Ближний Восток и Африка занимают пятое место в списке регионов с наибольшей долей кибератак, наблюдаемых X-Force: 4% в 2022 году по сравнению с 14% в 2021 году. наиболее целевой регион, на который приходится

31% атак, выявленных во всем мире. Европа заняла второе место — на нее пришлось 28% атак, Северная Америка — третье с 25%, а Латинская Америка — четвертое с 12%.

«Саудовская Аравия, как и большая часть региона, переживает масштабную цифровую трансформацию. Теперь, когда Королевство признано одной из самых связанных стран в мире, необходимо предпринять активные действия для предотвращения и пресечения кибератак», — сказал Фахад Аль-Анази, генеральный директор IBM в Саудовской Аравии. «Это необходимо для защиты национальных интересов, роста и развития. Применяя системный подход и проявляя предвидение, мы можем защитить Королевство в будущем, укрепив безопасность и предотвратив потенциальные кризисы».

Аль-Анази продолжил: «IBM Security предлагает корпоративные решения в области кибербезопасности, которые помогают компаниям процветать в условиях неопределенности. Являясь крупнейшим поставщиком корпоративной безопасности, мы разработали передовой и интегрированный портфель продуктов и услуг для корпоративной безопасности. Эти предложения — от нашей защиты от программ-вымогателей до решений для облачной безопасности — основаны на искусственном интеллекте и современном подходе к стратегии безопасности с использованием принципов нулевого доверия. Предоставляя нашим клиентам эти инструменты, мы даем организациям, которым мы помогаем, возможность эффективно управлять рисками».

Глобальный индекс X-Force Threat Intelligence Index показывает, что, хотя доля программ-вымогателей в инцидентах снизилась лишь незначительно (на 4 процентных пункта) в 2022 году, защитники добились большего успеха в обнаружении и предотвращении программ-вымогателей. Несмотря на это, злоумышленники продолжали вводить новшества: в отчете показано, что среднее время для завершения атаки программы-вымогателя сократилось с двух месяцев до менее чем четырех дней.

IBM Security X-Force Threat Intelligence Index отслеживает новые и существующие тенденции и шаблоны атак, используя миллиарды точек данных из сетевых и конечных устройств, реагирование на инциденты и другие источники.

Некоторые из ключевых выводов отчета за 2023 год включают:

Вымогательство: метод обращения злоумышленников. Наиболее распространенным результатом кибератак в 2022 году было вымогательство, которое в основном достигалось с помощью программ-вымогателей или компрометации корпоративной электронной почты. Европа была наиболее целевым регионом для этого метода, на нее приходилось 44% наблюдаемых случаев вымогательства, поскольку злоумышленники стремились использовать геополитическую напряженность.

Киберпреступники превращают общение по электронной почте в оружие. В 2022 году значительно возросло количество перехватов потоков, когда злоумышленники использовали скомпрометированные учетные записи электронной почты, чтобы отвечать в текущих разговорах, выдавая себя за первоначального участника. X-Force заметил, что количество попыток в месяц увеличилось на 100% по сравнению с данными 2021 года.

Устаревшие эксплойты все еще работают. Доля известных эксплойтов по отношению к уязвимостям снизилась на 10 процентных пунктов с 2018 по 2022 год из-за того, что количество уязвимостей достигло очередного исторического максимума. Полученные данные показывают, что устаревшие эксплойты позволяли старым вредоносным программам, таким как WannaCry и Conficker, продолжать существовать и распространяться.

В отчете представлены данные, собранные IBM по всему миру в 2022 году, чтобы предоставить полезную информацию о глобальном ландшафте угроз и информировать сообщество безопасности об угрозах, наиболее актуальных для их организаций…» ***(IBM report: Saudi Arabia continues to be targeted by cyber threat actors // Zawya (https://www.zawya.com/en/press-release/research-and-studies/ibm-report-saudi-arabia-continues-to-be-targeted-by-cyber-threat-actors-t5m56ul5). 20.03.2023).***

***

«Для некоторых из вас фраза «серфинг на плече» может быть новой или вы можете считать ее синонимом, но это не так.

Это не что иное, как злоумышленник, пытающийся получить конфиденциальную информацию, заглядывая через плечо и проверяя экран, прослушивая разговор или перехватывая нажатия клавиш с помощью соответствующих инструментов шпионажа.

С помощью этой техники хакеры могут украсть конфиденциальные данные, такие как пароли, номера кредитных карт, одноразовые пароли, личные идентификационные номера, имена пользователей и, в некоторых случаях, банковские реквизиты из соответствующего банковского приложения, что делает его реальной угрозой.

Где проходит серфинг на плече?

Такие случаи происходят в местах массового скопления людей, в торговых центрах, аэропортах и других транзитных станциях, а в некоторых случаях и в банкоматах. Иногда они могут украсть информацию у невинной жертвы, используя такие изощренные средства, как бинокли, камеры видеонаблюдения, общедоступные сети Wi-Fi и камеры-шпионы. Затем они используют данные для утечки данных, кражи личных данных, финансовых потерь и тому подобного…

Почему плохие актеры занимаются серфингом через плечо?

Точнее говоря, для кражи деталей в этой тактике, связанной с атаками социальной инженерии, особых усилий не требуется. Хакеру просто нужно отвлечь

внимание жертвы и украсть данные, а поскольку это происходит в течение короткого периода времени, это может оказаться прибыльным.

Как уберечься от плечевого серфинга?

Это просто, просто знайте, что скрывается в киберпространстве, и действуйте соответственно. Например, держать экран устройства подальше от посторонних, используя пароль из 14-16 символов, который представляет собой смесь буквенно-цифровых символов и 1-2 специальных символов, 2FA всякий раз, когда мы получаем доступ к онлайн-аккаунтам, избегая общедоступных сетей для доступа к электронной почте и банковскому счету. услуги и вместо этого использовать функцию точки доступа на мобильном телефоне 5G или 4G, никогда не нажимая на ссылки, отправленные неизвестными отправителями в SMS, электронной почте или в учетных записях в социальных сетях, и, наконец, соблюдая базовые правила кибербезопасности. ***(Naveen Goud. Is Shoulder Surfing a threat to Cybersecurity // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/is-shoulder-surfing-a-threat-to-cybersecurity/). 03.2023).***

***

«…Для хакеров и киберпреступников уже существует множество механизмов атак, включая использование вредоносных программ, программ-вымогателей, отказ в обслуживании и фишинговые кампании. По мере того, как технологии продолжают развиваться и совершенствоваться, меняются и методы и приемы хакеров для проведения кибератак. Одной из областей, в которой киберпреступники активно работают, является использование технологии дипфейков. Системы искусственного интеллекта и машинного обучения предлагают огромные технологические преимущества для компаний, а также потенциальные новые точки входа для решительных киберпреступников, стремящихся проникнуть в новые системы. Например, использование биометрических технологий для входа в систему стало мишенью для кибератак со стороны хакеров, использующих технологии глубокой подделки, чтобы попытаться

клонировать и подделывать аутентификацию по голосу, изображению и отпечатку пальца.

Компании сопротивляются, внедряя множественные аутентификации без пароля (например, push-уведомления на мобильных устройствах) и даже платформы поведенческой биометрии для контроля и ограничения несанкционированного доступа к системам. Поведенческая биометрия, в частности, использует программы непрерывной аутентификации для анализа шаблонов и поведения пользователя в течение его сеанса (т.е. не только во время процесса входа в систему), чтобы обнаружить подозрительную активность, которая отличается от их обычных индивидуальных моделей. Это может включать в себя действия мыши, движения клавиш, поведение сенсорного экрана и движение устройства.

Несмотря на такое технологическое развитие, компании должны помнить о двух вещах при рассмотрении своего профиля риска. Во-первых, подавляющее большинство внешних атак относительно просты и по-прежнему полагаются на индивидуальную человеческую ошибку, например, когда сотрудник нажимает на вредоносную ссылку в фишинговом электронном письме. Во-вторых, хотя внутренние атаки (например, со стороны недовольного сотрудника) случаются гораздо реже, чем внешние атаки, они, как правило, наносят гораздо больший ущерб.

Изменения в правовой сфере кибербезопасности

Правовая среда в области кибербезопасности, с которой сталкиваются международные компании, включает в себя сочетание устаревших, новых, частично совпадающих законов и законов, действующих в конкретных странах. В свете постоянно меняющегося ландшафта угроз кибербезопасности и изощренности инструментов, используемых киберпреступниками, в крупнейших мировых экономиках признается необходимость укрепления и развития законов о кибербезопасности.

Например, ЕС недавно принял Директиву (ЕС) 2022/2555 («НИШ 2»), целью которой является повышение общего уровня кибербезопасности в широком круге

организаций, работающих в ЕС (в том числе в энергетике, транспорте, вода, банковское дело, инфраструктура финансового рынка, здравоохранение, цифровая инфраструктура и секторы цифровых услуг). NIS 2 вводит ряд обязательств, связанных с кибербезопасностью, в том числе обязательства, связанные с организационным управлением, управлением операционными рисками и отчетностью о кибер-инцидентах. Каждое государство-член ЕС должно принять законы в своей юрисдикции, чтобы ввести в действие NIS 2 к 17 октября 2024 года.

Аналогичным образом, после консультаций с общественностью в начале 2022 года правительство Великобритании изложило свое предложение по обновлению правовой базы Великобритании в области кибербезопасности. Ожидается, что эта обновленная правовая база будет охватывать более широкий круг организаций, изменит подход к регулирующему надзору и расширит масштаб кибер-инцидентов, о которых необходимо сообщать регулирующим органам и затронутым лицам. Правительство Великобритании также в настоящее время проводит консультации по обновлению устаревшего законодательства, криминализирующего деятельность киберпреступников.

Компании, работающие в разных юрисдикциях, должны быть знакомы с законами о кибербезопасности, применимыми к их деятельности. В частности, компании должны понимать свои обязательства при разработке стратегий реагирования на нарушения кибербезопасности и системы управления рисками кибербезопасности, а также влияние, которое законы конкретной страны могут оказывать на эти системы (например, законность услуг «этичных хакеров»), а также нормативная отчетность. обязательства, которые вступают в силу после нарушения кибербезопасности.

Правовые и иные последствия нарушений кибербезопасности

Последствия нарушений кибербезопасности могут быть серьезными для компаний, которые от них страдают, начиная от крупных штрафов и санкций регулирующих органов, государственных проверок, длительных расследований регулирующих органов и даже уголовной ответственности. Сбои в бизнесе и потеря данных, ИС и конфиденциальной информации также могут быть

чрезвычайно разрушительными, а также очень дорогостоящими с точки зрения финансовых потерь, положения на рынке и затрат на меры по исправлению положения. Возможно, что еще более важно, компании, которые страдают от нарушений кибербезопасности, оказываются открытыми для негативного внимания средств массовой информации и неизмеримого ущерба от потери доверия и уверенности потребителей.

Компании также подвергаются угрозе судебного разбирательства со стороны клиентов, сотрудников и деловых партнеров, особенно в тех случаях, когда эти группы утверждают, что понесли реальные финансовые убытки. В США акционеры подали коллективные иски против компаний, когда объявленные нарушения кибербезопасности привели к падению цены акций компании, предположительно из-за неадекватных мер безопасности.

Обязательства по раскрытию

В случае серьезного нарушения кибербезопасности компании должны учитывать свои обязанности перед компанией по сдерживанию и устранению нарушения, а также любые обязательства, вытекающие из соответствующих законов и правил. Им также необходимо учитывать свои договорные обязательства и обязательства. Серьезным нарушением кибербезопасности, вероятно, будет событие, требующее раскрытия информации потребителям и регулирующим органам в соответствии с действующим законодательством, инвесторам и крупным акционерам в соответствии с инвестиционным соглашением или соглашением между акционерами/акционерами, а также банкам и кредиторам в соответствии с существенным долгом или другими соглашениями о финансировании и обеспечении.

Потенциальные новые инвесторы и покупатели компаний рассчитывают получить подробную информацию о любых существенных нарушениях кибербезопасности и рисках кибербезопасности в рамках их процесса должной осмотрительности, чтобы они могли учесть потенциальные затраты, связанные с этими проблемами, в своем финансовом моделировании и оценке, структуре своего предложения и общая стоимость сделки. Адекватность политик и практик

компании в области кибербезопасности обычно определяется заявлениями и гарантиями, которые должны быть даны в инвестиционном договоре или договоре купли-продажи, и на них распространяются требования о раскрытии информации. Покупатели и инвесторы часто обращаются за дополнительной договорной защитой посредством возмещения убытков, ценовых вычетов или удержания убытков, вытекающих из исторических нарушений кибербезопасности (будь то в виде потенциальных штрафов регулирующих органов, судебных исков клиентов или иным образом), и эти меры защиты могут оказать существенное влияние на экономику сделки. Приобретателям также потребуются гарантии адекватности программы кибербезопасности компании для целей планирования перехода и интеграции после закрытия сделки, особенно когда системы должны быть объединены или интегрированы, должен быть предоставлен доступ к общим системам и/или данные предназначены для совместного использования или обработки.

В случае публичных компаний, советы директоров и другие должностные лица должны будут тщательно рассмотреть вопрос о том, нужно ли раскрывать информацию о рисках и проблемах кибербезопасности соответствующим рынкам и/или регулирующим органам, например, в периодических публичных документах компании. В США как в недавнем решении суда, так и в Руководстве SEC подчеркивается важность обновления факторов риска в периодических отчетах для учета существенных изменений, в том числе связанных с рисками кибербезопасности. В случае серьезного несоблюдения могут быть суровые санкции.

Персональная ответственность директоров и должностных лиц?

Хотя судебные иски и действия регулирующих органов обычно направлены на компанию, пострадавшую от нарушения кибербезопасности, директорам и должностным лицам не следует успокаиваться на рисках личных претензий в связи с халатностью или нарушением фидуциарных обязанностей. В США против директоров компаний были предприняты прямые судебные иски, в том числе со стороны Министерства юстиции и Федеральной торговой комиссии, в ответ на

управление нарушением кибербезопасности, сообщение об этом нарушении и предполагаемые неспособности защитить личную информацию клиентов.

Вполне возможно, что британские и другие европейские власти решат последовать примеру своих американских коллег и привлечь директоров к личной ответственности и порицанию со стороны регулирующих органов в результате ошибок руководства, которые приводят к кибератаке или (что не менее важно) впоследствии неправильному обращению или отказ сообщить о нарушении кибербезопасности. Такой подход не будет отличаться от все более агрессивной позиции, уже занимаемой властями и регулирующими органами в нескольких юрисдикциях по вопросам, связанным с ESG.

Примечательно, что директива NIS 2, недавно введенная в ЕС, требует, чтобы законы, применяемые в каждом государстве-члене ЕС, уполномочивали органы управления соответствующих организаций анализировать меры по управлению рисками кибербезопасности, которые реализуются для соответствия NIS 2, и контролировать их выполнение. меры. Важно отметить, что органы управления могут быть привлечены к ответственности за сбои в реализации мер по управлению рисками кибербезопасности.

Снижение риска кибербезопасности

Компании могут многое сделать для снижения рисков кибербезопасности и одновременно помочь защитить положение своих директоров и должностных лиц. Британские регулирующие органы давно дали понять, что кибербезопасность — это вопрос на уровне совета директоров, который требует серьезного и значимого участия высшего руководства. На коммерческом уровне необходимы четкие рекомендации экспертов по кибербезопасности, а также профессиональные продукты и услуги, чтобы гарантировать наличие надлежащих и разумных мер кибербезопасности, чтобы программное обеспечение и системы постоянно обновлялись, проверялись, были надежными и пригодными для использования. Цель, чтобы доступ к ним контролировался должным образом, конечные точки были защищены, а данные были надлежащим образом скопированы.

С юридической точки зрения компании должны иметь политики и признанные стандарты, в том числе в отношении реагирования на инциденты, безопасности и хранения данных, а также надежные программы обучения и мониторинга сотрудников. Следует также следовать рекомендациям по удаленной аутентификации и авторизации сотрудников, чтобы ограничить несанкционированный доступ к корпоративному программному обеспечению, файлам и интрасети (что может включать в себя использование сторонних сервисов аутентификации). Это должно сочетаться с соответствующими структурами и процессами управления. Контракты с сотрудниками, поставщиками и третьими сторонами должны включать соответствующие положения по таким вопросам, как стандарты безопасности, доступ к данным, управление и контроль, а также ответственность. Необходимо тщательно продумать подходящее страхование кибербезопасности с достаточным покрытием для реагирования на инциденты и их устранения, уведомления о нарушениях, сбоев и убытков на уровне бизнеса, а также связанных с этим юридических вопросов, таких как нормативные штрафы и дополнительные расходы на консультации. Любые исключения из страхового полиса должны быть тщательно проверены.

В современных условиях наличие как надежных мер кибербезопасности, так и плана устранения нарушений кибербезопасности в случае их возникновения имеет важное значение для всех компаний. Те компании и советы, которые предпочитают игнорировать это, делают это на свой страх и риск». ***(Ian Ivory, F. Paul Pittman, John Timmons, Lawson Caisley, Alan Burke, Arlene Arin Hahn, Daniel Turgel. Cybersecurity Developments and Legal Issues // White & Case LLP (https://www.whitecase.com/insight-alert/cybersecurity-developments-and-legal-issues). 22.03.2023).***

***

«…В недавнем отчете Consumer Cybersecurity Trends исследователи RAV обнаружили, что в 2022 году 15% всех вредоносных веб-расширений были обнаружены в США. Кроме того, наиболее распространенная полезная нагрузка вредоносных расширений веб-браузера в первой половине 2022 года принадлежала семействам рекламного ПО, отслеживанию активности в Интернете и продвижению партнерских ссылок.

Рост числа вредоносных расширений вызывает беспокойство, поскольку пользователи не знают, когда они стали мишенью, и тем не менее они могут причинить устройствам большой ущерб. Вредоносные действия вредоносных расширений могут включать захват результатов поиска и захват главной вкладки или кражу личных данных, таких как информация о кредитной карте. Также распространена замена баннеров и рекламы вредоносными версиями, которые могут привести к загрузке вредоносных файлов, а также приглашение дропперов, которые могут привести к установке большего количества вредоносных программ на устройство.

Чаще всего эти расширения недоступны в Интернет-магазине Chrome, что может сильно разочаровать многих пользователей. Зачастую они даже не могут сказать, как и откуда появляется вредоносное расширение.

Компрометация многофакторной аутентификации

Хотя двухфакторная аутентификация (2FA) была впервые разработана в 80-х годах, она стала более популярной среди потребителей только в 2010-х годах. Одной из причин этой массовой потребности и стремительного роста популярности 2FA было то, что отдельные сотрудники начали использовать свои собственные смартфоны как в личных, так и в рабочих целях.

Развитие многофакторной аутентификации (MFA) сопряжено с дополнительными угрозами компрометации паролей и обхода этих аутентификаторов. Одной из таких растущих угроз является замена сим-карты, которая может привести к легкому сбою 2FA с помощью текстовых сообщений или электронной почты. Действительно, обход 2FA становится настолько

распространенным явлением, что я предсказываю грядущий сдвиг в отрасли, который будет включать трех- или даже четырехфакторную аутентификацию вместо двух. Домашние пользователи должны быть осведомлены о возможных угрозах и использовать как можно больше факторов аутентификации.

Продвинутая тактика фишинга

Фишинг будет по-прежнему представлять собой постоянную угрозу для всех потребителей. Поскольку фишинг основан на социальной инженерии, те, кто работает удаленно, могут не иметь возможности спросить совета у коллеги, прежде чем нажать на вложение, которого им следует избегать.

Поскольку эта стратегия взлома существует уже некоторое время, есть некоторые классические признаки, которые, как мы надеемся, уже знают потребители, например, неправильная грамматика, орфографические ошибки, необычные URL-адреса и т. д. Однако эволюция фишинга привела к появлению новых тактик, которые вы можете использовать. не знать. Популярные современные тенденции фишинга включают превращение документов Office в оружие, а также типичные угрозы фишинга по SMS и электронной почте, которые продолжают мучить домашних пользователей.

В 2023 году новые популярные приложения позволили злоумышленникам усилить свою игру — например, есть опасения, что чат-боты с искусственным интеллектом могут быть использованы для создания фишинговых электронных писем.

Малый и средний бизнес должен быть обеспокоен утечкой данных

Поскольку крупные компании продолжают вкладывать миллионы в укрепление своей кибербезопасности, злоумышленники все чаще обращаются к малому и среднему бизнесу (SMB) и частным лицам, чтобы получить свою зарплату. Но один большой удар, и малый бизнес вполне может оказаться не у дел.

Нарушение данных не только ставит под угрозу сам бизнес, но также влияет на доверие между клиентом и бизнесом и может привести к неоправданным финансовым потерям. Что может сделать малый бизнес, чтобы защитить себя и своих удаленных сотрудников?

Здравый смысл и образование на самом деле два самых больших актива домашних пользователей. Рекомендуются практические превентивные меры, такие как использование брандмауэра, а также использование других важных компонентов полного пакета кибербезопасности, включая VPN, DNS и решение EDR.

Стеганография

Стеганография происходит от древнего искусства сокрытия информации на виду у объектов, не вызывающих подозрений. В современном мире под стеганографией понимают практику сокрытия вредоносного кода внутри файла изображения, который при открытии выглядит нормально. Недавний пример произошел, когда хакеры Worok спрятали вредоносное ПО в файлах PNG и нацелились на высокопоставленных государственных чиновников.

Использование стеганографии во вредоносном ПО осуществляется путем деления программы на байты и разбрасывания этих байтов внутри информации изображения. Изображения представлены пикселями, где каждый пиксель определяется 24 битами. Есть несколько способов скрыть информацию с помощью пикселей, наиболее распространенным из которых является изменение младшего значащего бита пикселя. Таким образом, изменение цвета незаметно, а к нему можно добавить информацию. Эта новая угроза становится все более популярной, и AV-провайдеры должны обновлять свои системы, чтобы распознавать эти сложные угрозы.

Последние мысли

Пока в 2023 году темпы развития технологий и темпы их эксплуатации не показывают признаков замедления. Руководители предприятий и сотрудники должны принимать дополнительные меры для защиты, защиты и смягчения последствий любых текущих и возникающих угроз. Если сотрудникам предоставляется программное и аппаратное обеспечение организации для использования дома, организация должна отдавать приоритет использованию исправлений и обновлений по мере необходимости.

Точно так же использование самого современного программного обеспечения для кибербезопасности на рынке является обязательным. Новейшие инструменты, такие как EDR, следуют технологическим тенденциям. Это необходимо, так как мы не всегда можем предвидеть, куда может пойти тенденция киберпреступности». ***(Andrew Newman. 5 cybersecurity trends people who work from home need to know // Mansueto Ventures, LLC (https://www.fastcompany.com/90859303/5-cybersecurity-trends-people-who-work-from-home-need-to-know?partner=rss&utm_source=rss&utm_medium=feed&utm_campaign=rss+fastcompany&utm_content=rss). 04.03.2023).***

***

«Компанія ESET виявила новий бекдор, який поширюється китайською групою кіберзлочинців Mustang Panda з початку 2023 року. Шкідлива програма націлена на політичні та державні організації в Європі та Азії, а також на установи в Болгарії та Австралії.

Варто зазначити, що наразі група Mustang Panda все ще активна, а сплеск її діяльності відбувся після вторгнення росії в Україну.

Виявлений бекдор MQsTTang дозволяє зловмисникам виконувати довільні команди на комп'ютері жертви та отримувати результати. Поширюється шкідлива програма через архіви RAR з виконуваним файлом всередині. Назви цих файлів зазвичай пов'язані з дипломатією та паспортами.

«На відміну від більшості шкідливих програм групи MQsTTang не створена на основі існуючих сімейств або доступних проектів, — розповідає Александр Коте Сір, дослідник ESET. — Це свідчить про те, що Mustang Panda досліджує нові технології для своїх інструментів. Згодом стане зрозуміло, чи буде цей бекдор постійною частиною їхнього арсеналу, однак загроза є ще одним прикладом швидкого циклу розробки та розгортання шкідливих програм групою».

Телеметрія ESET підтверджує, що ціллю кіберзлочинців є невідомі організації в Болгарії та Австралії. Ще однією мішенню є державна установа в

Тайвані. Тоді як назви файлів-приманок вказують, що серед цілей загрози також є політичні та державні організації в Європі та Азії.

Для з'єднання з командним сервером шкідливе програмне забезпечення застосовує протокол MQTT. Цей протокол MQTT зазвичай використовується для з'єднання між пристроями Інтернету речей і контролерами та не застосовувався раніше відомими сімействами шкідливих програм.

У зв'язку з небезпекою атак спеціалісти ESET рекомендують дотримуватися основних правил кібербезпеки, зокрема не відкривати невідомі листи та документи, використовувати складні паролі та двофакторну автентифікацію, вчасно оновлювати програмне забезпечення, а також забезпечити надійний захист домашніх пристроїв та корпоративної мережі». ***(Герман Богапов. Новий бекдор атакує державні установи країн Європи та Азії // HiTech.Expert (https://expert.com.ua/156711-novyy-bekdor-atakuye-derzhavni-ustanovy-krain-yevropy-ta-azii.html). 02.03.2023).***

***

«В наш современный технологический век преступность вышла за рамки того, что было раньше. Сегодня преступники могут красть данные и деньги с помощью различных вредоносных программ, в том числе кейлоггеров.

Известным примером вредоносного ПО этого типа является Snake Keylogger…

Кейлоггер — это тип вредоносной программы, используемой для регистрации нажатий клавиш. Другими словами, кейлоггеры могут записывать каждую клавишу, нажатую на клавиатуре. Если вы вводите пароль, ведете текстовую беседу, вводите платежную информацию или делаете буквально что-то еще с помощью клавиатуры, кейлоггер примет это к сведению, если ваше устройство заражено.

Благодаря этому журналу злоумышленник, контролирующий программу, может видеть, что вы вводите на своем устройстве, что дает ему возможность украсть много данных.

Примеры известных кейлоггеров включают Spyrix, Ardamax и, конечно же, Snake Keylogger.

Snake Keylogger — это модульная вредоносная программа, созданная с использованием платформы для разработчиков.NET. Впервые он был обнаружен в дикой природе в ноябре 2020 года и, как известно, ворует учетные данные, данные буфера обмена и другую информацию. Как отдельные лица, так и организации могут стать жертвами Snake Keylogger, который можно купить на вредоносных торговых площадках, таких как хакерские форумы.

Snake Keylogger обычно распространяется через фишинговые кампании. Фишинг — популярная тактика мошенничества, с помощью которой киберпреступники крадут данные жертв через вредоносные ссылки и вложения. Фишинг распространен по электронной почте, но также может осуществляться с помощью SMS и сообщений или сообщений в социальных сетях. Snake Keylogger также может распространяться с помощью целевого фишинга, при котором конкретные жертвы преследуют определенную цель.

Когда Snake Keylogger отправляется потенциальной жертве, он содержится во вложении. Если получатель открывает вложение, ему предлагается открыть файл DOCX. Этот файл DOCX содержит макрос (разновидность компьютерного вируса), который позволяет запускать Snake Keylogger. Если жертва использует версию Microsoft Office с уязвимостями в системе безопасности (которые часто проявляются в виде недостатков программного обеспечения), кейлоггер может использовать их и заразить устройство. Читатели PDF, содержащие такие недостатки, также могут быть использованы Snake Keylogger для развертывания.

Snake Keylogger также может делать скриншоты на зараженном устройстве, предоставляя оператору еще больше возможностей для кражи ценной информации.

Затем Snake Keylogger может взять записанные данные и передать их злоумышленнику, который затем может использовать их любым удобным для них

способом. Злоумышленник может либо использовать ее напрямую (например, взломав банковский счет с помощью украденных учетных данных), либо продать скрытую информацию другим злоумышленникам на нелегальных торговых площадках. В даркнете полно таких платформ, где можно получить все виды данных, включая платежную информацию, учетные данные, адреса электронной почты и даже номера социального страхования.

Есть еще один аспект Snake Keylogger, который делает его особенно опасным. Snake Keylogger на самом деле имеет возможность обойти антивирусную защиту, которая часто выступает в качестве первой линии защиты для большинства людей. На самом деле, многие используют антивирус исключительно как форму защиты на своих устройствах, поскольку часто предполагается, что антивирусные программы могут обнаруживать и удалять все вредоносные программы.

Таким образом, если Snake Keylogger удастся обойти это программное обеспечение и не будут установлены другие защитные линии, целевое устройство может быть быстро заражено и использовано.

В прошлом Snake Keylogger обычно распространялся через вредоносные PDF-файлы. В одной из таких кампаний, по данным ThreatPost, использовалась уязвимость Office RCE 22-летней давности для распространения среди устройств Snake Keylogger.

Также существуют варианты Snake Keylogger, что является нормой для популярных вредоносных программ. Например, в конце 2021 года был обнаружен новый вариант Snake Keylogger. Как сообщает Fortinet, этот вариант представляет собой образец Microsoft Excel, отправляемый жертвам в виде вложения электронной почты.

Хотя Snake Keylogger может оказаться скрытой формой вредоносного ПО, есть вещи, которые вы можете сделать, чтобы избежать его.

Чтобы избежать Snake Keylogger, необходимо принять ряд мер безопасности, первой из которых является установка антивирусного программного обеспечения. Хотя Snake Keylogger может обходить антивирусные программы в определенных сценариях, крайне важно иметь на своих устройствах законного и эффективного

антивирусного поставщика для обнаружения клавиатурных шпионов и других форм вредоносных программ.

Кроме того, вы всегда должны быть осторожны с любыми вложениями электронной почты, которые вы получаете, особенно от новых или подозрительных отправителей. Вложения очень часто используются для распространения вредоносных программ, и Snake Keylogger является лишь одним из многих примеров. Если вы когда-либо получали вложение электронной почты от отправителя, которому вы не полностью доверяете, рассмотрите возможность его проверки через сканер вложений, который обнаружит любые возможные угрозы внутри.

Вы также должны помнить о расширении файла, используемого во вложениях, отправленных вам. Существуют определенные расширения файлов, которые часто используются при распространении вредоносных программ, включая.exe,.pdf,.zip,.doc и.rar.

Чтобы избежать нежелательной почты (которая часто используется для распространения вредоносных программ), убедитесь, что спам-фильтр вашего поставщика услуг электронной почты включен. Это гарантирует, что вся почта с признаками спама будет отправлена в отдельную папку, а не в основной почтовый ящик.

Вы также должны убедиться, что операционная система вашего устройства, а также все установленные приложения часто обновляются. Как упоминалось ранее, Snake Keylogger заражает устройства, используя уязвимости в программном обеспечении. Обновления часто сглаживают эти недостатки, а это означает, что киберпреступники больше не могут ими злоупотреблять. Вы можете запланировать для своих приложений и операционной системы автоматические обновления или просто часто проверять свои настройки и магазин приложений по умолчанию, чтобы узнать, не нужно ли обновлять обновления.

Признаки змеиного кейлоггера

Существуют предупреждающие знаки, которые могут указывать на наличие Snake Keylogger на вашем устройстве, в том числе...

Перегрев.

Медленная производительность.

Задержка нажатия клавиш.

Частые сбои.

Нажатия клавиш и/или курсор не отображаются на экране.

Если вы считаете, что ваше устройство заражено Snake Keylogger, ознакомьтесь с нашим удобным руководством по удалению, чтобы избавиться от него как можно скорее.

Благодаря возможности регистрировать данные, делать снимки экрана, извлекать ценную информацию и даже обходить антивирусную защиту, Snake Keylogger, несомненно, является опасной программой. Эта форма кейлоггера уже нацелена на многих жертв и может продолжать использоваться в злонамеренных эксплойтах в будущем. Поэтому обязательно следуйте приведенным выше советам, чтобы защитить себя от Snake Keylogger». ***(Katie Rees. What Is Snake Keylogger and Are You at Risk? // MUO (https://www.makeuseof.com/what-is-snake-keylogger-and-are-you-at-risk/). 11 03 2023).***

***

«В дикой природе была обнаружена новая версия опасного вредоносного ПО Xenomorph для Android, которое включает в себя ряд новых возможностей, включая возможность кражи учетных данных из 400 различных банковских приложений.

Первоначальное вредоносное ПО Xenomorph, впервые обнаруженное фирмой по кибербезопасности ThreatFabric в феврале прошлого года, представляло собой банковский троян, распространяемый через вредоносные приложения в магазине Google Play. Что делало его особенно опасным, так это то, как он использовал оверлеи 56 европейских банковских приложений для кражи учетных данных пользователей и слива их учетных записей.

Затем, в июне 2022 года, был выпущен Xenomorph v2 с капитальным пересмотром кода, который сделал вредоносное ПО модульным и более гибким.

Однако теперь, как сообщает BleepingComputer (открывается в новой вкладке), ThreatFabric снова обнаружила третью версию вредоносного ПО.

Эта новая версия предназначена для 400 банков и финансовых учреждений из США, Канады, Индии и ряда европейских стран, включая Chase, Citibank, American Express, ING, HSBC, Wells Fargo, Национальный банк Канады и другие…

Xenomorph v3 добавляет множество новых функций, которые делают его еще более опасным, в том числе возможность автоматически красть данные, такие как учетные данные и балансы счетов, но он также может выполнять банковские операции и переводить средства.

В своем отчете по этому вопросу ThreatFabric объясняет, что «Xenomorph теперь может полностью автоматизировать всю цепочку мошенничества, от заражения до кражи средств», что делает его одним из самых передовых и опасных вредоносных троянов для Android, находящихся в настоящее время в обращении. Помимо 400 банковских и финансовых учреждений, теперь он также может красть криптовалюту из нескольких криптокошельков.

Изучив образцы Xenomorph v3, ThreatFabric обнаружила специальный веб-сайт, рекламирующий последнюю версию вредоносного ПО. «вредоносное ПО как услуга» (MaaS Это намекает на тот факт, что Hadoken Security, создавшая вредоносное ПО, стремится распространять его, используя бизнес-модель). Таким образом, он будет продаваться другим киберпреступникам по модели подписки для использования в их атаках.

Однако на данный момент Xenomorph v3 распространяется через платформу Zombinder в магазине Google Play. Эта платформа особенно опасна из-за того, что создавшие ее хакеры нашли способ добавлять вредоносное ПО в легитимные приложения для Android. В отличие от вредоносных приложений, это обычные приложения для Android, содержащие вредоносную полезную нагрузку.

Обход MFA и кража файлов cookie

Если этого недостаточно, ATS-фреймворк Xenomorph v3 позволяет киберпреступникам автоматически извлекать учетные данные, проверять баланс счета, красть деньги и многое другое с зараженного Android-смартфона.

Платформа ATS вредоносного ПО также позволяет ему обходить многофакторную аутентификацию (MFA), которая обычно используется для блокировки таких типов автоматических транзакций. Вместо того, чтобы использовать текстовые SMS-сообщения для MFA в своих банковских приложениях, вы можете обойти это, используя вместо этого приложение для проверки подлинности, такое как Google Authenticator или Microsoft Authenticator. Однако не все банки в настоящее время предлагают такую возможность.

Xenomorph v3 даже включает похититель файлов cookie, который может забирать файлы cookie вашего телефона из диспетчера файлов cookie Android. Он делает это, запуская окно браузера законной службы и обманом заставляя жертву ввести свои учетные данные. Имея эти файлы cookie сеанса, хакер может перехватить веб-сеанс и завладеть вашими учетными записями.

Если вы еще не поняли, Xenomorph v3 — это очень серьезная угроза, которая может опустошить ваши банковские счета и завладеть другими вашими учетными записями в Интернете, поскольку она автоматически крадет пароли.

В настоящее время оно распространяется с помощью Zombinder в Play Store, поэтому вам нужно быть предельно осторожным при установке новых приложений на лучшие телефоны Android, даже если они поступают из официальных магазинов приложений. В то же время рекомендуется ограничить общее количество приложений, установленных на вашем телефоне.

Однако при установке новых приложений вы хотите сначала проверить их рейтинги и прочитать обзоры в Play Store. Отсюда вы также можете искать внешние обзоры на других сайтах, а видеообзоры еще лучше, поскольку вы можете увидеть приложение в действии. Изучить издателя приложения — хорошая идея, так как это может помочь вам определить, являются ли они законными.

Что касается защиты вашего телефона Android, вы должны убедиться, что Google Play Protect включен, поскольку он сканирует ваши существующие приложения и любые новые, которые вы устанавливаете, на наличие вредоносных программ. одно из лучших антивирусных приложений для Android. Для дополнительной защиты вы всегда можете установить вместе с ним

Скорее всего, это не последний раз, когда мы слышим о Xenomorph v3, тем более что его создатели хотят сделать его платным сервисом, который другие киберпреступники смогут использовать в своих атаках». ***(Anthony Spadafora. Xenomorph Android malware can steal passwords from 400 banking apps — protect yourself now // Future US, Inc. (https://www.tomsguide.com/news/xenomorph-android-malware-can-steal-passwords-from-400-banking-apps-protect-yourself-now). 10.03.2023).***

***

«Недавно обнаруженная вредоносная программа ботнета на основе Golang сканирует и заражает веб-серверы, на которых запущены службы phpMyAdmin, MySQL, FTP и Postgres.

По словам исследователей из Palo Alto Networks Unit 42, которые первыми обнаружили его в дикой природе и назвали GoBruteforcer, вредоносное ПО совместимо с архитектурами x86, x64 и ARM.

GoBruteforcer будет перебирать учетные записи со слабыми паролями или паролями по умолчанию для взлома уязвимых устройств *nix.

«Для успешного выполнения образцы требуют особых условий в системе-жертве, таких как использование определенных аргументов и уже установленных целевых служб (со слабыми паролями)», — сказали исследователи.

Для каждого целевого IP-адреса вредоносная программа начинает поиск служб phpMyAdmin, MySQL, FTP и Postgres. После обнаружения открытого порта, принимающего соединения, он попытается войти в систему, используя жестко заданные учетные данные.

После входа он развертывает IRC-бот на скомпрометированных системах phpMyAdmin или веб-оболочку PHP на серверах, на которых запущены другие целевые службы.

На следующем этапе атаки GoBruteforcer обратится к своему серверу управления и контроля и будет ждать инструкций, которые будут доставлены через ранее установленный IRC-бот или веб-шелл.

Ботнет использует модуль мультисканирования для поиска потенциальных жертв в рамках бесклассовой междоменной маршрутизации (CIDR), предоставляя ему широкий выбор целей для проникновения в сети.

Перед сканированием IP-адресов для атаки GoBruteforcer выбирает блок CIDR и нацеливается на все IP-адреса в этом диапазоне.

Вместо того, чтобы нацеливаться на один IP-адрес, вредоносное ПО использует сканирование блоков CIDR для доступа к разнообразному диапазону хостов с разными IP-адресами, увеличивая охват атаки.

GoBruteforcer, вероятно, находится в активной разработке, и ожидается, что его операторы будут адаптировать свою тактику и возможности вредоносного ПО для нацеливания на веб-серверы и опережать средства защиты.

«Мы видели, как это вредоносное ПО удаленно развертывало различные типы вредоносных программ в качестве полезной нагрузки, включая майнеры монет», — добавил Unit42.

«Мы считаем, что GoBruteforcer находится в активной разработке, и поэтому в ближайшем будущем могут измениться такие вещи, как исходные векторы заражения или полезная нагрузка». ***(Sergiu Gatlan. New GoBruteforcer malware targets phpMyAdmin, MySQL, FTP, Postgres // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/new-gobruteforcer-malware-targets-phpmyadmin-mysql-ftp-postgres/). 10.03.2023).***

***

Програми-вимагачі

«Городские власти Окленда подтвердили, что некоторая информация, украденная из городской компьютерной сети, была раскрыта хакерами-вымогателями, взломавшими городскую сеть в начале февраля.

Город работает над тем, чтобы определить, какие данные были опубликованы, и заявил, что уведомит лиц, затронутых выпуском данных. Тем

временем городских работников просят следить за своими банковскими выписками и кредитными картами.

На этой неделе некоторые городские службы были восстановлены и возобновили работу. Теперь люди могут оплачивать свои дорожные билеты онлайн. Телефонная линия 311 снова работает, и люди сообщают о поваленных деревьях и подобных проблемах.

Многие другие городские телефонные номера все еще не работают, а также веб-сайт, на котором бизнес-операторы могут платить налоги.

«Мы попытались пойти дальше (на городской веб-сайт) и заплатить налоги, и теперь нам нужно ждать, чтобы заплатить наши налоги», — сказала Кристал Вахпепа, владелица кухни Вахпепа.

Она сказала, что нет ничего плохого в том, чтобы держать свои деньги подольше, но неудобно постоянно сверяться с городом, чтобы узнать, когда она сможет заплатить. Она беспокоится, что может забыть и накопить штрафы за просрочку платежа.

«Особенно владелец малого бизнеса, у нас много дел и много вещей, через которые нам приходится маневрировать (и сейчас) мы должны маневрировать через эту (ситуацию с атакой программ-вымогателей)», — сказал Вахпепах.

Вахпепа открыла свой ресторан в Fruitvale Village более года назад.

«Это первый ресторан коренных американцев здесь, в Окленде», — сказал Вахпепах.

Срок уплаты налога на бизнес в Окленде был 1 марта. Крайний срок был продлен до 17 апреля, поскольку веб-сайт не работает.

«Проблемы с уплатой налогов — именно поэтому муниципалитеты становятся мишенью, потому что они предоставляют так много критически важных услуг. И, опять же, они пытаются причинить как можно больше страданий жертвам, чтобы заставить их платить», — сказал Дэвис Хейк., эксперт по кибербезопасности, живущий в Окленде.

Хейк работал на правительство США и является соучредителем Resilience, компании, которая предоставляет киберстрахование и работает с компаниями для предотвращения атак программ-вымогателей.

Он не работает непосредственно над делом Окленда, но знаком с группой, взявшей на себя ответственность за нападение. Группа называется Play.

«Play в частности была одной из самых активных групп в этом году. Они используют тактику под названием «Охота на крупную дичь», и в ее рамках они специально преследуют крупные, известные цели, у которых может быть много ресурсов, чтобы попытаться вымогать.... И это интересно, потому что многие инструменты, которые они используют, на самом деле связывают их с другими группами вымогателей, которые проводили атаки по всему миру. Поэтому неудивительно, что они нацелены на такой муниципалитет, как Окленд», — сказал Хейк.

Член городского совета Окленда Ноэль Галло сказал, что город работает с ФБР и экспертами по кибербезопасности, чтобы решить эту проблему. Он не сказал, сколько денег киберпреступники требуют от города, но признал, что это миллионы.

«У нас достаточно проблем, но с этой она затрагивает всех нас. И, как ни печально, если будут задействованы деньги, то это будут доллары наших налогоплательщиков, которые покроют расходы», — сказал член совета Галло». ***(Da Lin. Ransomware hackers release some stolen Oakland data // CBS Broadcasting Inc. (https://www.cbsnews.com/sanfrancisco/news/ransomware-hackers-release-some-stolen-oakland-data/). 04.03.2023).***

***

«Правительство США бьет тревогу в связи с операцией по вымогательству Royal, которая, по его словам, нацелена на многочисленные критически важные секторы инфраструктуры в Соединенных Штатах.

В совместном бюллетене, опубликованном в четверг, ФБР и агентство США по кибербезопасности CISA заявили, что программа-вымогатель Royal унесла

жизни нескольких человек в США и за рубежом, включая производственные, коммуникационные, образовательные и медицинские организации.

Предупреждение появилось после того, как в декабре Министерство здравоохранения и социальных служб США предупредило, что программа-вымогатель Royal «агрессивно» нацелена на сектор здравоохранения США. На сайте утечки в темной сети Royal в настоящее время среди жертв указаны службы здравоохранения Северо-Западного Мичигана и ортопедические консультанты Среднего Запада.

Банда вымогателей Royal впервые была обнаружена в начале 2022 года. В то время операция полагалась на сторонние программы-вымогатели, такие как Zeon, но с тех пор с сентября в атаках применялась собственная программа-вымогатель.

Правительство США предупреждает, что после получения доступа к сетям жертв — как правило, через фишинговые ссылки, содержащие загрузчик вредоносного ПО — агенты Royal «отключают антивирусное программное обеспечение и извлекают большие объемы данных» перед развертыванием программ-вымогателей и систем шифрования.

Эксперты по безопасности считают, что в состав Royal входят опытные злоумышленники-вымогатели из предыдущих операций, отмечая сходство между Royal и Conti, активной хакерской группой, связанной с Россией, которая была расформирована в июне 2022 года.

Программа-вымогатель Royal В ноябре 2022 года сообщалось стала самой популярной операцией по борьбе с программами-вымогателями, обогнав Lockbit. Последние данные показывают, что Royal несет ответственность как минимум за 19 атак программ-вымогателей в феврале, за 51 атакой, приписываемой LockBit, и 22 атаками, связанными с Vice Society.

Хотя большинство жертв Royal базируются в Соединенных Штатах, одной из наиболее известных жертв стала трасса Сильверстоун, одна из крупнейших трасс автогонок в Соединенном Королевстве. Среди других жертв, заявленных бандой, ICS, организация, которая предоставляет услуги кибербезопасности Министерству обороны США, школьному округу Далласа и другим.

Согласно информационному бюллетеню правительства США, требования выкупа, предъявляемые Royal, варьируются от 1 до 11 миллионов долларов, но пока неясно, сколько операция заработала на своих жертвах. В бюллетене отмечается, что члены королевской семьи также используют тактику двойного вымогательства, посредством чего они угрожают публично раскрыть зашифрованные данные, если жертва не заплатит выкуп.

«В наблюдаемых инцидентах члены королевской семьи не включают суммы выкупа и инструкции по оплате в первоначальную записку о выкупе», — предупредили CISA и ФБР. «Вместо этого примечание, которое появляется после шифрования, требует, чтобы жертвы напрямую взаимодействовали с злоумышленником через URL-адрес.onion», — ссылаясь на сайты Royal в даркнете.

CISA и ФБР опубликовали известные индикаторы компрометации программы-вымогателя Royal, а также тактику, методы и процедуры операций, которые, по их словам, были выявлены в ходе деятельности ФБР по реагированию на угрозы совсем недавно, в январе 2023 года. Агентства рекомендовали американским организациям применять меры по смягчению последствий и сообщать обо всех инцидентах с программами-вымогателями. В бюллетене отмечается, что CISA и ФБР не поощряют выплату выкупа». ***(Carly Page. US government warns Royal ransomware is targeting critical infrastructure // Yahoo (https://techcrunch.com/2023/03/03/us-government-royal-ransomware-advisory/). 03.03.2023).***

***

«…Производственные предприятия в 21 веке используют несколько компьютеризированных операционных систем для сбора, анализа и хранения данных. Эти системы физически контролируют большую часть оборудования и производства на своих объектах. Сложная взаимосвязь этих систем и компонентов помогла производителям повысить производительность и прибыльность. Но эта интеграция также сделала производителей более уязвимыми для программ-вымогателей и кибератак.

Согласно отчету Национальной ассоциации производителей, в 2021 году на обрабатывающую промышленность приходилось большинство инцидентов с программами-вымогателями. В других отчетах отмечается рост числа атак на производство в 2022 году, при этом до 75% атак были направлены на производственный сектор. Еще одна тревожная статистика: более половины пострадавших производителей не смогли восстановить данные из резервных копий.

Анатомия кибератаки на производителей

Производственная компания, как и большинство компаний, вероятно, не узнает, что подверглась атаке программы-вымогателя, пока ее системы, включая весь производственный цех, не будут закрыты и недоступны. Во многих случаях вся деятельность компании останавливается. С современными системами доставки точно в срок, являющимися нормой в производстве, даже остановка на несколько дней может иметь разрушительные последствия, особенно там, где затронутые заводы являются единственным источником ключевой детали или продукта. Злоумышленники знают, что компания будет терять значительные суммы денег и рискует потерять клиентов каждый день после отключения, и они будут использовать это, чтобы заставить выплатить выкуп.

Однако даже когда компания платит выкуп, нет никакой гарантии, что она сможет быстро возобновить свою деятельность. Часто восстановление работоспособности систем производителя может занять дни или недели. Некоторые системы могут быть даже невосстановимыми и должны быть полностью заменены.

Важность резервных копий данных

Надежные резервные копии данных имеют решающее значение, позволяя производителю быстро восстановить и возобновить работу после кибератаки. Поэтому один из первых шагов, который обычно предпринимает злоумышленник, — это удаление любых резервных копий на месте. Для обеспечения наилучшей защиты производителям следует рассматривать удаленные или облачные решения для резервного копирования в рамках своей общей стратегии резервного копирования данных. Удаленные резервные копии могут помочь производителям быстро восстановить данные в случае кибератаки.

Еще одним важным компонентом резервного копирования данных является регулярное тестирование, чтобы убедиться, что резервные копии жизнеспособны, а восстановленные системы работают нормально.

Устаревшие системы

Некоторые производители до сих пор используют устаревшие системы, резервное копирование которых невозможно. К ним могут относиться пользовательские системы, созданные сотрудниками, которые больше не работают в компании, или поставщиками, которые ушли из бизнеса. Эти системы могут работать на старых, неподдерживаемых операционных системах или оборудовании. Для производителей, у которых есть такие системы, кибератака может привести к полному нарушению работы бизнеса, пока не будет найдена замена систем.

Устаревшие системы, резервное копирование которых невозможно, следует заменить или защитить с помощью дополнительных мер безопасности.

Оценка систем управления производством

MES, или производственные исполнительные системы, являются нервным центром современных производственных операций. MES отслеживает, отслеживает, документирует и контролирует процесс производства от сырья до готовой продукции. Данные, хранящиеся в MES, также могут быть интегрированы с другими критически важными системами, такими как системы управления технологическими процессами…» ***(Roland J. De Monte, Jackson E. Biesecker. How Modern Manufacturing Plants Can Protect Against Ransomware, Cyberattacks // Jackson Lewis P.C. (https://www.jacksonlewis.com/publication/how-modern-manufacturing-plants-can-protect-against-ransomware-cyberattacks). 01.03.2023).***

***

«Банда вымогателей Clop начала вымогать деньги у компаний, чьи данные были украдены с помощью уязвимости нулевого дня в решении для безопасного обмена файлами Fortra GoAnywhere MFT.

В феврале разработчики решения для передачи файлов GoAnywhere MFT предупредили клиентов о том, что на открытых административных консолях используется уязвимость нулевого дня для удаленного выполнения кода.

GoAnywhere — это решение для безопасной передачи файлов через Интернет, которое позволяет компаниям безопасно передавать зашифрованные файлы своим партнерам, сохраняя при этом подробные журналы аудита того, кто получил доступ к файлам.

Хотя никаких подробностей о том, как использовалась уязвимость, не сообщалось, вскоре был выпущен экспериментальный эксплойт, а затем исправление для этой уязвимости.

На следующий день после выпуска патча GoAnywhere банда вымогателей Clop связалась с BleepingComputer и заявила, что несет ответственность за атаки.

Группа вымогателей заявила, что они использовали уязвимость в течение десяти дней, чтобы украсть данные у 130 компаний. В то время BleepingComputer не могла самостоятельно подтвердить эти утверждения, а Fortra не ответила на наши электронные письма.

С тех пор две компании, Community Health Systems (CHS) и Hatch Bank, сообщили, что данные были украдены в ходе атак GoAnywhere MFT.

Прошлой ночью банда вымогателей Clop начала публично эксплуатировать жертв атак GoAnywhere, добавив семь новых компаний на свой сайт утечки данных.

Общеизвестно, что только одна из жертв, Hatch Bank, была взломана с помощью этой уязвимости. Тем не менее, BleepingComputer узнал, что по крайней мере две другие зарегистрированные на бирже компании также украли свои данные с помощью этой уязвимости.

Во всех записях на сайте утечки данных говорится, что публикация данных «скоро», но есть скриншоты якобы украденных данных.

Кроме того, BleepingComputer сообщили, что жертвы начали получать требования о выкупе от банды вымогателей.

Хотя неясно, сколько требуют злоумышленники, ранее в декабре 2020 года они требовали выкуп в размере 10 миллионов долларов в аналогичных атаках с использованием уязвимости нулевого дня Accellion FTA.

Во время этих атак группа вымогателей украла большие объемы данных почти у 100 компаний по всему миру, при этом злоумышленники медленно сливали данные из компаний, требуя выкупа в миллионы долларов.

В число организаций, чьи серверы Accellion были взломаны, входят, среди прочего, энергетический гигант Shell, фирма по кибербезопасности Qualys, гигант супермаркетов Kroger и несколько университетов по всему миру, таких как Стэнфордский медицинский университет, Университет Колорадо, Университет Майами, Калифорнийский университет и Университет Мэриленда. Балтимор (UMB)». ***(Lawrence Abrams. Clop ransomware gang begins extorting GoAnywhere zero-day victims // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-begins-extorting-goanywhere-zero-day-victims/). 11.03.2023).***

***

«Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) объявило в понедельник о создании новой пилотной программы предупреждения об уязвимостях программ-вымогателей (RVWP).

Исходя из Закона об отчетах о кибер-инцидентах для критически важной инфраструктуры от 2022 года (CIRCIA) и координируемого Объединенной целевой группой по программам-вымогателям (JRTF), RVWP увидит, как CISA оценивает недостатки, обычно связанные с использованием известных программ-вымогателей.

После обнаружения этих уязвимостей Агентство предупредит объекты критической инфраструктуры с целью обеспечения смягчения последствий до инцидента с программами-вымогателями.

Для выявления объектов, уязвимых для ошибок, CISA будет полагаться на различные существующие службы, источники данных, технологии и органы, включая свою службу сканирования уязвимостей Cyber Hygiene.

Агентство подтвердило, что оно уже уведомило 93 организации, использующие экземпляры службы Microsoft Exchange, о ранее использованной уязвимости под названием «ProxyNotShell».

«Атаки программ-вымогателей продолжают наносить неприемлемый ущерб организациям по всей стране, в том числе организациям с богатыми целями и ограниченными ресурсами, таким как многие школьные округа и больницы», — сказал Эрик Гольдштейн, исполнительный помощник директора по кибербезопасности в CISA.

«RVWP позволит CISA предоставлять своевременную и полезную информацию, которая напрямую снизит распространенность вредоносных программ-вымогателей, затрагивающих американские организации».

Комментируя эту новость, Джейми Бут, заместитель главного консультанта Synopsys, сказал, что, хотя RVWP является хорошей отправной точкой для кибербезопасности, следует отметить, что проблемы и уязвимости редко проявляются изолированно.

«Всякий раз, когда уязвимость обнаруживается при внешнем сканировании, группы безопасности должны использовать это как возможность разорвать цикл поиска и исправления и выяснить, что вызвало выпуск этой уязвимости в производство, как найти другие подобные ей и как предотвратить это в будущем», — объяснил Бут.

«Эти усилия по сканированию — только начало, как с точки зрения федеральных усилий по кибербезопасности, так и для команд, [...] получающих информацию об уязвимостях».

Программа RVWP появилась через несколько недель после того, как Белый дом запустил свою Национальную стратегию кибербезопасности». ***(Alessandro Mascellino. CISA Creates New Ransomware Vulnerability Warning Program // Reed***

Exhibitions Ltd (https://www.infosecurity-magazine.com/news/cisa-creates-ransomware-warning/). 14.03.2023).

***

«Программы-вымогатели стали серьезной угрозой для бизнеса по всему миру, поскольку кибератаки становятся все более изощренными, что приводит к огромному финансовому ущербу для компаний, которые становятся их жертвами. Мало того, что важные файлы заблокированы, но простои и другие сбои, вызванные этими атаками, могут нанести ущерб работе вашей компании. Ниже мы развенчаем пять основных мифов и заблуждений, чтобы лучше понять программы-вымогатели и связанные с ними риски:

1. Атаки программ-вымогателей осуществляются опытными хакерами

Вопреки распространенному мнению, лишь немногие атаки программ-вымогателей осуществляются опытными «хакерами». Хотя вредоносный код, необходимый для фактического извлечения и шифрования файлов жертвы, может быть очень сложным, многие атаки совершаются неквалифицированными группами, которые просто покупают или даже арендуют вредоносное ПО. В этих случаях злоумышленникам нужно только придумать и распространить эффективное адресное фишинговое электронное письмо, которое побуждает пользователя просто щелкнуть зараженный файл или ссылку. Эффективный целевой фишинг сам по себе является искусством, но не требует технических «хакерских» навыков. Делая программы-вымогатели доступными для менее квалифицированных злоумышленников, создатели продвинутых программ-вымогателей могут масштабировать свои атаки и максимизировать отдачу от своих инвестиций в кодирование новых вариантов вредоносных программ.

Чтобы остановить атаку до того, как вредоносный код укоренится и нанесет ущерб вашему бизнесу, крайне важно постоянно контролировать вашу сеть, сканируя ее на предмет необычной активности и выявляя любые текущие фишинговые атаки. Быстро обнаруженная атака программы-вымогателя может быть остановлена на месте, а зараженные системы могут быть очищены и быстро

возвращены в оперативный режим. Аутсорсинговые решения по обнаружению угроз, предлагаемые поставщиками услуг управляемого обнаружения и реагирования (MDR), могут помочь защитить вас, активно выявляя подозрительную активность и быстро реагируя на любые предупреждения или индикаторы компрометации. При подозрении на атаку программ-вымогателей они могут принять немедленные меры, чтобы локализовать проблему до того, как она причинит вред. Чтобы помочь предотвратить атаку, важно обучить вашу команду тому, как распознавать фишинговые электронные письма и другие типы предшественников программ-вымогателей, чтобы ваша компания могла активно защищаться.

2. Бригады вымогателей нацелены только на крупные компании или организации

Большинство кампаний по вымогательству нацелены на своих жертв без разбора. На самом деле, большинство злоумышленников даже не знают личность жертвы, пока фишинговое электронное письмо не заставит ничего не подозревающего пользователя клюнуть на приманку. А поскольку количество организаций среднего размера намного превышает количество крупных компаний, подавляющее большинство организаций-жертв далеко не нарицательны. В действительности программы-вымогатели могут помешать вашему бизнесу независимо от его размера или финансовых ресурсов. Согласно данным Специального отчета о кибербезопасности за 2022 год, подготовленного RSM и Торговой палатой США, 23% руководителей среднего звена заявили, что их компания подверглась атаке программ-вымогателей или спросу на них в прошлом году.

Предприятия среднего размера особенно уязвимы, потому что они:

Как правило, имеют ограниченные ресурсы для кибербезопасности

Могут не знать о последних угрозах и мерах, которые им необходимо предпринять, чтобы защитить себя

Отсутствие всеобъемлющей стратегии безопасности

В значительной степени полагайтесь на облачные вычисления и стороннее программное обеспечение, которое часто становится мишенью для злоумышленников, использующих веб-сайты с вредоносным ПО, фишинговые электронные письма или вредоносные загрузки.

Чтобы защитить свою компанию, вы должны проводить регулярные аудиты и внедрять надлежащие методы проверки подлинности, такие как многофакторная проверка подлинности (MFA). Кроме того, вам следует инвестировать в комплексную стратегию безопасности или в стороннего поставщика управляемого обнаружения и реагирования (MDR), который включает в себя непрерывный мониторинг сетей и систем, применение политик и лучших практик, обучение сотрудников обнаружению вредоносной активности или угроз и резервное копирование данных на случай нападения. Вы также должны быть в курсе последних сведений об угрозах и принимать меры для защиты своей компании, проявляя бдительность в отношении своего присутствия в Интернете и следя за последними киберновостями, связанными с вашим сектором.

3. Программа-вымогатель не может быть остановлена на устройстве

Лучший способ не дать программам-вымогателям скомпрометировать ваши конечные точки — принять меры до того, как они будут заражены. Это включает в себя установку передовой антивирусной и антивирусной защиты нового поколения на основе искусственного интеллекта для защиты ваших данных. Но даже эту защиту можно обойти, поэтому вам необходимо обнаружение угроз в режиме реального времени. Если атака все-таки произойдет, вам следует обратиться за инструкциями в службу реагирования на инциденты (IR) или в группу MDR. После выявления вредоносного кода его можно изолировать и удалить с помощью специализированных инструментов или приложений, специально разработанных для предотвращения атак программ-вымогателей. В некоторых случаях вы даже сможете восстановить свои данные.

Предотвращение заражения программами-вымогателями требует многоуровневого подхода. Вы должны убедиться, что программное обеспечение и

системы поддерживаются в актуальном состоянии. Вы также должны бороться с потенциальными угрозами, используя настройки брандмауэра, которые регулярно контролируются для предотвращения несанкционированного доступа. Кроме того, шифрование данных необходимо, поскольку оно обеспечивает дополнительный уровень защиты в случае успешной атаки. Наконец, следует регулярно создавать резервные копии важных файлов, чтобы иметь доступную копию на случай заражения устройства.

4. Оплата выкупа гарантирует, что ваши данные будут восстановлены

Когда программа-вымогатель заражает устройство или сеть, может возникнуть соблазн заплатить выкуп, чтобы быстро вернуть ваши данные. К сожалению, гарантии нет, и хакеры не всегда выполняют свои обещания после оплаты. И даже когда они приходят с ключом дешифрования, процесс разблокировки ваших данных может быть каким угодно, но не простым, а иногда и невозможным. Не говоря уже о том, что выплата выкупа может побудить киберпреступников снова нацелиться на ваш бизнес в будущем, а также сигнализировать другим преступникам, что вы готовы уступить угрожающим требованиям.

Лучше всего работать с экспертами по реагированию на инциденты (IR), которые имеют опыт борьбы с этим типом атак. Эти специалисты могут оценить ситуацию, порекомендовать наилучший план действий и помочь вам восстановить доступ к вашим данным, не платя злоумышленникам. И если вы все же решите заплатить выкуп, квалифицированная команда IR может провести переговоры с злоумышленником и облегчить платеж в криптовалюте (конечно, только после проверки санкционного списка Управления по контролю за иностранными активами (OFAC) Министерства финансов). Кроме того, они могут помочь вам предотвратить подобные инциденты в будущем, приняв строгие меры кибербезопасности.

5. Усовершенствованное антивирусное программное обеспечение может защитить от всех программ-вымогателей.

Антивирусное программное обеспечение предназначено для выявления и защиты от известных вирусов и вредоносных программ, но оно не может обеспечить полную защиту от всех типов программ-вымогателей. Авторы постоянно разрабатывают новые формы вредоносного программного обеспечения, которые могут обойти традиционные решения, а некоторые умные варианты включают в себя методы обхода антивируса, которые затрудняют их обнаружение. Опытный — или просто удачливый — злоумышленник может обойти даже самые передовые инструменты нового поколения на основе ИИ.

Чтобы защитить себя от заражения программами-вымогателями, настоятельно рекомендуется использовать инструмент Endpoint Detection and Response, управляемый опытной командой охотников за угрозами. Многие компании считают, что аутсорсинг работы группе управляемого обнаружения и реагирования (MDR), занимающейся кибербезопасностью, является лучшим вариантом, особенно если они выступают в качестве партнера, а не просто поставщика. Партнер MDR будет создавать и поддерживать настраиваемые списки наблюдения и модели обнаружения, созданные на основе новейшей аналитики угроз, для круглосуточного обнаружения действий злоумышленников в режиме реального времени. Они также обеспечивают дополнительный уровень защиты, предоставляя сложные средства сдерживания, изоляции и IR-возможности при обнаружении программ-вымогателей…» ***(Jason Straight. Ransomware: The Top 5 Myths and Misconceptions // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102i9y5/ransomware-the-top-5-myths-and-misconceptions). 09.03.2023).***

***

«Спеціалісти компанії з кібербезпеки SecurityHQ назвали найнебезпечніше угрупування хакерів вимагачів, яке становить серйозну загрозу безпеці користувачів у багатьох країнах. За словами аналітиків, атаки зловмисників LockBit зазвичай спрямовані на державні установи та

підприємства у сферах охорони здоров'я, фінансів, промислових товарів, послуг.

Найчастіше жертвами атак угрупування стають США, Китай, Індія, Індонезія, Україна, Франція, Велика Британія та Німеччина. Хакери створили власну програму-вимагача LockBit, яка була вперше виявлена ще у вересні 2019 року. Раніше вона була відома під назвою ABCD через розширення «.abcd», що надається зашифрованим файлам. Зараз 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.

Початкові методи атак LockBit включають соціальну інженерію: фішинг, компрометація 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.

У 2022 році група LockBit повідомила про більшу кількість успішних атак, ніж будь-яка інша банда здирників. Ще однією особливістю хакерів LockBit є їхня програма винагороди за помилки (Bug Bounty). Група пропонує винагороду у розмірі $ 1 мільйон будь-кому, хто зможе ідентифікувати особистості хакерів.

Щодо кібератак на Україну, голова Державної служби спеціального зв'язку та захисту інформації Юрій Щиголь повідомив, що 9 з 10 кібератак відбуваються через необережність та необізнаність персоналу. «Щоб зменшити ризики, радимо усім компаніям, і учасникам медіаспільноти, зокрема, постійно проводити аудит кібербезпеки власних систем для вчасного виявлення ймовірних прогалин у захисті та визначення кроків для їх ліквідації», — розповів минулого тижня Щиголь журналістам Укрінформу». ***(Аналітики назвали найнебезпечніше угрупування хакерів вимагачів // No worries! (https://noworries.news/analityky-nazvaly-najnebezpechnishe-ugrupuvannya-hakeriv-vymagachiv/). 14.03.2023).***

***

«Банды вымогателей становятся все более напористыми и агрессивными в своих подходах к жертвам, прибегая к тактике сильного давления, включая кампании целенаправленного преследования с целью вымогательства денег, даже у тех, кто уделял внимание предотвращению программ-вымогателей и хранил резервные копии своих данных.

Об этом говорится в отчете, опубликованном сегодня отделом реагирования на инциденты и анализа угроз Palo Alto Networks Unit 42. Данные, которые взяты только из случаев, на которые ответило подразделение 42, поэтому ни в коем случае не являются полной или абсолютно точной оценкой объемов активности, показали, что банды вымогателей использовали преследование в качестве тактики в 20 раз чаще в прошлом году, чем в 2021 году.

Как правило, преследование в случае программ-вымогателей направлено на конкретного человека, часто занимающего руководящую роль в организации-жертве или ее клиентах. Это включает в себя серию все более агрессивных телефонных звонков и электронных писем, чтобы заставить их заплатить выкуп или заставить клиентов оказать давление на тех, кто уполномочен платить выкуп, чтобы сделать это. Это может также включать в себя киберпреступников, распространяющих информацию об атаке в социальных сетях или обращающихся к журналистам, работающим в сфере технологий.

Это дополняет существующие многоуровневые методы вымогательства, которые, помимо шифрования данных, включают эксфильтрацию и утечку данных, которые наблюдались в 70% атак в прошлом году и на 30% больше, чем в 2021 году, а также распределенные атаки типа «отказ в обслуживании» (DDoS), наблюдаемые примерно в 2% случаев программ-вымогателей. Эти тенденции, называемые двойным и тройным вымогательством, прочно утвердились с 2020 года.

«Группы вымогателей и вымогателей загоняют своих жертв в скороварку с конечной целью увеличить их шансы на получение денег», — сказала Венди Уитмор, старший вице-президент и глава подразделения 42 в Palo Alto Networks.

«Домогательство было связано с каждым пятым случаем использования программ-вымогателей, которые мы расследовали в последнее время, что свидетельствует о том, на что эти группы готовы пойти, чтобы добиться выплаты жалованья. Многие доходят до того, что используют украденную информацию о клиентах, чтобы беспокоить их и пытаться заставить организацию заплатить».

Исследователи Unit 42 присоединяются к растущему числу голосов, которые считают, что эти тенденции демонстрируют, как резервные копии, которые долгое время считались краеугольным камнем любой малоприличной стратегии предотвращения программ-вымогателей, больше не эффективны для защиты от воздействия сами по себе.

В то время как актуальность резервных копий в автономном режиме и регулярное тестирование остаются жизненно важной гарантией, Unit 42 обнаружила, что методы двойного и тройного вымогательства стали настолько эффективными, что банды вымогателей по-прежнему могут принуждать своих жертв к оплате, даже если данные резервируются. и защищены, а сбои в работе сведены к минимуму.

Часто, по их словам, простой угрозы раскрытия конфиденциальных данных, последующего ущерба для репутации и утраты доверия, а также угрозы штрафов со стороны регулирующих органов, ни один из которых нельзя предотвратить путем сохранения резервных копий, достаточно, чтобы заставить жертву поддержать вниз.

Действительно, Unit 42 заявила, что работала над рядом инцидентов, в которых жертвы изначально отказывались поддерживать идею выплаты выкупа, потому что их резервные копии были в порядке, но затем подвергались такому интенсивному преследованию, что в результате затраты превысили затраты на программу-вымогатель. требовать. Переговорщики LockBit использовали эту возможность как угрозу, пытаясь вымогать деньги у Royal Mail в начале этого года, хотя почтовая служба в конечном итоге стояла на своем.

Если они еще не сделали этого, Unit 42 рекомендует руководителям службы безопасности подготовить расширенный план действий для борьбы с более изощренными кампаниями по вымогательству.

Такой сценарий должен включать разработку комплексного плана реагирования на инциденты и соответствующие протоколы связи в кризисных ситуациях, установление цепочки подчинения, в которой должны участвовать заинтересованные стороны и кто уполномочен что делать — например, кто ведет переговоры, кто уполномочен подписывать на плате, если до этого дойдёт, и так далее.

В плане также должно быть указано, что сотрудники должны делать или избегать делать, если во время инцидента они подвергаются преследованиям по телефону или электронной почте. Персонал должен быть обучен методам домогательств, чтобы лучше подготовить их в этом отношении.

Лидеры безопасности также должны быть уверены, что они могут проводить оценку компрометации post-mortem, чтобы убедиться, что любые бэкдоры или другие индикаторы компрометации (IoC), такие как запланированные задачи или задания, удалены, чтобы сделать последующие атаки менее вероятными.

Исследователи Unit 42 заявили, что в ближайшие девять месяцев мы, вероятно, увидим рост вымогательства, связанного с внутренними угрозами, политически мотивированными попытками вымогательства, а также использованием программ-вымогателей и вымогательством, чтобы отвлечь внимание от атак, направленных на компрометацию цепочки поставок жертвы — или, в случае технологических компаний — их исходный код. Команда также предсказала, что в ближайшем будущем мы увидим «крупную компрометацию облачных программ-вымогателей». ***(Alex Scroxton. Ransomware gangs harass victims to 'bypass' backups // TechTarget (https://www.computerweekly.com/news/365532726/Ransomware-gangs-harass-victims-to-bypass-backups). 21.03.2023).***

***

«В новом отчете ENISA, Агентства кибербезопасности Европейского союза, в котором рассматриваются кибератаки, направленные на европейскую транспортную сеть за период почти двух лет, указывается, что программы-вымогатели стали серьезной угрозой.

В отчете ENISA, первом в истории анализе множества угроз кибербезопасности, с которыми сталкивается транспортный сектор в ЕС, картированы и изучены киберинциденты, направленные против авиационного, морского, железнодорожного и автомобильного транспорта в период с января 2021 года по октябрь 2022 года.

В течение этого периода были выявлены три основные угрозы:

атаки программ-вымогателей (38%)

угрозы, связанные с данными (30%)

вредоносное ПО (17%)

атаки типа «отказ в обслуживании» (16%)

фишинг/целевой фишинг (10%)

атаки на цепочку поставок (10%)

Что особенно интересно, так это то, как угрозы, по-видимому, изменились в период с 2021 по 2022 год: резко возросла доля атак программ-вымогателей, нацеленных на транспортный сектор, с 13% до 25%, а атак типа «отказ в обслуживании» — с 2%. % в 2021 году до 13% в 2022 году.

По словам ENISA, рост числа атак типа «отказ в обслуживании» — когда европейские аэропорты и железнодорожные компании подвергаются все более частым атакам — скорее всего, связан с хактивистами, большая часть которых, по-видимому, является ответом на вторжение России в Украину. Такие атаки часто приводят к сбоям в работе, препятствуя поездкам представителей общественности или нарушая движение товаров.

Между тем, доля угроз, связанных с данными (таких как взлом и утечка данных, которые часто включают учетные данные для входа в систему, данные сотрудников и клиентов, а также интеллектуальную собственность), снизилась по

сравнению с программами-вымогателями: с 21% в 2021 году до 9% в 2021 году. 2022.

Следует отметить, что в отчете ENISA рассматриваются только те инциденты кибербезопасности, о которых ему сообщалось. Авторы отчета признают, что «у нас все еще есть ограниченные знания и информация о таких инцидентах. Анализ в этом отчете показывает, что обнародованные инциденты — это лишь верхушка айсберга».

В 2024 году будет принята новая европейская директива (NIS2), которая призовет государства-члены повысить свою кибербезопасность во всех секторах промышленности, улучшить отчетность об атаках и обяжет страны собирать эффективные группы реагирования в рамках более широких усилий по улучшению защиты от государства. и негосударственные субъекты». ***(Europe's transport sector terrorised by ransomware, data theft, and denial-of-service attacks // Fortra, LLC and its group of companies (https://www.tripwire.com/state-of-security/europes-transport-sector-terrorised-ransomware-data-theft-and-denial-service). 23.03.2023).***

***

«Признавая постоянную угрозу, создаваемую атаками программ-вымогателей для организаций любого размера, Агентство по кибербезопасности и безопасности инфраструктуры (CISA) недавно объявило о создании Пилотной программы предупреждения об уязвимостях программ-вымогателей (RVWP), как это разрешено Законом об отчетах о кибер-инцидентах для критически важной инфраструктуры (CIRCIA). от 2022 года. С помощью RVWP CISA определит уязвимости, обычно связанные с известным использованием программ-вымогателей, и предупредит объекты критической инфраструктуры об этих уязвимостях, что позволит смягчить последствия до того, как произойдет инцидент с программами-вымогателями.

RVWP будет выявлять организации с доступными через Интернет уязвимостями, обычно связанными с известными субъектами программ-

вымогателей, используя существующие службы, источники данных, технологии и полномочия.

Недавно CISA инициировала RVWP, уведомив 93 организации, в которых запущены экземпляры службы Microsoft Exchange с уязвимостью под названием «ProxyNotShell», которая широко используется злоумышленниками-вымогателями.

«Атаки программ-вымогателей продолжают наносить неприемлемый ущерб организациям по всей стране, в том числе нацелены на богатые и бедные организации, такие как многие школьные округа и больницы, — сказал Эрик Гольдштейн, исполнительный помощник директора по кибербезопасности, CISA. — RVWP позволит CISA предоставлять своевременную и полезную информацию, которая напрямую снизит распространенность вредоносных программ-вымогателей, затрагивающих американские организации. Мы призываем каждую организацию срочно устранить уязвимости, выявленные этой программой, и принять строгие меры безопасности в соответствии с руководством правительства США по StopRansomware.gov».

RVWP будет координироваться и согласовываться с Объединенной целевой группой по программам-вымогателям (JRTF), межведомственной организацией, созданной CIRCIA и возглавляемой CISA и ФБР». ***(CISA starts ransomware vulnerability pilot program // BNP Media (https://www.securitymagazine.com/articles/99086-cisa-starts-ransomware-vulnerability-pilot-program). 20.03.2023).***

***

«Программы-вымогатели стали серьезной угрозой для бизнеса по всему миру, поскольку кибератаки становятся все более изощренными, что приводит к огромному финансовому ущербу для компаний, которые становятся их жертвами. Мало того, что важные файлы заблокированы, но простои и другие сбои, вызванные этими атаками, могут нанести ущерб работе вашей компании. Ниже мы развенчаем пять основных мифов и заблуждений, чтобы лучше понять программы-вымогатели и связанные с ними риски:

1. Атаки программ-вымогателей осуществляются опытными хакерами

Вопреки распространенному мнению, лишь немногие атаки программ-вымогателей осуществляются опытными «хакерами». Хотя вредоносный код, необходимый для фактического извлечения и шифрования файлов жертвы, может быть очень сложным, многие атаки совершаются неквалифицированными группами, которые просто покупают или даже арендуют вредоносное ПО. В этих случаях злоумышленникам нужно только придумать и распространить эффективное адресное фишинговое электронное письмо, которое побуждает пользователя просто щелкнуть зараженный файл или ссылку. Эффективный целевой фишинг сам по себе является искусством, но не требует технических «хакерских» навыков. Делая программы-вымогатели доступными для менее квалифицированных злоумышленников, создатели продвинутых программ-вымогателей могут масштабировать свои атаки и максимизировать отдачу от своих инвестиций в кодирование новых вариантов вредоносных программ.

Чтобы остановить атаку до того, как вредоносный код укоренится и нанесет ущерб вашему бизнесу, крайне важно постоянно контролировать вашу сеть, сканируя ее на предмет необычной активности и выявляя любые текущие фишинговые атаки. Быстро обнаруженная атака программы-вымогателя может быть остановлена на месте, а зараженные системы могут быть очищены и быстро возвращены в оперативный режим. Аутсорсинговые решения по обнаружению угроз, предлагаемые поставщиками услуг управляемого обнаружения и реагирования (MDR), могут помочь защитить вас, активно выявляя подозрительную активность и быстро реагируя на любые предупреждения или индикаторы компрометации. При подозрении на атаку программ-вымогателей они могут принять немедленные меры, чтобы локализовать проблему до того, как она причинит вред. Чтобы помочь предотвратить атаку, важно обучить вашу команду тому, как распознавать фишинговые электронные письма и другие типы предшественников программ-вымогателей, чтобы ваша компания могла активно защищаться.

2. Бригады вымогателей нацелены только на крупные компании или организации

Большинство кампаний по вымогательству нацелены на своих жертв без разбора. На самом деле, большинство злоумышленников даже не знают личность жертвы, пока фишинговое электронное письмо не заставит ничего не подозревающего пользователя клюнуть на приманку. А поскольку количество организаций среднего размера намного превышает количество крупных компаний, подавляющее большинство организаций-жертв далеко не нарицательны. В действительности программы-вымогатели могут помешать вашему бизнесу независимо от его размера или финансовых ресурсов. Согласно данным Специального отчета о кибербезопасности за 2022 год, подготовленного RSM и Торговой палатой США, 23% руководителей среднего звена заявили, что их компания подверглась атаке программ-вымогателей или спросу на них в прошлом году.

Предприятия среднего размера особенно уязвимы, потому что они:

Как правило, имеют ограниченные ресурсы для кибербезопасности

Могут не знать о последних угрозах и мерах, которые им необходимо предпринять, чтобы защитить себя

Отсутствие всеобъемлющей стратегии безопасности

В значительной степени полагайтесь на облачные вычисления и стороннее программное обеспечение, которое часто становится мишенью для злоумышленников, использующих веб-сайты с вредоносным ПО, фишинговые электронные письма или вредоносные загрузки.

Чтобы защитить свою компанию, вы должны проводить регулярные аудиты и внедрять надлежащие методы проверки подлинности, такие как многофакторная проверка подлинности (MFA). Кроме того, вам следует инвестировать в комплексную стратегию безопасности или в стороннего поставщика управляемого обнаружения и реагирования (MDR), который включает в себя непрерывный мониторинг сетей и систем, применение политик и лучших практик, обучение сотрудников обнаружению вредоносной активности или угроз и резервное

копирование данных на случай нападения. Вы также должны быть в курсе последних сведений об угрозах и принимать меры для защиты своей компании, проявляя бдительность в отношении своего присутствия в Интернете и следя за последними киберновостями, связанными с вашим сектором.

3. Программа-вымогатель не может быть остановлена на устройстве

Лучший способ не дать программам-вымогателям скомпрометировать ваши конечные точки — принять меры до того, как они будут заражены. Это включает в себя установку передовой антивирусной и антивирусной защиты нового поколения на основе искусственного интеллекта для защиты ваших данных. Но даже эту защиту можно обойти, поэтому вам необходимо обнаружение угроз в режиме реального времени. Если атака все-таки произойдет, вам следует обратиться за инструкциями в службу реагирования на инциденты (IR) или в группу MDR. После выявления вредоносного кода его можно изолировать и удалить с помощью специализированных инструментов или приложений, специально разработанных для предотвращения атак программ-вымогателей. В некоторых случаях вы даже сможете восстановить свои данные.

Предотвращение заражения программами-вымогателями требует многоуровневого подхода. Вы должны убедиться, что программное обеспечение и системы поддерживаются в актуальном состоянии. Вы также должны бороться с потенциальными угрозами, используя настройки брандмауэра, которые регулярно контролируются для предотвращения несанкционированного доступа. Кроме того, шифрование данных необходимо, поскольку оно обеспечивает дополнительный уровень защиты в случае успешной атаки. Наконец, следует регулярно создавать резервные копии важных файлов, чтобы иметь доступную копию на случай заражения устройства.

4. Оплата выкупа гарантирует, что ваши данные будут восстановлены

Когда программа-вымогатель заражает устройство или сеть, может возникнуть соблазн заплатить выкуп, чтобы быстро вернуть ваши данные. К сожалению, гарантии нет, и хакеры не всегда выполняют свои обещания после оплаты. И даже когда они приходят с ключом дешифрования, процесс

разблокировки ваших данных может быть каким угодно, но не простым, а иногда и невозможным. Не говоря уже о том, что выплата выкупа может побудить киберпреступников снова нацелиться на ваш бизнес в будущем, а также сигнализировать другим преступникам, что вы готовы уступить угрожающим требованиям.

Лучше всего работать с экспертами по реагированию на инциденты (IR), которые имеют опыт борьбы с этим типом атак. Эти специалисты могут оценить ситуацию, порекомендовать наилучший план действий и помочь вам восстановить доступ к вашим данным, не платя злоумышленникам. И если вы все же решите заплатить выкуп, квалифицированная команда IR может провести переговоры с злоумышленником и облегчить платеж в криптовалюте (конечно, только после проверки санкционного списка Управления по контролю за активами (OFAC) Министерства финансов иностранными). Кроме того, они могут помочь вам предотвратить подобные инциденты в будущем, приняв строгие меры кибербезопасности.

5. Усовершенствованное антивирусное программное обеспечение может защитить от всех программ-вымогателей.

Антивирусное программное обеспечение предназначено для выявления и защиты от известных вирусов и вредоносных программ, но оно не может обеспечить полную защиту от всех типов программ-вымогателей. Авторы постоянно разрабатывают новые формы вредоносного программного обеспечения, которые могут обойти традиционные решения, а некоторые умные варианты включают в себя методы обхода антивируса, которые затрудняют их обнаружение. Опытный — или просто удачливый — злоумышленник может обойти даже самые передовые инструменты нового поколения на основе ИИ.

Чтобы защитить себя от заражения программами-вымогателями, настоятельно рекомендуется использовать инструмент Endpoint Detection and Response, управляемый опытной командой охотников за угрозами. Многие компании считают, что аутсорсинг работы группе управляемого обнаружения и реагирования (MDR), занимающейся кибербезопасностью, является лучшим

вариантом, особенно если они выступают в качестве партнера, а не просто поставщика. Партнер MDR будет создавать и поддерживать настраиваемые списки наблюдения и модели обнаружения, созданные на основе новейшей аналитики угроз, для круглосуточного обнаружения действий злоумышленников в режиме реального времени. Они также обеспечивают дополнительный уровень защиты, предоставляя сложные средства сдерживания, изоляции и IR-возможности при обнаружении программ-вымогателей…» ***(Jason Straight. Ransomware: The Top 5 Myths and Misconceptions // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102i9y5/ransomware-the-top-5-myths-and-misconceptions). 09.03.2023).***

***

Фішингові атаки

«…Фактически, за две недели до августа 2022 года Национальный центр кибербезопасности Великобритании получил более 1500 сообщений о мошеннических «фишинговых» электронных письмах, якобы касающихся скидок на электроэнергию от Ofgem.

Это всего лишь один из примеров атак, которые используют киберпреступники. Есть и много других. А в организациях, которые находятся под давлением и пытаются снизить давление на расходы, такие атаки в стиле «социальной инженерии» с большей вероятностью увенчаются успехом и приведут к взлому. Учитывая ее поддержку Украины в войне против России, вполне вероятно, что спонсируемые российским государством субъекты продолжат усиливать свои атаки и на британские компании.

Вряд ли стоит удивляться тому, что недавно опубликованная официальная статистика показывает, что около 81% британских организаций испытали хотя бы одну успешную кибератаку в 2022 году. Кроме того, 83% считают, что кибератака более вероятна в ближайшие 12 месяцев.

Кроме того, как предсказывает PaloAlto Unit42, в этом году все больше людей будут прибегать к киберпреступлениям для получения финансовой выгоды, легкодоступные инструменты станут более доступными, а уязвимости будет легче использовать. Пересечение этих факторов в конечном итоге приведет к большему количеству инцидентов кибербезопасности.

Стоимость киберпреступления

Эти атаки также могут стоить организациям серьезных денег. По данным IBM, средняя стоимость утечки данных в Великобритании в 2022 году составила 5,05 млн долларов США, что ставит ее в пятерку самых дорогих стран в мире для утечки данных. Это не говоря уже о долгосрочном ущербе, который нарушение может нанести доверию и репутации компании.

Даже нарушение нормального функционирования бизнеса может иметь разрушительные последствия. Подумайте об этом: может ли ваша организация позволить себе 22 дня, которые требуются в среднем, чтобы вернуться к работе после взлома? Этот эффект может еще больше усилиться, если нарушение затронет ваши критически важные бизнес-приложения. Неудивительно, что половина малых предприятий, пострадавших от кибератак, разоряются в течение шести месяцев.

Также стоит помнить, что, учитывая процент британских предприятий, ставших жертвами кибератак в 2022 году, к кибератакам следует относиться как к чему-то, что произойдет, а не как к чему-то, что может произойти.

Инвестиции в правильное решение для кибербезопасности

Это делает инвестиции в правильное решение для кибербезопасности еще более важным. Хотя сейчас это может показаться крупными расходами, стоимость смягчения последствий и восстановления, вероятно, намного перевесит любые первоначальные затраты на технические средства контроля и экспертизу.

Хорошее решение для обеспечения кибербезопасности не только предупредит вас о новых угрозах и активно защитит вас от них, но и обеспечит наилучшие возможности для упреждающего реагирования в случае нарушения безопасности. Чем быстрее и эффективнее вы сможете это сделать, тем меньше будет влияние взлома.

Кроме того, он будет постоянно выявлять, оценивать, устранять и сообщать об уязвимостях программного обеспечения и сети вашей организации. В идеале он должен начинаться с выявления и устранения известных уязвимостей. Киберпреступники постоянно ищут пути проникновения в организацию, и неспособность устранить уязвимости так же хороша, как оставить для них дверь или окно открытым.

Небольшой удар может помочь вам избежать большого

В конечном счете должно быть ясно, что атаки киберпреступников не прекратятся в ближайшее время. Они также не станут менее дорогими для восстановления. Таким образом, даже компании, которые отчаянно ищут способы сократить расходы, должны рассмотреть возможность инвестирования в хорошее решение для обеспечения кибербезопасности». ***(JP Perez-Etchegoyen. Is the most cost-effective move in the cost of living crisis investing in cyber security solutions? // BetaNews, Inc (https://betanews.com/2023/03/07/cost-effective-move-cyber-security/). 07.03.2023).***

***

«За последние несколько месяцев израильтяне столкнулись со многими проблемами в своей повседневной жизни, и не все из них связаны с правительствами, протестами или реформами.

В то время как большинство людей знакомы с фишингом — кибератаками, замаскированными под сообщения из авторитетных источников — через электронные письма и телефонные звонки, недавний рой фишинга на основе текстовых сообщений задел отдельных лиц и учреждения по всей стране. Но большинство людей знают, что нельзя нажимать на неизвестную ссылку от незнакомцев, утверждающих, что они экзотический принц, или сообщение о том, что они выиграли в лотерею. Так почему же такие атаки увеличиваются как по частоте, так и по тяжести?

Ключевое отличие этих фишинговых атак заключается в том, что они поступают из очень знакомых, заслуживающих доверия источников

непосредственно в текстовые сообщения человека. Эти фишинговые схемы рассчитываются и нацелены на отдельных лиц через учреждения и приложения, которые они используют каждый день — от супермаркетов до Bit.

«Основываясь на наших оценках роста числа фишинговых атак в прошлом году, мы ожидаем, что в 2023 году средняя стоимость каждой утечки данных во всем мире превысит 5 миллионов долларов США за одну атаку, — сказал Кандид Уэст, вице-президент по исследованиям в области киберзащиты в Acronis. «В настоящее время на фишинг приходится примерно 76% всех кибератак, и обычным людям становится все труднее понять, какие сообщения они получают, являются законными или представляют собой попытку украсть их личную информацию»…

Acronis, всемирно известный лидер в области унифицированной кибербезопасности, предупреждает пользователей и компании о необходимости предпринять дополнительные шаги для защиты своей информации от злоумышленников. Основанная в 2003 году, компания открыла израильский офис и облачный центр обработки данных в 2021 году, предлагая решения, отвечающие постоянно растущим потребностям предприятий в области безопасности в различных отраслях.

Фишинговые атаки теперь также выходят за рамки отдельных лиц и могут создавать волны для целых организаций. В феврале 2023 года хакеры использовали методы фишинга, чтобы получить доступ к инфраструктуре Университета Технион и полностью заблокировать ее, потребовав более 1,7 миллиона долларов через программу-вымогатель, чтобы разблокировать ее. Acronis также подчеркивает, насколько жизненно важно для учреждений и предприятий обучать сотрудников тому, как защитить себя от фишинга из-за его потенциально разрушительных последствий.

«Наша цель как мирового лидера в области киберзащиты — сделать так, чтобы как можно больше людей сохраняли бдительность, когда речь идет о всех типах кибератак, особенно о фишинге», — добавил Вуэст. «При таких атаках наш лучший совет пользователям — проявлять крайнюю осторожность при получении текстовых сообщений или электронных писем, даже из авторитетных источников,

таких как их банк или приложение, которое они используют постоянно. Любые срочные дела или задачи, требующие вашей личной информации или проверки, должны решаться через веб-сайт компании или собственное приложение, а не через текст».

По мере того как фишинг становится все более изощренным и его все труднее распознать без надлежащих предупреждений, Acronis гарантирует, что организации любого размера останутся защищенными от многих возможных путей атак. Его технология охватывает секторы и использует защитные меры, основанные на приложениях машинного обучения и блокчейна.

Поскольку кибератаки не показывают признаков замедления, обычные люди должны помнить о том, что они могут стать мишенью. Ни один взлом не является слишком мелким, чтобы его можно было преследовать, и хакеры не откажутся от использования доверенных учреждений, которые мы считаем само собой разумеющимся, для доступа к наиболее уязвимым и эксплуатируемым пользовательским данным для собственной выгоды». ***(ARIEL SHAPIRA. Phishing cyberattacks are on the rise, but Arconis helps stop them – opinion // Jpost Inc. (https://www.jpost.com/business-and-innovation/opinion/article-734920). 20.03.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В рамках усилий международных правоохранительных органов федеральные власти в Лос-Анджелесе на этой неделе захватили интернет-домен, который использовался для продажи компьютерных вредоносных программ, используемых киберпреступниками для получения контроля над зараженными компьютерами и кражи большого количества информации.

Ордер на арест, утвержденный мировым судьей США 3 марта и приведенный в исполнение во вторник, привел к конфискации сайта http://www.worldwiredlabs.com, который предлагал троян удаленного доступа (RAT)

NetWire, сложную программу, способную нацеливаться и заражение всех основных компьютерных операционных систем. «RAT — это тип вредоносного ПО, которое позволяет осуществлять скрытое наблюдение, позволяя использовать «черный ход» для административного контроля и беспрепятственного и несанкционированного удаленного доступа к компьютеру жертвы без ведома или разрешения жертвы», — говорится в судебных документах, поданных в Лос-Анджелесе.

В рамках правоохранительных действий на этой неделе власти Хорватии во вторник арестовали гражданина Хорватии, который предположительно был администратором веб-сайта. Этот ответчик будет привлечен к ответственности хорватскими властями. Кроме того, во вторник правоохранительные органы Швейцарии захватили компьютерный сервер, на котором размещена инфраструктура NetWire RAT.

ФБР в Лос-Анджелесе в 2020 году начало расследование в отношении Worldlabs, единственного известного онлайн-дистрибьютора NetWire. Следователи под прикрытием из ФБР создали учетную запись на веб-сайте, оплатили план подписки и «создали настроенный экземпляр NetWire RAT с помощью инструмента Builder Tool», согласно показаниям под присягой в поддержку ордера на конфискацию.

Хотя на веб-сайте NetWire рекламировался как законный бизнес-инструмент для обслуживания компьютерной инфраструктуры, в заявлении под присягой говорится, что NetWire представляет собой вредоносное ПО, используемое в злонамеренных целях, программное обеспечение рекламировалось на хакерских форумах, а многочисленные компании, занимающиеся кибербезопасностью, и государственные учреждения задокументировали случаи использования NetWire. RAT используется в преступной деятельности.

«Сегодняшние действия являются свидетельством инноваций и гибкости, необходимых для борьбы с киберпреступниками, действующими без границ», — заявил прокурор США Мартин Эстрада. «Наш офис будет продолжать создавать международные альянсы для защиты наших сообществ от киберугроз. Преступники использовали NetWire в глобальном масштабе, и мы в ответ

демонтировали инфраструктуру, которая нанесла невыразимый вред жертвам по всему миру».

«Удалив Netwire RAT, ФБР повлияло на криминальную киберэкосистему, — сказал Дональд Алвей, помощник директора местного отделения ФБР в Лос-Анджелесе. «Глобальное партнерство, которое привело к аресту в Хорватии, также удалило популярный инструмент, используемый для захвата компьютеров, чтобы увековечить глобальное мошенничество, утечку данных и вторжение в сеть со стороны групп угроз и киберпреступников».

Это дело является результатом тесного сотрудничества правоохранительных органов Соединенных Штатов с Хорватией и другими глобальными партнерами. Полевой офис ФБР в Лос-Анджелесе; Министерство внутренних дел Хорватии, Управление уголовной полиции; Кантональная полиция Цюриха в Швейцарии; Европейский центр киберпреступности Европола; и Австралийская федеральная полиция провела расследование по этому делу.

Помощники прокурора США Лиза Фельдман из Секции по преступлениям в области кибербезопасности и интеллектуальной собственности и Максвелл Колл из Секции конфискации и возврата активов получили ордер на конфискацию интернет-домена. Существенную помощь в расследовании оказало Управление по международным делам Уголовного отдела Министерства юстиции». ***(Federal Authorities Seize Internet Domain Selling Malware // Culver City Observer (https://www.culvercityobserver.com/story/2023/03/16/news/federal-authorities-seize-internet-domain-selling-malware/12307.html). 16.03.2023).***

***

«На прошлой неделе ФБР арестовало человека, предположительно «Помпомпурина», администратора печально известного и популярного форума Breach. Через несколько дней после ареста новый администратор веб-сайта, посвященного киберпреступности, объявил, что они навсегда закрывают форум.

«Пожалуйста, считайте это окончательным обновлением для Breached», — написал новый администратор, известный как «Бафомет», в официальном канале Telegram. «Я закрою форум, так как я считаю, что мы можем предположить, что больше ничего не безопасно. Я знаю, что все хотят, чтобы форум работал, но нет никакой ценности в краткосрочной выгоде для того, что, вероятно, будет долгосрочной потерей, поддерживая Breached как есть»

…Очевидный, конец Breach Forums наступил примерно через год после того, как коалиция международных правоохранительных органов во главе с Министерством юстиции США захватила RaidForums еще один печально известный форум киберпреступников, где рекламировались и продавались взломанные базы данных. Breach Forums родился после распада RaidForums и служил почти той же цели и аудитории.

«Я хочу прояснить, что, хотя это первоначальное объявление не является положительным, это еще не конец. Я собираюсь создать еще одну группу Telegram для тех, кто хочет увидеть, что будет дальше. Вам позволено ненавидеть меня и не соглашаться с моим решением, но я обещаю, что грядущее будет лучше для всех нас», — написал Бафомет. «Дайте (sic) мне 24 часа, чтобы немного отдохнуть и подумать о том, как мы будем двигаться дальше. После этого я вернусь онлайн, и мы поговорим. Я никуда не иду».

В прикрепленном сообщении, которое было подписано ключом PGP Бафомета, чтобы доказать, что оно действительно было написано ими, они написали, что смогли подтвердить, что власти имеют доступ к машине Помпомпурина.

Бафомет объяснил, что во время переноса серверов форума он обнаружил, что кто-то зашел на один из серверов раньше, чем они.

«К сожалению, это, вероятно, приводит к выводу, что кто-то имеет доступ к машине Poms. Любые серверы, которые мы используем, никогда не используются совместно с кем-либо еще, поэтому кто-то должен знать учетные данные для этого сервера, чтобы иметь возможность войти в систему. Теперь я чувствую, что попал в положение, когда ничто не может считаться безопасным, будь то наши

конфигурации, исходный код или информация о наших пользователях — список бесконечен», — написал Бафомет. «Это означает, что я не могу подтвердить, что форум безопасен, что было главной целью с самого начала этого дерьмового шоу».

Федералы обвиняют Конора Брайана Фицпатрика в том, что он Помпомпурин, которому предъявлены обвинения в Нью-Йорке, а также в Восточном округе Вирджинии. Фитцпатрик обвиняется в заговоре с целью мошенничества с устройствами доступа.

В понедельник, через три дня после ареста Фитцпатрика и до того, как они обнаружили, что кто-то получил доступ к одному из серверов, Baphomet объявили, что переносят серверы форума, чтобы поддерживать работу Breach Forums.

Этот план больше не действует, но Бафомет сказал, что это не конец.

«Что касается того, что это значит сейчас, это сложно. В отличие от того, когда другие сообщества рухнут и все разбегутся, я по-дурацки все еще буду рядом», — написали они.

«Несмотря на то, что сообщество Breached будет умирать, я собираюсь продолжить общение с некоторыми администраторами форумов конкурентов и операторами различных сервисов, которые связались со мной за последние несколько дней. Я надеюсь работать с некоторыми из этих людей, чтобы создать новое сообщество, в котором будут лучшие черты Breached, и в то же время уменьшится количество поверхностей для атак, которые мы никогда не рассматривали должным образом. Как и в подобных вещах, я не сомневаюсь, что наша пользовательская база может быть поглощена другим сообществом, но если есть терпение, я надеюсь вернуть что-то, что будет конкурировать с любым другим сообществом, которое может занять наше место». ***(Lorenzo Franceschi-Bicchierai. Notorious hacking forum shuts down after administrator gets arrested // Yahoo (https://techcrunch.com/2023/03/21/notorious-hacking-forum-shuts-down-after-administrator-gets-arrested/). 21.03.2023).***

***

«…6 марта 2023 года Европол сообщил об арестах двух «вдохновителей» группы вымогателей DoppelPaymer, а также об изъятии устройств в ходе одновременных рейдов, проведенных немецкой и украинской полицией. В операции, которую координировал Европол, участвовали правоохранительные органы Дании и США. Немецкая полиция также выдала ордера на арест трех граждан России, проживающих в стране.

DoppelPaymer был наиболее активен в период с 2019 по 2021 год, но в июле 2021 года был переименован в «Гриф» в попытке избежать санкций из-за своих связей с Россией. Сообщается, что он нацелен на более чем 600 компаний по всему миру, уделяя особое внимание секторам здравоохранения, экстренной помощи и образования.

Это следует за чередой недавних побед правоохранительных органов в 2023 году. ФБР в сотрудничестве с Европолом и 13 другими правоохранительными органами тайно проникло в инфраструктуру банды вымогателей Hive в июле 2022 года. вниз его платеж и темные места утечки. Операция предотвратила выплату выкупа на сумму около 130 миллионов долларов, поскольку ФБР смогло предупредить цели Hive до того, как произошла атака, и получило и распространило ключи дешифрования.

В феврале 2023 года Национальное агентство по борьбе с преступностью Великобритании («NCA») в сотрудничестве с Управлением по контролю за иностранными активами Министерства финансов США («OFAC») разоблачило и наложило санкции на семерых киберпреступников, связанных с группой вымогателей, стоящей за вредоносным ПО Trickbot. а также штаммы Конти и РЮК. Эти лица теперь подлежат запрету на поездки и замораживанию активов, а также строго ограничены в использовании глобальной финансовой системы. Известно, что эта группа несет ответственность за некоторые из самых разрушительных атак программ-вымогателей в Великобритании на школы, предприятия и местные органы власти.

Министр иностранных дел Джеймс Клеверли сказал: «Налагая санкции на этих киберпреступников, мы посылаем им и другим лицам, причастным к

программам-вымогателям, четкий сигнал о том, что они будут привлечены к ответственности».

Совсем недавно, 9 марта 2023 года, усилия международных правоохранительных органов привели к аресту подозреваемого администратора трояна удаленного доступа NetWire («NetWire RAT»). NetWire RAT — это инструмент, используемый злоумышленниками для запуска фишинговых атак и эксфильтрации сетей. Он позволяет злоумышленнику удаленно выполнять команды, делать снимки экрана, а также загружать и загружать файлы. Домен (worldwiredlabs.com), используемый NetWire для продвижения своего сервиса, был конфискован ФБР, а швейцарская полиция отключила сервер, на котором размещен веб-сайт. ФБР заявило, что «удалив NetWire RAT, ФБР повлияло на криминальную киберэкосистему».

Кто выигрывает?

Международные усилия по борьбе с киберпреступностью находятся в центре внимания правительств по всему миру. 2 марта 2023 года администрация Байдена объявила об обновленной Национальной стратегии кибербезопасности, направленной на «подрыв и ликвидацию участников угроз » и « признание того, что правительство должно использовать все инструменты национальной власти скоординированным образом для защиты нашей национальной безопасности, общественной безопасности и экономического процветания».

Санкции и препятствия, установленные правоохранительными органами, безусловно, препятствуют работе киберпреступников. Conti, одна из самых активных групп вымогателей в 2021/2022 годах, была распущена в прошлом году (но затем переименована), и летом 2022 года после вторжения в Украину произошло заметное снижение атак программ-вымогателей. Но достаточно ли санкций и международных репрессивных мер, чтобы навсегда остановить и сдержать эти группы вымогателей? К сожалению нет.

Группы вымогателей движимы признанием сверстников, а также финансовым вознаграждением. После временного затишья в середине-конце 2022 года атаки программ-вымогателей снова участились. По мере того, как группы

вымогателей выходят из украинского конфликта, реорганизуются и разрабатывают более сложные технологии и методы для преодоления санкций и инфраструктурных препятствий, созданных правоохранительными органами, отчеты о тенденциях указывают на то, что они, вероятно, вернутся к уровням, наблюдавшимся в 2021 году.

Эксфильтрация личных данных будет ключевой тактикой вымогательства, предпочтительнее метода только шифрования. Целями, наиболее уязвимыми для атак, являются те организации, которые владеют большими объемами конфиденциальной личной информации, устаревших данных и имеют несовершенные системы кибербезопасности и мониторинга угроз. Безопасное автономное резервное копирование жизненно важно для восстановления, но оно не защитит личные данные от злоумышленников.

Сбор разведывательных данных и международное сотрудничество между правоохранительными органами, по-видимому, являются жизненно важными средствами борьбы с группами программ-вымогателей. Правительство подготовило пошаговое руководство о том, куда следует сообщать о киберинцидентах. Наш совет клиентам всегда заключался в том, чтобы сообщать о кибер-инциденте и указывать название группы злоумышленников, ответственных перед NCA и NCSC, с помощью онлайн-инструмента для сообщений на веб-сайте Action Fraud». ***(Hans Allnutt and Camilla Elliot. Cybercriminals vs law enforcement. Who is winning? // DAC Beachcroft LLP (https://www.dacbeachcroft.com/en/gb/articles/2023/march/cybercriminals-vs-law-enforcement-who-is-winning/). 23.03.2023).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Microsoft выпустила несколько исправлений, устраняющих ряд уязвимостей, недавно обнаруженных в некоторых популярных процессорах Intel.

Внеплановые обновления устранили в общей сложности четыре уязвимости, в совокупности описанные как «недостатки раскрытия информации в памяти ввода-вывода STale Data (MMIO)».

Другими словами, злоумышленник может использовать уязвимость в виртуальной машине для доступа к (конфиденциальным) данным на другой виртуальной машине.

Уязвимости отслеживаются как CVE-2022-21123 (чтение данных из общего буфера), CVE-2022-21125 (выборка данных из общего буфера), CVE-2022-21127 (обновление выборки данных из буфера специального регистра) и CVE-2022-21166. (Частичная запись регистра устройства).

«Злоумышленник, успешно воспользовавшийся этими уязвимостями, может получить доступ к привилегированным данным через границы доверия», — говорится в последующем бюллетене Microsoft.

«В средах с общими ресурсами (например, в некоторых конфигурациях облачных сервисов) эти уязвимости могут позволить одной виртуальной машине неправомерно получить доступ к информации из другой. В сценариях без просмотра в автономных системах злоумышленнику потребуется предварительный доступ к системе или возможность запуска специально созданного приложения в целевой системе для использования этих уязвимостей».

Microsoft также заявила, что, помимо мер по смягчению последствий для Windows Server 2019 и Windows Server 2022, никаких исправлений никогда не выпускалось. Теперь гигант из Редмонда взял дело в свои руки. Однако, согласно

BleepingComputer, набор обновлений для Windows 10, Windows 11 и Windows Server кажется «несколько запутанным»: «Из бюллетеней поддержки неясно, являются ли они новыми микрокодами Intel или другими мерами по смягчению последствий, которые будут применяется к устройствам», — пояснило издание.

Чтобы применить исправления, пользователям необходимо загрузить их на свои конечные точки (откроется в новой вкладке) вручную из каталога Центра обновления Майкрософт. Это ярлыки:

KB5019180 — Windows 10, версии 20H2, 21H2 и 22H2.

KB5019177 — Windows 11, версия 21H2

KB5019178 — Windows 11, версия 22H2

KB5019182 — Windows Server 2016

KB5019181 — Windows Server 2019

KB5019106 — Windows Server 2022

В публикации добавлено, что обновления следует применять с осторожностью, поскольку они могут вызвать проблемы с производительностью и даже могут быть неэффективными без отключения технологии Intel Hyper-Threading». ***(Sead Fadilpašić. Microsoft is fixing a load of serious Intel CPU security flaws // Future US, Inc. (https://www.techradar.com/news/microsoft-is-fixing-a-load-of-intel-cpu-security-flaws). 03.03.2023).***

***

«Microsoft OneNote, приложение для создания заметок, входящее в пакет офисных приложений Office 365, привлекает к себе все больше внимания по совершенно неправильным причинам.

Это следует за отчетом исследователей кибербезопасности, описывающим, как все больше и больше злоумышленников начинают использовать приложение для доставки вредоносного ПО ничего не подозревающим жертвам.

На этот раз исследователи из Zscaler опубликовали отчет, в котором OneNote описывается как «растущая угроза» для распространения вредоносных программ.

Способ доставки аналогичен способу доставки файлов Office с макросами. Злоумышленники генерировали файл OneNote, называемый NoteBook, оформляя его так, чтобы он выглядел как важный документ, такой как счет-фактура или что-то подобное. Внутри файла они размещали вредоносное вложение, способное загружать и запускать вредоносное ПО со стороннего сервера. Затем они размывали содержимое файла и накладывали на него кнопку с надписью «Нажмите здесь, чтобы просмотреть» или похожий призыв к действию.

Нажатие на кнопку активирует надстройку и запустит вредоносное ПО.

Затем файл будет распространяться обычным способом — по электронной почте. Ежедневно отправляются сотни тысяч фишинговых электронных писем, нацеленных на корпоративные конечные точки, персональные компьютеры и другие устройства, содержащие конфиденциальные данные клиентов и личные данные.

Прошлым летом Microsoft наконец запретила программам Office запускать макросы в файлах, загруженных из Интернета. Таким образом, компания эффективно пресекла один из самых популярных векторов атак среди киберпреступников. С тех пор хакеры усердно работали, ища альтернативные способы доставки вредоносных программ. Стали выделяться два метода — доставка файла ISO (тип архивного файла, который позволяет хакерам обходить электронную почту и антивирусную защиту) и доставка файлов NoteBook.

Чтобы защититься от этих типов атак, исследователи кибербезопасности обычно советуют здравому смыслу не загружать вложения электронной почты и не переходить по ссылкам в электронных письмах, содержание, адрес отправителя или строка темы которых кажутся даже отдаленно подозрительными». ***(Sead Fadilpašić. Microsoft OneNote is still being used to flood devices with malware // Future US, Inc. (https://www.techradar.com/news/microsoft-onenote-is-still-being-used-to-flood-devices-with-malware). 03.03.2023).***

***

«Спецификация Trusted Platform Module (TPM) 2.0 подвержена двум уязвимостям переполнения буфера, которые могут позволить злоумышленникам получить доступ или перезаписать конфиденциальные данные, такие как криптографические ключи.

TPM — это аппаратная технология, предоставляющая операционным системам защищенные от несанкционированного доступа функции шифрования. Его можно использовать для хранения криптографических ключей, паролей и других важных данных, что делает любую уязвимость в его реализации поводом для беспокойства.

Хотя TPM требуется для некоторых функций безопасности Windows, таких как измеряемая загрузка, шифрование устройства, System Guard в Защитнике Windows (DRTM), аттестация работоспособности устройства, он не требуется для других, более часто используемых функций.

Однако при наличии доверенного платформенного модуля функции безопасности Windows получают повышенную безопасность при защите конфиденциальной информации и шифровании данных.

Спецификация TPM 2.0 приобрела популярность (и вызвала споры), когда Microsoft сделала ее обязательным требованием для запуска Windows 11 из-за необходимых мер безопасности при загрузке и обеспечения надежной аутентификации при распознавании лиц Windows Hello.

Linux также поддерживает доверенные платформенные модули, но нет требований для использования модуля в операционной системе. Однако доступны инструменты Linux, которые позволяют приложениям и пользователям защищать данные в TPM.

Уязвимости TPM 2.0

Новые уязвимости в TPM 2.0 были обнаружены исследователями Quarkslab Франсиско Фалконом и Иваном Арсе, которые заявили, что уязвимости могут затронуть миллиарды устройств. Уязвимости отслеживаются как CVE-2023-1017 (чтение за пределами границ) и CVE-2023-1018 (запись за пределами границ).

Оба недостатка возникают из-за того, как спецификация обрабатывает параметры для некоторых команд TPM, позволяя локальному злоумышленнику, прошедшему проверку подлинности, использовать их, отправляя вредоносные команды для выполнения кода в TPM.

Согласно бюллетеню по безопасности Trusted Computing Group (TCG), разработчика спецификации TPM, это может привести к раскрытию информации или повышению привилегий.

Trusted Computing Group объясняет, что проблемы с переполнением буфера связаны с чтением или записью 2 байтов после конца буфера, переданного в точку входа ExecuteCommand().

Влияние этого зависит от того, что производители реализовали в этой области памяти, т. е. является ли она неиспользуемой памятью или содержит оперативные данные.

Координационный центр CERT опубликовал предупреждение об уязвимостях и в течение нескольких месяцев информировал поставщиков, пытаясь повысить осведомленность при картировании последствий. К сожалению, только несколько организаций подтвердили, что они затронуты.

«Злоумышленник, имеющий доступ к командному интерфейсу TPM, может отправлять в модуль вредоносные команды и запускать эти уязвимости», — предупредил CERT.

«Это позволяет либо доступ только для чтения к конфиденциальным данным, либо перезапись обычно защищенных данных, которые доступны только для TPM (например, криптографические ключи)».

Решением для затронутых поставщиков является переход на фиксированную версию спецификации, которая включает одно из следующих действий:

TMP 2.0 v1.59 Errata версии 1.4 или выше

TMP 2.0 v1.38 Errata версии 1.13 или выше

TMP 2.0 v1.16 Errata версии 1.6 или выше

Lenovo — единственный крупный OEM-производитель, выпустивший рекомендации по безопасности в отношении двух недостатков TPM, предупреждая,

что CVE-2023-1017 влияет на некоторые из его систем, работающих на чипах Nuvoton TPM 2.0.

Хотя для этих недостатков требуется аутентифицированный локальный доступ к устройству, важно помнить, что вредоносное ПО, работающее на устройстве, будет соответствовать этому условию.

TPM — это высокозащищенное пространство, которое теоретически должно быть защищено даже от вредоносных программ, работающих на устройстве, поэтому практическую важность этих уязвимостей нельзя игнорировать или преуменьшать.

Пользователям рекомендуется ограничить физический доступ к своим устройствам доверенными пользователями, использовать только подписанные приложения от надежных поставщиков и применять обновления прошивки, как только они станут доступны для их устройств». ***(Bill Toulas. New TPM 2.0 flaws could let hackers steal cryptographic keys // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-tpm-20-flaws-could-let-hackers-steal-cryptographic-keys/). 04.03.2023).***

***

Endor Labs, компания-разработчик программного обеспечения, которая обеспечивает безопасность и обслуживание программного обеспечения с открытым исходным кодом, выпустила отчет, в котором указаны 10 основных рисков безопасности и операционных рисков в программном обеспечении с открытым исходным кодом в 2023 году.

В отчете, подготовленном командой Endor Labs из Station 9, приняли участие более 20 главных специалистов по информационной безопасности известных компаний, включая Adobe, HashiCorp, Discord и Palo Alto Networks.

По данным Endor Labs, чрезмерная зависимость от программного обеспечения с открытым исходным кодом зафиксировала некоторые известные уязвимости, отмеченные как общие уязвимости и риски; эти уязвимости часто

упускаются из виду и могут быть использованы злоумышленниками, если не будут устранены.

«Программное обеспечение с открытым исходным кодом представляет собой золотую жилу для разработчиков приложений, но оно нуждается в не менее эффективных средствах обеспечения безопасности», — сказал Хенрик Плейт, ведущий исследователь безопасности в Endor Labs. «В среде, где более 80% кода в новых приложениях может поступать из существующих репозиториев, очевидно, что существуют серьезные риски».

Основные риски открытого исходного кода в 2023 году

Ниже выделены основные выводы отчета Endor Labs о 10 основных рисках с открытым исходным кодом в 2023 году.

1. Известные уязвимости

Отчет показал, что версия компонента с открытым исходным кодом может содержать уязвимый код, случайно добавленный его разработчиками. Уязвимость может быть использована в нижестоящем программном обеспечении, что может поставить под угрозу конфиденциальность, целостность или доступность системы и ее данных.

2. Компрометация легитимного пакета

Согласно отчету Endor, злоумышленники могут нацеливаться на законные ресурсы из существующего проекта или инфраструктуры распространения, чтобы внедрить вредоносный код в компонент. Например, они могут захватить учетные записи законных сопровождающих проектов или использовать уязвимости в репозиториях пакетов. Этот тип атаки может быть опасен, поскольку вредоносный код может распространяться как часть законного пакета и его трудно обнаружить.

3. Атаки путаницы в именах

Злоумышленники могут создавать компоненты с именами, похожими на имена законных компонентов с открытым исходным кодом или системных компонентов. Отчет Endor Labs показал, что это можно сделать с помощью:

Опечатка: Злоумышленник создает имя, которое является орфографической ошибкой имени исходного компонента.

Брандджекинг: Злоумышленник предлагает надежного автора.

Комбинированное приседание: злоумышленник играет с общими шаблонами именования в разных языках или экосистемах.

Эти атаки могут использоваться для того, чтобы заставить пользователей загружать и использовать вредоносные компоненты, которые они считают законными.

4. Необслуживаемое программное обеспечение

Согласно отчету Endor Labs, необслуживаемое программное обеспечение является эксплуатационной проблемой. Компонент или версия компонента больше не может активно разрабатываться, что означает, что исправления для функциональных и нефункциональных ошибок могут предоставляться не сразу или вообще не предоставляться первоначальным проектом с открытым исходным кодом. Это может сделать программное обеспечение уязвимым для использования злоумышленниками, нацеленными на известные уязвимости.

5. Устаревшее программное обеспечение

Для удобства некоторые разработчики используют устаревшую версию базы кода при наличии обновленных версий. Это может привести к тому, что проект упустит важные исправления ошибок и исправления безопасности, что сделает его уязвимым для эксплуатации.

6. Неотслеживаемые зависимости

Разработчики проекта могут не знать о зависимости от компонента по нескольким причинам:

Он не является частью спецификации программного обеспечения вышестоящего компонента.

Средства анализа состава программного обеспечения не запускаются или не обнаруживают его.

Зависимость устанавливается не с помощью менеджера пакетов, что может привести к проблемам с безопасностью, поскольку уязвимости в неотслеживаемой зависимости могут остаться незамеченными.

7. Лицензионный и регуляторный риск

Компонент или проект может не иметь лицензии или иметь лицензию, несовместимую с предполагаемым использованием, или требования которой не могут быть или не могут быть выполнены.

Использование компонентов в соответствии с их лицензионными условиями имеет решающее значение. Невыполнение этого требования, например использование компонента без лицензии или несоблюдение его условий, может привести к нарушению авторских прав или лицензии. В таких случаях правообладатель имеет право обратиться в суд.

Кроме того, нарушение законодательных и нормативных требований может ограничить или затруднить работу с определенными отраслями или рынками.

8. Незрелое программное обеспечение

Проект с открытым исходным кодом может не следовать передовым методам разработки, таким как использование стандартной схемы управления версиями, наличие набора регрессионных тестов или наличие руководств или документации по обзору. Это может привести к тому, что компонент с открытым исходным кодом не будет работать надежно или безопасно, что сделает его уязвимым для эксплуатации.

Использование незрелого компонента или проекта может привести к значительным операционным рискам. Например, программное обеспечение, которое зависит от него, может работать не так, как предполагалось, что приводит к проблемам с надежностью во время выполнения.

9. Неутвержденные изменения (изменяемые)

При использовании компонентов, идентичность которых при загрузке в разное время не гарантируется, существует значительный риск безопасности. Об этом свидетельствуют такие атаки, как Codecov Bash Uploader, когда загруженные скрипты передаются напрямую в bash без предварительной проверки их целостности. Использование изменяемых компонентов также представляет угрозу для стабильности и воспроизводимости сборок программного обеспечения.

10. Зависимость от недостаточного или чрезмерного размера

В отчете Endor указывалось, что чрезмерная/недостаточная зависимость от компонентов может быть операционным риском. Например, небольшие компоненты, содержащие всего несколько строк кода, подвержены тем же рискам, что и более крупные компоненты. Эти риски включают поглощение учетных записей, вредоносные запросы на вытягивание, а также непрерывной интеграции и непрерывной разработки. уязвимости конвейера

С другой стороны, огромные компоненты могут иметь множество функций, которые не нужны для стандартных вариантов использования. Эти функции увеличивают поверхность атаки компонента и могут привести к появлению неиспользуемых зависимостей, что приведет к их раздуванию.

Шаги, которые необходимо предпринять для снижения этих рисков с открытым исходным кодом

Вот советы от Endor Labs о том, как разработчики программного обеспечения и ИТ-менеджеры могут снизить эти риски, связанные с открытым исходным кодом.

Регулярно сканируйте код для обнаружения скомпрометированных пакетов

Предотвращение скомпрометированных пакетов — сложная проблема, поскольку не существует универсального решения. Чтобы решить эту проблему, организации могут обратиться к новым стандартам и платформам, таким как OpenSSF Secure Supply Chain Consumption Framework (S2C2F).

Они могут выбирать и расставлять приоритеты мер безопасности, которые лучше всего соответствуют их требованиям, исходя из их конкретных потребностей в безопасности и устойчивости к риску.

Проверьте, соответствует ли проект лучшим практикам разработки

Чтобы оценить качество и актуальность проекта, проверьте его документацию и примечания к выпуску на предмет полноты и своевременности. Ищите значки, указывающие на покрытие тестами или наличие конвейеров CI/CD, которые могут обнаруживать регрессии.

Кроме того, вы можете оценить проект, проверив количество активных сопровождающих и участников, частоту выпуска новых выпусков, а также количество открытых и закрытых проблем и запросов на вытягивание. Также

крайне важно искать информацию о стратегии обслуживания или поддержки проекта — например, наличие и даты версий долгосрочной поддержки.

Поддерживайте актуальность зависимостей и проверяйте характеристики кода перед их использованием.

Для обеспечения безопасности кода важна проверка как самого кода, так и характеристик проекта. Примеры характеристик кода, которые необходимо проверить, включают перехватчики до и после установки и закодированные полезные данные. Для характеристик проекта учитывайте репозиторий исходного кода, учетные записи сопровождающих, частоту выпуска и количество последующих пользователей.

Один из способов поддерживать актуальность зависимостей — использовать инструменты, которые генерируют запросы на слияние или вытягивание с предложениями по обновлению. Также важно сделать обновления зависимостей и повторяющиеся элементы невыполненной работы приоритетными.

Оцените и сравните инструменты анализа состава программного обеспечения

Команды безопасности должны убедиться, что инструменты SCA способны создавать точные спецификации как на грубом уровне, например, для зависимостей, объявленных с помощью инструментов управления пакетами, таких как Maven или npm, так и на мелкозернистом уровне, как отдельные файлы, включенные «вне диапазона» без использования менеджеров пакетов, например, для артефактов.

Используйте компоненты в соответствии с условиями лицензии с открытым исходным кодом

ИТ-руководители должны следить за тем, чтобы их разработчики программного обеспечения не использовали компоненты с открытым исходным кодом без лицензии, так как это может создать юридические риски. Чтобы обеспечить соответствие и избежать возможных юридических проблем, важно определить приемлемые лицензии для компонентов, используемых при разработке программного обеспечения.

Факторы, которые следует учитывать, включают в себя то, как компонент связан, модель развертывания и предполагаемую схему распространения. После того, как вы определили приемлемые лицензии, соблюдайте требования, изложенные в этих лицензиях с открытым исходным кодом». ***(Franklin Okeke. Top 10 open-source security and operational risks of 2023 // TechnologyAdvice (https://www.techrepublic.com/article/top-open-source-security-risks/). 03.03.2023).***

***

«CISA добавила уязвимость удаленного выполнения кода высокой степени серьезности (RCE) почти трехлетней давности в Plex Media Server в свой каталог недостатков безопасности, используемых в атаках.

Этот недостаток безопасности, отслеживаемый как CVE-2020-5741, позволяет злоумышленникам с правами администратора удаленно выполнять произвольный код Python в атаках низкой сложности, не требующих взаимодействия с пользователем.

Злоумышленники с «административным доступом к Plex Media Server могут злоупотреблять функцией загрузки с камеры, чтобы заставить сервер выполнять вредоносный код», согласно бюллетеню, опубликованному группой безопасности Plex в мае 2020 года, когда она исправила ошибку с выпуском Plex Media Server. 1.19.3.

«Это можно сделать, настроив каталог данных сервера так, чтобы он перекрывался с расположением контента для библиотеки, в которой была включена загрузка с камеры. Эту проблему нельзя было использовать без предварительного доступа к учетной записи Plex сервера».

Хотя CISA не предоставила никакой информации об атаках, в которых использовалась CVE-2020-5741, это, вероятно, связано с тем, что LastPass недавно обнаружил, что компьютер старшего инженера DevOps был взломан в прошлом году, чтобы установить кейлоггер, используя сторонний носитель. программная ошибка RCE.

Злоумышленники в конечном итоге получили доступ к учетным данным инженера и корпоративному хранилищу LastPass. Это привело к массовой утечке данных в августе 2022 года после того, как злоумышленники украли производственные резервные копии LastPass и резервные копии критически важных баз данных.

Сообщается, что Plex RCE использовался для взлома инженера LastPass

Несмотря на то, что LastPass не сообщила, какая программная уязвимость использовалась для взлома компьютера инженера, Ars Technica сообщила, что на домашнем компьютере сотрудника использовался программный пакет Plex.

По совпадению, в августе Plex также уведомил клиентов об утечке данных и попросил их сбросить свои пароли после того, как LastPass сообщил о второй собственной утечке.

В пятницу CISA также добавила критическую уязвимость в VMware Cloud Foundation (отслеживается как CVE-2021-39144), активно эксплуатируемую с начала декабря, в свой каталог известных эксплуатируемых уязвимостей (KEV).

Согласно обязательной оперативной директиве от ноября 2021 года (BOD 22-01), федеральные агентства США теперь также обязаны защищать свои системы от атак до 31 марта, чтобы блокировать попытки атак, которые могут быть нацелены на их сети, используя две уязвимости.

Хотя BOD 22-01 применяется только к федеральным агентствам, CISA настоятельно призвала все организации исправить эти ошибки для защиты от продолжающихся атак». ***(Sergiu Gatlan. CISA warns of actively exploited Plex bug after LastPass breach // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-plex-bug-after-lastpass-breach/). 11.03.2023).***

***

«…С распространением известных уязвимостей нулевого дня в критически важных бизнес-приложениях в сочетании с постоянно развивающейся изощренной тактикой злоумышленников организации

должны быть готовы противостоять любой угрозе, которая встретится на их пути. Вот несколько прогнозов того, что нас ждет в 2023 году.

Log4shell оказал значительное влияние на предприятия по всему миру, и многие из них все еще находятся под его влиянием по сей день. Почти каждый поставщик цепочки поставок программного обеспечения получил задание исправить печально известную уязвимость, подчеркнув, насколько сложно исправить недостатки, обнаруженные в часто используемых библиотеках.

К сожалению, есть много организаций, которые еще не установили исправления, а злоумышленники начинают их замечать. Киберпреступники все еще пользуются неисправленными уязвимостями Log4j более чем через год после их обнаружения. В сентябре 2022 года было обнаружено, что хакерская группа Lazarus использует уязвимость Log4j для атак на энергетические компании и проведения кампаний кибершпионажа.

В 2023 году мы можем ожидать еще больше инцидентов, связанных с эксплойтами Log4j. Кроме того, мы, вероятно, увидим, как киберпреступники ищут уязвимости в библиотеках с открытым исходным кодом в надежде найти следующую уязвимость Log4j.

…киберпреступники всегда ищут новые уязвимости и векторы атак. Однако они часто внимательно следят за известными уязвимостями, поскольку они могут дать им прямой доступ в сеть организации. уходит в среднем 97 дней Исследование Ponemon Institute показывает, что на администрирование исправления — с момента обнаружения уязвимости до момента выпуска, тестирования и полного внедрения исправления. Между тем исследование, которое мы провели в сотрудничестве с SAP и CISA, показало, что злоумышленникам может потребоваться менее 72 часов, чтобы начать использовать недостатки ERP после уведомления о выпуске исправления.

В 2023 году киберпреступники будут все чаще наносить удары по известным недостаткам кибербезопасности, особенно в системах, подключенных к Интернету, поскольку они часто являются наиболее прибыльными.

Программы-вымогатели исторически были одним из основных способов получения прибыли киберпреступниками. Однако, согласно исследованию Coalition (через CSO), которое показывает, что атаки программ-вымогателей и платежи программ-вымогателей немного снизились в 2022 году, вполне возможно, что злоумышленники отказываются от этой традиционной тактики. Вместо того, чтобы держать бизнес-активы и ценные данные в заложниках до тех пор, пока организации не заплатят, киберпреступники будут использовать гораздо более просчитанные методы для получения прибыли. Тактика группы угроз Elephant Beetle показывает, как злоумышленники могут незаметно вторгаться в критически важные бизнес-приложения и получать миллионы долларов в течение нескольких месяцев подряд, не оставляя следов...

По мере того, как экономический спад приближается к 2023 году, предприятия будут продолжать искать способы урезать свои бюджеты и использовать только те ресурсы, которые необходимы для бизнеса. Укрепление стратегий кибербезопасности останется первоочередной задачей в этом году, однако специалисты по безопасности должны более избирательно и стратегически подходить к своим инвестициям в технологии. Процессы, сосредоточенные вокруг приложений ERP, должны быть развернуты. Делая инвестиции в безопасные ERP-системы, специалисты по безопасности должны учитывать следующее:

1. Внедрите управление уязвимостями. Многим предприятиям не хватает прозрачности, бизнес-контекста и исследований угроз, необходимых для обнаружения и определения приоритетности критических недостатков, и они не могут распознать истинную поверхность атаки своего ландшафта приложений ERP. Управление уязвимостями может помочь устранить эти пробелы в безопасности. Изучая потенциальные инструменты для внедрения, группы безопасности должны специально искать автоматизированные возможности, которые могут предоставить им полную информацию о ландшафте критически важных для бизнеса приложений, а также дать им более глубокое понимание каждой уязвимости и ее уровня критичности.

2. Используйте риск-ориентированный подход к управлению уязвимостями. Чтобы критический недостаток не оказал серьезного влияния на их бизнес, организации должны развернуть программу управления уязвимостями на основе рисков, которая включает анализ угроз и наблюдение за действиями, пользователями и уязвимостями на уровне базы данных и приложений. Этот процесс может снять значительную нагрузку с команд с ограниченными ресурсами, помогая им правильно расставить приоритеты в первую очередь для наиболее важных уязвимостей, а не тратить слишком много времени и ресурсов на мелкие недостатки.

3. Разверните обучение безопасности приложений ERP. Успешная программа безопасности приложений ERP невозможна без надлежащего обучения. Команды безопасности должны понимать, как функционируют эти критически важные системы, а также методы, которые злоумышленники используют для их использования. Основные основы обучения работе с приложением ERP включают в себя:

• Основы архитектуры ERP и определение ее различных компонентов.

• Тактика, которую злоумышленники используют для использования неправильных конфигураций и известных уязвимостей.

• Сценарии после эксплуатации и способы защиты приложений ERP от этих угроз.

Когда речь заходит о тенденциях приложений ERP в 2023 году, ясно одно: эти ценные активы будут становиться все более целевыми. Мы обнаружили, что были сотни успешных эксплойтов в неисправленных приложениях SAP, и мы можем ожидать, что это число увеличится в ближайшие месяцы. Поскольку в этом году количество атак на ERP-приложения резко возросло, компаниям необходимо ускорить внедрение средств защиты критически важных для бизнеса приложений». ***(Juan Perez-Etchegoyen. Application Security Predictions For 2023 // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/03/21/application-security-predictions-for-2023/?sh=3e72609070b6). 21.03.2023).***

***

«Согласно новому отчету исследователей кибербезопасности Mandiant, когда хакеры ищут уязвимости нулевого дня, чтобы использовать их и закрепиться на целевой конечной точке (открывается в новой вкладке), они обычно обращают внимание на продукты Microsoft, Google или Apple. основные уязвимости нулевого дня были использованы в прошлом году, в основном для «большой тройки».

Нулевые дни — это недостатки, которые еще не были обнаружены исследователями безопасности, поэтому у ИТ-команд было нулевой день, чтобы исправить свои системы. Таким образом, они являются самым ценным достоянием каждого хакера, поскольку злоупотребление ими не вызывает тревоги.

Из всех возможных продуктов, которые могли стать мишенью, мошенники сосредоточили свои увеличительные стекла на операционных системах, веб-браузерах и продуктах для управления сетью. В Windows было использовано 15 уязвимостей, в Chrome — девять, в iOS — пять. MacOS замыкает четверку лидеров с четырьмя эксплуатируемыми уязвимостями нулевого дня.

Разбивая результаты географически, Mandiant говорит, что большинство нулевых дней было использовано спонсируемыми государством китайскими злоумышленниками (7), за ними следуют русские (2 — одно перекрывается) и северокорейцы (2). Происхождение троих установить не удалось. Тринадцать были использованы группами кибершпионажа.

Обычно они искали уязвимости, которые позволяли бы им получить повышенные привилегии, или запускали удаленный код на уязвимых устройствах (53 уязвимости из 55).

Между периферийной инфраструктурой и облачными сервисами мошенники в основном интересовались первым, поскольку эти продукты обычно не имеют надлежащей защиты от кибербезопасности и с большей вероятностью могут быть скомпрометированы без предупреждения ИТ-команд. В то же время, по мере того, как все больше компаний переходят в облако, количество раскрытых нулевых дней

может сократиться, поскольку поставщики облачных услуг по-разному сообщают об инцидентах безопасности, утверждает Mandiant.

В любом случае, в 2022 году было обнаружено меньше уязвимостей нулевого дня (55) по сравнению с предыдущим годом (80), и, хотя это звучит позитивно, 2022 год стал рекордсменом по количеству активно эксплуатируемых нулевых дней. Исследователи считают, что в этом году эта тенденция будет только ухудшаться». ***(Sead Fadilpašić. Microsoft, Google and Apple zero-days were a huge security threat in 2022 // Future US, Inc. (https://www.techradar.com/news/microsoft-google-and-apple-zero-days-were-a-huge-security-threat-in-2022). 21.03.2023).***

***

«…Согласно новому отчету компании Synopsys, занимающейся безопасностью, по крайней мере 84% кодовых баз имеют хотя бы одну уязвимость с открытым исходным кодом, а 48% имеют уязвимости с высоким риском, которые имеют известные эксплойты или классифицируются как допускающие удаленное выполнение кода.

В отчете Synopsys об анализе безопасности и рисков с открытым исходным кодом за 2023 г. были обнаружены постоянные доказательства того, что по мере того, как использование открытого исходного кода продолжает расти, растет и количество этого кода, который является уязвимым или устаревшим. Данные получены в результате аудита слияний и поглощений 1481 базы кода на предмет уязвимости и соответствия (а также еще 222, которые были проверены только на соответствие) в 17 отраслях в 2022 году. Подавляющее большинство (96%) содержат код с открытым исходным кодом.

Примерно 91% кодовых баз, проанализированных на наличие уязвимостей, содержали устаревшие компоненты с открытым исходным кодом, то есть разработчики имели доступ к обновлениям или исправлениям, но не применяли их. Идентичный процент содержал код с открытым исходным кодом, который не разрабатывался в течение последних двух лет, что указывает на то, что разработчики, вероятно, прекратили техническое обслуживание.

Майк МакГуайр, старший менеджер по программным решениям в Synopsys, сказал IT Brew, что популярность открытого исходного кода резко возросла, потому что он позволяет разработчикам сосредоточиться на пользовательском коде и опередить конкурентов на рынке, но также возлагает на них бремя регулярного обслуживания, обновлений и исправлений…

Разработчики могут принять решение не обновлять старый код с открытым исходным кодом, потому что исправления могут повлиять на функциональность, сказал Макгуайр IT Brew, или потому что они решили, что определенные уязвимости не являются приоритетными для устранения (например, код, работающий в закрытых системах). Во многих случаях им просто не хватает информации о том, какие компоненты устарели или даже что вообще находится в их кодовых базах. Кодовые базы в отчете Synopsys за 2023 год содержали в среднем 595 компонентов с открытым исходным кодом, большинство из которых являются транзитивными зависимостями, необходимыми для выполнения более важных задач.

«Из этих 595 компонентов на приложение только несколько из них, может быть, несколько — 10, 20, 30, 100 абсолютных максимумов — были фактически выбраны для внедрения командами разработчиков», — сказал МакГуайр.

В отчете Synopsys также отмечается значительный прогресс в решении еще одной потенциальной проблемы с открытым исходным кодом: лицензировании. Приблизительно 54 % всех кодовых баз, проверенных в 2022 году, содержали открытый исходный код с конфликтами лицензий, по сравнению с 65 % в 2020 году. иск о нарушении авторских прав.

Наиболее распространенными проблемами лицензирования, обнаруженными Synopsys, были конфликты с Creative Commons Attribution ShareAlike 3.0 и 4.0, за которыми следовали конфликты с GNU Lesser General Public License и Apache License». ***(Tom McKay. Open-source vulnerabilities widespread in codebases, report finds // Morning Brew, Inc. (https://www.itbrew.com/stories/2023/03/20/open-source-vulnerabilities-widespread-in-codebases-report-finds?utm_source=&utm_medium=syndication&utm_campaign=feed). 20.03.2023).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«OryxAlign запустила securyXDR, полностью управляемую расширенную платформу обнаружения и реагирования (XDR). Усовершенствованная форма управления антивирусом и вредоносным ПО, система является частью решения, которое позволит справиться с ожидаемым ростом изощренных фишинговых атак с использованием ИИ. Это будет полезно для малых и средних предприятий или тех, у кого есть гибридная и удаленная рабочая сила, в различных секторах, включая финансовые услуги, подбор персонала, юриспруденцию и многое другое.

Традиционно антивирусные системы работали изолированно, ограничиваясь обнаружением и реагированием на угрозы на отдельных устройствах или конечных точках. Ранее решением было обнаружение и реагирование на конечные точки (EDR). С ростом гибридной и удаленной работы, а также опорой на сетевое хранилище и облачные рабочие процессы теперь возникла необходимость в мониторинге угроз во всей ИТ-экосистеме компании.

«В 2023 году мы ожидаем резкого роста числа изощренных фишинговых атак с использованием ИИ, а также атак на конечные точки удаленных и гибридных сотрудников. Преступники могут сместить фокус внимания на малые и средние предприятия, поскольку считается, что они имеют более слабую защиту», — объясняет Натан Чарльз, руководитель отдела по работе с клиентами. «Но

поскольку мы объединяем нашу платформу XDR с EDR и управлением электронной почтой, мы можем бороться огнем с огнем.

«securyXDR — это наша новая платформа XDR для кибербезопасности, которая предлагается как полностью управляемая услуга в партнерстве с аутсорсинговым операционным центром безопасности (SOC), в котором работает 200 сотрудников по всему миру», — продолжает Натан. «Учитывая, что даже небольшие сети могут генерировать десятки тысяч предупреждений о кибербезопасности в день, управляемая служба securyXDR снизит нагрузку на внутренние ИТ-отделы, освободив их от ручного сортирования и реагирования на отдельные угрозы и сосредоточив внимание на более продуктивных проектах.

«Мы знаем, что потеря производительности после кибератаки может быть столь же разрушительной, как и первоначальный ущерб вашей ИТ-системе. Затраты на наличие системы XDR более чем окупятся в долгосрочной перспективе благодаря раннему обнаружению угроз. Более того, SOC имеют уникальную возможность реагировать на угрозы, применяя обширный опыт большого количества атак в своих управляемых сетях».

OryxAlign заявляет, что securyXDR отличается от других корпоративных платформ XDR тем, что предлагает настраиваемые планы обслуживания, основанные на потребностях клиентов. Например, пользователи могут выбрать продолжительность хранения файлов журналов, чтобы минимизировать затраты на хранение, выбрать настраиваемые точки восстановления для скомпрометированных конечных точек и установить свой выбор срочности ответа, обычно от одного до трех часов». ***(Beatrice. New security platform to fight AI-based cyber attacks // dcnnmagazine.com (https://dcnnmagazine.com/security/oryxalign-security-platform/). 16.03.2023).***

***