**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 – 2024

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., 2024.– №3 (березень) . – 339 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

«Установи Міністерства охорони здоров'я пройдуть аудит з кібербезпеки.

Про це повідомляє Міністерство охорони здоров'я, передає Укрінформ.

«Під час війни Міністерство охорони здоров'я має підвищений рівень загрози кібератак та спроб втручання у свої інформаційні системи та бази даних, тому потребує посилених заходів із кібербезпеки. Програму підвищення рівня кібербезпеки державних структур України реалізовує Представництво Фонду цивільних досліджень та розвитку США (CRDF Clobal) у співпраці з Державним департаментом США. Вона включає аудити із кібербезпеки вибраних МОЗ установ, модернізацію та постачання обладнання та програмного забезпечення, тренінги із кібербезпеки та програми наставництва тощо», - йдеться у повідомленні.

Як зазначають в МОЗ, ці заходи посилять спроможність установ, що є бенефіціарами проєкту, у сфері кібербезпеки, створюючи стійкі та адаптивні процеси захисту систем та даних.

Зокрема, як повідомили у міністерстві, CRDF Global у співпраці з командою експертів Cyber Unit Technologies провела перший тренінг для IT-спеціалістів та державних службовців для підвищення обізнаності про численні кіберзагрози сьогодення та надання практичних навичок щодо реагування на наявні загрози.

Учасники тренінгу отримали спеціальні знання та навички для оцінки наявних систем і створення надійного захисту від кіберзагроз та практично відпрацювали умовні реалістичні сценарії втручання в інформаційні системи, таким чином підвищуючи загальний рівень кібербезпеки своїх установ…» ***(Установи МОЗ пройдуть аудит із кібербезпеки // Укрінформ (https://www.ukrinform.ua/rubric-health/3835031-ustanovi-moz-projdut-audit-iz-kiberbezpeki.html). 03.03.2024).***

***

«29 лютого відбулася конференція «Кібердіагностика критичної інфраструктури: посилення цифрового захисту». Мета події — обмінятися досвідом та ідеями, отриманими під час реалізації Програми діагностики стану кібербезпеки операторів критичної інфраструктури (ОКІ) від Проекту USAID Кібербезпека.

Програма розроблена на основі настанов NIST Cybersecurity Framework, які допомагають організаціям удосконалити цифровий захист. На сьогодні запущено 40 кібердіагностик та 20 організацій отримали перші результати.

«Зараз триває перша у світі кібервійна, і наша країна займає в ній активну позицію, задає напрям та знаходить нові способи протистояти загрозам. Українські організації мають бути максимально захищені від кібератак. Тож кібердіагностика — перший та найважливіший крок на цьому шляху. Крім того, тема кібербезпеки актуальна для всіх громадян. Це показують результати платформи Дія.Освіта — понад 600 000 українців вже отримали сертифікати про успішне завершення навчання з кібербезпеки», — сказала заступник Міністра цифрової трансформації з питань європейської інтеграції Валерія Іонан.

Нещодавно було створено Талліннський механізм, який посилить кіберпідтримку України в цивільній сфері. Його мета — узгодити потреби України з можливостями донорів так, щоб допомога іноземних країн становила єдине ціле. Тож кібердіагностики можуть стати одним із важливих інструментів для залучення підтримки. Оскільки за їхніми результатами організації-учасники матимуть дорожні карти для поліпшення стійкості до кіберзагроз.

«Кібербезпека критичної інфраструктури — це один із пріоритетів національної безпеки України. Ми постійно працюємо над тим, щоб удосконалювати систему кіберзахисту ОКІ, і діагностика стану кібербезпеки є одним із важливих інструментів у цій роботі», — заявив заступник Голови Державної служби спеціального зв’язку та захисту інформації Олександр Потій.

Під час конференції учасники ознайомилися з нормативно-правовими вимогами до проведення кібердіагностик та підходами до оцінки рівня кіберзахисту ОКІ. А також обмінялися досвідом реалізованих кібердіагностик.

У межах Програми діагностики стану кібербезпеки ОКІ кожна організація-учасник, зокрема:

- проходить первинну оцінку стану кібербезпеки відповідно до NIST Cybersecurity Framework;
- визначає цільовий стан кібербезпеки — до якого організація-учасник має рухатися;
- отримує рекомендації, які передбачають high-level design, специфікації технічної архітектури та операційні моделі кібербезпеки (політики, настанови тощо про те, як побудувати кібербезпекову політику в організації);
- розробляє дорожню карту впровадження рекомендацій від двох місяців з урахуванням необхідних ресурсів;
- впроваджує рекомендації протягом 2-4 місяців;
- проходить повторну оцінку кібербезпеки згідно з NIST Cybersecurity Framework після впровадження рекомендацій.

За результатами проведення кібердіагностик організації-учасники отримають комплексну оцінку цифрової захищеності. Після впровадження наданих їм рекомендації вони зможуть підвищити рівень кіберзрілості та готовності до кіберінцидентів». ***(Посилюємо цифровий захист: кібердіагностика критичної інфраструктури // Кабінет Міністрів України (https://www.kmu.gov.ua/news/posyliuiemo-tsyfrovyi-zakhyst-kiberdiahnostyka-krytychnoi-infrastruktury). 01.03.2024).***

***

«В Україні діятиме новий покращений проект з кібербезпеки BRAMA (БРАМА). Зауважують, що це — синергія громадян, приватного та державного секторів у протидії дезінформації та незаконному контенту в інформаційному просторі.

Цілі проекту:

знищення російських осередків в Інтернеті

зменшення рівня булінгу та цькування в мережі

протидія наркотикам та шахрайству

навчання та тренінги з кібергігієни

просвіта населення щодо інформаційної гігієни

залучення та мотивація громадян до активної громадянської позиції

Для блокування того чи іншого джерела необхідно надсилати скарги і чим більше буде скарг, тим більша вірогідність того, що джерело буде заблоковано. Саме із цією метою ми пропонуємо нашим користувачам стати частиною «BRAMA».

Що пропонують учасникам:

можливість повідомити про джерело неприйнятного контенту, для подальшого масового надсилання скарг спільнотою та подальшим блокуванням такого джерела;

допомогти заблокувати джерело неприйнятного контенту, шляхом долученості до масового надсилання скарг;

отримати поради щодо медіа та кіберграмотності;

бути поінформованим про небезпечні схеми шахрайств, які ширяться мережею;

бути обізнаним, щодо фейків, які просувають вороги у наш медіапростір.

Станом на січень 2024 року учасниками спільноти заблоковано понад 26 тисяч джерел поширення неприйнятного контенту». ***(В Україні діятиме новий покращений проект з кібербезпеки BRAMA (БРАМА) // ТОВ «ТРК "Ритм"» (https://itvmg.com/news/v-ukraini-diyatime-noviy-pokrashcheniy-proekt-z-kiberbezpeki-brama-brama-94223). 04.03.2024).***

***

Кібервійна проти України

«Кіберфахівці з Головного управління розвідки України успішно провели спеціальну кібероперацію проти Росії, завдяки якій отримали доступ до серверів Міністерства оборони РФ.

Про це повідомляє пресслужба ГУР.

В результаті, українські спецслужби тепер мають доступ до програмного забезпечення для захисту та шифрування даних, яке застосовувалося російським оборонним відомством, а також до значної кількості конфіденційної службової інформації Міністерства оборони Росії.

Ця інформація дозволяє встановити повну будову системи російського Міноборони та його ланок. ГУР отримало доступ до наказів, звітів, розпоряджень, доповідей та інших документів, які циркулювали між понад 2000 структурних одиниць відомства РФ.

Також у розпорядженні воєнної розвідки України опинилась службова документація заступника міністра оборони РФ — Іванова Тімура. У ГУР зазначили, що саме цей заступник Сергія Шойґу відіграв важливу роль у тому, що кібератака стала успішною.

Отримані дані допомогли ідентифікувати генералітет, багатьох високих керівників структурних підрозділів Міноборони, а ще заступників, помічників, спеціалістів. Тобто, всіх, хто користувався програмою, до якої отримали доступ в ГУР.

«Робота у кіберпросторі Росії, спрямована на перешкоджання й параліч діяльності відповідальних за війну проти українського народу силових органів та посадовців держави-агресора, триває. Далі — буде!», - зазначили в українській розвідці…» ***(Кіберфахівці ГУР зламали сайт Міноборони Росії // бізнес/медіа бюро ekonomika+ (https://delo.ua/telecom/kiberfaxivci-gur-zlamali-minoboroni-rosiyi-429740/). 04.03.2024).***

***

«Заява представника Ростелекому про те, що РФ веде кібервійну з ГУР МОУ, яке загрожує російським виборам, свідчить про неготовність російської електронної системи виборів до викликів і означає, що результати «виборів» будуть намальовані.

Як передає Укрінформ, про це в ефірі телемарафону «Єдині новини» заявив представник ГУР Андрій Юсов, коментуючи заяву глави Ростелекому про те, що Росія веде кібервійну з ГУР МОУ.

«Насамперед приємно і дякуємо за комплімент, звичайно, це висока оцінка фахівців Головного управління розвідки в сфері кібербезпеки і всіх тих українців, хто допомагає ГУР і українським спецслужбам, на цифровому фронті в тому числі. Але окрім того, це зізнання неспроможності. Звичайно, ні про які електронні системи виборів на Росії не може йти мови, там виборів немає. По суті, цією заявою вони визнали, що ще на одній ділянці до виборів не готові, і результати будуть просто намальовані», - зазначив Юсов…» ***(Ростелеком визнає кіберзагрозу з боку ГУР для електронної системи виборів РФ – Юсов // Укрінформ (https://www.ukrinform.ua/rubric-ato/3839886-rostelekom-viznae-kiberzagrozu-z-boku-gur-dla-elektronnoi-sistemi-viboriv-rf-usov.html). 14.03.2024).***

***

«Росія розвиває й масштабує цілу систему кіберагресії на національному рівні. До неї залучають студентів російських ЗВО.

Про це повідомив керівник департаменту кібербезпеки СБУ Ілля Вітюк в інтерв'ю для Forbes.

За інформацією Вітюка, у СБУ є документи, які свідчать про запровадження цілої системи масштабування кіберагресії на національному рівні рф, — щонайменше, вона існує з 2016 року. У межах державної ініціативи офіцери-резервісти ГРУ й ФСБ навчають студентів кібернаступальних дій у відповідних технічних чи військових вишах. Після навчання здібних студентів можуть брати на роботу в урядові розвідувальні органи чи до спецслужб.

Російських студентів під час навчання, наприклад, залучають до створення програмних засобів, вивчення систем логістики, енергетики та водопостачання різних країн та України, зокрема.

«У жодній іншій країні світу немає такого, щоб людей системно вчили бути хакерами. росія почала з вишів, із часом дійде й до шкіл», — пояснив Вітюк.

Керівник департаменту кібербезпеки ще сказав, що інвестиції в російські кібератаки сягають мільярди рублів. І сума продовжує зростати.

За словами Вітюка, за останні два роки великої війни СБУ вдалося зафіксувати й відбити 9 тис кібератак — по 4,5 тис за кожен рік відповідно…» ***(В СБУ заявили, що на росії студентів системно навчають хакерства // ТОВ «ІНФОРМАЦІЙНЕ АГЕНТСТВО «НЬЮЗ ФЛЕШ» (https://ua.news/ua/war-vs-rf/v-sbu-zayavili-shho-na-rosiyi-studentiv-sistemno-navchayut-hakerstva). 05.03.2024).***

***

«У грудні 2023 року «Київстар» зазнав масштабної кібератаки, наслідки якої відчували абоненти оператора впродовж кількох днів. Про деталі розслідування інциденту розповів начальник департаменту кібербезпеки СБУ Ілля Вітюк.

Вітюк пояснив виданню Forbes, що наразі ще триває розслідування, але відомо, що хакери запустили програму руйнування інфраструктури. Щоб дізнатись послідовність їхніх дій, потрібно все відновити, а це займає багато часу.

Він додав, що кіберфахівці вже знайшли програму Mimikatz, яка краде паролі. «Так хакери потихеньку пробиралися мережами і підвищувалися в правах». Але першу точку входу поки не встановили. Розглядаються, зокрема, варіанти фішингу, компрометації чи вразливості системи.

Також СБУ не відкидає версію наявності інсайдера в самому «Київстарі». Тому всі працівники, з акаунтів яких була активність або які причетні до кібербезпеки компанії, ходять на допити.

«Під час допиту ми можемо виявити, що сприяло кібератаці, а що її ускладнювало, встановити хронологію подій. Усе це потрібно підкріпити як технічними даними, подальшими експертизами, так і допитами», – пояснив Вітюк.

Самому ж оператору СБУ порадила запровадити поліграф і перевіряти людей із критичними доступами.

«Сьогодні є багато сервісів та підприємств, до яких можна звернутися. У випадку такої великої компанії, як “Київстар”, оператор може легко найняти

власного фахівця й організувати штатний поліграф», – додав головний кіберспеціаліст СБУ.

Також Вітюк розповів, що слідство не має зразка вірусу, яким скористалися хакери. За його словами, тут більш важливе не шкідливе ПЗ, а те, що хакери отримали максимальний рівень доступу.

Наразі слідство переконане, що в кібератаці брало участь угруповання Sandworm, однак ще триває робота над доведенням цього. Крім того, СБУ ще з'ясовує, які конкретно люди стоять за атакою». ***(В СБУ розповіли деталі розслідування кібератаки на «Київстар» // Internetua (https://internetua.com/v-sbu-rozpovili-detali-rozsliduvannya-kiberataki-na-kiyivstar-). 06.03.2024).***

***

«На тлі фейкових президентських виборів у РФ фахівці ГУР МОУ та активісти групи «BO Team» здійснили низку успішних кібератак на об'єкти країни-агресорки.

ГУР продовжує вести кібервійну проти Росії

За словами української розвідки, цього разі її ціллю були не лише російські державні, а й приватні структури, які сплачують податки та фінансують війну проти України.

Також ГУР поділилося результатами своєї роботи протягом тижня з 11 по 18 березня 2024 року:

- була здійснена атака на ресурси ПАТ «Ростєлєком» — успішно вдалося вивести з ладу комунікаційне обладнання забайкальського та красноярського краю РФ;
- кіберфахівці ГУР змогли отримати доступ до системи електронного документообігу уряду Бєлгородщини та здійснили фейкові розсилки 12 тисячам місцевих чиновників;
- атаковано та виведено з ладу комунікаційне обладнання ТОВ «Бєлзнак»;

- атаковано та знищено інформаційні ресурси «муніципального бюджетного учєрєждєнія старооскольского городского многоотраслєвого проізводствєнного об’єдінєнія комунального хозяйства»;
- відбулася атака та знищення інфраструктуру ЗАТ «Томмолоко»;
- захоплено та знищено серверну інфраструктуру разом з резервними копіями хостінг-провайдера «1Gb.ru» та десятків тисяч веб-сайтів, які він обслуговував;
- виведено з ладу понад 40 мережевих пристроїв Mikrotik в «центрє управлєнія городскім автоелєктротранспортом» у Новосибірську.

Згідно з даними українських розвідників, збитки, яких вдалося завдати ворогу, сягають сотень тисяч доларів.

Варто зазначити, що чи не наймасштабніші кібератаки фахівців української розвідки на країну-агресорку відбувалися саме під час «виборів» Путіна.

Під ударом опинилися 185 серверів, які належать 19 організаціям у Росії — усі вдалося знищити.

Насамперед йдеться про регіональних провайдерів Інтернету, телекомунікаційних операторів, онлайн-магазин, навчальні платформи, промислові виробничі компанії, житловий квартал тощо…». ***(Богдан Колісник. Кібервійна проти Росії. ГУР розкрило подробиці нових масштабних атак // online.ua (https://news.online.ua/kiberviina-proti-rosiyi-gur-rozkrilo-podrobici-novix-masstabnix-atak-875194/). 19.03.2024).***

***

«У Росії в день початку президентських виборів 15 березня фіксуються збої в онлайн-голосуванні. Це справа рук кіберфахівців Головного управління розвідки Міноборони України.

Про це повідомило джерело у спецслужбах в коментарі «Громадському».

«Інформація відповідає дійсності. Працюють кіберфахівці ГУР МО», — сказав наш співрозмовник.

Зранку та в обід 15 березня одразу в низці регіонів РФ заявили про збої. Зокрема, масштабний збій стався на державному порталі «Госуслуги». На сайт не могли зайти жителі Московської, Тюменської, Новосибірської та інших областей.

Напередодні, 14 березня, голова «ростелекому» Михайло Осеєвський заявив, що Росія веде кібервійну з ГУР МО України, «яке вже тривалий час намагається зруйнувати всю інфраструктуру, створену для виборів». ***(ГУР атакувало онлайн-голосування на виборах в РФ, – ЗМІ // Новинарня (https://novynarnia.com/2024/03/15/gur-atakuvalo-onlajn-golosuvannya-na-vyborah-v-rf-zmi/). 15.03.2024).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Генеральний прокурор України Андрій Костін зустрівся в Києві з колегами з Міністерства юстиції США Натаном Бруксом і Тімом Ранком, а також з радником з правових питань посольства США в Україні Джаредом Кімболом й аташе ФБР з правових питань Крісом Гейгером.

Як передає Укрінформ, про це повідомляє Офіс генерального прокурора.

Зокрема, сторони обговорили стратегії розслідування російських кіберзлочинів, скоєних проти Української держави та країн-партнерів.

За словами Костіна, «масштаби кібероперацій Росії проти України неухильно зростають. Зафіксовано понад 800 спроб кібератак на державні установи та сервіси. Серед них – об'єкти енергетичної інфраструктури, які постійно перебувають під прицілом ворога».

Генпрокурор поінформував, що ворог також проводить інформаційні операції з метою дестабілізації українського суспільства та атакує телекомунікаційні системи, щоб позбавити громадян доступу до мобільного зв’язку та інтернету.

Він зауважив, що ефективне та всебічне розслідування цих злочинів передбачає впровадження передових методів та практик, аби притягнути винних до відповідальності.

Також додав, що досвід та підтримка американських колег у цих питаннях були б дуже цінними.

Окрім цього, обговорили посилення співпраці у сфері захисту інтелектуальної власності та боротьби з організованою злочинністю в кіберпросторі.

«Ми рішуче налаштовані й надалі посилювати роботу у цих сферах та впроваджувати інноваційні методи розслідування, аби зробити кіберпростір безпечнішим та ефективно протидіяти будь-яким новим загрозам», – наголосив Костін». ***(Костін обговорив з американськими колегами розслідування російських кіберзлочинів // Укрінформ (https://www.ukrinform.ua/rubric-society/3841562-kostin-obgovoriv-z-amerikanskimi-kolegami-rozsliduvanna-rosijskih-kiberzlociniv.html). 18.03.2024).***

***

Світові тенденції в галузі кібербезпеки

«У сучасну цифрову епоху для цифрових захисників з'явилися нові можливості кар'єрного зростання. Враховуючи нахил успіху для супротивників, ці можливості продовжуватимуть зростати й окупатимуться з часом. Вони не залежать від примх загальної економіки чи бізнес-бюджетних тенденцій, і для тих, хто готовий присвятити своє життя захисту цифрових коридорів, якими ми всі проходимо, винагорода є відчутною та глибокою.

За всі ці варіанти кар'єри платять від 80 000 до 350 000 доларів – залежно від досвіду та геолокації. Як правило, чим більша компанія, тим вища оплата. Хороші етичні хакери та архітектори можуть отримувати вищі ставки в 2024 році, оскільки тенденція до нульової довіри та оцінки ризиків продовжується, тоді як аналітики SOC, криміналісти та спеціалісти з IR можуть помітити невелике зниження через вплив генеративного ШІ.

Етичний хакер

Етичні хакери — це сучасні мандрівні лицарі. Озброївшись своїм розумом і досвідом, вони вирушають у цифрову пустелю, щоб виявити вразливі місця. Ці хакери в білому капелюсі є першою лінією захисту, і вони використовують свої повноваження на благо. У їхньому арсеналі є сертифікати, такі як Certified Ethical Hacker або Offensive Security Certified Professional, які відзначають їх як майстрів своєї справи. На знак визнання їхньої неоціненної служби вони отримують щедру винагороду.

Реагування на інциденти та криміналістика

Після цифрових зломів спеціалісти з реагування на інциденти виступають у ролі кіберрозшуків. Вони заглиблюються в таємниці кіберінцидентів, збирають воєдино пазл про те, як стався злом, оцінюють збитки та організовують шлях до відновлення.

Їхній досвід у цифровій криміналістиці робить їх незамінними в боротьбі з кіберзлочинністю, а їхнє глибоке розуміння кіберландшафту дозволяє їм передбачати майбутні загрози та протидіяти їм. Їх спеціальні знання викликають високу повагу та винагороду.

Архітектура та інженерія безпеки

Архітектори та інженери безпеки є майстрами будівництва цифрового світу. Вони розробляють проекти безпечних цифрових середовищ і гарантують, що кожен компонент – від коду до мережі – створений таким чином, щоб протистояти натиску кіберзагроз.

Їхня робота є основою безпеки цифрових інфраструктур, а їхні стратегічні проекти забезпечують цілісність і стійкість систем, на які ми покладаємося. Їхній досвід дуже цінується, а їх зарплата відповідає значущості їх внеску.

Аналітики SOC

Зростаюча витонченість кіберзагроз підвищила попит на аналітиків SOC – пильних охоронців, чиї очі прикуті до горизонту, шукаючи ознаки цифрових вторгнень. Озброєні складними інструментами, вони стежать за життєвою силою

мереж, готові миттєво реагувати на будь-яку загрозу, яка наважиться зламати цифрові ворота, а їхні зарплати відображають їхню пильність.

Управління ризиками та комплаєнс

Експерти з управління ризиками та відповідності захищають організації від кіберзагроз. Вони стратеги, які орієнтуються в лабіринті правил і потенційних вразливостей, щоб зміцнити захист від невидимих ворогів.

Їхній досвід не лише у захисті цифрових активів, але й у забезпеченні дотримання нормативних вимог робить їх безцінними, і їхні зарплати відповідають цьому факту.

Інженери безпеки додатків

В основі кожного додатка лежить робота інженерів із захисту додатків, тихих носіїв щита, які вбудовують безпеку в ДНК програмного забезпечення. Вони працюють у тіні, співпрацюючи з розробниками, щоб надати програмам захист, який є таким же непохитним, як і непомітним. Вони є останнім оплотом проти вторгнення, а їхня пильність і досвід приносять їм високу зарплату.

Герої кібербезпеки

Оскільки наше життя все більше переплітається з цифровим, спеціалісти з кібербезпеки постають героями, які ведуть невпинні битви в тихому просторі між бітами та байтами. Їхні перемоги рідко відзначають, але їхні невдачі широко висвітлюються. Винагорода від кар'єри фахівця з кібербезпеки виходить за межі високої винагороди. Це охоронці нашого цифрового майбутнього – чемпіони невидимої, але невід'ємної частини нашого повсякденного життя». ***(Steve King. What Are the Highest-Paying Cybersecurity Specialties? // Information Security Media Group, Corp. (https://www.databreachtoday.com/blogs/what-are-highest-paying-cybersecurity-specialties-p-3573?utm_source=flipboard&utm_content=other). 06.03.2024).***

***

«За оцінками, жінки займають лише одну чверть робочих місць у сфері кібербезпеки у всьому світі, і цей відсоток ще нижчий на керівних посадах

вищого рівня. Гендерний розрив помітний у приміщеннях, де розробляються кіберзакони та політика, відбувається дипломатія та розвиваються дослідження. Доступ до Інтернету та пов'язаних з ним цифрових технологій і їх використання є дуже гендерним фактором; Міжнародний союз телекомунікацій (МСЕ) повідомляє, що хоча жінки становлять приблизно половину світового населення, вони становлять непропорційно велику (і зростаючу) частку глобального офлайн-населення. За даними ITU, у 2023 році жінок було більше, ніж чоловіків, які не користуються ними, на 17 відсотків, порівняно з 11 відсотками у 2019 році. Розбіжність у значущому доступі також є функцією інших пересічних факторів, таких як місце розташування, економічна влада, вік, стать, расове або етнічне походження, соціальні та культурні норми та освіта, серед іншого. Ці фактори також відіграють важливу роль у здатності жінок розвивати цифрову грамотність, а також отримати доступ до галузей освіти, які підходять для кар'єри, пов'язаної з кібербезпекою.

Жінки, чоловіки та люди різної статі використовують Інтернет і цифрові технології по-різному. Дещо з цього є позитивним і навіть трансформуючим; Інтернет-платформи можна використовувати для особистого самовираження, політичної організації, освіти та побудови спільноти. Однак паралельно технологія поширює насильство та домагання, які вже зазнали жінки та маргіналізовані особи, в онлайн-простір і проявляється новими способами – обмін зображеннями без згоди, переслідування, тролінг, наклеп і доксінг тощо. Більше того, вибух генеративного штучного інтелекту (ШІ) у мейнстрім загострює гендерні та расові упередження та ще більше розпалює технологічне насильство за статтю. Якщо кіберзакони та політика мають бути ефективними у вирішенні цих вразливостей і практики експлуатації, тоді вони повинні враховувати різні уявлення про безпеку на основі життєвого досвіду.

Технологію іноді називають палкою з двома кінцями щодо статі: вона може відігравати ключову роль у з'єднанні людей і бути рушієм змін, прискорюючи доступ до можливостей. Проте надто часто його використовують проти жінок і

маргіналізованих осіб чи спільнот таким чином, що підриває зусилля щодо досягнення рівності.

Існуюча нерівність і гендерне насильство відтворюється в Інтернеті з руйнівними наслідками. Швидкість і масштаби, з якими інформація може поширюватися в Інтернеті, відрізняють його від інших видів фізичного насильства. Шкідливий вміст важче усунути, і його можна швидко та неодноразово поширювати, спричиняючи повторне жорстоке поводження та повторно травмуючи тих, хто пережив. Механізми правосуддя можуть бути повільними або відсутніми, оскільки правові системи та системи управління прагнуть наздогнати поширення нових технологій і платформ, таких як ШІ. Крім того, цифрове насильство часто сприймається не так серйозно, як фізичне, незважаючи на докази того, що воно може переходити в автономний режим і проявлятися через стеження, переслідування, примусовий контроль або фізичне насильство.

Шкода, завдана цифровим насильством, також впливає на участь жінок у суспільному житті. Для політиків, журналістів або правозахисників онлайн-середовище дозріло для маніпулювання особистою інформацією чи інтимними зображеннями (справжніми чи підробленими), щоб підірвати їхній вплив і стримати їх від участі в суспільному житті. Навіть для жінок, які не беруть активної участі в суспільному житті, непропорційні рівні насильства можуть утримувати їх від участі в Інтернеті, сприяючи зростанню цифрового розриву.

В епоху феміністської зовнішньої політики та широкого прагнення до досягнення гендерної рівності зростає підтримка включення гендерної точки зору в кібербезпеку на багатосторонньому рівні. Наприклад, на переговорах ООН з питань міжнародної кібербезпеки все частіше розглядається питання про те, як включити гендерні аспекти в аналіз кіберзагроз, механізми зміцнення довіри та нарощування потенціалу. Програма стипендій «Жінки в кібернетичному просторі» дозволяє жінкам-посадовцям на початку та середньому етапі кар’єри брати участь у сесіях поточної робочої групи ООН з міжнародних питань кібернетики. Стипендія стала важливим механізмом підтримки однолітків для жінок, які працюють у

кібердипломатії чи урядових групах реагування на комп'ютерні надзвичайні ситуації (CERT), а також сприяє різноманітності кіберпереговорів ООН.

Проте розширена участь також може бути палкою з двома кінцями. Коли в кімнаті, де домінують чоловіки, лише кілька жінок, часто припускають, що жінки порушуватимуть питання, пов'язані з жінками чи статтю. Подібні очікування часто поширюються на інших маргіналізованих осіб, які недостатньо представлені та мають різний пересічний досвід. Це накладає значний тягар у цих умовах на тих, хто в меншості, який, можливо, вже відчуває тиск через підвищені очікування та занепокоєння щодо сприйняття того, що їхня участь є лише «символом».

Звичайно, є умови, де різноманітність і обмін набутим досвідом є невід'ємною частиною розвитку ефективної політики. Збільшення критичної маси різних жінок, які беруть участь в організаціях з кібербезпеки та переговорах, сприятиме цим зусиллям. Однак не слід очікувати, що жінки та інші маргіналізовані особи будуть нести цю додаткову вагу самостійно. Ось чому уряди повинні продовжувати не лише інтегрувати гендерні аспекти у свою національну політику кібербезпеки, але й запроваджувати механізми підзвітності для підтримки значущої участі жінок і забезпечення гендерної чутливості як частини національної політики та програм.

Таким чином, «гендерна проблема» в кібербезпеці полягає не лише в розбіжностях у участі та диференційованих загрозах, а й у розв'язанні додаткового тягаря, який покладено на жінок і гендерні меншини, щоб бути нашими власними чемпіонами. Гендерне розмаїття стосується не лише жінок, і обов'язок усунення нерівності не повинен лягати виключно на жінок чи інші маргіналізовані групи. Для цього потрібно залучити всіх і визнати, що кібербезпека є спільною відповідальністю, яка має трансформаційний потенціал для зміцнення гендерної рівності та нашої безпеки, якщо підходити до неї всеосяжно». ***(Allison Pytlak, Lisa Sharland. Narrowing the Gender Gap in Cyber Security // Henry L. Stimson Center (https://www.stimson.org/2024/narrowing-the-gender-gap-in-cyber-security/). 08.03.2024).***

***

«У складному глобальному ландшафті ризиків, що постійно розвивається, кіберзлочинність і кібернезахищеність стали актуальними проблемами для бізнес-лідерів у всьому світі — як у найближчому майбутньому, так і в довгостроковій перспективі.

Відповідно до Звіту про глобальні ризики за 2024 рік, створеного Всесвітнім економічним форумом (ВЕФ) у співпраці з Маршем Макленнаном та іншими партнерами, керівники компаній оцінили кібернебезпеку як четвертий за значимістю ризик у найближчі роки та восьмий у наступному десятилітті. Для менеджерів з управління ризиками у Великій Британії резонансні атаки програм-вимагачів підштовхнули дискусію навколо кіберзлочинності до центру уваги.

Революційні досягнення, такі як штучний інтелект (ШІ), створюють нові загрози, особливо тому, що швидке прискорення та інтеграція цих технологій може наражати бізнес на непередбачену цифрову вразливість. Так само інновації, пов’язані зі штучним інтелектом, можуть виявитися важливими для боротьби з кіберзагрозами. Постає питання: як знайти баланс між використанням найкращих аспектів інновацій, захистом вашої організації від кіберризиків і підвищенням стійкості?

Обізнаність про переваги та ризики ШІ є обов’язковою

Поява штучного інтелекту відкрила для компаній потенційно трансформаційні можливості для підвищення ефективності, покращення процесу прийняття рішень і посилення стратегії кібербезпеки. Однією з важливих можливостей є можливість комп’ютерів ефективно виявляти та фільтрувати фішингові шахрайства з електронної пошти, зменшуючи ризик атак зловмисного програмного забезпечення.

Проте штучний інтелект також може мати шкідливий вплив на кібербезпеку компанії — від поширення дезінформації до використання вразливостей у цифрових мережах. Незважаючи на те, що компанії продовжують використовувати переваги штучного інтелекту, важливо, щоб співробітники були навчені тому, як

ефективно використовувати цю технологію, і були навчені розуміти притаманні ризики, які впливають на кібербезпеку.

Технології повинні збільшувати людський інтелект, а не замінювати його

Оскільки компанії продовжують використовувати нові технології, посилюючи свій підхід до кіберризиків, важливо розглянути, як штучний інтелект та інші інструменти можуть підтримувати прийняття рішень і вирішення проблем людьми, а не замінювати людські судження та досвід.

Наприклад, у моделях глибокого навчання, якщо правила, встановлені для алгоритмів ШІ, або набори даних, з яких він навчається, є неточними, відповіді також будуть такими. Люди потрібні для забезпечення достатньої якості, різноманітності та масштабу наданих даних, а також для перевірки результатів. Люди також можуть вирішувати потенційні упередження та етичні міркування, зрештою покращуючи продуктивність і надійність моделі.

Управління кіберризиками вимагає участі всієї компанії

Кіберризик — це стратегічна проблема для всієї компанії, яка впливає на всі куточки бізнесу. Зараз, як ніколи, проактивне планування має вирішальне значення для реагування на кібератаку та відновлення після неї. Однак дієвість і дієвість плану реагування на інцидент залежить від готовності та залученості залучених людей.

З цієї причини дуже важливо, щоб компанії мали надійні принципи впровадження, використання та оновлення технологій. Це включає в себе впровадження належних методів тестування, навчання, моніторингу та аудиту вздовж ланцюжка командування, починаючи з старшого персоналу та фільтруючи до кожного працівника. Це також може допомогти забезпечити відповідність місцевим і глобальним нормам, що стосуються того, як розробляються та використовуються технології. Регулярне тестування процедур і повторна оцінка процесів є важливою частиною цього контролю.

Проактивно реагуйте на кібернебезпеки

Інновації створюють можливості — як у тому, як компанії впроваджують нові технології, так і переглядають своє управління кіберризиками.

Як визнали бізнес-лідери з усього світу у Звіті про глобальні ризики 2024, кіберризики нікуди не зникнуть, а суб'єкти загроз лише знаходять більш витончені способи обійти заходи з кібербезпеки бізнесу. Щоб підвищити рівень готовності, організації повинні враховувати як переваги, так і ризики, пов'язані з новими інструментами, такими як штучний інтелект, забезпечити належну підготовку персоналу для використання та перевірки цих інструментів, а також створити єдину систему реагування в рамках всієї компанії». ***(Kelly Butler. Developments in AI provide innovative response to cyber risks // Marsh (https://www.marsh.com/uk/services/cyber-risk/insights/developments-in-ai-provide-innovative-response-to-cyber-risks.html). 05.03.2024).***

***

«Морська галузь є унікальною в багатьох відношеннях, але її залежність від ІТ-інфраструктури та телекомунікацій робить її так само вразливою до кібератак, як і будь-яку іншу галузь. У цій статті, яка є нашою першою в серії з трьох, присвячених морській кібербезпеці, ми описуємо загрози для галузі та доступні наразі вказівки, щоб допомогти компаніям реагувати на ці загрози.

Кіберризик тут, щоб залишитися...

Відповідно до останнього барометра ризиків від Allianz, кіберризики були бізнес-ризиками номер один у всіх галузях у всьому світі в 2024 році. Другим було порушення ланцюга поставок. Оскільки морський сектор відіграє ключову роль у глобальних ланцюжках поставок, легко зрозуміти, наскільки важливою є кіберстійкість як для судновласників, так і для їхніх клієнтів.

У 2023 році морська галузь стала жертвою кількох кібератак: порти в Австралії та Японії призупинили роботу через порушення кібербезпеки. Постачальники програмного забезпечення не були застраховані: платформа ShipManager DNV була тимчасово відключена через кібератаку, а кілька верфей і поромних переправ у Європі також, як повідомляється, постраждали від програм-вимагачів і DDoS.

З більшим рівнем автоматизованого обміну інформацією, більшим зв’язком на морі завдяки застосуванню LEO технологія супутникового зв’язку та широке використання Інтернету речей, поверхні атаки зростає, оскільки галузь стає все більш цифровою. Цифровізація може принести значні переваги з точки зору ефективності, безпеки та видимості, але також має потенціал для збільшення кількості вразливостей в IT- та OT-інфраструктурі судна та його компанії-оператора, надаючи суб’єктам загрози більше можливостей для отримання несанкціонованого доступу. Ймовірно, це прискориться, оскільки автономні судна продовжуватимуть розвиватися.

Хоча ця стаття присвячена навмисним кібератакам з боку зовнішніх зловмисників, важливо зазначити, що транспортування також стикається з ненавмисними внутрішніми загрозами від використання застарілих систем, старіння та поганої кібергігієни. Наприклад, багато систем OT працюють на програмному забезпеченні, для якого недоступні виправлення та оновлення для уразливостей або покращень. Крім того, програмне забезпечення може вийти з ладу через помилки та помилки користувача, або постачальники програмного забезпечення можуть припинити роботу, залишивши системи без підтримки. Ці загрози також необхідно враховувати при розробці ефективної системи управління ризиками кібербезпеки.

…а кіберзломи коштують дорого

Результати різних опитувань 2023 року вказують на те, що середня вартість кіберзлому для учасників судноплавної галузі становить багато сотень тисяч доларів, а середній викуп, сплачений кіберзлочинцям, становить кілька мільйонів доларів.

Крім цих значних первинних витрат, це витрати на перерву в бізнесі, витрати на захист претензій щодо фізичної втрати швидкопсувних вантажів, затриманих нападом, можливі фізичні втрати або пошкодження суден або їх обладнання, претензії, що виникають через забруднення або зіткнення, спричинені скомпрометованими бортовими системами. потенційні штрафи від регуляторів у

разі втрати або витоку конфіденційних персональних даних, а також витрати, пов’язані з порушенням договірних гарантій щодо кібербезпеки.

І останнє, але не менш важливе – це нефінансові витрати від кіберзлому, які можуть включати шкоду репутації та втрату комерційно конфіденційної інформації чи комерційної таємниці.

Обмежена обов'язкова нормативна база

ІМО ще не впоралася з морськими кіберризиками за допомогою комплексного обов’язкового кодексу. Натомість у 2017 році він видав рекомендації високого рівня. Ці рекомендації визначають морський кіберризик як:

«міра, до якої технологічний актив знаходиться під загрозою через потенційну обставину або подію, яка може призвести до пов’язаних з транспортуванням оперативних збоїв, збоїв у безпеці чи безпеці внаслідок пошкодження, втрати або зламу інформації чи систем».

Рекомендації встановлюють п’ять основних функціональних елементів управління кіберризиками, а саме: виявлення, захист, виявлення, реагування та відновлення.

У 2017 році ІМО також погодилася, що управління морськими кіберризиками має бути включено до систем управління безпекою, і що кіберризиками слід керувати відповідно до вимог Кодексу ISM. Отже, кіберризики необхідно оцінювати та керувати ними з такою ж увагою, як і фізичні ризики для суден, включаючи планування регулярного технічного обслуговування програмного забезпечення та активів ОТ так само, як і для фізичного обладнання судна.

ІМО продовжує сприяти більшій цифровізації в галузі через такі ініціативи, як дозвіл на використання електронних BDN та останні поправки до Конвенції FAL, які з 1 січня 2024 року передбачають використання морських єдиних вікон для електронного обміну даними між суднами та портами. Це поряд із його поточною роботою щодо розробки коду для морських автономних надводних кораблів (MASS). Чи буде це йти рука об руку з новим обов’язковим кодексом морської кібербезпеки, ще належить побачити, хоча кібербезпека була визначена як одна з потенційних прогалин у існуючих правилах.

У Великій Британії оператори великих суден можуть підпадати під дію Регламенту NIS 2018, якщо вони відповідають порогу, щоб кваліфікуватися як оператор основних послуг. Це означало б, що судновласник повинен відповідати мінімальним стандартам кібербезпеки та вимогам звітності про інциденти зі значним впливом.

Добровільне керівництво галузі

За відсутності будь-якого обов'язкового кодексу було розроблено кілька добровільних галузевих інструкцій, які містять вказівки щодо використання управління кіберризиками для зменшення як ймовірності, так і впливу атаки.

BIMCO, ICS та кілька інших галузевих організацій спільно розробили «Керівні принципи кібербезпеки на борту суден», які вже вийшли 4 тис видання. Це забезпечує підхід до кібербезпеки, що ґрунтується на оцінці ризику, відповідно до Кодексу ISM, і містить рекомендації щодо технічних і процедурних заходів, які судновласники можуть вжити для управління кіберризиками.

Рекомендації BIMCO були розроблені з посиланням на Концепцію кібербезпеки Національного інституту стандартів і технологій США (NIST), яка надає засновану на результатах методологію для розуміння, оцінки, визначення пріоритетів і передачі інформації про ризики кібербезпеки. NIST Framework щойно оновлено, версія 2 випущена наприкінці лютого 2024 року. Версія 2 включає нову шосту функціональну категорію управління, підкреслюючи необхідність включення кібербезпеки в загальну стратегію управління ризиками компанії та моніторингу за допомогою керівників вищої ланки так само, як фінансові та інші ризики.

Зосередження уваги на кіберуправлінні повторюється у Великій Британії, де уряд щойно опублікував заклик подати свої думки щодо запропонованого Кодексу практики кіберуправління. Проект Кодексу було опубліковано на тлі зниження зацікавленості правління кіберризиками та визнання того, що хоча кібернетичність є «основним ризиком» для більшості організацій, ключові особи, які приймають рішення, часто не є керівниками. Таким чином, проект Кодексу визначає очікування директорів щодо управління кіберризиками, включаючи «забезпечення

того, щоб кіберризики розглядалися як частину ширшої діяльності організації з управління ризиками підприємства та внутрішнього контролю, а також встановлення відповідальності за ризики з відповідними старшими керівниками за межами CISO». Для судновласників і менеджерів це означає забезпечення того, щоб кібербезпека не була лише справою IT-відділу чи ОГС, а контролювалася зверху вниз і була невід'ємною частиною культури компанії, її екіпажу та флоту.

Уряд Великобританії також опублікував свій «Практичний кодекс кібербезпеки для суден», останнє видання якого було опубліковано в липні 2023 року. Метою Кодексу є допомога організаціям у створенні оцінок кібербезпеки та планів кібербезпеки, як додатків до плана охорони судна, який вимагається згідно з Кодексом ISPS.

Міжнародна організація стандартів (ISO) також має спеціальні стандарти, спрямовані на морські технології та кібербезпеку на борту суден, а також загальні стандарти управління інформацією та безпеки, які можна застосовувати до берегових операцій.

Таким чином, не бракує структур, інструкцій і кодексів, які допоможуть судновласникам сформулювати стратегію кібербезпеки. Однак створення стратегії кібербезпеки – це лише перший крок; Щоб бути ефективною, стратегія має бути належним чином реалізована на всіх рівнях бізнесу та підтримуватися необхідним навчанням команди та тренуваннями. Його також необхідно регулярно переглядати та оновлювати перед обличчям нових і нових ризиків, а також щоразу, коли нова технологія (включаючи як програмне, так і апаратне забезпечення) додається на судно чи берег.

Гарантія якості

Рекомендації BIMCO не передбачають зовнішньої перевірки підходу судна чи компанії до управління кіберризиками. Однак, оскільки управління кіберризиками тепер вважається частиною SMS судна, яке саме повинно пройти перевірку для видачі необхідного документа про відповідність, принаймні ті елементи управління ризиками, які включені в SMS, підлягатимуть під зовнішній

нагляд з боку держави прапора. Крім того, для новобудов майбутні правила IACS (див. нижче) також призведуть до збільшення зовнішнього нагляду за класами.

Також можна очікувати більш суворого підходу від перевірок PSC, принаймні в портах Європи. Наприкінці 2023 року Європейське агентство з безпеки на морі опублікувало «Інструкції щодо забезпечення кібербезпеки на борту суден під час… інспекцій» з акцентом на обов'язкових елементах, які необхідно включити в оцінку безпеки судна та план безпеки судна, а також контрольний список для інспекторів. щодо кібергігієни на борту.

Кібербезпека від кіля догори

Наприкінці 2023 року IACS опублікував переглянуті уніфіковані вимоги E26 і E27, які мають застосовуватися класовими товариствами-членами до всіх новобудов, укладених на будівництво 1 липня 2024 року або після цієї дати. Вони окреслюють мінімальні кроки, які повинні бути виконані різними зацікавленими сторонами під час проектування, будівництво та експлуатація корабля для забезпечення його кібернетостійкості проти поточних і майбутніх загроз.

Ці UR визнають, що для ефективного управління кіберризиками на борту суден потрібен інтегрований підхід, який гарантує, що розрізнені системи, встановлені на борту, які, ймовірно, надходять від різних OEM-виробників і мають різні стандарти даних, протоколи та механізми безпеки, повинні розглядатися як «колективні». entity" починаючи з проекту корабля і далі.

Як і в інших згаданих вище структурах, ключові вимоги до кіберстійкості згруповані в п'ять функціональних категорій: ідентифікація, захист, виявлення, реагування, відновлення. Вимоги охоплюють усе: від інвентаризації активів суден (ідентифікація), до сегрегації мережі (захист) і моніторингу (виявлення), до планів реагування на інциденти (реагування, відновлення) і встановлення систем моніторингу, здатних виявляти та досліджувати аномалії (виявляти, реагувати, одужати).

Для судновласників та їхніх менеджерів вимоги вплинуть на те, що вони повинні показати, щоб пройти кожну щорічну та спеціальну перевірку, а також на те, які договірні умови необхідно узгодити з постачальниками для таких речей, як

підтвердження того, що виправлення безпеки та оновлення програмного забезпечення були протестовані. [6]. Судновласники та менеджери також повинні будуть створити затверджену класом «програму кібербезпеки та стійкості суден», документуючи, як вони виконали вимоги. Хоча багато з цього вже може бути включено до SMS, оцінки безпеки судна та плану, а також оцінки та плану кібербезпеки, якщо вони складаються окремо, це потрібно буде ретельно перевірити на відповідність вимогам IACS, щоб переконатися, що всі аспекти охоплено.

Договірний захист

Успішні операції з доставки вимагають взаємозв'язку між багатьма зацікавленими сторонами в різних цифрових і фізичних середовищах. Ця взаємозалежність від третіх сторін і швидкий потік інформації створюють ще один рівень уразливості кіберзахисту бізнесу. Контрагент зі слабким кіберконтролем може надати точку доступу до добре захищеного судна або власника.

Тому для судновласників важливо враховувати кібербезпеку третіх сторін, з якими вони взаємодіють, на додаток до своєї власної кібербезпеки, і, за необхідності, накладати гарантії кібербезпеки в контракти, які вони укладають із третіми сторонами.

Наприклад, у чартерні договори слід включити положення для забезпечення мінімальних стандартів кібербезпеки та обміну інформацією щодо інцидентів. Дивіться, наприклад, положення про кібербезпеку BIMCO, яке вимагає від сторін повідомляти, коли стався інцидент. Цей обмін інформацією про інциденти особливо важливий, оскільки на сьогоднішній день не існує уніфікованої системи звітності через IMO або інший глобальний галузевий орган, який міг би допомогти забезпечити завчасне попередження про загрози для галузі.

Рекомендації BIMCO підкреслюють особливі ризики, пов'язані зі зв'язками з місцевими агентами, де регулярно обмінюються конфіденційними комерційними та фінансовими даними. Для таких типів відносин власники можуть забажати встановити мінімальний набір вимог щодо кібербезпеки, які повинні прийняти всі

постачальники, так само, як і кодекс поведінки щодо боротьби з хабарництвом або санкцій.

Морське кіберстрахування

Впроваджуючи стратегію управління кіберризиками, судновласники повинні розглянути, яке страхове покриття вони вже мають і чи достатньо цього для реагування на всі можливі збитки, які можуть виникнути в результаті кібератаки. Багато стандартних морських полісів прямо виключають кіберзбитки або не розроблені для покриття всіх типів збитків, які можуть виникнути, наприклад переривання бізнесу та втрата даних.

Власники також повинні бути готові пояснити будь-яким потенційним страховикам, які кроки вони вжили для відповідального управління кіберризиками, а у разі порушення — як ці кроки допомогли їм зменшити та управляти збитками.

Морська кіберстійкість

Отже, що потрібно, щоб судно або компанія-власник/оператор судна були кіберстійкими? Це виглядатиме по-різному для кожного підприємства, флоту та корабля. Однак загальні елементи включають:

Ефективне управління зі спонсорською підтримкою керівників і зміцнення кібербезпеки як пріоритет на всіх рівнях бізнесу шляхом регулярних тренінгів.

Ретельна та детальна оцінка та розуміння кіберризиків компанії, яка здійснюється у партнерстві із зовнішніми технічними експертами та постачальниками апаратного та програмного забезпечення та яка регулярно переглядається та оновлюється.

Ефективні процедури реагування на надзвичайні ситуації, які знайомі всьому береговому персоналу та екіпажу.

Надійна політика безперервності бізнесу та на випадок непередбачених ситуацій, щоб звести до мінімуму збої в роботі.

Висновки

Морський кіберризик неможливо усунути, але ним можна належним чином керувати. Універсального, обов’язкового стандарту морської кібербезпеки не існує, але є кілька галузевих стандартів, на які компанії можуть покладатися. Ці

стандарти слід використовувати як відправну точку для розробки індивідуальної стратегії управління кіберризиками, яка враховує конкретні загрози, вразливі місця та ризики для вашої компанії та флоту». ***(Joanne Waters. An Introduction to Maritime Cyber Security for Ships // DAC Beachcroft (https://www.dacbeachcroft.com/en/What-we-think/An-introduction-to-maritime-cyber-security-for-ships). 11.03.2024).***

***

«Коли ми думаємо про кібербезпеку, «вразливість» у більшості сенсів зазвичай викликає занепокоєння. Ми шукаємо їх, щоб виправити та створити потужний захист, щоб зменшити їхні ризики. Особливо вражає те, що кібербезпека та мова, що її оточує, пов'язані з міцністю та стійкістю. Ця мова та її відчуття абсолютної сили також, здається, поширюються на персонал, який проводить свої дні, захищаючи організації від загроз.

Вразливість для бізнесу

Окрім просто мілітаристської та гіпермаскулінної мови, є також сильний елемент чуттєвості плаща та кинджала. Мій друг у галузі, керівник відділу кібербезпеки в рейтингу FTSE 100, проникливо вказав на це, назвавши це «культурою схожого на Джеймса Бонда», і це мені запам'яталося. Секретність навколо цієї професії шкодить нам. Нам потрібна певна вразливість.

Вразливість: «Бажання виявляти емоції або дозволяти бачити або знати свої слабкості».

Я говорю про емоційну відкритість і готовність співпрацювати та просити про допомогу. У цьому сенсі вразливість полягає в усвідомленні того, що настав час застосувати «менш мачо» підхід до кібербезпеки.

Зокрема, нам потрібен новий підхід до того, як фахівці з кібербезпеки консультують організації щодо захисту від кіберзагроз. Підприємства повинні бути більш відкритими щодо того, коли вони вразливі до атак, що часто починається з визнання того, що вони будуть атаковані.

Коли щось йде не так, потрібно брати на себе відповідальність, але без вказівки пальців. Супротивники стають все більш досвідченими, а інструменти злому тепер легко придбати для менш досвідчених. Це означає, що загрози, від яких захищаються захисники, є більш частими та складнішими, ніж будь-коли.

Ми повинні відійти від культури звинувачення до культури більшої відкритості щодо вразливості та розкриття порушень. Для цього знадобиться співпраця між галузями, спільне використання інформації та проблем. Бути більш відкритим і вразливим щодо вразливостей — це найкращий і найпростіший спосіб бути на крок попереду кіберзлочинців. Але ця зміна має відбуватися зверху.

Забагато мачизму

Справжньою основною проблемою тут є існуюча культура. Кібербезпека має проблему мачизму. Будь-хто, хто не був у цій галузі, миттєво впізнав би це, але для багатьох, хто працював у цій сфері роками, це може стати шоком. Ми маємо зробити краще з багатьох причин, але, мабуть, найголовніше те, що ця культура мачо робить нас менш безпечними.

За визначенням «мачизм» і маркетинговим іміджем, який просуває образи захисників і опухлих супергероїв, ми підкріплюємо цей образ мачо професіоналів з кібербезпеки. Ми захисники, які борються проти нападників і ворогів.

Якщо вам цікаво, чому важко залучити жінок на посади з кібербезпеки у вашій організації, почніть із вивчення мови вашої компанії, вашої маркетингової копії та опису ролі. Якби ви перевірили їх за допомогою інструменту мовного аналізу, ви, ймовірно, виявили б сильне чоловіче упередження. Нам потрібно краще розпізнавати несвідомі упередження та вживати заходів для усунення впливу цих упереджень.

Справа, звісно, набагато глибша за мову. Це симптоми ширшої моделі поведінки, яка робить роботу в сфері кібербезпеки часто негостинним місцем для жінок (а також для інших недостатньо представлених груп). У цьому випадку ми говоримо про явні та приховані переслідування та сексизм, які тривають досі.

Нам потрібно оновити нашу мову, тому що це те, що розповідає світу про нашу компанію та наші цінності. Але нам також потрібно звернути увагу на

пов’язану з цим культуру, яка цінує сильні чоловічі голоси над іншими та посилює цю цінність через сексистську поведінку. Жінок, які пройшли через процес вступу до спільноти кібербезпеки, зустрічає культура, яка змушує їх почуватися ще більше маргіналізованими. Не дивно, що ми маємо проблему найму та утримання персоналу.

Справа в тому, що в індустрії кібербезпеки все ще переважно домінують чоловіки. Вважається, що жінки складають лише 25% робочої сили в сфері кібербезпеки. Без розмаїття думок, поглядів і досвіду розвиток галузі й надалі сповільнюватиметься. Оскільки кіберзлочинці створюють нові, дедалі складніші проблеми, ми не можемо мати тих самих кількох голосів, які борються між собою за ті самі питання, щоб зберегти обличчя.

Технологія завжди була еволюцією та перспективним мисленням. Коли у нас немає різноманітності, нам бракує здатності до інновацій. У поєднанні з розривом навичок, про який широко говорять, ми як галузь — ніщо, якщо не залучити таланти з усіх сфер життя. Як наслідок, ми наразі не отримуємо переваг від багатства знань, які існують.

Дослідження показують, що представники меншин становлять 26% робочої сили з кібербезпеки, причому багато з цих працівників працюють на некерівних посадах. Упередження пригнічують інновації, а в сфері кібербезпеки ми зменшуємо нашу здатність випереджати загрози, що постійно змінюються.

Потреба зміни культури

Нам потрібна культурна зміна. Настав час звільнитися від ідеалів мачо минулого кібербезпеки. Кілька початкових речей, які чоловіки на керівних посадах можуть зробити краще: Почніть з відступу та звільнення місця для інших. Коли у вас є панелі на конференціях, переконайтеся, що є широка коаліція представників різних культур, рас і статей, попросивши їх говорити про свій досвід і знання, а не зосереджуватися на своїй статі, етнічній приналежності чи нейрорізноманітності.

Те ж саме стосується найму лідерів — заохочення жінок, людей з різним етнічним і культурним походженням і кандидатів з нервово-розрізненими структурами займати технічні керівні посади.

Подібним чином, як лідерам, створити культуру страху навколо кібербезпеки проблематично. Створення середовища відкритості, яке дозволяє працівникам визнавати помилки, не боячись догани, є хорошим способом зміцнення довіри та зменшення шкоди, коли виникають проблеми. Мачизм суперечить багатьом із цих характеристик. Ми повинні бути відкритими та чесними щодо проблем безпеки та потенційних вразливостей, щоб ми могли діяти належним чином і швидко». ***(Elliott Wilkes. Embracing Vulnerabilities: Cybersecurity And Machismo // Forbes (https://www.forbes.com/sites/forbestechcouncil/2024/03/14/embracing-vulnerabilities-cybersecurity-and-machismo/?sh=2767982c46db). 14.03.2024).***

***

«У епоху цифрових технологій кібербезпека стала головною проблемою як для організацій, так і для окремих осіб. Оскільки кіберзагрози постійно зростають, традиційних заходів безпеки вже недостатньо для забезпечення надійного захисту. Відчуйте трансформаційну силу штучного інтелекту (AI) і машинного навчання (ML), які революціонізують ландшафт кібербезпеки. Ці передові технології підвищують здатність систем безпеки виявляти, аналізувати й реагувати на потенційні загрози з безпрецедентною швидкістю й точністю.

Використовуючи AI та ML, фахівці з кібербезпеки можуть бути на крок попереду зловмисників, забезпечуючи безпеку та цілісність конфіденційних даних і систем. У цій статті ми дослідимо багатогранну роль штучного інтелекту та машинного навчання в кібербезпеці, заглибимося в їх застосування, переваги та перспективне майбутнє, яке вони чекають для створення більш безпечного цифрового середовища. Від прогнозної аналітики до автоматизованого реагування на інциденти, AI та ML змінюють наш підхід до кібербезпеки, роблячи її більш проактивною, інтелектуальною та ефективною перед обличчям нових кібервикликів.

1. Покращення виявлення загроз

Алгоритми штучного інтелекту та машинного навчання трансформують виявлення загроз, аналізуючи величезні масиви даних для виявлення шаблонів і

аномалій, які вказують на потенційні кіберзагрози. Ці технології можуть переглядати журнали, мережевий трафік та інші джерела даних у режимі реального часу, дозволяючи системам безпеки виявляти та позначати підозрілі дії з безпрецедентною швидкістю та точністю. Цей проактивний підхід значно скорочує час, необхідний для виявлення загроз, що дозволяє швидше реагувати та мінімізувати потенційну шкоду.

2. Адаптивне навчання для динамічного захисту

Однією з ключових переваг штучного інтелекту та машинного навчання в кібербезпеці є їх здатність навчатися та адаптуватися з часом. Оскільки ці системи стикаються з новими загрозами та сценаріями, вони постійно оновлюють свою базу знань, покращуючи свої можливості виявлення та реагування. Для працюючих професіоналів, які прагнуть залишатися попереду в цій динамічній галузі, отримання магістра з кібербезпеки в Інтернеті може надати необхідні знання та навички для ефективного використання штучного інтелекту та машинного навчання. Онлайн-диплом забезпечує гнучкість балансу між роботою та навчанням, гарантуючи, що експерти з кібербезпеки можуть продовжувати розвиватися разом зі швидко мінливим ландшафтом загроз.

3. Автоматизація реагування на інциденти

Штучний інтелект і машинне навчання не тільки революціонізують виявлення загроз, але й оптимізують реагування на інциденти. Автоматизуючи аналіз інцидентів безпеки та призначаючи відповідні дії, ці технології можуть значно скоротити час відповіді. Автоматизовані підручники та протоколи реагування дозволяють системам безпеки миттєво реагувати на загрози, часто без втручання людини. Ця автоматизація гарантує, що навіть перед обличчям складних атак захист залишатиметься надійним і стійким.

4. Прогнозна аналітика для проактивної безпеки

Прогнозна аналітика на основі штучного інтелекту та машинного навчання дає змогу фахівцям із кібербезпеки передбачати та пом’якшувати потенційні загрози до того, як вони матеріалізуються. Аналізуючи історичні дані та визначаючи тенденції, ці технології можуть прогнозувати майбутні моделі атак і

вразливості. Ця можливість прогнозування дозволяє організаціям прийняти більш проактивний підхід до кібербезпеки, впроваджуючи заходи для запобігання потенційним порушенням, а не просто реагуючи на них.

5. Покращення автентифікації та контролю доступу

AI і ML також покращують механізми автентифікації та контролю доступу. Аналізуючи поведінку користувачів, шаблони використання пристрою та інші контекстні дані, ці технології можуть реалізувати динамічні й адаптивні процеси автентифікації. Цей підхід підвищує безпеку, гарантуючи, що доступ надається на основі оцінки ризиків у реальному часі, зменшуючи ймовірність несанкціонованого доступу та потенційних порушень.

6. Боротьба з фішингом і соціальною інженерією

AI і ML є потужними інструментами в боротьбі з фішингом і атаками соціальної інженерії. Аналізуючи вміст електронної пошти, поведінку відправника та інші показники, ці технології можуть ідентифікувати та позначати підозрілі повідомлення, які можуть бути частиною фішингової кампанії. Це раннє виявлення допомагає запобігти тому, щоб користувачі стали жертвами шахраїв, і захищає конфіденційну інформацію від злому.

7. Захист Інтернету речей (IoT)

Оскільки кількість підключених пристроїв продовжує зростати, безпека екосистеми IoT стала критичною проблемою. AI та ML можуть відстежувати та аналізувати величезні обсяги даних, створених пристроями IoT, щоб виявляти потенційні вразливості та загрози. Надаючи інформацію про поведінку пристрою та мережевий трафік у реальному часі, ці технології допомагають забезпечити безпеку середовищ IoT.

8. Оптимізація комплаєнсу та управління ризиками

AI та ML також можуть допомогти організаціям підтримувати відповідність нормам кібербезпеки та керувати ризиками. Завдяки автоматизації аналізу даних відповідності та виявлення областей невідповідності ці технології можуть допомогти організаціям випереджати нормативні вимоги. Крім того, алгоритми ML

можуть оцінювати рівні ризику на основі різних факторів, що дозволяє приймати більш обґрунтовані рішення та розподіляти ресурси.

9. Усунення нестачі навичок у сфері кібербезпеки

Зростаюча складність кіберзагроз призвела до розриву в навичках у кадрах із кібербезпеки. Штучний інтелект і машинне навчання можуть вирішити цю проблему, автоматизувавши рутинні завдання та допомагаючи аналітикам у більш складних дослідженнях. Це не тільки підвищує ефективність, але й дозволяє фахівцям з кібербезпеки зосередитися на стратегічних та відчутних заходах.

10. Майбутнє AI та ML у кібербезпеці

Оскільки штучний інтелект і машинне навчання продовжують розвиватися, їх роль у кібербезпеці зростатиме. Майбутні розробки можуть включати більш складні моделі прогнозування, автономні системи безпеки та розширену інтеграцію з іншими технологіями. Постійний розвиток штучного інтелекту та машинного навчання обіцяє майбутнє, де кібербезпека буде більш проактивною, інтелектуальною та ефективнішою для захисту від загроз, що постійно змінюються.

Висновок

AI та ML роблять революцію в галузі кібербезпеки, пропонуючи інноваційні рішення для виявлення, запобігання та реагування на кіберзагрози. Ці технології змінюють підхід організацій до кібербезпеки: від покращення виявлення загроз до захисту пристроїв Інтернету речей і оптимізації відповідності. Дивлячись у майбутнє, продовження еволюції штучного інтелекту та машинного навчання обіцяє створення більш безпечного цифрового світу, де захист кібербезпеки є не лише реактивним, але й прогнозованим та адаптивним. Інтеграція штучного інтелекту та машинного навчання в кібербезпеку – це не просто тренд; це фундаментальний зсув до розумнішого та стійкішого підходу до захисту нашого цифрового життя». ***(James Andrew. The Role of AI and Machine Learning in Cybersecurity // TechBullion (https://techbullion.com/the-role-of-ai-and-machine-learning-in-cybersecurity/). 14.03.2024).***

***

«Зростаючий попит на компетентних фахівців з кібербезпеки свідчить про основну зміну; мова йде не лише про заповнення посад, а й про те, щоб на цих посадах були присутні люди, здатні впоратися з нюансами складності сучасних кіберзагроз. У цій статті досліджуються навички, необхідні, щоб виділитися серед натовпу експертів з кібербезпеки. Від володіння передовими технологіями до стратегічного розуміння – це компетенції, необхідні тим, хто прагне процвітати в сфері кібербезпеки.

Розуміння нових технологій

Перший крок до майстерності кібербезпеки полягає в розумінні нових технологій. Оскільки цифрова інфраструктура бізнесу стає все більш складною, інтегруючи нові інструменти та платформи, роль професіонала з кібербезпеки розвивається. Майстерність над цими технологіями є подвійною: захистити їх від потенційних вразливостей і зрозуміти, як зловмисники можуть ними скористатися. Ця подвійна перспектива гарантує, що заходи кібербезпеки є проактивними та стійкими, що робить їх квінтесенцією навичок для сучасного експерта з кібербезпеки.

Розширене виявлення загроз і реагування

Суть навичок кібербезпеки полягає в здатності виявляти сучасні загрози та протидіяти їм. Сучасний кібернетичний ландшафт пронизаний складними загрозами, які вимагають не лише пильності на поверхневому рівні. Фахівці з кібербезпеки повинні використовувати передову аналітику, ШІ та машинне навчання не лише як інструменти, а як невід'ємні компоненти свого стратегічного озброєння. Цей набір навичок спрямований на попередження кіберзагроз, формування передбачуваної позиції, яка пом'якшує ризики ще до того, як вони виявляться.

Правильні облікові дані

В освітньому контексті отримання онлайн-ступеню магістра з інформаційної безпеки має важливе значення для закладення фундаменту для міцної кар'єри в галузі кібербезпеки. Цей вчений ступінь — це більше, ніж просто академічне досягнення; це глибоке занурення в тонкощі кібербезпеки, що охоплює все,

починаючи від оборонних стратегій і закінчуючи етичними проблемами, пов’язаними з цифровим стеженням. Для тих, хто готовий взяти на себе керівну роль у сфері кібербезпеки, ця передова освіта є незамінною, пропонуючи як повну базу знань, так і спеціалізацію, необхідну для навігації в галузі викликів, що розвиваються.

Управління інцидентами та відновлення

Коли трапляються кіберінциденти, теоретичні знання кібербезпеки піддаються найвищому випробуванню. Тут важливою є здатність керувати такими інцидентами та відновлюватися після них. Навички в розробці та впровадженні чітких планів реагування на інциденти є безцінними, гарантуючи, що організації не лише готові реагувати на загрози, але й оснащені для відновлення з мінімальними наслідками. Цей аспект кібербезпеки підкреслює важливість стійкості, яка гарантує, що цілісність цифрових активів організації залишається незмінною навіть після кіберзлому.

Юридичні та етичні міркування

Сфера кібербезпеки виходить за межі технічної сфери, охоплюючи правові та етичні аспекти, які є однаково критичними. Професіонали в цій галузі повинні орієнтуватися в лабіринті законів, нормативних актів і етичних дилем, гарантуючи, що цифрові фортеці, які вони будують, не порушують права особи чи суспільні норми. Цей делікатний баланс між безпекою та етикою відображає багатогранну природу кібербезпеки, підкреслюючи потребу в професіоналах, які не лише володіють технологічними знаннями, але й мають етичні основи.

Розробка політики та стратегії кібербезпеки

В основі надійної позиції кібербезпеки лежить розробка переконливих політик і стратегій. Ця навичка — це щось більше, ніж технічна експертиза, що поєднує в собі елементи стратегічного передбачення та політичну проникливість. Фахівці з кібербезпеки, які досягли успіху в цій галузі, є архітекторами цифрової безпеки, розробляючи інфраструктури, які захищають не лише від поточних загроз, але й запобігають майбутнім уразливостям. Їхня робота гарантує, що заходи

кібербезпеки є комплексними, плавно інтегрованими в ширшу організаційну стратегію та адаптуються до цифрового ландшафту, що постійно змінюється.

Експертиза безпеки в хмарі

Перехід до хмарних обчислень підкреслив необхідність досвіду хмарної безпеки. Цей набір навичок передбачає всебічне розуміння хмарної архітектури та унікальних проблем безпеки, які вона створює. Професіонали, які вміють працювати з хмарною безпекою, мають завдання розробити та впровадити надійні заходи безпеки для захисту хмарних систем і даних. Їхній досвід гарантує, що організації можуть використовувати переваги хмарних обчислень, мінімізуючи ризики, пов'язані з витоком даних і кібератаками. У міру того як хмарні сервіси продовжують розвиватися, так само повинні розвиватися стратегії, які використовуються для їх захисту, що робить досвід хмарної безпеки незамінним активом у наборі інструментів кібербезпеки.

Штучний інтелект і машинне навчання в кібербезпеці

Інтеграція штучного інтелекту (AI) і машинного навчання (ML) у кібербезпеку є зміною парадигми виявлення та пом'якшення загроз. Ці технології пропонують безпрецедентні можливості для визначення закономірностей, автоматизації систем реагування та прогнозування потенційних загроз на основі величезних наборів даних. Володіння AI та ML у сфері кібербезпеки дозволяє фахівцям не лише ефективніше реагувати на інциденти, але й передбачати та нейтралізувати загрози до того, як вони виникнуть. Цей проактивний підхід до кібербезпеки на основі штучного інтелекту та машинного навчання встановлює новий стандарт для механізмів цифрового захисту, що робить його критично важливим навиком для майбутнього кібербезпеки.

Безпечна розробка програмного забезпечення

У епоху, коли програмне забезпечення пронизує всі аспекти особистого та професійного життя, розробка безпечного програмного забезпечення стала наріжним каменем кібербезпеки. Ця навичка включає в себе здатність проектувати, розробляти та підтримувати програмне забезпечення з урахуванням безпеки, гарантуючи, що програми стійкі до атак із самого початку. Професіонали, які

кваліфіковані в розробці безпечного програмного забезпечення, можуть суттєво зменшити ризик порушення безпеки, що робить його життєво важливою компетентністю в розробці цифрових рішень. Ця навичка передбачає кодування, а також глибоке розуміння потенційних вразливостей і способів їх запобігання, підкреслюючи важливість міркувань безпеки в життєвому циклі розробки програмного забезпечення.

Безпека Інтернету речей

Експоненційне зростання Інтернету речей (IoT) відкрив новий рубіж у кібербезпеці. Фахівці з безпеки Інтернету речей знаходяться на передньому краї захисту ряду взаємопов'язаних пристроїв, які потенційно можуть служити точками входу для кібератак. Їхній досвід має вирішальне значення для усунення унікальних вразливостей пристроїв Інтернету речей, від гаджетів для розумного дому до промислових датчиків. Цей набір навичок вимагає детального розуміння як апаратних, так і програмних аспектів пристроїв IoT, гарантуючи бездоганну інтеграцію заходів безпеки для захисту від широкого спектру загроз.

Попереду в полі

Сектор кібербезпеки постійно розвивається під впливом технологічного прогресу та нових загроз. Навички, висвітлені в цій статті, представляють передовий край кібербезпеки, необхідний для професіоналів, які прагнуть досягти успіху в цій динамічній сфері. Дивлячись у майбутнє, неможливо переоцінити важливість постійного навчання та адаптації. Фахівці з кібербезпеки, які лідируватимуть, — це ті, хто приймає інновації, розуміє тонкощі цифрового захисту та готовий долати виклики завтрашнього дня. Розвиваючи ці передові навички, професіонали можуть захистити від поточних загроз, а також передбачити та нейтралізувати виклики, які чекають попереду». ***(James Andrew. The Future of Cybersecurity: 10 Skills That Will Set You Apart // TechBullion (https://techbullion.com/the-future-of-cybersecurity-10-skills-that-will-set-you-apart/). 14.03.2024).***

***

«Світова кібербезпека перебуває на перехресті великих викликів і загроз, масштаби яких уже відчувають дослідники. За даними AAG IT, у 2021 році кількість кібератак зросла на 125% і продовжує збільшуватися щороку. Це помічають бізнеси та постійно збільшують свої витрати на кібербезпеку.

За даними Cybersecurity Ventures, у 2004 році світовий ринок кібербезпеки становив лише $3,5 млрд. Однак в найближчі два роки ця сума має зрости до $1,75 трлн. Серед жертв кібератак є як великі компанії типу eBay, так і мікробізнеси із сотнею клієнтів. Який сигнал ми отримуємо від цієї статистики? Дуже простий: кіберзлочинці збільшують свою активність і створюють загрозу для всіх без винятку компаній.

Для українського бізнесу ситуація має ще більш загрозливий вигляд. Окрім злочинців, метою яких є збагачення, Україну постійно атакує ворог. Кібератаки є частиною повномасштабної війни, яку РФ розв'язали в нашій країні, і до якої готувалися задовго до 2022 року. Напередодні вторгнення, у перші 10 місяців 2021 року, в Україні зафіксували 280 000 атак. Більшість із них були націлені на уряд та критично важливі сайти, наприклад банківські системи. Однак частково постраждав і бізнес.

У цій статті ми розповімо, чому нікому не варто нехтувати кібербезпекою, а також чому бекапування даних простий і надійний спосіб вберегти свою інформацію.

Кібератаки — не випадковість

Керівники бізнесів не люблять витрачати гроші на малопомітні проєкти та дуже рідко вкладаються у напрямки, які не приносять користь тут і зараз. Красномовний факт: у 2020 році 49% підприємців в Україні вели облік у табличних сервісах, хоча на ринку вже існувало низка якісних CRM-систем на будь-який смак. Люди вважали, що перехід на CRM занадто складний і не принесе користі їхній компанії.

Така недооцінка сьогодні присутня й у сфері кібербезпеки. Керівники компаній іноді озвучують небезпечну думку: «Ми маленька компанія, навіщо

хакерам інформація про моїх клієнтів?». Схоже, багато підприємців справді не розуміють мотиви злочинців, тому розглянемо їх детальніше.

Заробіток. Більшість кіберзлочинців спрямовані на заробіток грошей. Вони можуть використовувати кібератаки для вимагання викупу, крадіжки фінансової інформації, крадіжки конфіденційної інтелектуальної власності або для оцінки фінансових ресурсів компанії.

Крадіжка особистої інформації. Кіберзлочинці можуть атакувати бізнес з метою крадіжки особистої інформації про клієнтів або співробітників, яку потім можна використовувати для шахрайства, шпигунства або ідентифікації.

Злам в цілях розваг. Деякі кіберзлочинці можуть влаштовувати кібератаки просто для задоволення або випробування власних навичок без будь-якої конкретної мети чи вигоди.

Політичні мотиви та війна. Хакери з РФ можуть атакувати українські компанії, щоб завдати шкоди економіці країни.

Кіберзлочинцям складно атакувати компанії, які добре захищені. Простіше знайти слабке місце і вдарити в нього. Це робить усі хакерські атаки невипадковими. Тобто, якщо бізнес не дбає про кіберзахист, то сам збільшує свої шанси потрапити під одну з атак.

Що таке бекапування даних і для чого воно потрібне?

Один з найпростіших способів зберегти свої дані — створити їхню резервну копію. Резервне копіювання даних (бекапування) — це процес створення копій важливих даних і зберігання їх на іншому носії або в іншому місці. Це дає можливість відновити ці дані у випадку втрати або пошкодження.

Найсучаснішим і найзручнішим способом зберігати резервну копію сьогодні є хмарне середовище. 65% компаній кажуть, що вони використовують хмару як основне сховище даних для бекапування.

Залежно від сервісу, бекапування може мати різний вигляд. Існують послуги, які автоматично створюють копію кожні 24 години, шифрують їх та відправляють у хмару. Часто такі сервіси копіюють лише нові дані, або інформацію, яка зазнала змін. Це пришвидшує процес і робить його непомітним для бізнесу.

Є декілька причин, чому бекапування даних потрібне бізнесу:

Кібертероризм. Злочинці не зможуть шантажувати вас доступом до ваших даних, якщо у вас є копія. Навіть якщо комусь вдасться стерти всю інформацію та вимагати викуп за її повернення, ви зможете швидко все відновити й продовжити роботу.

Людський фактор. Виникають ситуації, коли співробітники випадково видаляють, якусь важливу базу даних, після чого її неможливо відновити. Залежно від важливості цієї інформації збитки можуть бути як незначними, так і катастрофічними.

У 2021 році, один зі співробітників поліції в місті Даллас випадково видалив важливий архів розміром 23 терабайти. В ньому зберігалися файли, фото, докази та інші документи для близько 17 500 справ в офісі окружного прокурора. Здогадайтеся, чи була в поліції Далласа резервна копія цих даних? Звісно ні.

Проблеми виникли через випадковий збіг обставин: співробітник абияк ставився до своєї роботи, якимось чином отримав доступ до великої кількості важливих даних, а поліція не подбала про бекап. Тобто навіть без хакерів чи кіберзлочинців у доволі захищеній структурі стаються форс-мажори із важкими наслідками.

Як обрати сервіс для бекапування даних

Під час вибору сервісу для резервного копіювання даних важливо врахувати кілька ключових аспектів. Перш за все, слід чітко визначити ваші потреби: які дані потрібно копіювати і яка частота резервних копій необхідна. Також важливо врахувати обсяг даних, який ви плануєте зберігати, оскільки деякі сервіси можуть мати обмеження на місткість сховища або розраховувати вартість на основі обсягу даних.

Додатково варто звернути увагу на заходи безпеки, такі як шифрування даних під час передачі та зберігання, а також наявність механізмів автентифікації. Вибираючи, слід оцінити зручність використання інтерфейсу користувача та можливості відновлення даних із резервних копій у випадку втрати чи

пошкодження інформації. Не менш важливою є масштабованість сервісу, його надійність та якість підтримки, яку він надає своїм користувачам.

Наприклад, в UCloud бекапування передбачає повне охоплення: резервне копіювання дисків, розділів, файлів і тек, віртуальних машин. Копії зберігаються в надійному дата-центрі UCloud Німеччини. Вартість копіювання одного терабайту обійдеться компанії всього в $10 на місяць.

Короткий висновок

Бекапування — це створення резервної копії важливих даних для бізнесу. На жаль, багато компаній досі нехтують безпекою своєї інформації й зберігають усе в одному місці. За таких умов вони стають слабкою ціллю для кібертерористів, які можуть викрасти інформацію і вимагати за неї викуп.

Навіть, якщо хакери пройдуть повз вашу компанію, проблеми можуть виникнути всередині. Людський фактор не варто ігнорувати: випадкові видалення чи обстріли росіян ставлять під загрозу ваші дані. Бекапування за допомогою хмари — це простий, надійний і недорогий спосіб зберегти дані та забезпечити стабільно роботу компанії». ***(Під прицілом кібертерористів — навіщо потрібне бекапування // HiTech.Expert. (https://expert.com.ua/178882-pid-prycilom-kiberterorystiv-navischo-potribne-bekapuvannya.html). 13.03.2024).***

***

«Однією з найпоширеніших помилок у кібербезпеці завантаження файлів є те, що певних інструментів «достатньо» самих по собі — це просто не так. У нашому останньому технічному документі генеральний директор і засновник OPSWAT Бенні Чарні детально розглядає, що потрібно для запобігання загрозам зловмисного програмного забезпечення в сучасному середовищі безпеки завантаження файлів, що постійно розвивається, і значною частиною цього є розуміння того, де є підводні камені та як їх уникайте їх.

Першим кроком у цьому процесі є розуміння того, що трьох інструментів або рішень, які часто використовуються, недостатньо. Давайте розглянемо цю концепцію та детальніше розглянемо краще рішення.

Розуміння виклику

Сучасні веб-програми є складними, вони використовують підключені до Інтернету IT-системи, які взаємодіють із критично важливими системами OT, а також використовують широкий спектр хмарних провайдерів і протоколів. Усі ці системи передають і зберігають дуже конфіденційні та цінні дані в уряді, охороні здоров'я, енергетиці, фінансах та інших критично важливих секторах по всьому світу, несучи з собою загрози, здатні завдати серйозної шкоди.

Безпека завантаження файлів для виявлення та запобігання проникненню зловмисного програмного забезпечення є критично важливою. Оскільки цей вектор загрози зростає та поверхня атаки поширюється, забезпечення безпеки цих секторів стає надзвичайно важливим. Ось чому розробка — і впровадження — надійної та перевіреної стратегії безпеки має першочергове значення для просування вперед.

Знаряддя торгівлі

Одного засобу просто недостатньо. Нижче наведено три найпоширеніші інструменти, які, якщо вони використовуються окремо для захисту завантаження файлів, не забезпечують належного захисту, і чому це так:

1. Сканування файлів проти шкідливих програм #

Кожен знайомий із захистом від зловмисного програмного забезпечення, але не всі засоби захисту від зловмисного програмного забезпечення або режими сканування однакові. Інтригує те, що досі існує багато плутанини щодо показників ефективності, коли йдеться про «постійний» захист у режимі реального часу, який відстежує всю систему, порівняно зі, скажімо, статичними стратегіями сканування файлів, які потрібно запускати вручну або за розкладом. Сканування в режимі реального часу може демонструвати майже 100% ефективність, тоді як статичне сканування, навпаки, помітно нижче з показниками в діапазоні між 6-76%. Щоб уникнути помилкового відчуття безпеки, організації повинні точно знати, що вони отримують з кожним режимом розгортання.

2. Брандмауери веб-додатків #

Багато експертів вважають, що завдяки встановленню брандмауера веб-додатків (WAF) вони захищені від зловмисного завантаження файлів. Насправді це

зовсім не так, оскільки брандмауери веб-додатків захищають насамперед від атак на прикладному рівні (OSI Layer 7). Вони не мають спеціального дизайну для запобігання зараженню зловмисним програмним забезпеченням, яке може вражати інші рівні або поширюватися іншими каналами, наприклад вкладеннями електронної пошти чи знімними носіями. Крім того, вони борються із зашифрованим трафіком (наприклад, https) і зазвичай покладаються на єдине рішення для захисту від шкідливих програм для виявлення загроз.

3. Пісочниця #

Ізольоване програмне середовище — це метод, який спочатку використовувався для аналізу зловмисного програмного забезпечення шляхом ізоляції та виконання підозрілих файлів у контрольованому середовищі, щоб зрозуміти їх поведінку та виявити потенційні ознаки зловмисного програмного забезпечення. Поодинці пісочниці стикаються з такими обмеженнями, як слабкість до передових і часових методів ухилення, які маскують або затримують зловмисні дії та тригери, що стосуються середовища, в адаптивному шкідливому програмному забезпеченні. Вони ресурсомісткі, схильні до хибних спрацьовувань і негативів і пропонують обмежене охоплення, характерне для шкідливих програм на основі файлів.

Кібербезпека поглибленого захисту

Отже, якщо ви не можете покладатися лише на ці методи, яка відповідь? Це одна з областей, у яких OPSWAT витратив останні 20 років на інновації. Наша платформа MetaDefender використовує провідні на ринку технології, яким довіряють у всьому світі, щоб створити просту в розгортанні, інтегровану за проектом стратегію кібербезпеки з поглибленим захистом для безпеки завантаження файлів.

Мультисканування

Оскільки ефективність окремих рішень для захисту від зловмисного програмного забезпечення для статичного аналізу коливається від 6% до 76%, ми вирішили інтегрувати кілька комерційно доступних рішень у наше рішення та отримати вигоду від їх спільної потужності. Оскільки понад 30 провідних

механізмів захисту від зловмисного програмного забезпечення працюють одночасно, наші показники ефективності ледве соромляться 100% і оптимізовані для швидкості.

Deep Content Disarm and Reconstruction (Deep CDR)

Щоб ще більше зміцнити наш захист, ми запровадили унікальну методологію, яка називається Deep Content Disarm and Reconstruction (Deep CDR). Наша унікальна технологія, нагороджена рейтингом AAA, 100% захисту від SE Labs, забезпечує повну безпеку на основі запобігання завантаженню файлів шляхом нейтралізації потенційних загроз, перш ніж вони можуть завдати шкоди. Він оцінює та перевіряє тип і узгодженість файлів і перевіряє розширення файлів, щоб запобігти маскуванню, і попереджає організації, якщо вони зазнають атаки. Потім він розділяє файли на окремі компоненти та видаляє потенційно шкідливі об’єкти та відновлює придатні для використання файли, реконструюючи метадані, зберігаючи всі характеристики файлу.

Проактивне запобігання втраті даних (Proactive DLP)

Модуль проактивного запобігання втраті даних (DLP) від OPSWAT був розроблений спеціально для вирішення зростаючих проблем щодо відповідності та регулювання, витоку даних і ризиків, пов’язаних із завантаженням файлів. Наше рішення виявляє та захищає конфіденційну інформацію в різних типах файлів, включаючи шаблони на основі тексту, зображень і відео.

Адаптивна пісочниця в реальному часі

Щоб подолати обмеження традиційної пісочниці, OPSWAT розробив унікальну пісочницю на основі емуляції з адаптивним аналізом загроз. У поєднанні з нашими технологіями Multiscanning і Deep CDR він забезпечує комплексний багаторівневий підхід до виявлення та запобігання зловмисному програмному забезпеченню. Наш підхід, заснований на емуляції, може швидко деобфускатувати та аналізувати навіть найскладніше, сучасне та екологічно відповідальне шкідливе програмне забезпечення менш ніж за 15 секунд…» ***(Demystifying a Common Cybersecurity Myth // The Hacker News***

(https://thehackernews.com/2024/03/demystifying-common-cybersecurity-myth.html). 13.03.2024).

***

«…Уважніший погляд на індустрію кібербезпеки показує явну проблему — гендерний розрив, який зберігається, незважаючи на прогрес в інших професіях. Статистика показує, що з 2018 по 2023 рік кількість жінок, які працюють у сфері кібербезпеки в Індії, зросла більш ніж на 10%. Це стало зростанням приблизно з 11% до 22% завдяки зусиллям таких ініціатив, як CyberShikshaa та корпоративних ініціатив щодо інклюзії та різноманітності, які залучили в організації різноманітну робочу силу. Хоча це обнадійлива тенденція, все ще існує величезна прогалина, яку потрібно подолати, і необхідно докласти зусиль, щоб подолати цю прогалину як в академічних колах, так і в промисловості.

Орієнтування в професійних викликах

Незважаючи на зусилля організацій для сприяння гендерній рівності, жінки продовжують стикатися з проблемами на робочому місці, починаючи від дискримінації на робочому місці, браку впевненості та навіть синдрому самозванця. Несвідомі упередження та гендерні стереотипи в галузі перешкоджають професійному росту жінок, підкреслюючи необхідність зміни організаційної культури. Важливо створити сприятливе середовище, яке дає жінкам можливість використовувати свої навички та розвивати стійкість.

Створення мережі підтримки

Програми наставництва та мережеві спільноти мають вирішальне значення для розвитку кар’єри, особливо для жінок у сфері технологій, які можуть не бачити так багато жіночих моделей для наслідування. Крім того, заохочення культури підтримки та співпраці в галузі забезпечує обмін знаннями та розвиток навичок. Ці ініціативи можуть не тільки подолати гендерний розрив, але й створити середовище, в якому жінки відчуватимуть себе спроможними процвітати під керівництвом досвідчених наставників.

Сприяння різноманітності та інклюзивності

Важливо відстоювати ініціативи на робочому місці, які сприяють рівним можливостям. Співпраця та різноманітне мислення мають вирішальне значення для розробки інноваційних та ефективних стратегій кібербезпеки, що вимагає різноманітної робочої сили. Такі заходи, як хакатони та квести з програмування, можуть об'єднати команди та допомогти жінкам продемонструвати свої навички з перших рук. Неупереджений підбір персоналу за допомогою анонімного найму на основі кваліфікації також може допомогти внести більше різноманітності в організацію. Стратегії розвитку навичок і найму, зосереджені на сприянні розмаїттю, збагачують пул талантів і сприяють створенню більш стійкої робочої сили з кібербезпеки.

Шлях вперед

Розширення прав і можливостей жінок у сфері кібербезпеки є вирішальним напрямком для галузі. Визнання унікальних проблем, з якими стикаються жінки, сприяння підтримці мережі та кидання гендерних норм прокладають шлях до більш інклюзивного цифрового майбутнього.

Оскільки загрози кібербезпеці стають дедалі складнішими, вкрай важливо враховувати різноманітні точки зору. Заклик до дії зрозумілий: організації, лідери галузі та професіонали повинні об'єднатися, щоб створити ландшафт кібербезпеки, який процвітає на різноманітності, забезпечуючи безпечніший і стійкіший цифровий світ для всіх». ***(Geetha Ramanna. Expert voice | Empowering women in cybersecurity: Navigating challenges & breaking barriers // India Dot Com Private Limited (https://www.wionews.com/business-economy/expert-voice-empowering-women-in-cybersecurity-navigating-challenges-breaking-barriers-699950). 14.03.2024).***

***

«Нове опитування стверджує, що 74 відсотки всіх порушень кібербезпеки викликані людським фактором. Відповідно до даних, опублікованих у звіті The State of Email and Collaboration Security 2024 від Mimecast, кіберзагрози зростають

безпрецедентними темпами, і наступний рік буде сповнений кіберзлочинності та інцидентів, які очікуються напередодні напруженого виборчого року, який очолює понад 50 країн. на вибори. З новими загрозами, такими як штучний інтелект і технологія deepfake, ставки на ефективний кіберзахист вищі, ніж будь-коли.

Mimecast розширив восьме видання цього щорічного звіту, включивши в нього інформацію про безпеку спільної роботи на додаток до електронної пошти. SOECS базується на поглибленому глобальному опитуванні 1100 фахівців з інформаційних технологій та кібербезпеки.

Основні моменти цьогорічного звіту включають:

Людський ризик є найбільшою прогалиною в безпеці сьогодення, і IT-команди повинні краще озброїти співробітників потрібними інструментами та навчанням. 74 відсотки всіх кіберзломів викликані людським фактором, включаючи помилки, викрадені облікові дані, неправильне використання привілеїв доступу або соціальну інженерію.

IT-команди активно посилюють свої оборонні стратегії, особливо в умовах, коли штучний інтелект створює нові виклики. Поява штучного інтелекту прискорює поширення фішингу та програм-вимагачів, спрощуючи зловмисникам здійснення успішних атак. 8 із 10 респондентів стурбовані новими загрозами, які створює штучний інтелект, а 67 відсотків кажуть, що атаки за допомогою штучного інтелекту незабаром стануть нормою. Оскільки компанії готуються до нових загроз, вони розглядають кіберризики як більшу бізнес-проблему, а не лише IT-проблему.

Електронна пошта залишається основним вектором атаки для кіберзагроз, таких як фішинг, спуфінг і програми-вимагачі, але інструменти для співпраці створюють нові та небезпечні точки входу для зловмисників. 70 відсотків очікують, що інструменти для співпраці створять нові загрози, а 69 відсотків вважають, що атака на основі інструментів для співпраці ймовірно зашкодить їхній компанії.

«Нові інструменти та технології, такі як AI та deepfakes, а також поширення платформ для співпраці змінюють спосіб роботи суб’єктів загрози; але люди залишаються найбільшою перешкодою для захисту компаній від кіберзагроз», —

сказав Марк ван Задельхофф, генеральний директор Mimecast. «Команди з кібербезпеки та IT повинні працювати з ширшими бізнес-лідерами, щоб надати пріоритет розумінню людських ризиків. За допомогою правильних інструментів і навчання компанії можуть краще захищатися від загроз і керувати людськими ризиками». ***(Neil Franklin. Three quarters of cybersecurity breaches are down to human error // Workplace Insight (https://workplaceinsight.net/three-quarters-of-cybersecurity-breaches-are-down-to-human-error/). 13.03.2024).***

***

«Згідно з даними GlobalData, незважаючи на спад активності угод M&A у секторі технологій, медіа та телекомунікацій (TMT), кібербезпека виділяється як стійкий викид.

У міру ескалації кіберзагроз компанії віддають перевагу інвестиціям у можливості кібербезпеки, що призведе до різкого зростання відповідних угод M&A протягом 2023 року. Це стійке зростання підкреслює критичну важливість кібербезпеки перед обличчям ландшафту загроз, що розвивається, і дедалі складніших кібератак, заявляє GlobalData, відома компанія з обробки даних і аналітики.

Угоди, пов’язані з кібербезпекою, досягли 42 мільярдів доларів у 2023 році, що робить цю тему другою за величиною серед 100 найпопулярніших угод. Тим часом загальна вартість глобальних угод злиття та поглинання TMT різко впала на 46 відсотків у 2023 році до 403 мільярдів доларів, що є значним зниженням порівняно з 745 мільярдами доларів, зафіксованими в попередньому році. Подібним чином обсяг угод скоротився на 26 відсотків і склав 451 угоду в 2023 році порівняно з 609 угодами в 2022 році.

70 відсотків респондентів зазначили, що кібербезпека або вже руйнує їхню галузь, або очікує, що це станеться протягом наступних 12 місяців. У звіті наголошується на зростаючій загрозі атак, які фінансуються державою, і зростаючій складності атак програм-вимагачів.

Найбільшою угодою з кібербезпеки 2023 року стало придбання компанією Cisco Splunk за 30 мільярдів доларів, що також вважається найбільшою угодою в секторі TMT за рік. За цим придбанням послідувало придбання Honeywell за 5 мільярдів доларів бізнесу Carrier Global з глобальних рішень для доступу та придбання Thales компанії Imperva за 4 мільярди доларів.

Незважаючи на стійкість кібербезпеки, у 2023 році в діяльності TMT M&A домінувала тема зв'язку, завдяки чому вартість угод M&A на суму 72 мільярди доларів від найбільших угод TMT, оголошених протягом року. Основні угоди у сфері зв'язку включали придбання Kohlberg Kravis Roberts (KKR) і Abu Dhabi Investment Authority бізнесу фіксованого зв'язку Telecom Italia за 20 мільярдів доларів і злиття Vodafone UK з Hutchison 3G UK (Three UK) за 19 мільярдів доларів.

У ширшому аналізі звіт класифікує всі великі угоди, оголошені між 2021 і 2023 роками, у відповідних секторах TMT, таких як апаратне забезпечення, програмне забезпечення та послуги, Інтернет і медіа та телекомунікаційні послуги, з детальною інформацією про теми, що керують кожною угодою.

Значна кількість угод M&A була зумовлена сектором прикладного програмного забезпечення в TMT, на суму 114 мільярдів доларів США за 86 угодами, за якими йшли телекомунікаційні послуги, IT-послуги, музика, кіно та ТБ, а також сектор програмного забезпечення для корпоративної безпеки, Прія Топпо, Thematic Intelligence. Про це заявив аналітик GlobalData.

Заглядаючи вперед, звіт визначає потенційні майбутні цілі придбання на основі поточних ринкових тем. Незважаючи на значну зміну динаміки злиттів і поглинань у 2023 році, відзначену значним зниженням вартості та обсягу угод, GlobalData очікує помірного відновлення протягом 2024 року, оскільки інфляційний тиск зменшиться, а процентні ставки впадуть. Однак компанії повинні активно вирішувати проблеми з регуляторними органами та бути готовими піти на поступки, щоб отримати схвалення угод в умовах посиленого регуляторного контролю». ***(Cybersecurity Emerges as Resilient Force Amid Declining TMT Deal Activity in 2023 // InfotechLead.com (https://infotechlead.com/security/cybersecurity-***

emerges-as-resilient-force-amid-declining-tmt-deal-activity-in-2023-83640). 13.03.2024).

***

«Недостатня кількість жінок у сфері кібербезпеки є складною проблемою, яка відображає ширші соціальні, освітні та робочі фактори. Незважаючи на критичну важливість кібербезпеки для захисту нашого цифрового світу, жінки значно недостатньо представлені в цій сфері. Ця невідповідність не лише висвітлює загальногалузеві проблеми рівності та різноманітності, але й підкреслює втрачену можливість для команд з кібербезпеки отримати вигоду з ширшого спектру точок зору та навичок.

Нам потрібно дослідити причини такої недостатньої представленості, включаючи стереотипи та упередження, освітні бар'єри, культуру на робочому місці та відсутність видимості та зразків для наслідування, а також нам потрібно розглянути наслідки та потенційні стратегії змін.

У моїй кар'єрі жінки були більш талановитими, працьовитими та новаторськими, і вони демонстрували більше творчих навичок, ніж їхні колеги-чоловіки, незалежно від посади чи функції.

Стереотипи та соціальні упередження

Коріння недостатньої представленості лежать глибоко в суспільних стереотипах і упередженнях, які формують сприйняття з молодого віку. Це було правдою для всіх професій у всі часи. Кібербезпека, як і багато інших галузей STEM, страждає від стереотипу про те, що це професія, де домінують чоловіки та підходять для них.

Ці стереотипи підкріплюються медіа-зображеннями, суспільними очікуваннями та навіть маркетингом іграшок та ігор, які непомітно спрямовують хлопчиків і дівчаток на традиційні гендерні ролі. Дівчат менше заохочують займатися технічною діяльністю або цікавитися комп'ютерами та технологіями, що призводить до гендерного розриву в інтересах і впевненості в цих сферах з раннього віку.

Освітні бар'єри

Ця суспільна упередженість поширюється на систему освіти, де дівчата часто стикаються з неприємним середовищем у предметах STEM. Відсутність жіночих зразків для наслідування в цих сферах, гендерно упереджені методи навчання та іноді відверте знеохочення сприяють зниженню інтересу дівчат і участі в STEM, до якого відносно недавно входить кібербезпека.

Навчальні заклади часто не спроможні створити інклюзивну навчальну програму, яка висвітлює внесок жінок у технологію, або запровадити методи навчання, які однаково залучають усіх учнів. Це зрозуміло, оскільки переважна більшість тих, хто керує цими програмами, — чоловіки, але це не можна вибачити.

Освітні бар’єри призводять до меншої кількості жінок, які здобувають вищу освіту в галузі кібербезпеки, що ще більше закріплює цикл недостатнього представництва. Проте навіть у 2024 році, дехто скаже, не існує справжньої проблеми, яку можна було б вирішити, заохочуючи молодих жінок до навчання в галузі STEM. Тож проблема починає нагадувати проблему першого світу, яка слабо шукає рішення.

Я не погоджуюсь. Я вважаю, що більшість із того, що турбує нас сьогодні, — це брак компетентності, який викликає синдром самозванця. І багато практиків просто занадто перевантажені реаліями роботи в галузі кібербезпеки, щоб адекватно вирішити цю проблему. Я не знаю жодного CISO, який би знав усе про все. Тих небагатьох, яких я знаю, хто знає найбільше, у такій меншості, їх недостатньо, щоб проводити майстер-класи з усього, що повинні знати всі практики.

Це не провина практиків. Натиск нових технологій наближається до нас настільки швидко, що було б дивом, якби будь-який CISO міг охопити, засвоїти та зберегти всі ці знання в той момент, коли це необхідно, щоб допомогти йому виконувати свою роботу.

Культура та практика на робочому місці

Для жінок, які долають ці освітні перепони та вступають у сферу кібербезпеки, культура та практика на робочому місці можуть створювати додаткові перешкоди для утримання та просування.

Технологічну індустрію, включно з кібербезпекою, справедливо критикували за її «братську культуру», яка може бути непривітною і навіть ворожою до жінок. Ця культура характеризується практиками та ставленнями, які знецінюють внесок жінок, ігнорують їх для підвищення по службі та складних проектів, а також піддають їх переслідуванням та дискримінації.

Нещодавнє різке зростання чисельності співробітників з інших культур, багато з яких звикли до знецінення жінок поза межами робочої сили, не приносить належного результату та не сприяє реформам. Таке середовище не тільки відлякує жінок від того, щоб залишатися в цій сфері, але й відмовляє інших від участі в цій сфері.

Відсутність видимості та зразків для наслідування

Недостатня кількість жінок у сфері кібербезпеки також самозберігається через відсутність видимих жіночих моделей для наслідування в цій галузі. Жінки, які розглядають кар'єру в сфері кібербезпеки, часто знаходять кілька прикладів успішних жінок-професіоналів, які їх надихають. Така відсутність видимості сприяє помилковому уявленню про те, що кібербезпека не є життєздатною або приємною кар'єрою для жінок.

Відсутність жінок-наставників і зразків для наслідування означає, що жінкам, які прагнуть займатися кібербезпекою, не вистачає керівництва, підтримки та можливостей для спілкування, які є вирішальними для розвитку кар'єри та просування в будь-якій сфері.

Наслідки недостатнього представництва

Недостатня кількість жінок у сфері кібербезпеки має значні наслідки для жінок і для галузі в цілому. Ті, хто наполягає на різноманітності в командах, кажуть, що наявність ширшого діапазону точок зору та досвіду покращує креативність, інновації та вирішення проблем у сфері кібербезпеки, але цей аргумент підтверджується слабкою статистикою. Небезпека тут полягає в тому, що

як тільки блиск трофеїв DEI зникне, зникнуть і гроші, і колись багатообнадійливі програми відступлять за набагато об'єктивнішою та хиткішою практикою найму.

Відсутність жінок у сфері кібербезпеки означає, що ця сфера втрачає можливості для покращення креативності, критичного мислення, інновацій та сократівського вирішення проблем у той час, коли попит на кваліфікованих фахівців із кібербезпеки зростає, а справжня витонченість кіберзагроз розширюється. Ця недостатня представленість також сприяє зростанню гендерної різниці в оплаті праці та економічної нерівності, з якою стикаються жінки.

Стратегії змін

Вирішення проблеми недостатньої представленості жінок у сфері кібербезпеки вимагає багатогранного підходу, який усуває першопричини. Дії включають:

Заохочуйте ранній інтерес: Ініціативи щодо залучення дівчат до кібербезпеки та STEM з раннього віку мають вирішальне значення. Створюйте освітній контент і програми, які є інклюзивними та привабливими для дівчат, а також усувають стереотипи та упередження в суспільстві та ЗМІ.

Реформувати освіту: школи та університети повинні прийняти інклюзивні навчальні програми та методи навчання, які заохочують участь усіх статей. Збільшення видимості жіночих моделей для наслідування в освіті з кібербезпеки та надання стипендій і можливостей для жінок також може допомогти подолати розрив.

Змініть культуру на робочому місці: організації в галузі кібербезпеки повинні активно працювати над створенням інклюзивної культури на робочому місці, яка цінує гендерну різноманітність. Це включає впровадження політики проти дискримінації та домагань, просування жінок на керівні посади та надання наставництва та можливостей кар'єрного розвитку для жінок.

Збільшення видимості та мережевих контактів: підвищення видимості жінок у сфері кібербезпеки через ЗМІ, конференції та керівні посади може надихнути більше жінок приєднатися до цієї сфери. Стимулюйте мережі та спільноти для

жінок у сфері кібербезпеки для надання підтримки, наставництва та можливостей розвитку кар'єри.

Сприяти адвокації та змінам політики: уряди та індустріальні організації можуть відігравати певну роль у сприянні гендерному різноманіттю в кібербезпеці через політику, нормативні акти та ініціативи, які заохочують залучення та просування жінок.

Кинувши виклик стереотипам, усунувши освітні та робочі бар'єри та підвищивши видимість жінок у цій галузі, ми можемо розпочати вирішення цієї невідповідності. Це не лише питання чесності та справедливості, але й стратегічний імператив для індустрії кібербезпеки, яка отримає величезну користь від повної участі жінок. Незалежно від того, що вони непропорційно дивляться програми чи читають теми, які викликають інтелектуальну цікавість, дані говорять нам, що жінки просто кращі в цьому, ніж чоловіки.

Прийняття різноманітності та сприяння інклюзивному середовищу збагатить сферу кібербезпеки ширшим спектром перспектив, навичок та інновацій, що зробить наш цифровий світ більш безпечним». ***(Steve King. Why Are There Fewer Women Than Men in Cybersecurity? // Information Security Media Group, Corp. (https://www.databreachtoday.com/blogs/are-there-fewer-women-than-men-in-cybersecurity-p-3584?utm_source=flipboard&utm_content=other). 15.03.2024).***

***

«У нещодавньому опитуванні, проведеному компанією Genetec, 36% респондентів у всьому світі сказали, що вони хочуть інвестувати в інструменти, пов'язані з кібербезпекою, щоб покращити своє середовище фізичної безпеки протягом наступних 12 місяців. У галузі, де кібербезпека не завжди була на першому місці, результати опитування показують, що респонденти починають усвідомлювати, що ці кіберзагрози реальні, а їхні системи фізичної безпеки є потенційною платформою для кібератак.

Використання пристроїв IoT допомогло організаціям покращити безпеку та контролювати діяльність у великих розподілених просторах. Однак разом із

перевагами підключення, доступності, мобільності та обміну даними з'являються ризики для кібербезпеки. Такі пристрої, як камери відеоспостереження, зчитувачі контролю доступу та панелі сигналізації, можуть забезпечити точку входу для отримання доступу до мереж великих і малих підприємств через їхні системи фізичної безпеки.

Захист цих пристроїв має першочергове значення, а нові стратегії керування доступом до цих пристроїв є критично важливими. Компанії все більше усвідомлюють важливість проактивного захисту від кіберзагроз і потенційної вразливості своїх пристроїв IoT.

Що можуть зробити організації, щоб зменшити загрози кібербезпеці?

Бути проактивним – це перша лінія захисту. Нижче наведено деякі міркування, які слід враховувати, намагаючись захистити свої системи від загроз кібербезпеці, а також дотримуватися стандартів і законів кібербезпеки.

1. Співпрацюйте з постачальником фізичної безпеки, для якого кібербезпека є головним пріоритетом

Виберіть постачальника фізичної безпеки, який інвестує значні кошти в кібербезпеку. Є кілька запитань, які допоможуть визначити, чи вживають вони необхідних заходів кібербезпеки. Наприклад, чи сертифіковані вони третьою стороною? Чи відповідають вони SOC2? Чи мають вони сертифікат ISO 27001? Чи використовують вони найкращі практики IT-безпеки?

Подумайте про те, щоб вибрати постачальника фізичної безпеки, який робить кібербезпеку пріоритетом як підхід зверху вниз у всьому, що вони роблять. Це включатиме спеціальні групи або відділи з кібербезпеки та партнерство з постачальниками, які поділяють такий самий рівень відданості кібербезпеці.

Деякі заходи кібербезпеки важко реалізувати в масштабі, наприклад, оновлення мікропрограми або зміна паролів. Компанія, яка займається кібербезпекою, допоможе вам розробити правильну позицію кібербезпеки для масштабування. Вони можуть перевірити своїх постачальників і партнерів пристроїв Інтернету речей, щоб переконатися, що вони мають зрілість і довговічність, щоб задовольнити ваші потреби в кібербезпеці як зараз, так і в міру

зростання вашої організації. Так само вони будуть співпрацювати з постачальниками, які поділяють те саме бачення важливості кібербезпеки.

2. Розгляньте рішення з вбудованими засобами кібербезпеки

Незважаючи на те, що система фізичної безпеки може опинитися під загрозою, існує багато способів додатково зменшити ризик зловмисних атак. Вибір рішення вимагає від компаній визначити, чи рішення розроблено з урахуванням безпеки та має вбудовані засоби кібербезпеки. Коли продукт розроблено, створено, закодовано та перевірено з безпекою за замовчуванням, такі важливі функції, як автентифікація, авторизація, шифрування та конфіденційність, вбудовані в систему. Ці заходи також гарантують, що лише ті, хто має встановлені привілеї, зможуть отримати доступ до вказаних активів, даних і програм.

Автентифікація – процес автентифікації користувача є першим рівнем керування ідентифікацією. Це запобігає потраплянню ваших даних у чужі руки. Сучасна багатофакторна автентифікація (MFA) перевіряє особу користувача, тому лише схвалені користувачі можуть отримати доступ до інформації.

Авторизація – авторизація допомагає визначити права доступу особи чи організації. Адміністратор організації може визначати права різних осіб і налаштовувати більш-менш обмежувальні привілеї доступу залежно від їхніх ролей і рівня доступу, якого вони намагаються досягти.

Шифрування – шифрування захищає конфіденційність даних компанії як під час передачі, так і під час зберігання. Коли дані зашифровані, вони стають непридатними для використання, якщо до них не звернуться авторизовані користувачі. Шифрування не може бути ефективним без автентифікації, яка гарантує, що ви надаєте доступ до своїх даних авторизованим користувачам. Якщо ваш постачальник фізичної безпеки має вбудоване шифрування, конфіденційні дані захищені за умовчанням.

Конфіденційність за задумом – немає компромісу, коли йдеться про максимальну конфіденційність і безпеку. Рішення безпеки, які пропонують захист конфіденційності за проектом, дозволяють компаніям мати більше контролю над своїми даними, щоб відповідати нормам і безпечно зберігати ці дані. Постачальник

послуг фізичної безпеки може допомогти своїм клієнтам визначити, хто має права доступу до конфіденційного відеоматеріалу, не перешкоджаючи деталям, необхідним для завершення розслідування.

3. Зведіть до мінімуму вразливості, перейшовши до гібридного або хмарного підходу

Перенесення вашої фізичної безпеки в хмару або використання гібридного підходу може ще більше знизити ризики вашої кібербезпеки. Сучасні хмарні системи включають багато рівнів кібербезпеки, розроблених не тільки для захисту від зловмисників, але й від помилок людини.

Перехід до хмари також допомагає розділити відповідальність за кібербезпеку з вашим провайдером хмари. Постачальники, які вживають передових заходів кібербезпеки, часто пропонують можливість оптимізувати технічне обслуговування та оновлення, що має вирішальне значення для забезпечення безпеки систем. Використовуючи гібридне або хмарне рішення, ви завжди матимете доступ до найновіших вбудованих функцій кібербезпеки, включаючи елементи керування конфіденційністю, надійну автентифікацію користувачів і різні інструменти моніторингу стану системи. Щойно останні версії та оновлення стануть доступними, їх буде негайно надіслано у вашу систему. Це допомагає вашим системам фізичної безпеки залишатися захищеними від вразливостей і активно контролюватися для виявлення та захисту від кібератак.

Де зустрічаються кібербезпека та фізична безпека

Щоб якнайкраще захистити вашу організацію від кібератак, фізична безпека та кібербезпека йдуть рука об руку. Системи фізичної безпеки з вбудованими функціями безпеки та конфіденційності можуть краще забезпечити захист людей, просторів і активів. Так само надійний постачальник може запропонувати командний підхід, щоб переконатися, що вся ваша екосистема розроблена, побудована та керована з урахуванням наскрізної безпеки вашої організації». ***(George Moawad. A proactive approach to cyber and physical security // TechDay (https://securitybrief.co.nz/story/a-proactive-approach-to-cyber-and-physical-security). 13.03.2024).***

***

«Компанія Trustwave оприлюднила вичерпний звіт під назвою «Ландшафт технологічних загроз 2024: Брифінг Trustwave про загрози та стратегії пом'якшення», в якому висвітлюються унікальні виклики кібербезпеки, з якими стикається технологічний сектор. Звіт пропонує практичні ідеї та стратегії для лідерів у сфері кібербезпеки, наголошуючи на необхідності надійних заходів безпеки в умовах, де багато цінних даних та інтелектуальної власності.

Завдяки значному об'єму даних та інтелектуальної власності технологічний сектор став основною мішенню для кіберзагроз. Ці атаки можуть мати серйозні наслідки, скомпрометувати конфіденційну інформацію, компанії та суттєво підірвати довіру користувачів. Ця шкода поширюється за межі зламаної компанії, впливаючи на безпеку багатьох інших підприємств, які залежать від цих технологій.

Звіт є результатом масштабного дослідження Trustwave SpiderLabs, яке вивчало потік атак, використовуваних групами загроз, надаючи розуміння їх тактики, техніки та процедур. Технологічний сектор стикається з унікальним ландшафтом загроз, який підживлюється декількома факторами, зокрема, постійно розширюваною поверхнею атак. Це зростання зумовлене стрімкою популярністю постачальників програмного забезпечення як послуги (SaaS), розвитком хмарної інфраструктури та різким зростанням кількості взаємопов'язаних пристроїв, які часто ростуть із швидкістю, яка перевищує швидкість заходів безпеки.

Корі Деніелс, директор з питань інформації та безпеки (CISO) у Trustwave, зазначає, що постійні інновації, які просувають технології вперед, можуть бути контрпродуктивними. «Наше нове дослідження розкриває заплутану мережу небезпек, з якими стикається індустрія технологій. Навіть незначний пролом у безпеці може завдати шкоди компанії та спричинити каскадні збої в життєво важливих системах, на які ми покладаємось, включаючи внутрішні бізнес-операції, програмне забезпечення та продукти, яким довіряють клієнти, і інфраструктура, що

підтримує ланцюги поставок. Щоб мінімізувати ризики, випереджаючи загрози, безпека має бути вбудована на кожному етапі життєвого циклу технології».

У звіті Trustwave SpiderLabs представлено аналіз груп загроз та їхніх методів протягом усього циклу атаки, починаючи від початкової точки опори до вилучення. Особлива увага приділяється технологічній інфраструктурі та технологіям програмного забезпечення. Основні висновки звіту показують, що три групи програм-вимагачів (LockBit 3.0, Clop, ALPHV, також відомі як BlackCat) спричинили понад 60 відсотків заяв про атаки на технологічні організації. Існує значна кількість критичних систем і пристроїв: 12 мільйонів пристроїв, пов'язаних із технологічною індустрією, відкрито. Фішинг продовжує залишатися основною загрозою, оскільки майже 40 відсотків шкідливих PDF-файлів видаються під такі авторитетні бренди, як Geek Squad, PayPal і McAfee. У звіті також наголошується на зростаючій поширеності електронних листів, згенерованих штучним інтелектом, фішингу або компрометації бізнес-електронної пошти (BEC), а Trustwave SpiderLabs ділиться інформацією щодо їх виявлення.

Звіт Trustwave відіграє вирішальну роль у розпізнаванні поточних викликів і майбутніх загроз для ландшафту кібербезпеки технологічної галузі. Він слугує тривожним дзвіночком не лише для технологічних компаній, але й для всіх компаній, які покладаються на технології, підкреслюючи необхідність надійних комплексних заходів кібербезпеки для захисту конфіденційних даних і активів». ***(Sean Mitchell. Trustwave report unveils cybersecurity challenges in technology sector // TechDay (https://securitybrief.co.nz/story/trustwave-report-unveils-cybersecurity-challenges-in-technology-sector). 21.02.2024).***

***

«Цифровий світ, у якому ми живемо, неминуче призводить до кібератак, які становлять загрозу для багатьох компаній, незалежно від розміру чи сектору. Складність кібератак зростає, тому жодна організація не застрахована, однак вони можуть зменшити ризик, захистивши свої цінні активи та конфіденційні дані.

Одним із ефективних способів досягнення вищезазначеного є інвестування в навчання співробітників кібербезпеці.

Метою навчання з кібербезпеки є надання співробітникам необхідних навичок і знань для виявлення загроз і їх нейтралізації, що зменшить ризик витоку даних та інших кіберінцидентів.

Тут ми підкреслюємо, як тренінги з кібербезпеки для ваших співробітників можуть принести користь вашому бізнесу та чому це вкрай важливо для захисту вашої організації від кіберзагроз, які можуть призвести до згубних наслідків.

Статистика кібербезпеки у Великобританії

Опитування Cyber Breaches Survey 2023 показало, що 32% підприємств Великобританії постраждали від кібератак протягом останнього року. Він підкреслив значну загрозу кібератак для безпеки бізнесу. Ця цифра включає лише ті, про які було повідомлено, оскільки багато кібератак можуть статися без реєстрації. Також повідомлялося, що середня вартість однієї кібератаки для бізнесу становить 20 900 фунтів стерлінгів.

Ця цифра не включає шкоду, завдану репутації компанії, витрати на відновлення та емоційний вплив на залучених осіб.

Більше того, існують інші серйозні наслідки атаки, які можуть призвести до регулятивних штрафів і покарань відповідно до Законів про захист даних (DPA) 1998, 2018 років і Положення про конфіденційність та електроніку (PECR).

Компанії, які порушують GDPR, також можуть розраховувати на адміністративні штрафи в розмірі до 20 000 000 євро або до 4% від загального світового річного обороту за попередній фінансовий рік, що є вищим.

Незважаючи на ці ризики, багато компаній залишаються вразливими до них. У Великій Британії лише 6% підприємств мають сертифікат Cyber Essentials, і лише 1% мають Cyber Essentials Plus. Однак це пов’язано з недостатнім усвідомленням переваг цих кваліфікацій.

Пріоритет кібербезпеки має вирішальне значення для бізнесу, щоб усунути наслідки кібератаки. Високий відсоток компаній підкреслив, що досвід кібератак призводить до того, що компанії повинні інвестувати в достатню кібербезпеку.

Крім того, компанії повинні ознайомитися з перевагами таких сертифікатів, як Cyber Essentials і Cyber Essentials Plus, які можуть допомогти підвищити безпеку та зменшити ризик кібератак. Інвестуючи в кібербезпеку та отримуючи необхідні сертифікати, підприємства можуть уникнути регулярних штрафів, репутаційної шкоди та фінансових втрат.

Сертифікат Cyber Essentials

Якщо підприємства отримують сертифікат Cyber Essentials, вони можуть продемонструвати своїм клієнтам і партнерам зобов'язання щодо кібербезпеки, а також вжити необхідних заходів для захисту від кіберзагроз.

У процесі сертифікації компанії можуть розраховувати на доступ до оптимальних заходів IT-безпеки, таких як брандмауери, безпечна конфігурація, контроль доступу та захист від шкідливих програм, і їх впровадження. Це гарантує, що підприємства мають надійні процеси безпеки, таким чином зменшуючи ризик витоку даних та інших інцидентів кібербезпеки.

Крім того, компанії, які отримають сертифікат Cyber Essentials, можуть отримати нові можливості для бізнесу. Багато державних контрактів і тендерів вимагають від постачальників сертифікату Cyber Essentials, що робить його обов'язковим для виграшу таких контрактів.

Компанії також можуть бути включені до довіреного реєстру постачальників на веб-сайті NCSC, що також може допомогти потенційному клієнту перевірити облікові дані компанії щодо кібербезпеки, що може поставити їх попереду своїх конкурентів.

Жоден бізнес не має імунітету до кібербезпеки

По всій Великобританії були витоки даних, які вплинули на такі популярні компанії, як JD Sports, Virgin Media, WHSmith, LastPass, Uber тощо.

Так, навіть такі великі компанії, як Uber, вказують на те, що навіть найбільші та найвідоміші компанії не захищені від загроз.

У 2022 році в Uber стався злам, під час якого зловмисники придбали облікові дані співробітника Uber у темній мережі. Співробітник увімкнув MFA, однак, щоб обійти це, зловмисник зв'язався з ним через WhatsApp, видаючи себе за члена

групи безпеки, і засипав людину повідомленнями MFA. Щоб позбутися цього, співробітник схвалив запит, який дозволив зловмиснику обійти всі заходи безпеки.

Це підкреслює, що навіть маніпулюючи однією особою в компанії, зловмисник міг отримати доступ до всіх внутрішніх даних, таких як Slack, Jira, HackerOne Reports та багато іншого. Це призвело до того, що особиста інформація понад 57 мільйонів користувачів Uber була скомпрометована.

Durham Johnston Comprehensive School також зазнала витоку даних на початку 2023 року. Сумнозвісна банда програм-вимагачів Vice Society змогла викрасти конфіденційну інформацію, що призвело до підтвердження ICO, що вона розслідує інцидент, і це призвело до штрафів GDPR.

Причини кібератак на бізнес

Кібер-зловмисники використовують різні методи, зокрема зловмисне програмне забезпечення, фішинг, соціальну інженерію та інші методи, щоб отримати доступ до конфіденційної інформації, порушити операції або завдати шкоди репутації компанії.

Мотиви для атак можуть бути різними, включаючи фінансову вигоду, політичні чи ідеологічні мотиви та навіть особисту помсту, яку зловмисник може мати на бізнесі. Кібератаки на бізнес стають все більш поширеними через зростаючу залежність від цифрових технологій та Інтернету, тому підприємствам необхідно інвестувати в заходи кібербезпеки для запобігання та пом’якшення таких атак.

Найпоширеніші кіберзагрози:

Порушення даних

Фішингові листи

Крадіжка інтелектуальної власності

програми-вимагачі

Соціальна інженерія

Корпоративне шпигунство

Як вони можуть статися?

Погана практика пароля

Відсутність багатофакторної автентифікації (MFA)

Неправильна конфігурація безпеки

Використання незахищених мереж

Недостатня обізнаність співробітників щодо кібербезпеки

Одним із факторів, що найбільше сприяють кібератакам на бізнес, є людська помилка. Багато атак, як-от фішинг і атаки соціальної інженерії, успішно покладаються на помилку людини. Співробітники можуть ненавмисно натиснути посилання або завантажити вкладені файли, які містять зловмисне програмне забезпечення, або піддатися тактиці соціальної інженерії, яку використовують зловмисники.

Відсутність навчання з питань безпеки може збільшити людські помилки через недостатню обізнаність щодо кібербезпеки або необережні дії, як-от використання ненадійних паролів або надання облікових даних для входу.

Тут йдеться не лише про інвестиції в технологічні рішення безпеки, які зменшують ризики кібербезпеки, а й пропагують важливе навчання та оптимізацію передових IT-практик. Це допомагає створити культуру обізнаності про безпеку та пильності, щоб мінімізувати ризик людської помилки.

Що включає навчання з кібербезпеки?

Інвестування в навчання з питань кібербезпеки є ефективним способом допомогти окремим особам і організаціям захистити себе від кібератак.

Якщо співробітники та користувачі ознайомлені з ризиками та найкращими методами, пов’язаними з онлайн-безпекою, навчання може допомогти запобігти кібератакам, витоку даних та іншим загрозам безпеці.

Безпека паролів, фішинг електронної пошти, зловмисне програмне забезпечення та тактика соціальної інженерії зазвичай розглядаються в рамках навчальної програми.

Запобігання загрозам може привести до підвищення обізнаності про їх існування та надання практичних порад щодо їх усунення. Окремі особи та організації можуть розробити сильнішу позицію безпеки та зменшити свою вразливість до кібератак.

Крім того, регулярні тренінги з кібербезпеки допоможуть вашим співробітникам і користувачам зберегти її пріоритетність, а також сприятимуть розвитку культури обізнаності про безпеку в усій організації, особливо коли ви отримаєте нових керівників.

Висновок

Навчання з кібербезпеки допоможе вашій організації:

- Отримайте краще розуміння ландшафту загроз.
- Покращте обізнаність працівників щодо безпеки.
- Дізнайтеся, як застосовувати ефективні заходи протидії онлайн-загрозам.
- Отримайте показник рентабельності інвестицій (ROI), порівнявши кількість інцидентів до та після навчання з кібербезпеки.
- Продемонструйте свою відданість захисту даних клієнтів, а також збереженню та покращенню репутації свого бренду серед клієнтів і партнерів.
- Кращий захист вашого бізнесу та активів.
- Уникніть сплати штрафів за непрохідність аудиту, досягнувши галузевої відповідності.
- Покращуйте свої можливості реагування на інциденти у разі будь-яких проблем.

Результат:

- Мінімізація людських помилок, що веде до підвищення продуктивності співробітників.
- Зниження ризиків, пов’язаних з помилками або недбалістю співробітників.
- Дайте своєму персоналу більше володіння кібербезпекою.
- Підвищуйте моральний дух і впевненість вашого співробітника.
- Звільніть час для кіберекспертів, щоб зосередитися на більш складних питаннях.

Це також приносить користь персоналу поза роботою, оскільки вони можуть запровадити культуру безпеки у своєму повсякденному житті.

Культура безпеки з найкращими практиками, коли люди можуть вільно ділитися будь-якими проблемами чи занепокоєннями щодо кібербезпеки, є

важливою метою керівників інформаційної безпеки (CISO)». ***(Stephen Kellie. How to Protect Your Data With Cyber Security Training // FE News (https://www.fenews.co.uk/skills/how-to-protect-your-data-with-cyber-security-training/). 19.03.2024).***

***

«Хакерська індустрія не сповільнюється, це точно. Але десь у безкінечній грі в хакерів ми втратили з поля зору, як ми сюди потрапили.

Остання подія на фронті безпеки полягає в тому, що зловмисники дедалі частіше відмовляються від зловмисного програмного забезпечення як основного способу зламу мереж. Їм швидше й ефективніше зосередитися на крадіжці даних облікового запису, використанні вразливостей програмного забезпечення або атаці через ланцюг постачання програмного забезпечення.

Зрештою, навіщо грабіжнику намагатися зламати замок, якщо він може просто пройти через незачинені двері або залізти через відкрите вікно.

Зловмисникам дешевше та легше, ніж будь-коли, отримати облікові дані з мінімальними зусиллями. Особливо це стосується хмарних платформ; за останні кілька років виникла ціла кримінальна індустрія у формі брокерів доступу, які продають на аукціоні дані для входу та інші облікові дані іншим зловмисникам.

Оскільки хмарна інфраструктура стає дедалі складнішою та життєво важливою для бізнесу, існує цілком реальний ризик того, що поєднання поганої безпеки та розумних хмарних зловмисників створить неймовірно вороже середовище для більшості галузей.

У сфері кібербезпеки клієнт завжди помиляється

Організації не так часто чи добре виконують виснажливу роботу з виправлення недоліків безпеки. І, так, як ми бачили, ланцюжки поставок програмного забезпечення можна дуже легко зламати. Але в усьому цьому одне фундаментальне питання залишається непоставленим; хто насправді повинен нести провину, коли щось йде не так?

Чи звинувачувати ми нещасливого, перенапруженого працівника, який натискає правдоподібне повідомлення з проханням оновити свій пароль? Можливо, це помилка технічної команди, яка не взялася за сізіфове завдання виправити свої системи чи навчити своїх користувачів бути підозрілими до всього. Можливо, ви можете звинуватити IT-директора, оскільки він не міг дозволити собі провести аудит безпеки, або генерального директора, який урізав бюджет безпеки.

Хоча це правда, що на всіх залучених осіб, ймовірно, можна приписати певний рівень провини, зазвичай найбільше лягає на IT-команду та кінцевих користувачів. Саме вони найбільше намагаються робити правильні речі, не маючи волі.

Реальність така, що клієнтам дуже важко визначити, безпечна чи ні певна частина програмного забезпечення. Як зазначають технічні консультанти Білого дому з Офісу національного кібердиректора, це проблема, яка існує десятиліттями. Відсутність показників значно ускладнює безпеку.

«Виробники програмного забезпечення не мають достатнього стимулу виділяти відповідні ресурси для безпечної розробки, а їхні клієнти не вимагають вищої якості програмного забезпечення, оскільки вони не знають, як її виміряти», — йдеться в новому звіті.

Може здатися дивним, що Білий дім втручається, але це відображає ставки, на які ми граємо. Правильна безпека IT зараз є питанням національного значення.

Ті, у кого найширші плечі, повинні нести найбільший тягар

Якщо ми хочемо виправити системні проблеми безпеки в програмному забезпеченні, нам потрібно по-новому поглянути на те, хто насправді відповідальний. Мені важко згадати будь-яку іншу галузь, де покупці та користувачі продукту змушені витрачати стільки часу, щоб виправити та виправити його самостійно.

Звичайно, технічні компанії мають стимули продавати своє програмне забезпечення якнайшвидше – класична ідея постачати мінімальний життєздатний продукт є основним принципом індустрії технологій. Однак ідея про те, що програмне забезпечення завжди матиме недоліки, стало нормалізованою, а

виправляти їх – завдання клієнтів. Якщо кожне програмне забезпечення потребує постійного оновлення, компаніям, які купують програмне забезпечення, буде набагато важче оцінити, що створено добре, а що є цифровим швейцарським сиром.

Недостатньо лише звинувачувати компаній-розробників програмного забезпечення, ми також маємо змінити модель, щоб зробити безпеку більш важливою для їхньої бізнес-моделі. Як сказав колишній технічний директор NCSC у своєму прощальному блозі в 2022 році, «ми прямо очікуємо, що ці компанії керуватимуть нашими ризиками для національної безпеки через довірених осіб, часто навіть не повідомляючи їм».

Намагатися повністю керувати кібербезпекою, ігноруючи комерційний контекст постачальників, «не видається розумним», сказав він. Це може означати більше регулювання, більше стандартів і кращі способи вимірювання того, наскільки безпечним є програмне забезпечення, щоб усі ми могли краще вибирати, що купувати. Зробити безпеку більш актуальною для прибутку компаній, що займаються програмним забезпеченням, неминуче є частиною цього.

Як би ми це не робили, настав час перекласти більшу частину відповідальності на тих, хто справді створює програмне забезпечення, а не на тих, хто намагається продовжити свою роботу». ***(Steve Ranger. A robust cyber security industry requires software vendors to pull their weight – so why are customers working so hard? // Future US, Inc. (https://www.itpro.com/security/a-robust-cyber-security-industry-requires-software-vendors-to-pull-their-weight-so-why-are-customers-working-so-hard). 18.03.2024).***

***

«Знайти постачальника кібербезпеки може бути складно. Існує кілька доступних варіантів, і часто важко прогорнути маркетинговий матеріал, щоб справді оцінити, наскільки вони можуть задовольнити ваші конкретні вимоги.

В епоху дедалі складніших загроз штучного інтелекту та розвитку груп програм-вимагачів також може бути важко визначити, які ваші потреби в першу

чергу. Існує велика різниця між внутрішніми навичками безпеки на великому підприємстві та в меншій компанії, і ваші вимоги відображатимуть це.

Пошук правильного постачальника для ваших цілей може здатися складним, але за правильного підходу це можна зробити. Ось усе, що вам потрібно знати.

Що шукати в найкращому постачальнику засобів кібербезпеки

Обираючи постачальника, ви повинні шукати партнерство, а не просто закупівлю ліцензії, каже Льюїс Дьюк, керівник відділу аналізу загроз у Trend Micro. «Запитайте про їхню стратегію; це збігається з вашим? Наскільки вони комунікабельні та чи здатні вони допомагати вирішувати конкретні виклики у вашому секторі?»

Компанії повинні переконатися, що постачальники мають підтверджену репутацію та досвід у сфері кібербезпеки, каже Джошуа Паулус, керівник відділу безпеки та ідентифікації Intelliworx. Тим часом фірми, які працюють у строго регульованих секторах, таких як охорона здоров'я та фінанси, повинні переконатися, що постачальник має повне розуміння відповідних галузевих норм і вимог відповідності.

Шукайте сертифікати, зокрема ISO 27001, SOC2 та інші, які можуть бути актуальними у вашому секторі, каже Дьюк.

Однією з найважливіших послуг, яку може запропонувати постачальник засобів кібербезпеки, є моніторинг IT-майна вашого бізнесу, каже Льюїс Вест, керівник відділу кібербезпеки в кадровій фірмі Hamilton Barnes.

Наскільки комплексною буде ця послуга, залежить від пакету постачальника та ціни, яку ви готові заплатити. За його словами, стандартна пропозиція зазвичай включає забезпечення захисту та моніторингу протягом звичайних робочих годин. «Але якщо вам потрібен додатковий рівень обслуговування, доступні моделі за викликом, де за потреби надається підтримка».

Хороший постачальник кібербезпеки знадобиться час, щоб дізнатися про ваші проблеми та бізнес-операції, каже Пол МакЛетчі, консультант зі стратегії безпеки в Daisy. Будьте обережні з постачальниками, які негайно починають

просувати рішення, перш ніж вони ознайомляться з відповідними рухомими частинами у вашому бізнесі, каже він.

Недорогі випробування для постачальників кібербезпеки

Перш ніж звертатися до постачальника, перевірте, чи є у нього якісь варіанти для низького або безкоштовного початкового залучення, радить МакЛатчі. «Деякі надають вступне оцінювання безпеки безкоштовно або, принаймні, можуть бути відкритими для початкового семінару без зобов'язань».

Ви також повинні проявляти обережність, спілкуючись із постачальниками, які пропонують надто оптимістичний погляд на те, що їхні продукти чи послуги вирішать усі проблеми кібербезпеки вашої організації, каже МакЛатчі. «Ризик ніколи не можна повністю усунути, незалежно від того, наскільки фантастичним є запропоноване рішення».

Менше турбуйтеся про «приголомшливий штучний інтелект та віджети наступного покоління», а зосередьтеся на головному питанні: чи справді це рішення захистить мою організацію?», — каже Девід Корлетт, віце-президент із управління продуктами VIPRE Security Group. Він також рекомендує керівникам звернути увагу на незалежні агенції з тестування, такі як AV Comparatives або Virus Bulletin, які постійно документують методики тестування.

Постачальники часто говорять про переваги інтеграції своїх рішень. Однак такі пропозиції можуть бути химерними та не підвищити безпеку, каже він.

Багато постачальників будуть готові адаптувати свої послуги, каже Вест. «Завжди варто поговорити з ними, а не припускати, що вони суворо дотримуватимуться рекламованих пакетів».

Яким підприємствам потрібен постачальник засобів кібербезпеки?

Звичайно, не всім компаніям потрібен постачальник засобів кібербезпеки. За словами Веста, головна причина, через яку компаніям варто розглянути можливість використання такої системи, полягає в тому, щоб залучити команду експертів, які зможуть надавати постійну підтримку.

Якщо все ще не зрозуміло, краще почати зі стратегії управління ризиками для вашої існуючої системи безпеки, каже МакЛетчі. «Які системи та сервіси керують

щоденними бізнес-операціями? Який би був вплив, якби вони зазнали невдачі? Які найпомітніші кіберзагрози для організації? Ці та інші запитання можуть принаймні підштовхнути фірми до базового розуміння зрілості їхніх поточних можливостей безпеки».

Першим кроком для бізнесу є перевірка його інфраструктури, включаючи зовнішню мережу, яка, ймовірно, буде підключена до сторонніх хмарних сервісів, а також внутрішньої IT-інфраструктури, погоджується Самір Десаї, віце-президент із управління продуктами GTT. «Якщо виявлено потенційні ризики та больові точки, з якими неможливо впоратися всередині країни, одним із варіантів є звернення до постачальника послуг керованої безпеки (MSS P), який може залучити широкий спектр рішень кібербезпеки з досвідом і налаштувати їх відповідно до потреб унікальні потреби бізнесу».

Не вірте всьому, що вам говорять. Жоден постачальник не може забезпечити все необхідне, від брандмауерів і безпечної операційної системи до захисту кінцевих точок і електронної пошти, каже Корлетт. «Підприємства повинні остерігатися будь-якого постачальника, який стверджує, що робить все добре».

Постачальники кібербезпеки для малого та середнього бізнесу проти підприємств

Ваші потреби також залежатимуть від розміру вашого бізнесу. МСП, ймовірно, виграють від MSSP, які пропонують пакетні рішення та вирішують повсякденні завдання, каже Дьюк. Проте підприємства можуть вибрати кількох спеціалізованих постачальників залежно від своїх потреб у безпеці, додає він.

Також варто розглянути, скільки постачальників послуг безпеки вам потрібно, враховуючи вашу схильність до ризику, поверхню атаки та сектор, у якому ви працюєте.

МСП, як правило, не мають спеціального IT-персоналу чи технічного досвіду, доступного для великих компаній, тому важливо, щоб вони віддавали пріоритет постачальникам, які пропонують більш зручні рішення, говорить Паулюс. «Вони повинні запропонувати прості процеси розгортання та управління

без необхідності додаткового часу та ресурсів для запуску та запуску систем кібербезпеки».

Групи внутрішньої безпеки можуть вирішити проблему. Загалом компанії повинні мати внутрішню команду безпеки разом із постачальником засобів кібербезпеки через їхні різні навички, каже Вест. «Часто зовнішні постачальники забезпечують найбільшу цінність у моніторингу мереж і виявленні проблем і вразливостей, про які потім можна повідомити внутрішній команді, яка вирішить проблему».

Наявність внутрішньої групи безпеки може надати підприємствам кращий контроль над операціями, ніж зовнішній постачальник. Зрештою, вони найкраще розуміють IT-середовище своєї організації, каже Паулюс. «Але чого вони не можуть зробити, так це подолати всі ризики безпеки самостійно або гарантувати 100% безпеку від усіх кіберзагроз. Співпраця із зовнішніми постачальниками може допомогти компаніям покращити рівень безпеки та ефективно вирішувати проблеми». ***(Kate O'Flaherty. How to choose the best cyber security vendor for your business // Future US, Inc. (https://www.itpro.com/security/how-to-choose-the-best-cyber-security-vendor-for-your-business). 18.03.2024).***

***

«…У звіті Sophos «Майбутнє кібербезпеки в Азіатсько-Тихоокеанському регіоні та Японії» виявлено, що виснаження та втома є широко поширеними, причому дев’ять із 10 працівників страждають певним чином. Причини включають брак ресурсів і тривожну втому, що часто призводить до занепокоєння або незалученості співробітників.

Організації, опитані у звіті, визнають, що виснаження та втома сприяють зниженню продуктивності команди, успіху деяких кібератак і тому, що співробітники вирішують шукати нові ролі або повністю залишають галузь. ШІ називають однією з потенційних підтримок у майбутньому.

Вигорання серед кіберпрофесіоналів є проблемою, відомою роками в Азіатсько-Тихоокеанському регіоні

Вигорання в сфері кібербезпеки є загальновідомою проблемою. Ендрю Пейд, генеральний менеджер з оборонних операцій у Банку Співдружності Австралії, сказав, що після того, як понад два десятиліття тому перейшов у відділ кібербезпеки в Резервному банку Австралії, багато колег пішли через виснаження.

Дослідження, проведені в Австралії та Новій Зеландії за останні роки, надали докази цієї проблеми:

Дослідження 2023 року, проведене Cybermindz та Університетом Аделаїди за участю 119 кіберпрофесіоналів в Австралії, показало, що ці працівники отримали вищі оцінки за шкалою вигорання, ніж загальне населення, і в деяких випадках перевищували показники вигорання, з якими стикаються медичні працівники на першому місці.

Більше половини (54%) австралійських фахівців з кібербезпеки, які визнали стан готовності Mimecast до програм-вимагачів, повідомили, що кібератаки мають згубний вплив на їх психічне здоров'я, і майже чверть (22%) думали залишити свою поточну посаду.

Опитування Lacework, опубліковане в 2022 році, показало, що більша частка (57%) кіберпрофі в Австралії або шукає нових роботодавців, або розглядає можливість залишити галузь; 87% тих, хто хотів залишити галузь, назвали причиною вигорання від робочого навантаження.

Проблема вигоряння кібербезпеки раніше приховувалася

Джинан Бадж, керівник відділу дослідження безпеки та ризиків Forrester в Азіатсько-Тихоокеанському регіоні, написав, що до 2018 року « вигоряння» у сфері кібербезпеки обговорювалося «тихим і обережним пошепки», але публікація нових досліджень підняла дискусію в регіональних організаціях.

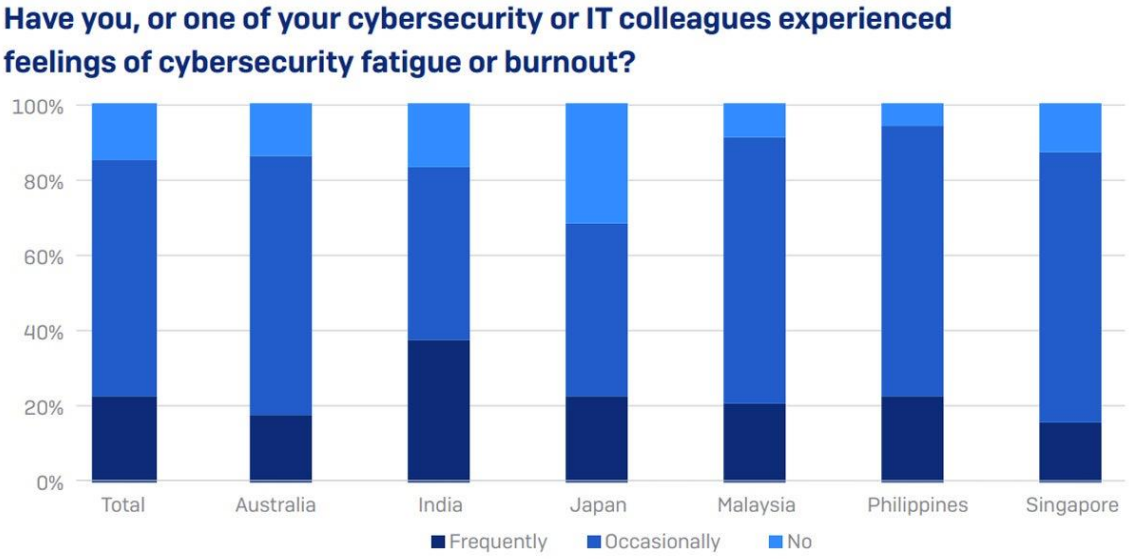
Опитування Sophos показує, що проблема широко поширена та зростає

Опитування «Майбутнє кібербезпеки в Азіатсько-Тихоокеанському регіоні та Японії», проведене компанією Technology Research Asia для Sophos, показало, що в регіоні широко поширені «вигоряння» та «втома» у сфері кібербезпеки. Також виявилося, що у 2024 році проблема погіршується, а не покращується.

Опитування показало, що 85% компаній відчувають втому та виснаження серед кібер- та IT-фахівців; 23% стикалися з проблемою «часто», а 62% «іноді» (мал. А).

Дев'ять із 10 (90%) компаній заявили, що протягом останніх 12 місяців зросли виснаження та втома, причому 30% компаній сказали, що підвищення зросло «значно».

Там, де співробітники були опитані та відповідали безпосередньо, 90% усіх кібер- та IT-працівників Азійсько-Тихоокеанського регіону сказали, що на них негативно вплинули виснаження та втома.



Малюнок А: 85% компаній сказали, що вони відчували виснаження та втому серед співробітників відділу кібербезпеки та IT у всьому регіоні. Зображення: Sophos.

Індія серед країн Азіатсько-Тихоокеанського регіону найбільше постраждала від вигорання

Вигорання та втома найбільш поширені в Індії, де 37% організацій заявили, що з цією проблемою стикаються співробітники «часто», що вище середнього регіонального показника (23%). Індія також мала найвищі (48%) показники «значного» зростання виснаження та втоми за останній рік.

Основні причини професійного вигорання в азіатсько-тихоокеанській професії кібербезпеки

Згідно зі звітом Sophos, існує п’ять головних причин вигорання в регіоні (мал. В):

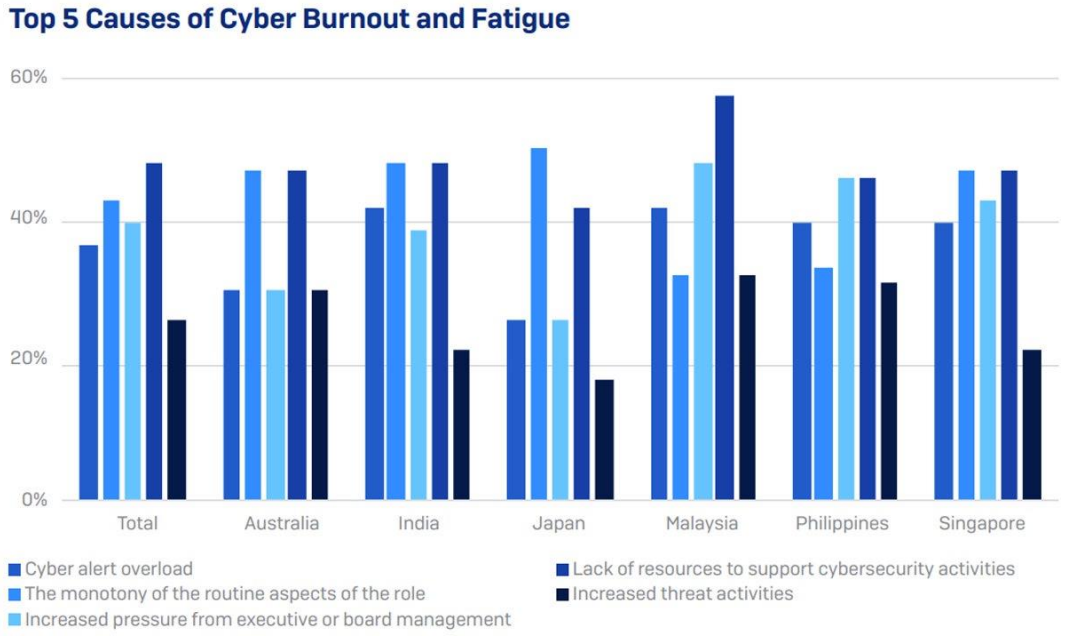
Відсутність ресурсів для підтримки діяльності з кібербезпеки та персоналу.

Поєднання монотонної рутини зі складними моментами діяльності.

Посилення тиску з боку правління та виконавчого керівництва в регіоні.

Перевантаження сповіщень від різноманітних інструментів і систем кібертехнологій.

Збільшення активності загроз, що створює «постійне» середовище.



Малюнок Б. Перевантаження кібернетичними оповіщеннями та брак ресурсів є одними з факторів, які сприяють втомі та виснаженню кібербезпеки в регіоні. Зображення: Sophos.

Вигорання має наслідки для окремих людей і організацій

Співробітники відділу кібербезпеки та організації піддаються ризику, коли відбувається вигорання. У звіті Sophos зазначається, що в час дефіциту кібернавичок і дедалі складнішого середовища загроз стабільність і продуктивність співробітників є важливими для захисту організацій.

Індивідуальна ефективність кібербезпеки погіршилася через проблему вигорання

Люди відчувають сильну суміш провини, апатії, відчуженості та тривоги через виснаження та втому. Наприклад, Sophos виявила, що 41% професіоналів із синдромом вигоряння вважали, що вони недостатньо старанні у своїй роботі, а 34% відчували підвищений рівень тривоги, якщо зазнали порушення чи атаки.

Крім того, 31% відчували цинізм, відстороненість і апатичність щодо кібердіяльності та обов'язків, тоді як 30% заявили, що виснаження та втома спонукають їх або піти у відставку, або змінити кар'єру. Крім того, 10% відчували провину за те, що вони не могли зробити більше для підтримки діяльності з кібербезпеки.

Роботодавці бачать зниження продуктивності, більше порушень і плинність персоналу

Індивідуальні проблеми продуктивності призводять до ризиків для роботодавців. Sophos виявила, що ключовими впливами є:

Втрата 4,1 години на тиждень серед кібер- та IT-професіоналів через виснаження та втому. Філіппіни та Сінгапур зазнали найбільшого зниження продуктивності в регіоні через цю проблему, втрачаючи 4,6 години та 4,2 години на тиждень відповідно.

У 17% організацій було визначено, що виснаження чи втома сприяли або були безпосередньо відповідальними за порушення кібербезпеки. Крім того, 17% виявили, що проблема пов'язана з уповільненням часу реагування на інциденти безпеки.

Близько 23% обороту в сфері кібербезпеки організації пояснюють виснаженням і втомою. Величезні 38% звільнень були пов'язані з проблемою в Сінгапурі, тоді як 28% малайзійських організацій потребували «перейти» на роботу через стрес і виснаження.

Роботодавці реагують на проблему вигоряння кібербезпеки

Дослідження Sophos показують, що загалом роботодавці не ігнорують зростаючу проблему вигорання. У всьому регіоні 71% опитаних компаній заявили, що вони запровадили та активно надають послуги консультування щодо стресу фахівцям із IT та кібербезпеки.

Це не означає, що організаційна культура завжди відкрита для вирішення проблеми. В Австралії лише 40% працівників, які порушили це питання перед своїм роботодавцем, отримали позитивну відповідь, у порівнянні з 83% працівників в Індії та 73% у Малайзії.

Технології можуть зіграти певну роль у боротьбі з професійним вигоранням

У звіті дослідження Sophos говориться, що, незважаючи на втому від тривоги, технології відіграють значну роль у майбутньому. У звіті йдеться про те, що покращена автоматизація та використання набору рішень для кібербезпеки зі штучним інтелектом, що розвивається, можуть допомогти пом'якшити деякі аспекти причин вигорання.

У Sophos дійшли висновку, що втома та виснаження є критичними проблемами, які негативно впливають на працівників і можливості компанії в Азіатсько-Тихоокеанському регіоні.

«Знижена концентрація уваги та вищий рівень уразливості, а також вищий рівень кібербезпеки та відтік IT-співробітників є реальними проблемами для багатьох організацій», — йдеться у звіті». ***(Ben Abbott. Sophos: Cyber Security Professional Burnout Is Widespread, Creating Risk for APAC Organisations // TechnologyAdvice (https://www.techrepublic.com/article/sophos-report-cybersecurity-burnout-apac/). 15.03.2024).***

***

«Сучасні технології революціонізують спосіб ведення бізнесу в різних галузях, завдяки чому більше робочих процесів і процесів стають оцифрованими, ніж будь-коли раніше. Це відкриває простір для більш спрощених і ефективних операцій, але, на жаль, це також відкриває потенціал для кіберзлочинності, щоб порушити корпоративний ландшафт. І оскільки кіберзагрози стають більш масштабними та складнішими, ніж будь-коли, розширення можливостей вашої робочої сили через навчання з кібербезпеки тепер є необхідністю.

Навчання з кібербезпеки не слід розглядати просто як натискання на відтворення серії відео. Оскільки злочинці постійно знаходять нові способи порушити заходи безпеки, це вимагає постійного обговорення та регулярних інструктажів щодо останніх рекомендацій. Це допоможе перетворити співробітників на більш пильних охоронців вашої конфіденційної ділової інформації, захищаючи кожен аспект вашої цифрової присутності.

У цій публікації в блозі ми розшифруємо найважливіші способи, за допомогою яких навчання кібербезпеці може загострити інстинкти ваших співробітників, дозволяючи їм виявляти – і зупиняти – загрози, перш ніж вони переростуть у кризу. Незалежно від того, чи ви новачок, чи міжнародний конгломерат, освічені співробітники є вашим найсильнішим союзником у невпинній боротьбі з кіберзагрозами.

Розуміння різних типів загроз

Кіберзагрози мають різні форми, і сучасні злочинці використовують все більш витончені методи, щоб обманом змусити людей надати цінну інформацію. Коли співробітники належним чином навчені різним типам небезпек, з якими зазвичай стикається бізнес, вони краще розумітимуть, як кібератаки можуть проявлятися в реальному світі. Навчання надасть вашій команді не лише інформацію про те, «що», а й «чому» та «як» потенційних кібератак. Приклади поширених ризиків кібербезпеки:

Фішинг. Фішингові атаки найчастіше проявляються у вигляді електронних листів, текстових повідомлень або веб-сайтів, де жертвам пропонується поділитися особистими даними або випадково завантажити шкідливі віруси.

Відмова в обслуговуванні. Злочинці, які часто називають DoS-атаками, використовуватимуть цей тип атак, щоб націлитися на мережі компанії, щоб порушити процеси та робочі процеси. Вони можуть заважати працівникам виконувати повсякденні завдання, що коштує бізнесу часу та грошей. Мотиви такого типу кіберзлочинності можуть включати політичні плани, викуп від холдингових компаній або вплив на репутацію бізнесу.

Людина-посередині. Цей нав’язливий стиль атаки дозволить злочинцям прослуховувати внутрішні комунікації, розташовуючись фактично між двома сторонами. Це може призвести до того, що хакери зможуть безпосередньо почути та викрасти конфіденційну інформацію, якою можна маніпулювати для власної вигоди.

Визначення червоних прапорців

Коли співробітники дізнаються про те, як можуть виглядати різні атаки, вони зможуть краще помітити потенційні тривожні прапорці, перш ніж вони переростуть у більш серйозну проблему. Навчання співробітників здатності виявляти ці червоні прапорці та негайно повідомляти про них є найефективнішим способом посилити цифровий захист вашої компанії, незалежно від того, працює ваша команда в офісі чи у віддалених місцях.

Є багато поширених проблем, які можуть свідчити про те, що щось не так. Часто співробітники помічають орфографічні помилки чи друкарські помилки, або злочинці відчувають явне відчуття терміновості. Крім того, важливо звертати особливу увагу на номери телефонів, адреси електронної пошти та імена, додані до будь-яких повідомлень, які ви отримуєте. Якщо є будь-які сумніви щодо того, чи людина на іншому кінці може бути не тим, за кого себе видає, завжди краще покласти трубку та зв’язатися з нею безпосередньо за контактними даними, які ви зібрали самостійно.

Створення культури безпеки

Коли кібербезпека стає постійною темою для обговорення та навчання у вашій організації, це сприяє створенню культури, яка надає пріоритет безпечним практикам. Ця культурна зміна означає, що підтримка та оптимізація заходів безпеки стає спільною відповідальністю, коли кожен член команди бере активну участь у захисті активів компанії. Це дає змогу всім – від найвищого керівництва до новачків – приймати обґрунтовані рішення, коли вони стикаються з потенційними загрозами, при цьому кожен член бізнесу відіграє вирішальну роль.

Свого часу кібербезпека могла розглядатися як просто відповідальність IT-відділу або найвищого керівництва. Однак завдяки ефективному навчанню

кібербезпека починає проникати в кожну команду та відділ у бізнесі, що робить обов'язком кожного дотримуватися належних практик. Це приносить користь не тільки членам команди, але коли безпека стає ключовою частиною культури вашої компанії, клієнти та потенційні замовники отримують впевненість у тому, що ви надійна організація, що покращує імідж вашого бренду.

Регулярні тренінги допомагають закріпити найкращі практики, які мають стати другою натурою для кожного працівника. До них належать використання надійних паролів, розпізнавання підозрілих електронних листів і розуміння протоколів компанії для обробки конфіденційних даних. Вкоренивши ці звички, ваша робоча сила може діяти як згуртований охоронець від кібервторгнень.

Використання реальних життєвих сценаріїв

Включення сценаріїв із реального життя до вашого навчання є одним із найефективніших способів навчання працівників. Кіберзлочинці рідко використовують шаблонний підхід, намагаючись скомпрометувати захист компанії, і ці вправи можуть допомогти контекстуалізувати абстрактні загрози, роблячи їх більш відчутними та легшими для розуміння, коли вони з'являються насправді. Коли співробітники бачать, як їхні дії можуть безпосередньо вплинути на безпеку організації, вони, швидше за все, серйозно сприймуть свою роль в управлінні кібербезпекою.

Кіберзагрози постійно розвиваються, а це означає, що навчання вашої робочої сили також має розвиватися. Постійне навчання гарантує, що ваша команда буде в курсі останніх тенденцій безпеки, інструментів і передових методів. Це готує їх передбачати нові загрози та швидко реагувати на них.

Взяти на себе зобов'язання постійно навчатися

Оснащення вашої робочої сили навчанням з кібербезпеки допоможе захистити ваш бізнес у майбутньому. Це не тільки сприяє активній позиції щодо потенційних загроз, але й зміцнює загальну безпеку організації. З огляду на такі високі ставки для великих і малих компаній, інвестиції в безперервну освіту їхніх співробітників у сфері безпеки є не просто стратегічним кроком – це дуже важливий». ***(Alex Trafford, Thomas Murray. How does cyber security training equip***

your workforce to spot threats? // HR DIRECTOR (https://www.thehrdirector.com/cyber-security-training-equip-workforce-spot-threats/). 21.03.2024).

***

«Кібербезпека стоїть на передньому краї пріоритетів бізнесу, захищаючи від постійно зростаючої загрози кібератак, націлених на конфіденційні дані та критичну інфраструктуру. У сучасному взаємопов'язаному світі наслідки порушення виходять за межі втрати даних, впливаючи на репутацію бренду та довіру клієнтів і потенційно спричиняючи значні фінансові штрафи.

Оскільки кіберзлочинці використовують все більш витончені методи, потреба в надійних заходах кібербезпеки стає все більш очевидною. Компанії, незалежно від розміру чи сектору, знаходяться в постійній гонці за адаптацією та захистом своїх цифрових екосистем. Інтеграція передових технологій і стратегічних методів кібербезпеки більше не є можливістю, але необхідна для забезпечення безперервності роботи та дотримання нормативних вимог.

Інновації в кібербезпеці захищають від поточних загроз і передбачають майбутні вразливості, що робить їх критично важливою інвестицією для будь-якого бізнесу, який прагне процвітати в цифровій економіці. Ця стаття розглядає роль технологій і людського розуміння в посиленні заходів кібербезпеки, пропонуючи цінні вказівки для компаній, які прагнуть захистити свої цифрові домени.

Еволюція кіберзагроз

Як уже згадувалося, кіберзагрози суттєво трансформувалися, вимагаючи динамічної та обґрунтованої стратегії реагування. Розуміння цих змін є першим кроком до надійного захисту. Компанії повинні проводити регулярні оцінки безпеки, щоб виявити потенційні вразливості та бути в курсі останніх типів кібератак.

Впровадження передових систем виявлення загроз, які використовують аналіз поведінки, може допомогти виявити аномалії, що вказують на кіберзагрозу, перш ніж вона завдасть шкоди. Навчання та навчання персоналу щодо останніх

кіберзагроз і тактик фішингу також є важливими, оскільки поінформовані співробітники є першою лінією захисту від кібератак.

Передові технології, що формують кібербезпеку

Впровадження штучного інтелекту (AI) і машинного навчання (ML) дає компаніям перевагу в запобіганні кіберзагрозам і боротьбі з ними. Компанії повинні розглянути можливість інтеграції рішень безпеки на основі ШІ, які можуть аналізувати шаблони, прогнозувати потенційні загрози та автоматизувати реагування на інциденти безпеки.

Технологія блокчейн пропонує ще один рівень безпеки, особливо для компаній, які покладаються на цілісність транзакцій і даних. Впровадження блокчейну може посилити захист даних шляхом створення записів, захищених від підробки. Тим часом, оскільки квантові обчислення стають доступнішими, компанії повинні залишатися попереду, досліджуючи квантово-стійкі методи шифрування для захисту конфіденційної інформації від майбутніх загроз.

Роль людського досвіду

Хоча технології відіграють вирішальну роль, людський фактор залишається незамінним у кібербезпеці. Компанії повинні інвестувати в безперервний професійний розвиток своїх команд з кібербезпеки, гарантуючи, що вони мають досвід для управління складними кіберзагрозами та реагування на них.

Розвиток культури безпеки в організації також є життєво важливим. Це передбачає регулярне навчання співробітників, зосереджене на передових практиках захисту даних і розпізнавання загроз. Компанії також можуть отримати вигоду від співпраці з консультантами з кібербезпеки, щоб отримати зовнішню інформацію та стратегії, адаптовані до їхніх конкретних потреб.

Покращення кібербезпеки в бізнесі

Для ефективного зміцнення кібербезпеки компаніям пропонується прийняти комплексну стратегію, яка поєднує технологічні досягнення з ретельним стратегічним плануванням. В основі цього підходу лежить безпечне керування передачею файлів — важлива сфера, яку часто використовують кіберзловмисники. Застосування програмного забезпечення для керованої передачі файлів, подібного

до програми Progress, стає обов’язковим, забезпечуючи надійне рішення, яке захищає дані під час передачі та в стаціонарному стані, суттєво зменшуючи ризик несанкціонованого доступу та наступних порушень даних. Це кероване рішення для передачі файлів повинно мати можливість шифрувати дані як у стані спокою, так і під час передачі, забезпечуючи високий рівень безпеки конфіденційної інформації.

Крім того, впровадження багатофакторної автентифікації (MFA) у всіх цифрових інтерфейсах підвищує безпеку, вимагаючи кількох форм перевірки перед наданням доступу, тим самим додаючи істотний бар’єр проти спроб вторгнення. Оновлення програмного забезпечення та систем за допомогою регулярних оновлень і виправлень має вирішальне значення для усунення прогалин у безпеці та зміцнення захисту від нових загроз.

Виклики та міркування

Запровадження нових технологій кібербезпеки створює певний набір проблем, включаючи вартість впровадження та потребу в спеціальних навичках для керування цими системами. Компанії повинні зважити ці фактори та потенційну вартість кібератаки, часто виявляючи, що інвестиції в технології безпеки приносять дивіденди у вигляді захищених активів і довіри клієнтів.

Також необхідно враховувати етичні міркування, зокрема щодо ШІ та конфіденційності. Організації повинні забезпечити відповідність своїх заходів кібербезпеки правовим стандартам і поважати конфіденційність клієнтів, збалансовуючи потреби безпеки з етичними міркуваннями.

Заклик до дії: застосування інновацій у кібербезпеці

Як для компаній, так і для окремих осіб впровадження інновацій у сфері кібербезпеки не є обов’язковим — воно має важливе значення для виживання у все більш цифровому світі. Бути в курсі нових технологій і тенденцій кібербезпеки може допомогти організаціям передбачити й пом’якшити потенційні загрози. Інвестиції в кібербезпеку – це інвестиції в майбутнє бізнесу, збереження його діяльності, репутації та довіри клієнтів.

Оскільки кіберзагрози продовжують розвиватися, наші підходи до кібербезпеки також повинні розвиватися. Поєднання досвіду людини, що базується на передових технологіях, і проактивної стратегії формує основу ефективного кіберзахисту. Впроваджуючи інновації та приділяючи пріоритет безпеці, компанії можуть впевнено рухатися в епоху цифрових технологій, захищаючи свої активи та майбутнє.

Цей підхід до кібербезпеки, зосереджений як на технологіях, так і на людському досвіді, забезпечує комплексну стратегію для компаній, які прагнуть захистити свої цифрові ландшафти. Завдяки безперервному навчанню, інвестиціям у сучасні технології та вихованню культури обізнаності про безпеку організації можуть зміцнити свій захист від складних кіберзагроз сьогоднішнього та майбутнього. ***(Mark Edwards. Innovation in action: Technology's role in strengthening cybersecurity measures // AZ Big Media (https://azbigmedia.com/business/technology/innovation-in-action-technologys-role-in-strengthening-cybersecurity-measures/). 21.03.2024).***

***

«Незалежно від масштабу організації, кібератаки та інші інциденти кібербезпеки, такі як втрата даних або інциденти з торговцями/постачальниками, становлять значну загрозу для бізнесу в усьому світі. Швидкий пошук в Інтернеті легко ідентифікує поточні кібератаки проти корпорацій, що працюють у сучасній глобальній економіці, зокрема American Express і Change Health. Завдяки поширенню додатків, які використовують цілодобове з'єднання, ми опиняємося вплетеними в складний сценарій кіберзанепокоєння, що розвивається. З огляду на це, компанії повинні мати доступ до досвідчених професіоналів, які добре знаються на питаннях безпеки та конфіденційності даних.

За даними Allianz Risk Barometer, кіберінциденти, такі як атаки програм-вимагачів, витоки даних і збої в роботі IT, викликають найбільше занепокоєння для компаній у всьому світі в 2024 році. Перерви в бізнесі посідають друге місце в їх

звіті, що на одну сходинку від кіберінцидентів. Стихійні катастрофи (№3), зміни в законодавстві та регулюванні (№4) і макроекономічні зміни (№5) завершують п’ятірку найважливіших глобальних бізнес-ризиків на 2024 рік.

Не дивно, що дослідження висвітлює кібератаки та пов’язану з ними втрату даних як головний корпоративний ризик. З року в рік це занепокоєння перевершило інші серйозні ризики, такі як регуляторні проблеми, зміна клімату та загрози нестачі кваліфікованих працівників, і залишається стабільним. Кіберінциденти, які займають перше місце, просто відображають ескалацію загроз, спричинених кіберзлочинністю, а також глибокий фінансовий і репутаційний вплив на компанії та керівників.

У звіті Allianz Risk Barometer зазначено: «кіберзагрози постійно розвиваються, оскільки хакери та злочинці отримують доступ до нових технологій або знаходять нові способи використання старих уразливостей. Хакери починають використовувати мовні моделі на основі штучного інтелекту (ШІ), щоб збільшити швидкість і обсяг атак програм-вимагачів, а також створювати нове шкідливе програмне забезпечення та створювати дуже переконливі фішингові електронні листи та глибокі фейки. Такі атаки, ймовірно, поширяться протягом 2024 року».

Вплив пандемії COVID-19 продовжує загострювати вразливі місця, оскільки багато організацій перейшли на постійну або гібридну віддалену роботу, створивши сприятливий ґрунт для кіберзлочинців для проведення операцій. Крім того, людська помилка все ще є причиною більшості тригерів нульового пацієнта, які ми бачимо в ситуаціях щоденного реагування на інциденти, що дозволяє початкове вторгнення в мережу та робить навчання співробітників ключовим компонентом найкращих практик. Згідно з прогнозами, до початку наступного десятиліття лише діяльність програм-вимагачів обійдеться жертвам у 265 мільярдів доларів США. Ці приголомшливі цифри підкреслюють необхідність для компаній зміцнювати свою позицію кібербезпеки.

Щоб пом’якшити кіберризики, організації повинні прийняти найкращі практики щодо дотримання вимог щодо кібербезпеки та конфіденційності:

Прийняти та впровадити офіційну структуру кібербезпеки, тобто. NIST CSF 2.0.

Зіставлення даних: виконайте перевірку зіставлення даних, щоб задокументувати особисту інформацію, якою володіє ваша компанія, спосіб збирання даних і звідки (потік даних), а також будь-які треті сторони, яким надаються дані (наприклад, сторонні організації, які обробляють ваші дані). дані компанії).

Проводити щорічну оцінку впливу на конфіденційність і кіберризиків.

Створіть і регулярно оновлюйте зовнішні політики конфіденційності та умови веб-сайтів/додатків, щоб окреслити заходи щодо обробки та захисту даних. Більшість повідомлень про конфіденційність, які наразі використовуються міжнародними організаціями, недостатні для цілей відповідності відповідно до чинних норм щодо даних. Повідомлення про конфіденційність мають бути чіткими та зрозумілими та містити всю необхідну інформацію, як зазначено у відповідних положеннях щодо даних, щоб отримати дійсну згоду суб’єктів даних.

Вимоги щодо ведення записів адрес: від контролерів даних може вимагатися вести ретельний, точний і повний облік персональних даних, які вони збирають, а також того, як ці дані обробляються, використовуються та зберігаються. Перевірте свої поточні процедури ведення записів і за потреби внесіть зміни та вдосконалення.

Оцініть процедури зберігання даних: Контролерам даних дозволяється зберігати дані про суб’єктів лише до тих пір, поки це необхідно для мети, з якою дані були спочатку отримані. Кожна компанія повинна оцінити свої поточні процедури зберігання даних, і багатьом доведеться внести зміни в процеси зберігання та збереження даних, щоб відповідати вимогам.

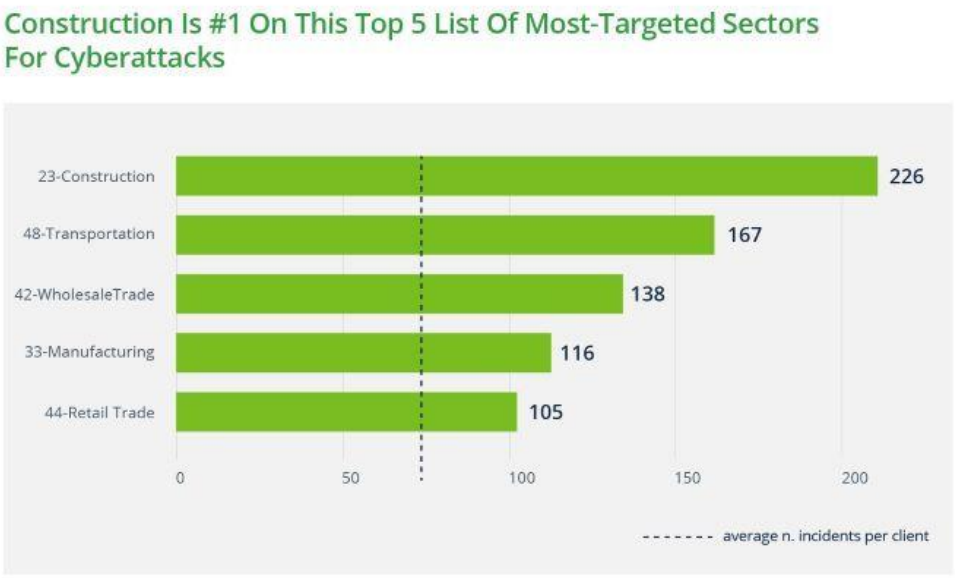
Навчання співробітників: усі співробітники повинні пройти належне навчання, щоб переконатися, що вони обізнані про поточні кіберризики та дотримуються відповідних процедур зменшення ризиків і обробки даних. Ведіть записи про навчання та запроваджуйте постійне навчання, щоб гарантувати, що співробітники постійно проходять тестування на новітні кіберризики.

Оновити політику та процедури. Компанії повинні встановити чіткий набір політик захисту даних, як внутрішніх, так і зовнішніх, таких як корпоративна політика захисту даних, план реагування на інциденти (контрольний список для реагування на порушення даних), політики, пов'язані з обробкою та збереженням даних клієнтів (включно з доповненнями до обробки даних (DPA)), політикою сторонніх постачальників/постачальників, політикою щодо працівників (включаючи довідник для співробітників і політикою віддаленої роботи), умовами електронної комерції або веб-сайтами та політикою конфіденційності…» ***(Craig S. Horbus. Still on Top: Cybersecurity Incidents Ranked #1 Global Business Threat in 2024 // Dinsmore & Shohl LLP. (https://www.dinsmore.com/publications/still-on-top-cybersecurity-incidents-ranked-1-global-business-threat-in-2024/). 12.03.2024).***

***

«…Будівельна галузь завжди мала кіберризик. Протягом багатьох років експерти з кібербезпеки попереджали підрядників про те, що вони є мішенями для атак програм-вимагачів, крадіжок з метою фішингу та витоку даних/викрадення конфіденційної інформації. Сьогодні промислове шпигунство в будівельній галузі та геополітичні кіберзриви зростають.

Керовані сервісні компанії, які відстежують кібератаки та реагують на них, чітко розуміють важливість ризику для галузі. Наприклад, у щорічному звіті ReliaQuest про кіберзагрози за 2023 рік будівельна галузь посідає перше місце в списку найбільш цільових секторів (за ним йде транспорт) із середнім показником 226 інцидентів на рік.



Source: ReliaQuest's 2023 Annual Cyber-Threat Report

Як наслідок, будівельна галузь зазнала величезних втрат, включаючи викрадені або неправильно спрямовані кошти та невдалі пропозиції через збої в системі, а також пошкодження бренду майбутніми домовленостями про співпрацю, втраченими контрактами та довірою клієнтів, на додаток до каскадних витрат на реагування на кіберінциденти, як-от відновлення системи та виплати викупу.

Щоб пояснити масштаб наслідків кібератаки, варто сказати, що масштабна подія програм-вимагачів має високу ймовірність спричинити серйозні збої в ланцюжку поставок і навіть може вплинути на постачальників або клієнтів, якщо зловмисне програмне забезпечення поширюється за межі компанії або конфіденційні дані. витік. Не слід недооцінювати фінансові наслідки такої атаки, оскільки атакувана будівельна компанія зазнає масштабних збоїв у роботі, особливо коли користувачі будуть заблоковані у важливих системах, необхідних для просування або завершення проекту. Крім того, коли кібератака призводить до значної затримки в доставці проекту або компрометує ланцюжок постачання, це може завдати значної репутаційної шкоди, особливо якщо відбувається витік дуже конфіденційних даних. Це, у свою чергу, спричиняє страждання та/або фінансові збитки для інших компаній або осіб, пов’язаних із бізнесом.

Чому так сильно постраждав будівельний сектор?

У будівельній галузі є кілька факторів, які роблять її більш привабливою для злочинців, а іноді й мішенню.

Відсутність інвестицій в інфраструктуру кібербезпеки: суб'єкт без належної кібергігієни та кіберархітектури означає суб'єкт, який легко атакувати та вимагати. Грошові кіберзлочинці зможуть докладати небагато зусиль для отримання максимальної вигоди. Багато інженерно-будівельних компаній працюють з обмеженою маржею. Ефективна та значуща реалізація технологій і програмного забезпечення, а також супутня конфіденційність даних і відповідність вимогам безпеки вимагають виділених корпоративних ресурсів, управління та інвестицій, які часто розглядаються як витрати в балансі. Відповідно, у будівництві багато компаній не інвестували належним чином у кібербезпеку і дорого платять, коли зазнають атаки.

Ціль для тих, хто шукає конфіденційну інформацію: для національних держав, які прагнуть отримати цінну інформацію про інфраструктуру, інтелектуальну власність або доступ до важливих громадських робіт, будівельна галузь є слабкою ланкою та легкою мішенню для доступу. Приклади інформації, на яку націлені кіберзлочинці, включають власні плани та проекти будівництва, інформацію про безпеку об'єктів та іншу інтелектуальну власність.

Швидке впровадження нових технологій: інженерні та будівельні послуги, що підтримуються такими технологіями, як штучний інтелект, розширена аналітика, кіберфізичні системи, машинне навчання та робототехніка, проклали шлях до підвищення продуктивності, ефективності, підключення та покращення пропозицій послуг. Однак кібернетичний ризик і ризик конфіденційності даних часто ігнорується в гонці за впровадження нових технологій, що створює значний ризик.

Покладення на застарілі системи є значною проблемою в будівельній галузі. Застарілі або вичерпані операційні системи створюють значні можливості для кіберзлочинців. Операційна система, яка більше не підтримується, матиме відомі вразливості, і оскільки підтримка закінчилася, виправлення будуть недоступні. Часто сама подія шифрування руйнує застарілу операційну систему або пристрій, запобігаючи будь-якому відновленню.

Ризик для третіх сторін: постачальники, які підключені до спільної мережі, часто можуть становити непомітну загрозу. Кіберризики третіх сторін включають потенційні порушення даних через уразливості в IT-середовищі постачальника та можуть призвести до фінансових, репутаційних і регуляторних наслідків/наслідків.

Відсутність нормативних актів, пов'язаних із кібербезпекою: протягом багатьох десятиліть здавалося, що будівельний сектор не мав багатьох нормативних актів щодо безпеки даних, тоді як такі сектори, як фінансові послуги, підлягають суворому регулюванню. Однак уряд США дедалі активніше регулює та вимагає від державних підрядників відповідності кібербезпеки Концепції Національного інституту стандартів і технологій (NIST) і далі посилює відповідність Сертифікації моделі зрілості кібербезпеки. Все частіше ті, хто укладає контракти з федеральним урядом, повинні демонструвати ефективні практики кібербезпеки та захисту даних як засіб ведення бізнесу. Здатність будівельної компанії брати участь у тендерах або брати участь у федеральних будівельних проектах вимагатиме кібер-зрілості як умови.

Основні заходи кібербезпеки для будівельної галузі

Усі будівельні компанії та підрядники повинні знати про кіберризики, з якими стикається їхня галузь.

Вживання заходів для забезпечення належного контролю для захисту здатності підприємства функціонувати та його коштовностей включає, але не обмежується:

Багатофакторна автентифікація для всіх облікових записів віддаленого доступу, веб-пошти, привілейованих і адміністративних облікових записів.

Навчання співробітників із симуляцією фішингу. Перевізники кіберстрахування часто пропонують навчання співробітників як додаткову цінність до страхового полісу.

Суворий подвійний контроль із вимогами зворотного виклику для змін платіжного рахунку та маніпулювання рахунками-фактурами для пом'якшення шахрайства соціальної інженерії.

Ефективні конфіденційної інформації стратегії запобігання витоку, як-от дані співробітників, комерційні таємниці, як-от системи ціноутворення та контрактних ставок, схеми та інженерні дані операційної технології (OT).

Виявлення кінцевої точки та реагування (EDR), включаючи керування мобільними пристроями (MDM) для пристроїв у польових умовах для відстеження та видалення вкрадених або втрачених гаджетів.

Ізольоване програмне середовище, яке пропонує контрольоване середовище перед розгортанням нового та/або оновленого програмного забезпечення, включаючи виправлення.

Сегментовані, перевірені, перевірені та захищені резервні копії для всіх критичних систем і баз даних. Зауважте, що деякі кіберполітики можуть допомогти у разі роботі перерв у через кібератаки.

Перевірений і щорічно оновлюваний план реагування на інциденти, включаючи готовність до програм-вимагачів, планування ресурсів/списки завдань і стратегії зв'язків з громадськістю». ***(David Anderson. Building Defenses Against Cyber Risk in the Construction Sector // Assurex Global & IBN Partner (https://woodruffsawyer.com/property-casualty/cybersecurity-in-construction/). 19.03.2024).***

***

«Важливість обізнаності про кібербезпеку неможливо переоцінити. Оскільки цифрова сфера стає невід'ємною частиною нашого повсякденного життя, від особистого банківського обслуговування до глобальної торгівлі, потенційний вплив кіберзагроз виходить далеко за межі індивідуальних незручностей, створюючи значні ризики для нашої особистої конфіденційності, фінансової безпеки та навіть національної безпеки.

Оскільки кіберзагрози стають все більш витонченими, ми використовуємо передові технології та тактики, залишаючись поінформованими та пильними є нашою першою лінією захисту від цих невидимих ворогів. Ця стаття має на меті ознайомити вас з основними порадами щодо навчання кібербезпеці, щоб ефективно

захистити своє цифрове середовище, гарантуючи, що ви та ваші дані залишатиметесь у безпеці у світі, де зростає зв'язок.

Розуміння ландшафту кіберзагроз

Розуміння ландшафту кіберзагроз є основою для розробки ефективних стратегій кібербезпеки. Загрози зростають не тільки в масштабах, але й у складності, оскільки кіберзлочинці постійно винаходять нові методи використання вразливостей.

Ці загрози охоплюють широкий спектр тактик, у тому числі зловмисне програмне забезпечення, яке може вивести з ладу цілі системи, фішингові шахрайства, призначені для того, щоб ввести в оману людей для розкриття конфіденційної інформації, і атаки програм-вимагачів, які блокують доступ до критично важливих даних, вимагаючи значні викупи. Крім того, ситуація ускладнюється діяльністю національних державних акторів, які займаються кібершпигунством, прагнучи викрасти секретну інформацію або зруйнувати критично важливу інфраструктуру заради стратегічних здобутків.

Мотиви, що спричиняють ці кіберзагрози, різноманітні, починаючи від фінансової вигоди, як це можна побачити у крадіжці особистих даних і фінансових шахрайствах, до ідеологічних цілей, зокрема поширення пропаганди чи зрив політичних процесів. Таким чином, розуміння цього складного ландшафту має ключове значення як для окремих осіб, так і для організацій для розробки надійних засобів захисту, забезпечення конфіденційності, цілісності та доступності їхніх цифрових активів у середовищі, де кіберзагрози є постійним викликом, що розвивається.

10 порад щодо навчання кібербезпеці

Щоб краще захистити ваше цифрове середовище, ми ознайомимося з десятьма навчальними порадами щодо кібербезпеки. Як загальне зауваження, тренінги з кібербезпеки спрямовані на те, щоб навчити співробітників ставати більш свідомими в Інтернеті. Зрештою, мета полягає в тому, щоб допомогти їм виявити та пом'якшити загрози до того, як вони завдадуть шкоди.

1. Розпізнавайте та уникайте фішингових атак

Фішингові атаки є поширеною формою кіберзагроз, коли зловмисники маскуються під надійну особу, щоб викрасти конфіденційну інформацію. Ці атаки часто здійснюються у вигляді електронних листів, повідомлень або телефонних дзвінків. Щоб не стати жертвою фішингу:

Скептично ставтеся до небажаних повідомлень, особливо тих, що закликають до негайних дій.

Перевірте особу відправника, перевіривши його електронну адресу або зв'язавшись з організацією безпосередньо через офіційні канали.

Уникайте натискання на посилання або завантаження вкладень із невідомих або підозрілих джерел.

2. Використовуйте надійні унікальні паролі

Паролі є ключем до нашого цифрового життя. Використання надійних унікальних паролів для кожного вашого облікового запису значно знижує ризик несанкціонованого доступу. Ось кілька порад щодо створення надійних паролів:

Використовуйте комбінацію великих і малих літер, цифр і спеціальних символів.

Уникайте використання інформації, яку легко вгадати, як-от дні народження чи загальні слова.

Спробуйте використати парольну фразу, яка є послідовністю слів або речень, які легко запам'ятати, але важко вгадати.

Використовуйте надійний менеджер паролів, щоб надійно відстежувати свої паролі.

3. Увімкніть багатофакторну автентифікацію (MFA)

Багатофакторна автентифікація додає додатковий рівень безпеки, вимагаючи двох або більше методів перевірки для отримання доступу до облікового запису. Це може включати те, що ви знаєте (пароль), те, що у вас є (мобільний пристрій), або те, чим ви є (біометрична перевірка). Увімкнення MFA, де це можливо, може значно підвищити вашу безпеку.

4. Оновлюйте програмне забезпечення та системи

Кіберзловмисники часто використовують уразливості в застарілому програмному забезпеченні та системах. Регулярне оновлення вашої операційної системи, програм і мікропрограми є критично важливим механізмом захисту. Увімкніть автоматичні оновлення, де це можливо, і будьте в курсі будь-яких виправлень безпеки, випущених постачальниками програмного забезпечення.

5. Будьте обережні з громадським Wi-Fi

Загальнодоступні мережі Wi-Fi хоч і зручні, але часто небезпечні. Кіберзлочинці можуть перехоплювати дані, що передаються через ці мережі, включаючи паролі та фінансову інформацію. Під час використання публічної мережі Wi-Fi:

Уникайте доступу до конфіденційної інформації, такої як онлайн-банкінг.

Використовуйте віртуальну приватну мережу (VPN) для шифрування підключення до Інтернету.

Розгляньте можливість використання мобільних даних для конфіденційних транзакцій, якщо сумніваєтеся.

6. Регулярно створюйте резервні копії даних

Регулярне резервне копіювання даних може стати порятунком у разі кібератаки, наприклад програми-вимагача, коли ваші дані стають заручниками. Переконайтеся, що у вас є кілька резервних копій, включаючи принаймні одну офлайнову резервну копію, щоб захистити від втрати даних.

7. Навчайте себе та інших

Важливо бути в курсі останніх кіберзагроз і найкращих практик безпеки. Слідкуйте за авторитетними джерелами новин про кібербезпеку, відвідуйте вебінари та беріть участь у тренінгах. Не менш важливо навчати людей навколо вас, включаючи родину, друзів і колег, оскільки кібербезпека — це колективна робота.

8. Захистіть свою домашню мережу

Ваша домашня мережа є шлюзом до вашого особистого, а іноді й пов’язаного з роботою цифрового життя. Його забезпечення передбачає:

Зміна імені користувача та пароля маршрутизатора за замовчуванням.

Увімкнення шифрування WPA3 у вашій мережі Wi-Fi.

Вимкнення функцій, якими ви не користуєтеся, наприклад дистанційне керування.

Регулярне оновлення мікропрограми маршрутизатора.

9. Будьте уважні до тактики соціальної інженерії

Соціальна інженерія використовує людську психологію, а не технічні методи злому для отримання доступу до систем, мереж або фізичних місць. Будьте обережні з небажаними телефонними дзвінками, візитами або повідомленнями електронної пошти від осіб, які запитують про працівників або іншу внутрішню інформацію. Завжди перевіряйте особу запитувача та законність запиту.

10. Застосуйте заходи безпеки пристрою

Зі збільшенням кількості пристроїв, підключених до Інтернету, безпека цих пристроїв є першорядною. Це включає:

Встановлення надійного програмного забезпечення безпеки на ваших пристроях.

Увімкнення захисту брандмауером.

Будьте обережні щодо програм, які ви завантажуєте, і дозволів, які вони запитують.

Фізична безпека ваших пристроїв, особливо в громадських місцях.

Навчання з питань кібербезпеки не є обов’язковим; це необхідність. Застосувавши ці важливі поради, ви зможете значно підвищити рівень безпеки та випередити кіберзагрози. Пам’ятайте, кібербезпека – це не одноразова спроба, а постійний процес навчання, адаптації та пильності. Будьте в курсі, залишайтеся в безпеці та сприяйте безпечнішому цифровому світу для всіх». ***(Alicia Hope. Essential Cybersecurity Awareness Training Tips to Stay Ahead of Threats // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/essential-cybersecurity-awareness-training-tips-to-stay-ahead-of-threats/). 21.03.2024).***

***

«У сучасному взаємопов'язаному цифровому ландшафті кібербезпека стала першорядною для компаній будь-якого розміру. Однак для малого бізнесу з обмеженими ресурсами та досвідом орієнтуватися в складній сфері кібербезпеки може бути складно. Ця стаття має на меті демістифікувати кібербезпеку, розбиваючи 10 важливих заходів, які кожен малий бізнес повинен запровадити, щоб захистити свої цінні активи та конфіденційну інформацію.

Розуміння важливості кібербезпеки:

Перш ніж заглиблюватися в конкретні заходи, важливо зрозуміти, чому кібербезпека є важливою для малого бізнесу. Хоча великі корпорації можуть здаватися більш привабливими цілями для кібератак, малі підприємства однаково вразливі. Насправді, згідно з останніми дослідженнями, майже половина всіх кібератак спрямована на малий бізнес.

1. Проводьте регулярні оцінки безпеки:

Першим кроком до зміцнення кібербезпеки вашого бізнесу є проведення регулярних оцінок безпеки. Ці оцінки включають оцінку ваших поточних заходів безпеки, виявлення потенційних вразливостей і розробку стратегій для їх усунення. Проводячи періодичні оцінки, ви можете випереджати нові загрози та гарантувати, що ваші засоби захисту кібербезпеки актуальні.

2. Впроваджуйте політику надійних паролів:

Ненадійні паролі є однією з головних причин витоку даних. Щоб підвищити кібербезпеку вашого бізнесу, запровадьте політику надійних паролів, яка вимагає від співробітників створювати складні паролі та регулярно їх змінювати. Крім того, подумайте про впровадження багатофакторної автентифікації (MFA), щоб додати додатковий рівень безпеки для ваших систем і облікових записів.

3. Захистіть свою мережу:

Безпека вашої мережі має важливе значення для захисту конфіденційних даних вашого бізнесу від несанкціонованого доступу. Почніть із захисту своєї мережі Wi-Fi за допомогою надійного пароля та шифрування. Крім того, подумайте про впровадження брандмауера для моніторингу та контролю вхідного та

вихідного мережевого трафіку, таким чином запобігаючи проникненню кіберзагроз у ваші системи.

4. Підтримуйте програмне забезпечення в актуальному стані:

Застаріле програмне забезпечення може становити значні ризики для безпеки вашого бізнесу. Хакери часто використовують відомі вразливості в застарілому програмному забезпеченні для здійснення кібератак. Щоб зменшити цей ризик, переконайтеся, що всі програми та операційні системи регулярно оновлюються останніми виправленнями та виправленнями безпеки.

5. Навчіть співробітників передовим практикам кібербезпеки:

Людська помилка є однією з основних причин порушень кібербезпеки. Щоб мінімізувати цей ризик, навчайте своїх співробітників найкращим практикам кібербезпеки. Проведіть навчання, як розпізнавати спроби фішингу, уникати натискання підозрілих посилань або вкладень і негайно повідомляти про будь-які інциденти безпеки. Розвиваючи культуру обізнаності про кібербезпеку, ви можете надати своїм співробітникам можливість стати першою лінією захисту від кіберзагроз.

6. Регулярно створюйте резервні копії даних:

Втрата даних може мати руйнівні наслідки для малого бізнесу. Щоб зменшити ризик втрати даних через кібератаки, нещасні випадки чи збої апаратного забезпечення, важливо регулярно створювати резервні копії даних. Запровадьте надійну стратегію резервного копіювання та відновлення даних, яка включає резервне копіювання як на місці, так і за його межами. Крім того, регулярно перевіряйте свої системи резервного копіювання, щоб переконатися, що вони функціонують правильно.

7. Обмежте доступ до конфіденційної інформації:

Не всім співробітникам потрібен доступ до конфіденційної інформації. Щоб мінімізувати ризик внутрішніх загроз і несанкціонованого доступу, обмежте доступ до конфіденційних даних лише тим співробітникам, яким вони потрібні для виконання своїх службових обов’язків. Впроваджуйте контроль доступу на основі

ролей (RBAC), щоб забезпечити дотримання прав доступу на основі ролей і обов'язків співробітників в організації.

8. Відстежуйте та виявляйте підозрілу активність:

Проактивний моніторинг є критично важливим для виявлення та реагування на кіберзагрози в реальному часі. Впровадьте надійну систему моніторингу та виявлення, яка постійно стежить за підозрілою діяльністю у вашій мережі, наприклад спробами несанкціонованого доступу або незвичайними моделями мережевого трафіку. Крім того, установіть процедури реагування на інциденти для швидкого розслідування та пом'якшення інцидентів безпеки.

9. Шифруйте конфіденційні дані:

Шифрування — це ефективний спосіб захистити конфіденційні дані вашого бізнесу від несанкціонованого доступу, навіть якщо вони потраплять до чужих рук. Впроваджуйте протоколи шифрування для шифрування даних як під час передачі, так і в стані спокою. Шифруючи конфіденційну інформацію, ви можете гарантувати, що навіть якщо її перехоплять або викрадуть, вона залишиться нечитабельною та непридатною для неавторизованих сторін.

10. Будьте в курсі та адаптуйтеся:

Ландшафт кібербезпеки постійно розвивається, регулярно з'являються нові загрози. Щоб випереджати кіберзлочинців, важливо бути в курсі останніх тенденцій кібербезпеки, загроз і найкращих практик. Підпишіться на інформаційні бюлетені з кібербезпеки, відвідуйте галузеві конференції та беріть участь у форумах з кібербезпеки, щоб бути в курсі подій у цій галузі. Крім того, будьте готові відповідно адаптувати свою стратегію кібербезпеки, щоб ефективно протидіяти новим і появам загроз.

висновок:

Кібербезпека – це не разова спроба, а постійний процес, який вимагає пильності, відданості та здатності до адаптації. Впровадивши 10 основних заходів, викладених у цій статті, малі підприємства можуть значно підвищити рівень кібербезпеки та захистити свої цінні активи від кіберзагроз. Пам'ятайте, інвестиції в кібербезпеку сьогодні – це інвестиції в майбутню стійкість і успіх вашого

бізнесу». ***(Demystifying Cybersecurity: 10 Essential Measures for Small Businesses // TechBullion (https://techbullion.com/demystifying-cybersecurity-10-essential-measures-for-small-businesses/). 20.03.2024).***

***

«У сучасному кібернетичному середовищі, яке швидко розвивається та постійно змінюється, організації по всьому світу стикаються з безліччю викликів. Від високого попиту на ресурси з кібербезпеки до частої зміни керівників у сфері кібербезпеки та виникнення складних проблем із дотриманням нормативних вимог, цифровий світ створює низку перешкод для бізнесу. У відповідь на ці виклики все більше організацій звертаються до досвідчених рішень аутсорсингу, щоб ефективно захистити свої цифрові межі.

Основні напрямки уваги та сучасні виклики кібербезпеці:

Високий попит на ресурси з кібербезпеки: оскільки кіберзагрози стають дедалі складнішими, зростає попит на кваліфікованих фахівців з кібербезпеки. Цей попит часто перевищує пропозицію, роблячи організації вразливими та потребуючими надійних рішень.

Часта зміна керівних кадрів у сфері кібербезпеки: у секторі кібербезпеки спостерігається значна зміна кадрів, особливо на таких ключових посадах, як керівники служби безпеки (CSO). Ця зміна може призвести до неузгодженості в стратегіях кібербезпеки та вразливості організаційної безпеки.

Виникаючі проблеми дотримання нормативних вимог: оскільки нормативні акти швидко розвиваються, організаціям важко йти в ногу з вимогами відповідності, оскільки їм часто не вистачає досвіду та ресурсів, необхідних для того, щоб випереджати законодавчі та нормативні зміни.

Потреба у звітах про стан і інформаційну панель у режимі реального часу. Зацікавленим сторонам, зокрема радам директорів та інвесторам, все частіше потрібна актуальна інформація про стан кібербезпеки організації. Потреба в даних і звітності в реальному часі стає критично важливим аспектом організаційної прозорості та довіри.

Єдина точка відмови в керівництві кібербезпеки: залежність від окремих ОГС або керівників кібербезпеки часто створює «єдину точку відмови» в стратегії кібербезпеки організації. Ця залежність може становити значні ризики, якщо її не вирішити належним чином.

У світлі цих проблем Ван Стіл, акціонер LBMC Cybersecurity, наголошує на перевагах аутсорсингу рішень кібербезпеки. «Правління директорів, інвестори, ділові партнери та інші зацікавлені сторони часто запитують про положення або стратегію організації в галузі кібербезпеки, і можливість відповісти на це запитання за допомогою звітів про статус і інформаційну панель у реальному часі є неймовірною розкішшю. Ресурси з кібербезпеки користуються великим попитом, а середній термін перебування на посаді керівника служби безпеки становить менше трьох років. Кожна ОГС має власне стратегічне бачення та тактичний план, які нерозривно пов’язані з цією особою, створюючи потенційну «єдину точку провалу». Хоча концепція єдиної точки відмови добре відома в кібербезпеці, вона рідко зосереджується на лідерстві та стратегії програми кібербезпеки. Доповнивши окрему особу сторонньою комплексною програмою кібербезпеки, компанії можуть значно знизити ризик єдиної точки збою, що кардинально змінює правила для організацій», — говорить Стіл.

Аутсорсинг функцій кібербезпеки може запропонувати безліч переваг. Він надає доступ до команди експертів із різноманітними спеціалізованими наборами навичок, забезпечує безперервність стратегій кібербезпеки, незважаючи на зміни в керівництві, і допомагає орієнтуватися в складному ландшафті проблем відповідності. Крім того, він вирішує проблему єдиної точки відмови, розподіляючи відповідальність між командою, а не окремою особою, підвищуючи загальну безпеку організації.

Оскільки цифровий світ продовжує розвиватися, перехід до зовнішніх рішень із кібербезпеки є не просто тенденцією, а стратегічною необхідністю для організацій, які прагнуть залишатися стійкими та безпечними перед обличчям зростаючих кіберзагроз». ***(Leading the Charge in Cybersecurity: Embracing Outsourced Solutions to Navigate an Evolving Digital Landscape // Morningstar, Inc.***

(https://www.morningstar.com/news/globe-newswire/9067700/leading-the-charge-in-cybersecurity-embracing-outsourced-solutions-to-navigate-an-evolving-digital-landscape). 22.03.2024).

***

«Коли справа доходить до кібербезпеки, складається відчуття, що ландшафт постійно змінюється. Що ж, це слушна думка, враховуючи, що кіберзлочинці регулярно вдосконалюють свою тактику та невпинно шукають діри в захисті в усіх галузях.

Легкі, невдалі цілі? Малий і середній бізнес (SMBs). Вони часто зберігають цінні клієнтські та фінансові дані, але ось де починається проблема: їм бракує складної безпеки, як у великих корпорацій. Це створює беззаперечно вразливу комбінацію. Вплив успішної кібератаки може бути величезним і руйнівним для цих організацій. Втрачений дохід. Збої в роботі. Серйозна шкода репутації. Малі підприємства просто не можуть дозволити собі серйозний інцидент.

Усвідомлюючи наслідки, розумно вважати, що посилення кібербезпеки більше не є необов'язковим. Це очевидна потреба, яку малий бізнес більше не може не помічати. Що тоді робити малим і середнім підприємствам? Застосуйте надійний захист, щоб зупинити будь-яку загрозу. У сучасному середовищі занадто багато поставлено на карту, щоб зробити системи вразливими. Продовжуйте читати цей матеріал, щоб розблокувати свої корисні інструменти.

Фактор уразливості SMB

SMB часто стають цілями кіберзлочинців; Насправді дослідження показують, що 43% кібератак спрямовані на малий бізнес. Це пояснюється тим, що найчастіше їхня безпека слабша, ніж у великих підприємств. Навіть із застосуванням певних заходів безпеки малому та середньому бізнесу часто все одно потрібен спеціальний IT-персонал великих компаній і можливості цілодобового моніторингу. Звичайно, злочинці знають про ці прогалини, тому використовують їх.

Ці атаки бувають різних форм — фішингові шахрайства, які викрадають паролі, програми-вимагачі, які блокують важливі дані, розподілені атаки типу

«відмова в обслуговуванні» (DDoS), які переповнюють веб-сайт компанії, і багато інших. Фінансові та операційні невдачі від одного успішного порушення можуть бути суттєвими, а в деяких випадках навіть можуть назавжди закрити малий бізнес. І це останнє, що ви хочете, щоб сталося.

Як автоматизація може розблокувати стійкість

Автоматизація кібербезпеки з'явилася як спосіб розблокувати стійкість до загроз. Ось огляд автоматизованих рішень, які можуть принести користь малому та середньому бізнесу:

1. Автоматизоване керування життєвим циклом сертифіката

Однією з життєво важливих сфер автоматизації для малого та середнього бізнесу є керування життєвим циклом цифрових сертифікатів, зокрема, сертифікатів рівня безпечних сокетів/транспортного рівня (SSL/TLS). Вони шифрують зв'язок між веб-браузерами та серверами, захищаючи онлайн-транзакції та перевіряючи автентичність веб-сайту.

Однак відстеження термінів дії, забезпечення своєчасного оновлення та координація встановлення сертифікатів із центрами сертифікації є складними завданнями, які важко виконати вручну, особливо в малих і середніх підприємствах із дуже обмеженим персоналом IT-безпеки. Ця складність зростає експоненціально, оскільки нові стандарти веб-безпеки зміщуються в бік скорочення термінів дії сертифікатів.

Автоматизовані сертифікати як сервісні рішення полегшують ці головні болі, автоматично відстежуючи інвентаризацію сертифікатів у мережах, ініціюючи оновлення за потреби та безперешкодно керуючи життєвими циклами сертифікатів. Це гарантує, що критично важливе шифрування не втрачає чинності та запобігає позначенню веб-сайтів як небезпечних у браузерах, захищаючи довіру клієнтів і повсякденні бізнес-операції.

2. Постійне сканування загроз

Бути на крок попереду кіберзагроз, що постійно розвиваються, вимагає проактивного моніторингу. Інструменти автоматичного сканування — це додатковий співробітник служби безпеки, який невтомно шукає можливі зловмисне

програмне забезпечення, відомі вразливості програмного забезпечення та підозрілу активність у мережах і системах 24/7.

Вони функціонують як система постійного попередження, швидко сповіщаючи групи безпеки SMB про потенційні загрози, перш ніж вони стануть повномасштабними порушеннями. Такий підхід забезпечує належне усвідомлення ризиків і їх пом’якшення в рамках ландшафту кібербезпеки.

Інструменти також можуть сканувати безперервно за встановленим розкладом або в режимі реального часу, забезпечуючи пильний захист навіть поза стандартними робочими годинами з 9 до 5, коли персонал може бути мінімальним. Виявляючи загрози на ранній стадії, автоматичне виявлення дозволяє швидше реагувати на інциденти, значно скорочуючи вікно можливостей, яке мають зловмисники, щоб отримати свою першу опору.

3. Постійне оновлення програмного забезпечення

Невиправлені вразливості програмного забезпечення? Вважайте їх відкритими дверима для кіберзлочинців, які хочуть проникнути сюди. Проте, маючи обмежені бюджети та зосередженість, IT-командам малого та середнього бізнесу часто доводиться наздоганяти впровадження постійних оновлень безпеки, які випускають постачальники. Автоматизація керування виправленнями допомагає подолати цю поширену проблему, яка залишає прогалини в безпеці, яких можна уникнути.

Рішення для автоматичного розгортання виправлень використовують доступні оновлення, щоб закрити ці діри, щойно виправлення стануть доступними. Завдяки автоматичному аудиту систем для виявлення незавершених виправлень, першочерговому визначенню найважливіших із них і розгортанню оновлень за встановленим розкладом, вони виключають послідовність і своєчасність.

Постійна автоматизація гарантує, що системи малого та середнього бізнесу оновлюються практично після публікації виправлень постачальників, а не залишаються вразливими протягом днів чи тижнів.

Переваги автоматизованої кібербезпеки

Ось деякі з переваг, які компанії можуть отримати від автоматизації кібербезпеки:

1. Підвищена ефективність і точність

Багатьом власникам і менеджерам малого та середнього бізнесу потрібна допомога, щоб збалансувати потреби в кібербезпеці з обмеженим часом, бюджетом і власними технічними ноу-хау. Нещодавнє дослідження кібербезпеки дає більш чітку картину: 94% керівників інформаційної безпеки (CISO) невеликих груп безпеки кажуть, що вони страждають від таких перешкод, як брак персоналу (40%) і надмірний ручний аналіз (37%).

Автоматизація пропонує спосіб боротьби з цією проблемою. Використовуючи інструменти, які автоматизують повторювані, трудомісткі завдання, компанії можуть оптимізувати свої операції безпеки, зменшити кількість помилок персоналу служби безпеки та посилити загальний захист.

Автоматизовані рішення найкращі в тих сферах, де ручні процеси схильні до помилок. Навіть невеликі недогляди, як-от неправильно налаштовані правила брандмауера або пропуск необхідного оновлення програмного забезпечення, можуть перерости в серйозні проблеми та створити шлях для атак. Системи автоматизації постійно впроваджують політики безпеки та застосовують латки, щоб закрити ці вразливі прогалини.

2. Зниження витрат

Попередні витрати, пов’язані з автоматизацією кібербезпеки, є причиною того, що багато малих і середніх підприємств не впровадили ці типи інструментів. Загалом компанії інвестують у кібербезпеку в середньому 22% свого IT-бюджету, що можна вважати високими інвестиціями для малого та середнього бізнесу.

Однак розгляд витрат на автоматизацію через довгострокову призму економії коштів є вирішальним. Інвестування в надійні профілактичні інструменти допоможе уникнути важких грошових витрат, пов’язаних із потенційною кібератакою — втраченого доходу, відновлення, штрафів і шкоди репутації.

Крім того, автоматизація зменшує накладні витрати, пов’язані з процесами безпеки вручну, покращує узгодженість і дає змогу неукомплектованим командам безпеки малого та середнього бізнесу підтримувати складніші обов’язки з економічною ефективністю.

З роками ці переваги ефективності та зниження ризиків суттєво збільшуються порівняно з постійним реагуванням на порушення та відновленням після них.

3. Допоміжний охоронний персонал

Автоматизація покращує існуючі групи IT/безпеки, зменшуючи перевантаження сортуванням. Він автоматично виконує важливі завдання, зокрема розгортання сертифікатів, сканування вразливостей і виправлення вразливостей.

Що буде далі? Співробітники відділу кібербезпеки на малих підприємствах тепер можуть зосередити свою енергію на стратегії захисту більшої картини, глибокому аналізі загроз і розумінні «чому» інцидентів. Цей збалансований підхід, що поєднує повну автоматизацію з людським розумінням і можливістю адаптації, є тим, що зрештою зміцнює загальну безпеку малого та середнього бізнесу.

Висновок

З плином днів кіберзагрози стають все більш прогресивними. На щастя, інструменти автоматизації швидко стають доступними, щоб допомогти захищати малий і середній бізнес у будь-який час. Дозволяючи програмному забезпеченню виконувати повторювані завдання безпеки у фоновому режимі, ці компанії можуть звільнити свої невеликі IT-команди, щоб вони могли зосередитися на інших важливих справах.

Так, інвестиції в засоби автоматизації вимагають певних початкових витрат, але не засмучуйтесь. Ви не втрачаєте гроші надарма. На даний момент подумайте про це як про вартість максимально безпечного ведення бізнесу». ***(Jon Stojan. Unlocking resilience: The business case for cybersecurity automation // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/tech-science/unlocking-resilience-the-business-case-for-cybersecurity-automation/article). 22.03.2024).***

***

«Цифрова бухгалтерська революція стала величезною перевагою для ефективності, обслуговування та зростання бухгалтерських фірм. Однак це також створило новий світ уразливостей для зловмисників, які націлені на бізнеси в Інтернеті.

Оскільки цифрові інструменти стають все більш інтегрованими в структуру бізнес-операцій, наголос на кібербезпеці ніколи не був таким критичним. Для бухгалтерів, які працюють з конфіденційними фінансовими даними, це означає новий рівень відповідальності та обізнаності. Кількість кібератак, фішингових схем і витоків даних зростає – у звіті наприкінці 2023 року було виявлено, що 20% компаній стали жертвами кібератак за останній рік, що на 67% частіше зазнавало кіберінциденту, ніж фізичного. крадіжки. Але з відповідними інструментами та процесами під рукою бухгалтери можуть бути підготовлені.

Загрози в хмарному світі

Перехід до хмарного обліку став трансформаційним, пропонуючи масштабованість, ефективність і віддалений доступ. Однак це також створює певні ризики, такі як перехоплення даних, несанкціонований доступ і збої в роботі.

Бухгалтери відіграють вирішальну роль у захисті своїх фірм і клієнтів від цих загроз, що вимагає глибокого розуміння хмарної інфраструктури та потенційних вразливостей. Останні урядові вказівки щодо цього питання – новий Кодекс практики кіберуправління – вимагають від компаній не лише посилити свої заходи кібербезпеки, але й забезпечити їх відповідність національним стандартам і найкращим практикам.

Як і у випадку з більшістю проблем відповідності, існує висока ймовірність того, що тягар ляже на бухгалтерські фірми, коли мова заходить про забезпечення відповідності МСП. З огляду на суворі заходи на горизонті, зараз настав час переглянути та вдосконалити свої стратегії кіберуправління.

Це означає застосування цілісного підходу до кібербезпеки, що включає управління ризиками, планування реагування на інциденти, навчання співробітників, а також безпечну розробку та розгортання безпечних цифрових інструментів. Це підвищує планку для компаній, коли мова заходить про вибір

програмного забезпечення, консультування клієнтів і управління робочим процесом. Але це також створює можливість взяти на себе провідну роль у роботі з клієнтами в цьому швидкоплинному середовищі.

ШІ та ризик

Штучний інтелект (ШІ) був однією з найдинамічніших історій технологій останнього часу. У той час як постачальники програмного забезпечення роками впроваджували елементи штучного інтелекту та машинного навчання (ML) у продукти поетапно, запуск таких інструментів для споживачів, як ChatGPT, підлив масла у вогонь, даючи будь-кому можливість використовувати потужні інструменти штучного інтелекту.

Це палка з двома кінцями в кібербезпеці. Хоча він може зміцнити захист шляхом виявлення незвичайних шаблонів і прогнозування потенційних порушень, системи штучного інтелекту самі по собі можуть бути цілями складних кібератак. Для компаній, які використовують інструменти штучного інтелекту для обробки даних клієнтів, це передбачає розуміння його обмежень, забезпечення прозорих процесів обробки даних і підтримку актуальних протоколів безпеки для зменшення ризиків. Це може включати:

- Політики щодо того, які дані можна використовувати з інструментами ШІ
- Процеси анонімізації даних клієнта
- Навчання для клієнтів щодо того, коли та як використовувати інструменти ШІ
- Як говорити з клієнтами про безпеку

Бухгалтери повинні взяти на себе активну роль у забезпеченні безпеки клієнтів. Як і у випадку з багатьма проблемами безпеки, найбільшою загрозою для ваших клієнтів можуть бути вони самі. Такі шахрайства, як фішингові атаки, часто покладаються на те, щоб завоювати довіру клієнта, щоб змусити його добровільно надати конфіденційну інформацію. Тому важливо переконатися, що ваші клієнти усвідомлюють ризики – зрештою, надійна безпека у світі нічого не означає, якщо ваш клієнт відмовиться від свого пароля.

Повідомлення клієнта про кібербезпеку має бути чітким, повчальним і заспокійливим.

Розкажіть клієнтам про поширені ризики, такі як соціальна інженерія та програми-вимагачі.

Підкресліть важливість колективного підходу до безпеки.

Розробка та поширення надійної політики безпеки може допомогти клієнтам у прийнятті найкращих практик і розуміти свою роль в екосистемі кібербезпеки.

Перетворення програмного забезпечення на союзника

Вибір правильних технологічних рішень є невід'ємною частиною кібербезпеки. Слід запитати постачальників про їхні заходи безпеки, політику обробки даних і стандарти відповідності.

Бухгалтери також повинні виступати за рішення, які пропонують багаторівневі функції безпеки, такі як двофакторна автентифікація (2FA) і механізми контрольованого доступу.

Однією з найбільш вразливих областей будь-якого робочого процесу є передача даних. Саме тут інтегровані рішення з підтримкою API, як-от пакет бухгалтерського обліку Bright, можуть мати величезне значення. Зводячи до мінімуму можливості ручних методів передачі даних, таких як електронні листи чи електронні таблиці, бухгалтери можуть зберігати конфіденційні дані в безпеці під час передачі, заощаджуючи час на ручні процеси.

Проактивний підхід до кібербезпеки

Будучи зберігачами фінансових даних компаній, бухгалтери знаходяться на передовій боротьби з кіберзлочинністю, хочуть вони цього чи ні. Це не обов'язково означає, що радники повинні раптово стати експертами з кібербезпеки, але це означає взяти на себе певний рівень відповідальності.

Це починається з безпечних інструментів і процесів. Щоб дізнатися більше про те, як Bright забезпечує безпеку наших клієнтів, чому б не замовити дзвінок одному з наших експертів з безпеки». ***(Cybersecurity, the cloud and AI: What you need to know // Sift (https://www.accountingweb.co.uk/community/industry-insights/cybersecurity-the-cloud-and-ai-what-you-need-to-know). 21.03.2024).***

***

«Світова кібербезпека перебуває на перехресті великих викликів і загроз, масштаби яких уже відчувають дослідники. За даними AAG IT, у 2021 році кількість кібератак зросла на 125% і продовжує збільшуватися щороку. Це помічають бізнеси та постійно збільшують свої витрати на кібербезпеку.

За даними Cybersecurity Ventures, у 2004 році світовий ринок кібербезпеки становив лише $3,5 млрд. Однак в найближчі два роки ця сума має зрости до $1,75 трлн. Серед жертв кібератак є як великі компанії типу eBay, так і мікробізнеси із сотнею клієнтів. Який сигнал ми отримуємо від цієї статистики? Дуже простий: кіберзлочинці збільшують свою активність і створюють загрозу для всіх без винятку компаній.

Для українського бізнесу ситуація має ще більш загрозливий вигляд. Окрім злочинців, метою яких є збагачення, Україну постійно атакує ворог. Кібератаки є частиною повномасштабної війни, яку РФ розв'язали в нашій країні, і до якої готувалися задовго до 2022 року. Напередодні вторгнення, у перші 10 місяців 2021 року, в Україні зафіксували 280 000 атак. Більшість із них були націлені на уряд та критично важливі сайти, наприклад банківські системи. Однак частково постраждав і бізнес.

У цій статті ми розповімо, чому нікому не варто нехтувати кібербезпекою, а також чому бекапування даних простий і надійний спосіб вберегти свою інформацію.

Кібератаки — не випадковість

Керівники бізнесів не люблять витрачати гроші на малопомітні проєкти та дуже рідко вкладаються у напрямки, які не приносять користь тут і зараз. Красномовний факт: у 2020 році 49% підприємців в Україні вели облік у табличних сервісах, хоча на ринку вже існувало низка якісних CRM-систем на будь-який смак. Люди вважали, що перехід на CRM занадто складний і не принесе користі їхній компанії.

Така недооцінка сьогодні присутня й у сфері кібербезпеки. Керівники компаній іноді озвучують небезпечну думку: "Ми маленька компанія, навіщо

хакерам інформація про моїх клієнтів?”. Схоже, багато підприємців справді не розуміють мотиви злочинців, тому розглянемо їх детальніше.

Заробіток. Більшість кіберзлочинців спрямовані на заробіток грошей. Вони можуть використовувати кібератаки для вимагання викупу, крадіжки фінансової інформації, крадіжки конфіденційної інтелектуальної власності або для оцінки фінансових ресурсів компанії.

Крадіжка особистої інформації. Кіберзлочинці можуть атакувати бізнес з метою крадіжки особистої інформації про клієнтів або співробітників, яку потім можна використовувати для шахрайства, шпигунства або ідентифікації.

Злам в цілях розваг. Деякі кіберзлочинці можуть влаштовувати кібератаки просто для задоволення або випробування власних навичок без будь-якої конкретної мети чи вигоди.

Політичні мотиви та війна. Хакери з РФ можуть атакувати українські компанії, щоб завдати шкоди економіці країни.

Кіберзлочинцям складно атакувати компанії, які добре захищені. Простіше знайти слабке місце і вдарити в нього. Це робить усі хакерські атаки невипадковими. Тобто, якщо бізнес не дбає про кіберзахист, то сам збільшує свої шанси потрапити під одну з атак.

Що таке бекапування даних і для чого воно потрібне?

Один з найпростіших способів зберегти свої дані — створити їхню резервну копію. Резервне копіювання даних (бекапування) — це процес створення копій важливих даних і зберігання їх на іншому носії або в іншому місці. Це дає можливість відновити ці дані у випадку втрати або пошкодження.

Найсучаснішим і найзручнішим способом зберігати резервну копію сьогодні є хмарне середовище. 65% компаній кажуть, що вони використовують хмару як основне сховище даних для бекапування.

Залежно від сервісу, бекапування може мати різний вигляд. Існують послуги, які автоматично створюють копію кожні 24 години, шифрують їх та відправляють у хмару. Часто такі сервіси копіюють лише нові дані, або інформацію, яка зазнала змін. Це пришвидшує процес і робить його непомітним для бізнесу.

Є декілька причин, чому бекапування даних потрібне бізнесу:

Кібертероризм. Злочинці не зможуть шантажувати вас доступом до ваших даних, якщо у вас є копія. Навіть якщо комусь вдасться стерти всю інформацію та вимагати викуп за її повернення, ви зможете швидко все відновити й продовжити роботу.

Людський фактор. Виникають ситуації, коли співробітники випадково видаляють, якусь важливу базу даних, після чого її неможливо відновити. Залежно від важливості цієї інформації збитки можуть бути як незначними, так і катастрофічними.

У 2021 році, один зі співробітників поліції в місті Даллас випадково видалив важливий архів розміром 23 терабайти. В ньому зберігалися файли, фото, докази та інші документи для близько 17 500 справ в офісі окружного прокурора. Здогадайтеся, чи була в поліції Далласа резервна копія цих даних? Звісно ні.

Проблеми виникли через випадковий збіг обставин: співробітник абияк ставився до своєї роботи, якимось чином отримав доступ до великої кількості важливих даних, а поліція не подбала про бекап. Тобто навіть без хакерів чи кіберзлочинців у доволі захищеній структурі стаються форс-мажори із важкими наслідками.

Як обрати сервіс для бекапування даних

Під час вибору сервісу для резервного копіювання даних важливо врахувати кілька ключових аспектів. Перш за все, слід чітко визначити ваші потреби: які дані потрібно копіювати і яка частота резервних копій необхідна. Також важливо врахувати обсяг даних, який ви плануєте зберігати, оскільки деякі сервіси можуть мати обмеження на місткість сховища або розраховувати вартість на основі обсягу даних.

Додатково варто звернути увагу на заходи безпеки, такі як шифрування даних під час передачі та зберігання, а також наявність механізмів автентифікації. Вибираючи, слід оцінити зручність використання інтерфейсу користувача та можливості відновлення даних із резервних копій у випадку втрати чи

пошкодження інформації. Не менш важливою є масштабованість сервісу, його надійність та якість підтримки, яку він надає своїм користувачам.

Наприклад, в UCloud бекапування передбачає повне охоплення: резервне копіювання дисків, розділів, файлів і тек, віртуальних машин. Копії зберігаються в надійному дата-центрі UCloud Німеччини. Вартість копіювання одного терабайту обійдеться компанії всього в $10 на місяць.

Короткий висновок

Бекапування — це створення резервної копії важливих даних для бізнесу. На жаль, багато компаній досі нехтують безпекою своєї інформації й зберігають усе в одному місці. За таких умов вони стають слабкою ціллю для кібертерористів, які можуть викрасти інформацію і вимагати за неї викуп.

Навіть, якщо хакери пройдуть повз вашу компанію, проблеми можуть виникнути всередині. Людський фактор не варто ігнорувати: випадкові видалення чи обстріли росіян ставлять під загрозу ваші дані. Бекапування за допомогою хмари — це простий, надійний і недорогий спосіб зберегти дані та забезпечити стабільно роботу компанії». ***(Данил Бєлов. Під прицілом кібертерористів — навіщо потрібне бекапування // HiTech.Expert. Хостинг (https://expert.com.ua/178882-pid-prycilom-kiberterorystiv-navischo-potribne-bekapuvannya.html). 13.03.2024).***

***

Сполучені Штати Америки

«…Законодавці штату наполягають на створенні цілодобового оперативного центру безпеки, який допоможе державним коледжам і університетам контролювати та реагувати до зламів мережі.

Оскільки ці типи кібератак стають загрозою, яка швидко розвивається, спричиняючи дорогі перерви в критично важливих операціях, центр безпеки створить постійний центр для запобігання, захисту та реагування на ці атаки.

Місцевий експерт з кібербезпеки поділився, що це означає для установ штату.

«Вища освіта справді зазнає великої кількості різноманітних атак». Том Холт — професор кримінального правосуддя в Університеті штату Мічиган.

Холт сказав: «Деякі з них можна компенсувати досить швидко, тому їхній вплив є мінімальним». Але це стосується не всіх випадків. «Щось на кшталт інциденту з програмами-вимагачами може коштувати мільйони доларів. Витік даних або щось подібне також може коштувати мільйони доларів».

У березні інцидент із кібербезпекою спричинив закриття Lansing Community College на тиждень. У заяві коледжу, надісланій News 10, йдеться,

«Хоча ми не можемо коментувати справу в судовому процесі, LCC не має доказів того, що інформація, пов'язана з цим інцидентом кібербезпеки, була використана не за призначенням. LCC надав сповіщення постраждалим особам із великої обережності, щоб детально розповісти про кроки, які можна та потрібно вжити для захисту від шахрайства та крадіжки особистих даних. Додаткова інформація про інцидент доступна на нашому веб-сайті за адресою www.lcc.edu/alert.html».

Холт назвав центр хорошою ідеєю. «Коли ми думаємо про відмінності в організаційних можливостях, можливо, є університети, які мають менші ресурси або менше часу та інтенсивності, які можна присвятити певній інфраструктурі. Таким чином, його централізація може забезпечити більш узгоджену роботу безпеки в усіх сферах».

Очікується, що експлуатаційні витрати для центру безпеки будуть оплачені членами-учасниками.

Поштовх для центру безпеки було передано до комітету для асигнувань. У разі схвалення послуги будуть доступні для державних шкіл, коледжів і бібліотек по всьому штату». ***(Ta'Niyah Jordan. State lawmakers push for higher education protection against growing cyber security threat // Gray Television, Inc. (https://www.wilx.com/2024/03/01/state-lawmakers-push-higher-education-protection-against-growing-cyber-security-threats/). 02.03.2024).***

***

У сфері кібербезпеки Міністерство внутрішньої безпеки (DHS) і його Агентство з кібербезпеки та безпеки інфраструктури (CISA) відіграють

ключову роль у захисті критичної інфраструктури США. Оскільки DHS досліджує інтеграцію штучного інтелекту (ШІ) для посилення заходів кібербезпеки, державні підрядники опиняються в авангарді цього трансформаційного зусилля. Однак прогрес у впровадженні штучного інтелекту не обходиться без недоліків. Нещодавня оцінка Управління підзвітності уряду («GAO»), опублікована 7 лютого 2024 року, проливає світло на важливі сфери, на яких підрядники повинні зосередити свої зусилля, щоб забезпечити успішне впровадження ШІ.

Виконавчий наказ (EO) № 13960, виданий у 2020 році, зобов'язує DHS вести перелік випадків використання ШІ. Перевірка GAO цього переліку виявила неточності, виявивши помилкову класифікацію певних випадків використання кібербезпеки як штучного інтелекту. Ці розбіжності підкреслюють важливість для підрядників забезпечення точності документування додатків штучного інтелекту в їхніх проектах відповідно до вимог DHS.

Більше того, у звіті GAO було розглянуто дотримання DHS ключових практик, викладених у його структурі підзвітності AI. Незважаючи на те, що DHS досяг прогресу у використанні штучного інтелекту, залишаються прогалини, зокрема в повному запровадженні ключових методів штучного інтелекту GAO, таких як документування джерел даних і забезпечення надійності даних. Для державних підрядників це підкреслює необхідність прискіпливої уваги до деталей протягом усього процесу розробки ШІ, від збору даних до розгортання моделі.

Для підрядників, які займаються проектами кібербезпеки, звіт GAO служить дорожньою картою для навігації в тонкощах впровадження ШІ. Дотримуючись рекомендацій GAO, підрядники можуть посилити можливості DHS у сфері кібербезпеки та покращити захист життєво важливої інфраструктури. Крім того, дотримання цих рекомендацій може посилити конкурентоспроможність підрядників у забезпеченні майбутніх державних контрактів.

Згода DHS з рекомендаціями GAO свідчить про прагнення вдосконалити свої ініціативи щодо ШІ. Проте обов'язок державних підрядників лягає на те, щоб вони активно дотримувалися цих інструкцій і сприяли вдосконаленню практики

кібербезпеки. Співпраця між підрядниками та державними установами буде важливою для подолання викликів і максимального використання потенціалу ШІ для захисту безпеки нашої країни...» ***(Patrick K. Burns and Meredith Thielbahr. Enhancing U.S. Cybersecurity Infrastructure: Implications for Government Contractors in AI Implementation // Gordon Rees Scully Mansukhani, LLP. (https://www.grsm.com/publications/2024/enhancing-u-s-cybersecurity-infrastructure-implications-for-government-contractors-in-ai-implementation). 03.2024).***

***

«28 лютого 2024 року президент Байден підписав виконавчий указ 14117 про «Запобігання доступу країн, що викликають занепокоєння, до масових конфіденційних даних американців і даних, пов'язаних з урядом Сполучених Штатів» (ЕО). ЕО закликає Міністерство юстиції (DOJ) оприлюднити правила, щоб запобігти широкомасштабній передачі конфіденційних персональних даних і даних, пов'язаних з урядом США, «країнам, що викликають занепокоєння».

Білий дім назвав новий виконавчий указ «найзначнішим виконавчим кроком, який будь-який президент коли-небудь вживав для захисту безпеки даних американців». Буде дві можливості для публічного коментаря до того, як будуть видані остаточні положення, яких сторони повинні будуть дотримуватися.

Огляд

ЕО прагне обмежити доступ «країн, що викликають занепокоєння» до масиву конфіденційних персональних даних американців і даних, пов'язаних з урядом США, якщо такий доступ становитиме «неприйнятний ризик для національної безпеки Сполучених Штатів». У довідці фактів, що супроводжує ЕО, зазначається, що «продаж даних американців створює значні ризики для конфіденційності, контррозвідки, шантажу та інших ризиків для національної безпеки, особливо для військовослужбовців або спільноти національної безпеки».

ЕО стверджує, що брокерські компанії, угоди зі сторонніми постачальниками, трудові угоди, інвестиційні угоди та інші подібні домовленості можуть надавати прямий і безперешкодний доступ до конфіденційних даних

американців і, таким чином, створювати неприйнятні ризики для національної безпеки США. Таким чином, ЕО уповноважує Генерального прокурора запобігати широкомасштабній передачі персональних даних американців "країнам, що викликають занепокоєння". Крім того, ЕО наказує багатьом іншим федеральним департаментам і відомствам вжити заходів, включаючи оприлюднення нових правил і положень, щоб приборкати потік «чутливих персональних даних» до «країн, що викликають занепокоєння».

Конфіденційні персональні дані широко визначені ЕО та включають персональні ідентифікатори, геолокацію та пов’язані дані датчиків, біометричні ідентифікатори, людські дані (тобто дані, отримані від людей, які характеризують або кількісно визначають біологічні молекули людини або метаболічні дані), особисті дані про здоров’я, особисті фінансові дані або будь-яка їх комбінація. Однак, які саме типи даних охоплюються цими категоріями, ЕО не встановлюється і буде встановлено в нормативних актах, що впроваджують ЕО. Ми очікуємо, що нормативне визначення, ймовірно, з часом розшириться завдяки прогресу в нових технологіях, таких як штучний інтелект (ШІ), який дозволяє отримати більше особистих уявлень з різноманітних, здавалося б, непов’язаних даних.

Відповідно до країн, визначених у нормативних актах, що впроваджують виконавчий наказ 13873 «Захист інформаційно-комунікаційних технологій і ланцюга постачання послуг». У попередньому повідомленні про запропоновану нормотворчість (ANPRM), опублікованому Міністерством юстиції у зв’язку з ЕО, зазначено, що Міністерство юстиції розглядає можливість визначення Китаю (включаючи Гонконг і Макао), Росії, Куби, Ірану, Венесуели та Північної Кореї як «країн, що викликають занепокоєння».

Міністерство юстиції розглядає дворівневий підхід до впровадження ЕО, згідно з яким певні категорії «транзакцій з дуже конфіденційними даними» будуть заборонені, тоді як інші категорії транзакцій будуть обмежені та можуть здійснюватися за умови, що вони відповідають певним заздалегідь визначені вимоги безпеки для пом'якшення доступу до даних «країнами, що викликають занепокоєння». Міністерство юстиції розглядає можливість визначення двох класів

заборонених транзакцій із даними: (1) транзакції з посередницькими даними та (2) транзакції, пов'язані з передачею масових геномних даних людини або біозразків людини, з яких можна отримати геномні дані людини. Міністерство юстиції також розглядає три класи обмежених транзакцій даних: (1) угоди з постачальниками (включаючи угоди про технологічні послуги та угоди про хмарні послуги); (2) трудові договори; та (3) інвестиційні угоди. Вимоги щодо безпеки, які застосовуються до цих обмежених транзакцій, встановлюватиме Агентство з кібербезпеки та безпеки інфраструктури Міністерства внутрішньої безпеки.

Білий дім охарактеризував політичні цілі ЕО як «конкретні, ретельно вивірені дії» з мінімізації заявленого ризику, пов'язаного з доступом «країн, що викликають занепокоєння» до масиву конфіденційних персональних даних і даних, пов'язаних з урядом США. Президент Байден продовжував наголошувати на важливості всеосяжного федерального законодавства про конфіденційність, знову закликаючи Конгрес прийняти федеральний законопроект про конфіденційність, особливо зосереджений на дітей.

Важливо, що ЕО не висуває жодних загальних вимог до локалізації даних і підкреслює, що США залишаються відданими просуванню відкритого глобального Інтернету та підтримують транскордонні потоки даних і сприяють відкритим інвестиціям. Зосередженість ЕО на перспективних обмеженнях вихідних потоків даних відрізняється від більш вузьких індивідуальних дій, пов'язаних із конкретними транзакціями через такі процеси, як Комітет з іноземних інвестицій у Сполучених Штатах (CFIUS) і Комітет з оцінки іноземної участі. в оглядах сектору телекомунікаційних послуг США (Team Telecom), а також зосереджено увагу на ризиках від іноземних технологій і послуг, що використовуються в Сполучених Штатах відповідно до правил Бюро промисловості та безпеки (BIS) щодо інформаційно-комунікаційних технологій і послуг (ICTS), заповнення діра, яку, на думку адміністрації, ці попередні органи залишили відкритою.

Ключові висновки

Заборони та обмеження щодо певних транзакцій із даними. Компанії, які беруть участь у транзакціях, які включають велику кількість конфіденційних

персональних даних або даних, пов’язаних із урядом США (наприклад, продаж або ліцензування доступу до таких даних), можуть очікувати нових правил відповідно до ЕО. Зокрема, транзакції, пов’язані з брокерськими послугами даних або геномними даними людини, можуть бути заборонені, якщо вони стосуються «країн, що викликають занепокоєння» або «охоплених осіб» (тобто осіб, пов’язаних із «країнами, що викликають занепокоєння», як це буде визначено в правилах Міністерства юстиції). Інші транзакції, пов’язані з угодами з постачальниками, трудовими угодами чи інвестиційними угодами, можуть бути обмежені, якщо вони стосуються «країн, що викликають занепокоєння», або «осіб, яких це стосується».

Зосередьтеся на «країнах, що викликають занепокоєння»: обмеження ЕО зосереджені на національній безпеці та спрямовані на передачу конфіденційних персональних даних до «країн, що викликають занепокоєння», якими Міністерство юстиції розглядає можливість визначити Китай (включно з Гонконгом і Макао), Росію, Кубу, Іран, Венесуела та Північна Корея. Однак Міністерство юстиції розглядає широке визначення «охоплених осіб», яке включало б осіб і компанії, що підпадають під юрисдикцію «країни, що викликає занепокоєння», і включало б іноземних працівників і підрядників цих осіб або організацій. 11 Крім того, для усунення ризику «реекспорту» конфіденційних даних до країн, що викликають занепокоєння, Міністерство юстиції розглядає можливість вимагати, щоб іноземці, на яких не поширюється дія, погоджувалися не перепродавати та не надавати доступ до заборонених або обмежених даних «країні занепокоєння» або «охоплена особа».

Зростаюча увага до мережевої інфраструктури: ЕО визначає підводні кабелі та закордонні центри обробки даних як центри ризику для масових конфіденційних персональних даних або даних, пов’язаних з урядом США. Компанії можуть очікувати створення нових правил, спрямованих на таку інфраструктуру.

Шість категорій конфіденційних персональних даних: ANPRM вказує, що шість категорій конфіденційних персональних даних охоплюватимуть: (1) персональні ідентифікатори громадян США, які охоплюються; (2) особисті фінансові дані; (3) особисті дані про стан здоров’я; (4) точні геолокаційні дані; (5)

біометричні ідентифікатори; і (6) геномні дані людини. Ці широкі категорії конфіденційних персональних даних, які збирає ANPRM, є досить загальними та не охоплюють багато типів персональних даних, які вважаються конфіденційними згідно з іншими законами штатів і федеральними законами США. Це доповнює те, що вже є складною системою захисту даних у США, і вимагає від компаній бути пильними, розуміючи численні зобов'язання та обмеження, які можуть виникнути з будь-якою категорією конфіденційних персональних даних.

Обсяг захищених даних, імовірно, з часом розшириться. Компанії можуть очікувати, що типи захищених даних (тобто, що є конфіденційними персональними даними) будуть предметом значних дебатів під час двох раундів публічних коментарів, які, за словами Міністерства юстиції, відбудуться до того, як він випустить остаточні правила. Незалежно від прийнятих початкових визначень, широке формулювання, яке використовується для встановлення прийнятних категорій у ЕО, означає, що обсяг охоплених даних може з часом збільшуватися та, ймовірно, буде збільшуватися, особливо коли моделі штучного інтелекту, які використовують такі дані, вдосконалюються та дозволяють розширити ідентифікацію осіб з даних, які наразі є менш чутливими на їхньому обличчі.

Підвищена увага до штучного інтелекту: занепокоєння з приводу неправильного або зловмисного використання штучного інтелекту пронизує ЕО і керує його цілями. ЕО зазначає, що розвиток можливостей і алгоритмів штучного інтелекту посилює ризики, пов'язані зі збором великої кількості конфіденційних даних «країнами, що викликають занепокоєння», наприклад, розпізнавання шаблонів у кількох непов'язаних наборах даних і потенційна деанонімізація даних. ЕО додає постійних зусиль адміністрації Байдена щодо управління та пом'якшення ризиків, пов'язаних зі ШІ.

Чіткі заклики до дії для федеральних департаментів і агентств

ЕО є закликом до дії для федерального уряду з широкими повноваженнями для багатьох департаментів і агенцій щодо створення нових правил і забезпечення виконання для розробки інструкцій щодо передачі даних і безпеки для усунення потенційних ризиків, пов'язаних із накопиченням, зберіганням, передачею та

продажем конфіденційної інформації. особисті дані «країнами, що викликають занепокоєння».

Заборонені та обмежені операції

Розділ 2 ЕО наказує Генеральному прокурору, у координації з міністром внутрішньої безпеки та після консультацій з керівниками інших відповідних відомств, протягом 180 днів видати пропоновані нормативні акти, щоб заборонити або обмежити охоплені транзакції, пов’язані з великою кількістю конфіденційних даних або урядом США. -пов'язані дані, де транзакція:

- включає дані, пов’язані з урядом США, або велику кількість конфіденційних персональних даних США;
- підпадає під клас операцій, які були визначені Генеральним прокурором як такі, що становлять неприйнятний ризик для національної безпеки США;
- було розпочато, очікує на розгляд або буде завершено після дати набрання чинності ПН: 28 лютого 2024 р.;
- не має права на звільнення, передбачене в ліцензії, виданій відповідно до постанов, виданих Генеральним прокурором у відповідь на ЕО, або не має дозволу на це; і
- зазвичай не стосується надання фінансових послуг.

Водночас ANPRM заявляє, що нова програма не має на меті перешкоджати всім транзакціям даних із «країнами, що викликають стурбованість», або особами, які підпадають під їх юрисдикцію. Скоріше очікується, що увага буде зосереджена на забороні або обмеженні певних типів операцій із даними між особами США та «країнами, що викликають занепокоєння» (або особами, які перебувають під їхнім контролем чи юрисдикцією), включаючи (1) конкретні категорії конфіденційних персональних даних понад - встановити порогові значення масового обсягу або (2) конкретні категорії даних, пов’язаних з урядом США, незалежно від обсягу.

Те, як Генеральний прокурор остаточно визначає певні терміни та поняття, такі як порогові значення масових конфіденційних даних, «охоплені особи» та «захищені транзакції з даними», суттєво впливатиме на обсяг обмежень щодо операцій з даними. Широкий обсяг може охоплювати більше, ніж традиційний

брокер даних, і охоплювати транзакції від іноземних філій, зареєстрованих у США, які передають масові колекції споживчих даних назад материнським організаціям у відповідних країнах. Як наслідок, глобальні компанії зі споживачами, які мають філії в США, повинні контролювати процес розробки правил ANPRM, щоб визначити його охоплення…

Термін особа, на яку поширюється дія, має широке визначення в ЕО, що включає як організації, що належать або контролюються «країнами, що викликають занепокоєння», так і іноземних осіб, які є працівниками або підрядниками таких організацій або «країн, що викликають занепокоєння». ANPRM передбачає встановлення частки власності, необхідної для ініціювання включення як «охопленої особи», на рівні 50 або більше відсотків власності, прямої чи непрямої. Крім того, ANPRM також передбачає створення публічного списку охоплених осіб, подібного до списків санкцій, які веде Управління контролю за іноземними активами (OFAC) Міністерства фінансів.

Крім того, ANPRM визначає охоплену транзакцію даних як «будь-яку транзакцію, яка включає в себе будь-які конфіденційні персональні дані США або пов’язані з урядом дані та включає: (1) брокерські дані; (2) угоду з постачальником; (3) трудову угоду; або (4) інвестиційний договір». Де транзакція означає «будь-яке придбання, утримання, використання, передачу, транспортування, експорт або операцію з будь-якою власністю, в якій зацікавлена іноземна країна або її громадянин».

Вимоги безпеки до транзакцій

На додаток до нормативних актів, виданих Генеральним прокурором, Розділ 2 ЕО також керує Міністром внутрішньої безпеки, який діє через Директора Агентства з кібербезпеки та безпеки інфраструктури (CISA), у координації з Генеральним прокурором і за консультацією. з керівниками інших відповідних відомств, щоб опублікувати вимоги безпеки для обмежених транзакцій, які, якщо їх дотримуватимуться, зменшуватимуть ризики, пов’язані з такими транзакціями. Міністр внутрішньої безпеки також несе відповідальність за видачу вказівок щодо безпеки для таких вимог.

Запропоновані правила та вимоги безпеки мають бути встановлені шляхом повідомлень і коментування правил, щоб забезпечити громадськості можливість надати свій внесок щодо заходів. ЕО також вимагає встановлення процесу видачі ліцензій для дозволу на операції, які в іншому випадку були б заборонені або обмежені.

Захист конфіденційних персональних даних

У розділі 3 ЕО розглядаються питання національної безпеки США, пов'язані з доступом «країн, що викликають занепокоєння», до масових конфіденційних персональних даних і даних, пов'язаних з урядом США, через мережеву інфраструктуру (наприклад, підводні кабелі), що підпадає під іноземну юрисдикцію чи контроль, і через центри обробки даних розташовані в іноземних юрисдикціях. Розділ 3 також вживає подальших заходів для захисту конфіденційних персональних даних на ринку охорони здоров'я та обмеження певних транзакцій із брокерськими компаніями. ЕО розширює попередні зусилля виконавчої гілки влади щодо вирішення проблеми ланцюга поставок і підключений пристрій кібербезпека, щоб запобігти загрозам для інформації та систем компаній США, уряду США та споживачів.

Перегляд ліцензії та вказівки від Team Telecom: Team Telecom спрямовано:

- переглянути існуючі ліцензії на підводні кабельні системи, якими володіють або керують особи, що належать, контролюються чи підпадають під юрисдикцію чи керівництво відповідної країни, або які закінчуються в межах юрисдикції відповідної країни;
- видати нові вказівки щодо розгляду заявок на отримання ліцензії та існуючих ліцензій, включаючи оцінку ризиків третіх сторін, пов'язаних із доступом до даних «країнами, що викликають стурбованість»; і
- оцінити ризики для національної безпеки та правоохоронних органів, пов'язані з новими ліцензіями, пов'язаними з доступом зацікавлених країн до масиву конфіденційних персональних даних.

Нові обмеження щодо даних на ринку охорони здоров'я: згідно з ЕО, технологічний прогрес (наприклад, штучний інтелект) все частіше дозволяє

«країнам, що викликають занепокоєння» з доступом до великих наборів даних, використовувати такі дані для деанонімізації або повторної ідентифікації даних для отримання інформації. в інформацію про громадян США. ЕО наказує міністрам оборони, охорони здоров'я та соціальних служб, у справах ветеранів і директору Національного наукового фонду розглянути можливість вжиття заходів, у тому числі видання нормативних актів, щоб заборонити надання допомоги, яка дозволяє отримати доступ до масових конфіденційних персональних даних «країнами». викликає занепокоєння». Виконавчі агенції повинні подати звіт про хід виконання цих завдань президенту протягом одного року після ЕО.

Нові обмеження щодо посередництва даних від CFPB: ЕО заохочує Бюро захисту прав споживачів (CFPB) розглянути можливість вжиття заходів для усунення ризику національній безпеці, створеного посередництвом у роботі з даними, і посилити дотримання федерального закону про захист прав споживачів. Зокрема, ЕО пропонує, щоб CFPB продовжував працювати над пропозиціями щодо нормотворення, які він визначив у вересні 2023 року на засіданні консультативної групи малого бізнесу щодо нормотворення споживчих звітів. Директор CFPB Рохіт Чопра опублікував заяву після оголошення ЕО, в якій зазначено, що цього року CFPB запропонує нові правила, щоб «стримувати» брокерів даних від «збирання та продажу надзвичайно конфіденційних даних» іноземним покупцям.

Усунення прогалин у правилах національної безпеки

ЕО є частиною більшої поточної ініціативи Білого дому щодо захисту конфіденційних особистих даних американців і підвищення безпеки цифрової інфраструктури. Послання президента Байдена до Конгресу щодо ЕО підкреслило ці передбачувані ризики, стверджуючи, що «доступ до конфіденційних персональних даних американців або даних, пов'язаних з урядом Сполучених Штатів, збільшує здатність «країн, що викликають занепокоєння», брати участь у широкому діапазоні зловмисної діяльності, включаючи шпигунство, вплив, кінетичні чи кібероперації, або для виявлення інших потенційних стратегічних переваг над Сполученими Штатами». ЕО прагне заповнити прогалину в наборі інструментів національної безпеки, який виконавча влада зібрала в останні роки,

наближаючи Сполучені Штати до цілісної структури для управління ризиками безпеки даних в рамках існуючих органів виконавчої влади.

Адміністрація Байдена стверджує, що ЕО дозволить Сполученим Штатам запровадити чіткі, перспективні загальногалузеві правила для масових транзакцій із конфіденційними особистими даними, зосередивши увагу на вихідних потоках даних США. Роль ЕО у стратегії національної безпеки ставить його поруч із правилами ICTS, зусилля щодо просування надійних постачальників мережевого обладнання 5G і архітектури Open RAN, посилення перевірки підводних кабельних з'єднань і ліцензій на посадку, CFIUS, що перевіряє вхідні інвестиції (причому конфіденційні персональні дані є особливою увагою обох розширених юридичних повноважень відповідно до Закону про модернізацію аналізу ризиків іноземних інвестицій) 2018 рік і розпорядження президента Байдена CFIUS від 2022 року), діяльність Team Telecom, майбутня програма, що регулює певні зовнішні інвестиції, і нещодавнє розширення експортного контролю, спрямованого на передові напівпровідники.

Наслідки для політики США щодо транскордонних потоків даних

ЕО є однією з кількох нещодавніх дій, які викликають сумніви щодо того, наскільки Сполучені Штати все ще підтримують відкриті транскордонні потоки даних. Сполучені Штати рішуче підтримували відкриті транскордонні потоки даних у минулих угодах про вільну торгівлю та на міжнародних форумах, зокрема у нещодавній Угоді між США, Мексикою та Канадою (USMCA) та Угоді про цифрову торгівлю між США та Японією (US-Japan DTA). містить найсильніші зобов'язання щодо захисту транскордонних потоків даних, які містяться в будь-яких торгових угодах. 28 Незважаючи на цей запис, у 2023 році Офіс торгового представника США (USTR) відмовився від захисту положень торгової угоди, які забезпечують вільний транскордонний потік даних, виступають проти вимог локалізації серверів і захищають вихідний код від розголошення. Скасування USTR викликало запеклі дебати у Вашингтоні, але ступінь, до якого він представляє значущу зміну напрямку для Сполучених Штатів, залишається незрозумілим.

Адміністрація Байдена продовжує підтримувати ініціативи щодо транскордонних потоків даних, такі як політика G7 щодо вільного потоку даних із довірою (DFFT). Адміністрація посилалася на ці поточні ініціативи в повідомленні ЕО, стверджуючи, що ЕО узгоджується з «давньою підтримкою Сполучених Штатів надійного вільного потоку даних». ANPRM Міністерства юстиції також стверджує, що дії «ретельно відкалібровані» для підтримки «давньої підтримки Сполученими Штатами концепції «вільного потоку даних з довірою». На знак визнання його важливості для економіки та прав людини в Інтернеті».

Зокрема, розділ 2(g) ЕО забороняє правилам вимагати внутрішнього зберігання та обробки даних як частину реалізації ЕО, що звужує те, як ЕО може оскаржувати існуючі норми. Зобов'язання проти мандатів на локалізацію серверів даних у USMCA та американсько-японському DTA не включають виняток публічної політики, як той, що міститься в зобов'язаннях щодо транскордонних потоків даних. Незважаючи на запевнення адміністрації щодо вузького підходу, обмеження ЕО — особливо в поєднанні з нещодавніми діями USTR — все ще можуть викликати занепокоєння та ризики для галузей, які залежать від цифрових послуг.

Наслідки для потоків даних у США

Хоча ЕО безпосередньо не впливає на систему передачі персональних даних між ЄС і США або UK-US Data Bridge, 33 Організації, які передають дані до США, повинні стежити за розробкою нормативних актів ЕО. Це буде особливо цікаво для організацій, розташованих у юрисдикціях (або під впливом) юрисдикцій, які накладають обмеження на міжнародну передачу даних (наприклад, ЄС і Великобританія), оскільки імплементаційні правила та нові вимоги відповідності можуть вплинути на статус відповідності міжнародної передачі даних структури, які були прийняті для задоволення вимог законодавства не США.

Організації в Європі десятиліттями підлягали обмеженням на передачу даних, а передача даних до США була особливою причиною для занепокоєння в останні роки. Це призвело до розробки низки стратегічних варіантів структурування внутрішньої та зовнішньої міжнародної передачі даних, що

стосується організацій, на які поширюється дія законів у різних юрисдикціях (включаючи США).

Запровадження подальших заходів захисту та обмежень у США щодо передачі даних до юрисдикцій, які створюють підвищений ризик неправомірного використання, буде сприйнято як позитивний крок для багатьох у юрисдикціях (таких як Європа), які зараз накладають обмеження на передачу.

Можливості для відгуків зацікавлених сторін

Оскільки уряд розробляє імплементаційні нормативні акти ЕО, у зацікавлених сторін буде багато можливостей надати відгуки щодо пропозицій уряду. Компанії, задіяні в постраждалих галузях, включаючи брокерів даних і постачальників хмарних послуг, які зацікавлені в результатах, можуть надати коментар Міністерству юстиції у відповідь на ANPRM. ANPRM також спеціально шукає технічний відгук щодо ключових термінів та інших конкретних питань. Важливі визначення, якими керуватиметься імплементація правил, включають визначення «особи США», «операції з даними, на які поширюється дія», «країни, що викликають занепокоєння», «особи, на яких поширюється дія», «посередництво в даних», «конфіденційні персональні дані» та «урядові дані США». пов’язані дані». Міністерство юстиції має розглянути коментарі громадськості в остаточному правилі, тому участь у процесі громадського обговорення може допомогти сформувати остаточний результат, а відповідь Міністерства юстиції може повідомити про будь-які потенційні юридичні оскарження в разі публікації остаточного правила. ANPRM Міністерства юстиції буде відкритий для публічних коментарів протягом 45 днів після запланованої публікації у Федеральному реєстрі 5 березня 2024 року». ***(John Timmons, Hope Anderson, Cristina Brayton-Lewis, Farhad Jalinous, Karalyn Mildorf, F. Paul Pittman, Earl Comstock, Ian Saccomanno and Andrew L. Black. New Executive Order Seeks to Protect Americans' Sensitive Personal Data // White & Case (https://www.whitecase.com/insight-alert/new-executive-order-seeks-protect-americans-sensitive-personal-data). 04.03.2024).***

***

«…29 лютого 2024 року Білий дім і Міністерство торгівлі («Комерція») оголосили про публікацію попереднього повідомлення про запропоновану нормотворчість («ANPRM») для підтримки розслідування урядом США щодо ризиків для національної безпеки підключених транспортних засобів («CV»), які включають інформаційно-комунікаційні технології та послуги («ICTS») з Китаю та інших «іноземних противників».

Торговельне бюро промисловості та безпеки («BIS») опублікувало ANPRM у Федеральному реєстрі 1 березня 2024 року, щоб отримати відгуки від зацікавлених сторін галузі, які «допоможуть BIS у визначенні технологій та учасників ринку, які можуть бути найбільш прийнятними для регулювання». Сюди входять виробники оригінального автомобільного обладнання («OEM»), постачальники першого, другого та третього рівнів, компанії з продажу запчастин і постачальники послуг. BIS зокрема розглядає можливість запропонувати правила, які б 1) забороняли певні транзакції з «іноземними супротивниками» за участю ICTS, невід'ємної частини підключених транспортних засобів, і 2) дозволяли учасникам ринку брати участь в інших заборонених транзакціях, якщо ризики їхньої національної безпеки можуть бути достатньо зменшені.

ANPRM прагне отримати коментарі щодо ряду питань, пов’язаних із (i) ризиками та вразливими сторонами включення ICTS у підключені транспортні засоби, (ii) ефективністю заходів пом’якшення наслідків для транзакцій ICTS із залученням підключених транспортних засобів, (iii) потенційними механізмами впровадження для накладення обмежень щодо транзакцій ICTS із залученням підключених транспортних засобів, і (iv) потенціал для механізму схвалення для деяких інших заборонених транзакцій. BIS збирає коментарі протягом 60 днів на ці теми, серед іншого, як значний крок до імплементації правил, що обмежують транзакції ICTS в автомобільному секторі. Період подання коментарів закінчується 30 квітня 2024 року.

ANPRM було видано згідно з виконавчим наказом (EO) 13873 (EO, виданим адміністрацією Трампа в 2019 році), який надає Коммерції повноваження переглядати, пом’якшувати або забороняти транзакції ICTS з організаціями, які

підпадають під юрисдикцію «іноземного противника». і слідує моделі нещодавніх дій агентства, додаючи пов’язані програмні додатки до обсягу транзакцій ICTS, які підлягають перевірці.

Цей ANPRM є частиною ширших зусиль адміністрації Байдена щодо усунення ризиків національній безпеці США, пов’язаних із розширеним охопленням китайських технологій підключення (наприклад, підключених програмних додатків, навігації, допомоги водієві та інших розширених функцій) і підключених транспортних засобів у Автомобільний ринок США. Адміністрація стурбована великою кількістю конфіденційних даних, які транспортні засоби збирають про пасажирів і водіїв, включаючи інформацію, зібрану за допомогою камер і датчиків. Це занепокоєння також поширюється на здатність підключених транспортних засобів збирати інформацію про критичну інфраструктуру, а також на здатність цих транспортних засобів дистанційно керувати та відключати. На додаток до видання нових правил відповідно до ICTS EO, адміністрація також розглядає можливість підвищення тарифів на імпорт китайських транспортних засобів і запчастин у рамках більш широкого перегляду тарифів розділу 301 на китайський імпорт. Ці кроки віддзеркалюють нещодавні занепокоєння, висловлені також законодавцями на Капітолійському пагорбі, і можуть заборонити китайським автовиробникам продавати транспортні засоби, включно з електромобілями, на ринку США з причин, пов’язаних як з національною безпекою, так і з загальною економічною конкурентоспроможністю США. ринку.

Громадські коментарі щодо запропонованого правила мають бути подані до 30 квітня 2024 року.

Фон

У травні 2019 року адміністрація Трампа видала розпорядження 13873 «Захист інформаційно-комунікаційних технологій і ланцюга постачання послуг». EO оголосив необмежене розгортання та використання іноземних супротивників ICTS у ланцюгах поставок США надзвичайною ситуацією та уповноважив міністра торгівлі заборонити певні операції з ICTS, які були «спроектовані, розроблені, виготовлені або поставлені особами, що належать, контролюються з боку

іноземного супротивника або підпадає під його юрисдикцію чи керівництво» та становлять «неприйнятний ризик» для національної безпеки або «невиправданий ризик» для критичної інфраструктури.

У подальших правилах імплементації Commerce виклав процедури, за допомогою яких агентство може переглядати транзакції ICTS, щоб визначити, чи становлять вони надмірний або неприйнятний ризик через участь іноземного супротивника. Цю структуру було розширено, щоб охопити конкретні загрози ICTS, наприклад підключене програмне забезпечення з іноземних країн-супротивників. Ця найновіша норма BIS в рамках EO підтримує нещодавно заявлену місію BIS щодо впровадження програми ICTS.

Визначення підключених транспортних засобів

ANPRM шукає інформацію щодо визначення «підключеного транспортного засобу», який агентство пропонує визначити як «автомобільний транспортний засіб, який інтегрує бортове мережеве обладнання з автомобільними програмними системами для зв'язку через виділений зв'язок малого радіусу дії, стільниковий телекомунікаційний зв'язок, супутниковий зв'язок або підключення іншого бездротового діапазону до будь-якої іншої мережі чи пристрою».

Щоб належним чином визначити сферу визначення CV для правил, які включають ICTS, невід'ємні від CV, BIS шукає інформацію щодо:

Чи слід і яким чином BIS вносити зміни до свого визначення CV, і якщо так, то як переглянуте визначення дозволить BIS краще врахувати ризики національної безпеки, що виникають через класи транзакцій, що включають ICTS, невід'ємну частину CV;

Чи є термін «підключений транспортний засіб» достатньо широким, щоб охоплювати автономні транспортні засоби, електромобілі або інші альтернативні джерела енергії та пов'язані технології, чи існує кращий термін для опису цього широкого обсягу;

Чи існують інші загальновживані визначення для CV, які BIS має враховувати при визначенні класу транзакцій ICTS, включаючи визначення від промисловості, громадянського суспільства та іноземних організацій.

Ризики та вразливі місця підключених транспортних засобів

ANPRM також шукає інформацію про конкретні ризики національній безпеці, створені ланцюгом постачання CV ICTS, зокрема від ICTS з Китаю. BIS виділяє CV ICTS із Китаю як значну проблему через операції кібершпигунства в країні, її правову структуру, яка надає державі право кооптувати приватні компанії для досягнення своїх цілей, і повідомляє, що автовиробники в Китаї юридично зобов'язані передавати дані в реальному часі дані про транспортні засоби, включаючи інформацію про геолокацію, до центрів моніторингу китайського уряду.

BIS також прагне зрозуміти, як прогрес у технології підключення до автомобілів може наражати CV або сектори, які вони підтримують, на нові форми кіберексплуатації та вразливості. BIS пропонує ідентифікувати наступні автомобільні програмні системи як ICTS, невід'ємну частину CV, які, швидше за все, становлять надмірні або неприйнятні ризики, якщо їх використовують іноземні супротивні організації: (i) операційні системи транспортних засобів; (ii) телематичні системи; (iii) передові системи допомоги водієві; (iv) автоматизовані системи водіння; (v) супутникові або стільникові телекомунікаційні системи; та (vi) системи керування акумулятором.

Оцінюючи, як запровадити правила, застосовні до цих програмних систем, ANPRM запитує коментарі з широкого кола тем, включаючи:

Склад ланцюжка постачання CV ICTS (включаючи, які частини ланцюга постачання CV ICTS зацікавлені сторони вважають невід'ємною частиною CV, які частини ланцюга постачання наразі надходять з іноземних країн-супротивників, які існують альтернативи для ICTS, що надходять з іноземних країн-супротивників, і де зберігаються дані CV ICTS);

Взаємовідносини між OEM-виробниками CV та постачальниками ICTS у Сполучених Штатах (включаючи відносини між OEM-виробниками та постачальниками хмарних послуг, можливостями OEM-віддаленого доступу та збору даних, а також характер партнерства OEM-розробників програмного забезпечення);

Які ICTS, інтегровані в CV, найбільш вразливі до компрометації та використання (включаючи системи збору даних і датчики, системи підключення та віддаленого доступу, системи керування акумулятором і заряджання), а також інформацію про цикл розробки програмного забезпечення для цих систем.

Механізми авторизації та заходи пом'якшення

Нарешті, ANPRM шукає інформацію щодо механізмів, за допомогою яких BIS може дозволити заборонену в іншому випадку транзакцію CV ICTS із заходами пом’якшення, які дозволяють забезпечити достатній моніторинг для вирішення проблем національної безпеки США.

Зокрема, ANPRM збирає коментарі щодо:

Коли тимчасовий дозвіл буде необхідним, щоб уникнути збоїв у ланцюзі поставок або інших небажаних наслідків;

Критерії та заходи пом’якшення, які BIS має враховувати при розгляді заявки на отримання тимчасового дозволу (наприклад, найкращі практики кібербезпеки, стандарти розробки програмного забезпечення);

Чи слід BIS моделювати свою процедуру авторизаційного механізму на основі програм авторизації інших агентств, таких як Управління з контролю за іноземними активами або процедури ліцензування BIS.

Наступні кроки

Компанії, які оцінюють вплив нормативних актів, які можуть дотримуватися цього ANPRM, включно з виробниками оригінального обладнання, постачальниками автомобільного обладнання, компаніями післяпродажного обслуговування запасних частин і постачальниками послуг, повинні враховувати свій глобальний ланцюг постачання ICTS, ступінь, до якого він включає ICTS, інтегровану в підключені транспортні засоби, а також стандарти кібербезпеки та найкращі практики». ***(Ajay Kuntamukkala, Kelly Ann Shaw, Stephen F. Propst, Patrick Miller and Meghan Anand. Biden Administration investigates national security risks of Chinese connected vehicles in the U.S. // Hogan Lovells (https://www.engage.hoganlovells.com/knowledgeservices/news/biden-administration-***

investigates-national-security-risks-of-chinese-connected-vehicles-in-the-us). 05.03.2024).

***

«Національний інститут стандартів і технологій («NIST») випустив суттєве оновлення своєї структури, розширивши його сферу дії та охоплення, щоб охопити ширшу аудиторію та нові ризики кібербезпеки та проблеми управління.

26 лютого 2024 року NIST випустив свою оновлену Cybersecurity Framework 2.0 («CSF 2.0»), яка є першим великим оновленням оригінальної структури 2014 року. Ця подія має значні правові наслідки, оскільки організації все частіше звертаються до інфраструктури NIST для розробки та впровадження програм кібербезпеки та вимірювання їх ефективності. У той час як оригінальна структура була призначена для організацій критичної інфраструктури, CSF 2.0 зосереджена на низці організацій будь-якого розміру, сектору та рівня зрілості кібербезпеки, і представляє еволюцію найкращих практик і методологій, адаптованих для вирішення нових проблем управління кібербезпекою, що розвиваються. Незважаючи на те, що CSF 2.0 зберігає оригінальні компоненти, він розширює свою сферу дії, включаючи вказівки щодо кіберуправління та управління ризиками, штучного інтелекту, ланцюжка постачання та управління ризиками третіх сторін, архітектури нульової довіри та безпеки Інтернету речей.

Основною основною зміною є запровадження управління кібербезпекою та управління ризиками як центральної функції структури. Відповідно, CSF 2.0 додає Govern до початкових п’яти ключових функцій: Identify, Protect, Detect, Respond і Recover. Функція управління зосереджується на управлінні ризиками кібербезпеки та нагляді за допомогою розподілу ролей, обов’язків і повноважень для узгодження ризиків кібербезпеки організації з існуючим корпоративним управлінням ризиками. Цей новий акцент на управлінні збігається з випадками, коли федеральні регулятори притягували виконавче керівництво до відповідальності за збої в

кібербезпеці. Оновлена структура також містить новий довідковий інструмент, спеціальні посібники для швидкого початку роботи та приклади впровадження.

Основна увага CSF 2.0 на управлінні ризиками кібербезпеки відбувається після нових зобов'язань щодо управління ризиками кібербезпеки та розкриття інформації, накладених Комісією з цінних паперів і бірж на публічні компанії. Крім того, державні установи все більше впроваджують у контракти та субконтракти вимоги, які вказують на вказівки NIST щодо захисту конфіденційної інформації, включаючи нещодавно опубліковане правило Міністерства оборони, яке викладає сертифікацію моделі зрілості кібербезпеки (CMMC) 2.0. Як додатковий приклад актуальності цієї структури, Федеральна торгова комісія («FTC») вказала на структуру кібербезпеки NIST як узгоджену з підходом, заснованим на процесах, якого FTC очікує від суб'єктів господарювання при реалізації програм кібербезпеки.

Оскільки регулюючі органи впроваджують CSF 2.0 як основу для різноманітних підходів до забезпечення кібербезпеки, організаціям слід активно оцінювати свої програми управління кібербезпекою та управління ризиками, щоб зменшити ризики судових розглядів і правозастосування». ***(Donald F. Mcgahn II (Don), Mauricio F. Paez, Lisa M. Ropple, Schuyler J. Schouten and D. Grayson Yeargin. NIST Extends its Cybersecurity Framework to Cover Evolving Threats and Governance // Jones Day (https://www.jonesday.com/en/insights/2024/03/nist-extends-its-cybersecurity-framework-to-cover-evolving-threats-and-governance). 03.2024).***

***

«Білий дім опублікував пропозицію щодо бюджету на 2025 фінансовий рік у розмірі 7,3 трильйона доларів, і адміністрація знову хоче збільшити витрати на кібербезпеку.

У кількох розділах бюджетного плану президента Байдена на 2025 рік згадуються витрати на кібербезпеку. Це включає 13 мільярдів доларів на фінансування кібербезпеки в цивільних департаментах і агентствах.

Адміністрація хоче, щоб агентство з кібербезпеки CISA мало бюджет у 3 мільярди доларів, що означає збільшення на 103 мільйони доларів. Цей бюджет включає 470 мільйонів доларів США на розгортання засобів виявлення кінцевих точок і реагування на них та інших мережевих інструментів, майже 400 мільйонів доларів США на внутрішню кібербезпеку та аналітичні можливості та понад 150 мільйонів доларів США на звітування про кіберподії критичної інфраструктури та координацію безпеки.

Минулого року CISA заявила, що у неї недостатньо персоналу, щоб реагувати на значні атаки OT у кількох місцях одночасно, і запросила додаткове фінансування для поїздок підрядників, необхідних для надання послуг реагування на інциденти.

Нова бюджетна пропозиція також має на меті розширити можливості Міністерства юстиції щодо боротьби з кіберзагрозами. Це включає додаткові 25 мільйонів доларів США на можливості ФБР з кіберреагування та 5 мільйонів доларів на розширення нового відділу, орієнтованого на кібернетичні проблеми, у відділі національної безпеки Міністерства юстиції. У бюджетному плані також пропонується виділити 2 мільйони доларів, щоб Міністерство юстиції могло підтримати виконання розпорядження про безпеку та безпеку штучного інтелекту.

Білий дім хоче зміцнити штучний інтелект, кібербезпеку та стійкість в енергетичному секторі, пропонуючи 455 мільйонів доларів на «розширення кордонів штучного інтелекту для науки та технологій, а також підвищення безпеки, безпеки та стійкості штучного інтелекту».

Що стосується кібербезпеки в секторі охорони здоров’я, бюджет передбачає 800 мільйонів доларів США на допомогу лікарням у покращенні безпеки, а також додаткові 500 мільйонів доларів США на програму стимулювання, щоб заохотити всі лікарні інвестувати в передові методи кібербезпеки. Адміністрація Байдена також хоче отримати 141 мільйон доларів на продовження зміцнення здатності HHS захищати та захищати свої системи та інформацію.

Безпека підприємства також передбачена бюджетним планом, який включає 150 мільйонів доларів США на рахунок підвищення кібербезпеки Міністерства фінансів, що на 50 мільйонів доларів більше, ніж у 2023 році.

Більше фінансування також буде надано Міністерству фінансів, щоб допомогти йому запровадити архітектуру нульової довіри та інші зусилля з кібербезпеки.

Бюро фіскальної служби отримає додаткові 24 долари порівняно з 2023 роком, на загальну суму майже 400 мільйонів доларів, щоб «поліпшити безпеку основних державних фінансових систем шляхом модернізації та переведення всіх додатків для мейнфреймів у безпечну хмару». ***(Eduard Kovacs. White House Budget Proposal Seeks Cybersecurity Funding Boost // SecurityWeek (https://www.securityweek.com/white-house-budget-proposal-seeks-cybersecurity-funding-boost/). 13.03.2024).***

***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) нещодавно оголосило про пріоритети кібербезпеки на 2024 рік для Об'єднаного співробітництва з кіберзахисту (JCDC). Шість пріоритетів згруповані в три основні напрямки, розроблені для гармонізації цілей кібербезпеки та зусиль між державними та галузевими партнерствами для захисту критичної інфраструктури. На перший погляд може здатися, що ці пріоритети не пов'язані з вашою повсякденною операційною діяльністю.

Ось практичні рекомендації щодо кібербезпеки, щоб узгодити стратегію кібербезпеки операційних технологій (OT) із пріоритетами JCDC, що покращить стійкість вашої кібербезпеки.

Фокус 1: Захист від розширених операцій постійної загрози (APT).

Пріоритет 1: виявлення та захист від зловмисних зловживань з боку учасників APT, особливо тих, яких підтримує Китайська Народна Республіка, на інфраструктурі США та проти неї.

Рекомендація: Використовуйте зовнішніх постачальників послуг аналізу загроз, які зосереджені на галузях критичної інфраструктури та суб'єктах загроз національних держав. Ці рішення забезпечують індикатори компрометації, які можуть бути впроваджені в такі технології кібербезпеки, як брандмауери та керування подіями безпеки та інформацією, покращуючи захист від кіберзагроз і їх виявлення. Вони також надають тактику, методи та процедури, що використовуються суб'єктами загроз, покращуючи пріоритезацію вразливостей, полювання на загрози та можливості реагування на інциденти. Наявність правильного інтелекту полегшує прийняття кращих рішень і дає змогу покращити виявлення загроз і реагування на них.

Пріоритет 2: Підготуйтеся до великих кіберінцидентів.

Рекомендація: кажуть, що практика робить досконалого. Не прагніть до досконалості, але практикуйте свої процедури реагування на інциденти достатньо, щоб стати професіоналом. Масштабна кібератака на об'єкти критичної інфраструктури може мати катастрофічні фізичні наслідки для навколишнього середовища, безпеки людей і доступності державних послуг. Реагування на кіберінциденти в середовищах OT вимагає іншого підходу. Ефективне реагування передбачає безперебійну координацію між кібер-, фізичними та оперативними командами, що може стати реальністю лише за умови регулярного реагування на інциденти. Виконуйте щонайменше щорічні вправи, але ідеальним є щоквартальний ритм.

Фокус 2: підвищення рівня кібербезпеки

Пріоритет 3: Допоможіть державним і місцевим виборчим органам захистити свої мережі та інфраструктуру від кіберзагроз у рамках ширшої діяльності CISA щодо безпеки виборів.

Рекомендація: навіть якщо ви не берете безпосередньої участі у виборчій інфраструктурі та механізмах, ваша організація все одно відіграє певну роль у забезпеченні чесного та безпечного виборчого процесу. Будьте в курсі наративних атак, які використовують дезінформацію та дезінформацію у зв'язку з вашою компанією для маніпулювання сприйняттям. Оновіть свою програму аналізу загроз,

щоб відстежувати відкриті та темні веб-джерела на наявність таких типів атак. Вбудуйте в свій план реагування на інциденти процеси, щоб швидко визначити точність інформації та повідомити правду, щоб мінімізувати вплив на ваш бренд і відновити довіру до виборчого процесу.

Пріоритет 4: помітно зменшити вплив програм-вимагачів на критичну інфраструктуру.

Рекомендація: у 2023 році кількість програм-вимагачів різко зросла й не має ознак сповільнення. Немає швидкого рішення щодо загрози програм-вимагачів, тому організації повинні зосередитися на основах кібербезпеки, зокрема інвестувати в технології, розроблені для ОТ, які відповідають випадкам використання, таким як виявлення та ідентифікація активів. Паралельно розгортайте інструменти виявлення загроз і аномалій, будуючи решту своєї стратегії кібербезпеки. Щоб збільшити охоплення та мінімізувати збої, вам слід запланувати поєднання рішень безпеки ОТ для пасивного й активного сканування.

Пріоритет 5: досягти відчутного прогресу на шляху до світу, де технології безпечні за своїм дизайном.

Рекомендація: було б легко звернути увагу на розробників і виробників оригінального обладнання (OEM), але покупці також несуть відповідальність. Покупці повинні чинити тиск на OEM-виробників, вимагаючи більш потужних функцій кібербезпеки, таких як надійний контроль доступу, замість того, щоб чекати, поки законодавчі акти приведуть до змін, і бути готовими платити за це. Пристрої промислової автоматизації довго живуть у середовищі ОТ, тому цю зміну слід розпочати сьогодні.

Фокус 3: Передбачте нові технології та ризики

Пріоритет 6: Зменшення ризику, який створює штучний інтелект для критичної інфраструктури.

Рекомендація: не хвилюйтеся зараз про штучний інтелект в середовищах ОТ і зосередьтеся на захисті хмарних розгортань. Хмарні рішення не можна вважати новою технологією, але впровадження в середовищах ОТ зростає та становить значний ризик для роботи критичної інфраструктури. Це вимагає впровадження

надійного режиму керування хмарою, обов'язкового інструментарію безпеки та інструментів для всіх хмарних робочих навантажень. Вбудуйте безпеку в хмарні розгортання з самого початку, щоб реалізувати переваги, які може запропонувати хмара, мінімізуючи ризики». ***(Put New Joint Cyber Defense Collaborative Priorities Into Action // Forbes (https://www.forbes.com/sites/forrester/2024/03/14/put-new-joint-cyber-defense-collaborative-priorities-into-action/?sh=59191911752f). 14.03.2024).***

***

«Реальність кібербезпеки для компаній полягає в тому, що зловмисники весь час компрометують системи та мережі, і навіть добре керовані програми запобігання зламу часто мають справу зі зловмисниками всередині своїх периметрів.

5 березня Агентство національної безпеки (NSA) продовжило свої рекомендації щодо найкращих практик для федеральних відомств, опублікувавши свій останній Інформаційний бюллетень з кібербезпеки (CIS) щодо мережевих і середовищних компонентів своєї системи нульової довіри. Документ NSA рекомендує організаціям сегментувати свої мережі, щоб обмежити доступ неавторизованих користувачів до конфіденційної інформації за допомогою сегментації. Це тому, що потужні заходи кібербезпеки можуть зупинити перетворення компромісів у повномасштабні зломи, обмеживши доступ усіх користувачів до тих ділянок мережі, у яких вони не мають законної ролі.

Керівництво від NSA також дозволяє групам безпеки надавати керівництву сильніші бізнес-обгрунтування для захисту безпеки, але CISO повинні встановити очікування, оскільки впровадження є багаторівневим і складним процесом.

Незважаючи на те, що документ спрямований на державні організації та галузі, пов'язані з обороною, діловий світ може отримати вигоду від вказівок щодо нульової довіри, каже Стів Вінтерфельд, консультант CISO гіганта інтернет-послуг Akamai.

«Реальність полягає не в тому, [чи] у вас є випадки несанкціонованого доступу, а в тому, чи вдасться вам їх зафіксувати, перш ніж вони стануть

порушенням», — каже він. «Ключ — це «видимість із контекстом», яку може забезпечити мікросегментація, підкріплена здатністю швидко ізолювати зловмисну поведінку».

Компанії почали ініціативи з нульової довіри, щоб зробити свої дані, системи та мережі складнішими для компрометації та, якщо вони скомпрометовані, уповільнити зловмисників. Фреймворк — це надійний набір вказівок щодо того, як діяти далі, але реалізувати його нелегко, — каже Майк Местровіч, CISO у Rubrik, постачальнику послуг безпеки даних і нульової довіри.

«Більшість мереж еволюціонували з часом, і дуже важко повернутися назад і перебудувати їх, зберігаючи бізнес», — говорить він. «Це можливо, але це може бути дорогим як з точки зору часу, так і грошей».

Ось шість висновків із вказівок NSA.

1. Вивчіть усі сім основ нульової довіри

В останньому документі Агентства національної безпеки йдеться про п’ятий стовп із семи стовпів нульової довіри: мережу та середовище. Проте інші шість стовпів є не менш важливими й показують, «наскільки широкомасштабною та трансформаційною має бути стратегія нульової довіри, щоб бути успішною», — говорить Ешлі Леонард, генеральний директор Syxsense, фірми, що займається автоматизованим керуванням кінцевими точками та вразливими місцями.

«Компанії, які хочуть розпочати роботу з нульовою довірою, я б настійно заохочував їх переглянути інформаційні листи NSA щодо користувачів і пристроїв — першого та другого стовпів нульової довіри відповідно», — каже він. «Якщо компанія тільки починає роботу, дивлячись на цей стовп мережі та середовища, це все одно, що поставити віз перед конем».

2. Очікуйте, що зловмисники порушать ваш периметр

Стовп мережі та середовища плану нульової довіри NSA спрямований на те, щоб зупинити зловмисників від розширення злому після того, як вони вже скомпрометували систему. Інструкції NSA вказують на порушення Target 2013 року — без прямого вказівки компанії — через те, що зловмисники проникли через вразливість у сторонній системі HVAC компанії, але потім змогли пересуватися

через мережу та заразити пристрої торгових точок. зі шкідливим програмним забезпеченням.

Компанії повинні припустити, що вони будуть скомпрометовані, і знайти способи обмежити або уповільнити зловмисників, заявив директор відділу кібербезпеки NSA Роб Джойс у заяві, оголосивши про публікацію документа NSA.

«Організації повинні працювати з думкою, що загрози існують у межах їхніх систем», — сказав він. «Це керівництво має на меті озброїти власників і операторів мереж процесами, необхідними їм для пильного протистояння, виявлення та реагування на загрози, які використовують слабкі місця або прогалини в архітектурі їхнього підприємства».

3. Відобразіть потоки даних для початку

Керівництво NSA є багаторівневою моделлю, де компаніям слід починати з основ: відображення потоків даних у їхніх мережах, щоб зрозуміти, хто до чого має доступ. У той час як інші підходи до нульової довіри були задокументовані, як-от архітектура нульової довіри NIST SP 800-207, основи NSA дають можливість організаціям думати про засоби контролю безпеки, каже Вінтерфельд з Akamai.

«Розуміння потоку даних насамперед забезпечує ситуаційне усвідомлення того, де та які потенційні ризики», — каже він. «Пам’ятайте, ви не можете захистити те, про що не знаєте».

4. Перейдіть до макросегментації

Після розгляду будь-яких інших фундаментальних компонентів компаніям слід почати свій набіг на стовп мережі та середовища, сегментуючи свої мережі — можливо, спочатку широко, але з дедалі більшою деталізацією. Основні функціональні сфери включають сегменти «бізнес-бізнес» (B2B), сегменти, орієнтовані на споживача (B2C), операційні технології, такі як IoT, мережі торгових точок і мережі розробки.

Після сегментації мережі на високому рівні компанії повинні прагнути до подальшого вдосконалення сегментів, каже Местрович з Rubrik.

«Якщо ви можете визначити ці функціональні області роботи, тоді ви можете почати сегментувати мережу так, щоб автентифіковані об’єкти в жодній із цих

областей не мали доступу без виконання додаткових вправ автентифікації в будь-яких інших областях», — говорить він. «У багатьох відношеннях ви побачите, що дуже ймовірно, що користувачам, пристроям і робочим навантаженням, які працюють в одній області, насправді не потрібні права або ресурси для роботи в інших областях».

5. Зрілий до програмно-визначеної мережі

Мережі з нульовою довірою вимагають від компаній здатності швидко реагувати на потенційні атаки, що робить програмно-визначену мережу (SDN) ключовим підходом не лише до мікросегментації, але й до блокування мережі під час потенційного компрометування.

Проте SDN — не єдиний підхід, каже Вінтерфельд з Akamai.

«SDN більше стосується управління операціями, але залежно від вашої інфраструктури це може бути не оптимальним рішенням», — каже він. «Тим не менш, вам дійсно потрібні типи переваг, які надає SDN, незалежно від того, як ви створюєте своє середовище».

6. Усвідомте, що прогрес буде повторюватися

Нарешті, будь-яка ініціатива нульової довіри — це не одноразовий проект, а постійна ініціатива. Організаціям потрібно не лише мати терпіння та наполегливість у розгортанні технології, але й командам із безпеки необхідно переглянути план і змінити його, коли вони стикаються з труднощами та їх подолають.

«Коли ви думаєте про те, щоб розпочати шлях із нульовою довірою, їхні вказівки щодо відображення потоків даних, а потім їхнього сегментування є доречними, — говорить Вінтерфельд, — але я б додав, що це часто повторюється, оскільки у вас буде період відкриття, який вимагатиме оновлення плану». ***(Robert Lemos. 6 CISO Takeaways From the NSA's Zero-Trust Guidance // Informa PLC (https://www.darkreading.com/cybersecurity-operations/6-ciso-takeaways-nsa-zero-trust-guidance?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 15.03.2024).***

***

«Настав податковий сезон 2024 року, і мільйони американців готують свої фінансові звіти та звіти за 2023 рік, щоб подати їх до Служби внутрішніх доходів США (IRS). Згідно з даними IRS, у 2022 році приблизно 213,4 мільйона (81,2%) податкових декларацій було подано в електронному вигляді, а індивідуальні податкові декларації, подані онлайн, становили ще більші 92,8%. Зі збільшенням кількості американців, які передають свої податкові декларації стороннім постачальникам програмного забезпечення, для окремих осіб і компаній надзвичайно важливо залишатися пильними, щоб захистити свою конфіденційну особисту та фінансову інформацію від кіберзагроз.

Keeper Security ділиться поширеними кіберзагрозами, які спостерігаються під час податкового сезону, щоб допомогти платникам податків США не стати їх жертвою.

Фішингові шахрайства. Кіберзлочинці стають все більш досвідченими у своїх можливостях видавати себе за IRS, компанії з підготовки податків та інші організації, пов’язані з податками, щоб отримати доступ до вашої особистої та фінансової інформації. Шахраї знають, що споживачі перебувають у стані сильної тривоги щодо потенційних перевірок або штрафів, використовуючи фішингові повідомлення, які містять тривожні висловлювання або погрози, спрямовані на те, щоб налякати одержувачів і змусити їх надати особисту інформацію. Крім того, зловмисники можуть підробити перевірені служби підготовки податків, щоб отримати інформацію та облікові дані. Фішингові шахрайства можна запускати через телефонні дзвінки (вішинг), текстові повідомлення, електронні листи та push-повідомлення. Щоб запобігти фішинговим атакам, не відкривайте вкладення та не натискайте посилання з невідомих джерел, переконайтеся, що інформацію запитує надійне джерело, і перевірте посилання, щоб переконатися, що вони не ведуть вас на шкідливий сайт. IRS не буде надсилати небажані електронні листи, телефонні дзвінки чи текстові повідомлення з проханням надати конфіденційну інформацію чи оплату.

Програми-вимагачі/зловмисні програми. Зловмисні фішингові атаки можуть призвести до завантаження зловмисного програмного забезпечення, зокрема програм-вимагачів, на ваш пристрій. Зловмисне програмне забезпечення дозволяє хакерам отримати доступ до вашої податкової інформації, а також до інших конфіденційних активів і облікових даних, які зберігаються на вашому пристрої. Ворожі програми-вимагачі та зловмисне програмне забезпечення можуть заблокувати ваші облікові записи через шифрування на вашому жорсткому диску та вимагати оплати за відновлення доступу. Ви можете випередити цю кіберзагрозу, маючи надійну резервну копію. Переконайтеся, що всі ваші конфіденційні фінансові документи зберігаються принаймні в одному іншому місці, наприклад у зашифрованому цифровому сховищі, як-от Secure File Storage Keeper. Важливо також переконатися, що ви регулярно оновлюєте програмне забезпечення, щоб виправляти відомі вразливості та недоліки безпеки в старіших версіях, якими можуть скористатися кіберзлочинці. Подумайте про придбання антивірусного програмного забезпечення із захистом від зловмисного програмного забезпечення, перш ніж почати відкривати конфіденційні документи або підключатися до служби підготовки податків.

Крадіжки особистих даних. Щоразу, коли ви ділитеся та завантажуєте особисту ідентифікаційну інформацію (PII) в Інтернет, ви можете наражатися на ризик викрадення особистих даних. Крадіжка особистих даних — це підвищена кіберзагроза, до якої ніколи не слід ставитися легковажно, особливо під час завантаження конфіденційної та часто незамінної інформації, зокрема номерів соціального страхування та реквізитів банківських рахунків. Щоб мінімізувати ризики, дуже важливо захистити свою податкову та фінансову звітність за допомогою надійних і унікальних паролів, які містять принаймні 16 символів і містять великі та малі літери, цифри та символи. Платникам податків також слід увімкнути двофакторну автентифікацію (2FA), коли це можливо, як додатковий крок для підтвердження вашої особи під час входу в систему.

Перехоплення документів. Хоча ви можете зробити майже все, щоб захистити свою власну конфіденційну інформацію та документи, немає жодної

гарантії, що сторонні податкові постачальники чи навіть довірені бухгалтери дотримуються того самого рівня безпеки. Якщо вам потрібно поділитися документами, завантажте та зберігайте їх у захищеному цифровому сховищі, наприклад у менеджері паролів із зашифрованими можливостями обміну. Розумно уникати загальнодоступних мереж Wi-Fi як найкращу практику, але дуже важливо ділитися лише конфіденційними документами в надійних і зашифрованих мережах Wi-Fi. Оскільки більшість загальнодоступних мереж Wi-Fi не зашифровані, кіберзлочинці часто націлюються на ці мережі, щоб отримати інформацію, що передається через них. Податкові документи містять інформацію, цінну для кіберзлочинців, тому важливо переконатися, що ваш мережевий маршрутизатор оновлено найновіше програмне забезпечення та захищено надійним унікальним паролем.

Незалежно від того, чи використовуєте ви стороннє програмне забезпечення для подання податкової звітності чи спілкуєтеся зі своїм бухгалтером віртуально, життєво важливо стежити за цими поширеними зловмисними загрозами, які невпинно шукають доступ до вашої конфіденційної інформації, облікових даних і документів. Зберігаючи старанність, дотримуючись найкращих практик кібербезпеки та вживаючи необхідних запобіжних заходів, окремі особи та організації будуть з меншою ймовірністю стати жертвами кіберзлочинців цього податкового сезону…» ***(Keeper Security Issues Top Cyber Threats To Watch Out for this Tax Season // Cision US Inc. (https://www.prnewswire.com/news-releases/keeper-security-issues-top-cyber-threats-to-watch-out-for-this-tax-season-302092134.html). 19.03.2024).***

***

«Експерти з кібербезпеки б’ють на сполох через недофінансування водопровідних і каналізаційних установ по всій країні, оскільки адміністрація Байдена закликає штати краще захищати сектор від зростаючих кіберзагроз.

У четвер адміністрація скликала державні агентства охорони навколишнього середовища, охорони здоров’я та внутрішньої безпеки на віртуальну зустріч, щоб

обговорити поточні зусилля щодо покращення кібербезпеки у водному секторі. Зустріч відбулася після листа, який Білий дім і Агентство з охорони навколишнього середовища надіслали всім губернаторам США у вівторок із попередженням, що хакери, пов’язані з урядами Ірану та Китаю, становлять значну загрозу системам питної води та каналізації по всій країні.

«Системи питної води та каналізації є привабливою мішенню для кібератак, оскільки вони є життєво важливим сектором інфраструктури, але їм часто не вистачає ресурсів і технічних можливостей для впровадження суворих практик кібербезпеки», — йдеться в листі.

Експерти розповіли Information Security Media Group, що сектору водопостачання та водовідведення США бракує фінансування та технічних ресурсів для дотримання федеральних рекомендацій щодо кібербезпеки, навіть незважаючи на широкий спектр безкоштовних і недорогих ресурсів, запущених в останні роки через Агентство з охорони навколишнього середовища та кібербезпеки та безпеки інфраструктури.

«У багатьох випадках необхідно надати більше технічних ресурсів [або] субсидувати цим комунальним підприємствам, щоб мати можливість фактично запровадити навіть найпростіші основи кібербезпеки», — сказала Дженніфер Лін Вокер, директор відділу кіберзахисту інфраструктури Water Information Sharing and Analysis. центр.

CISA створила державні та місцеві програми грантів на кібербезпеку для комунальних підприємств, а також державні оборотні фонди чистої води та питної води. Агентство з кіберзахисту США також пропонує місцеву технічну допомогу та навчальні ресурси для водопровідних органів, на додаток до безкоштовної послуги сканування, яка шукає вразливості в Інтернеті.

ФБР і EPA також надають ряд наборів інструментів і контрольних списків дій у разі інцидентів у сфері кібербезпеки для власників і операторів секторів водопостачання та водовідведення, а також програму кібербезпеки секторів систем водопостачання та водовідведення, яка може надавати технічну підтримку для місцевого персоналу.

«Державні та місцеві агенції хронічно відчувають нестачу фінансування, а кібербезпека — це стаття, дорога стаття, яка не входила в бюджети більшості агенцій кілька років тому», — сказав Шон Добі, головний технолог платформи пом'якшення загроз Semperis. «CISA та інші урядові установи зараз надають своєчасну інформацію, рекомендації, певну технічну допомогу та певне фінансування, але агентства історично не є організаціями швидкого реагування».

Водний сектор США, який включає приблизно 148 000 державних систем водопостачання та понад 52 000 громадських систем, все частіше розглядається як головна мішень для іноземних супротивників і кіберзлочинців. CISA, EPA та ФБР у січні опублікували спільний посібник із реагування на інциденти, спрямований на те, щоб допомогти системам водопостачання та водовідведення розробити плани реагування на інциденти та посилити зусилля з обміну інформацією з федеральним урядом.

Експерти давно попереджають, що федеральні мандати з кібербезпеки для водного сектору часто не мають супутніх механізмів фінансування. Рік Джеффарес, президент Асоціації сільського водопостачання Джорджії, у січні свідчив Конгресу про старіння робочої сили у водному секторі Джорджії, де середній вік працівника становить 58 років.

«Реальність така: більшості сільських комунальних підприємств не вистачає фінансових ресурсів і внутрішнього досвіду, щоб захистити себе», — сказав Джеффарес законодавцям.

Експерти повідомили ISMG, що більші та краще фінансовані водні органи влади зазвичай мають достатньо ресурсів і фінансування, щоб належним чином виконати рекомендації, викладені в листі Білого дому до губернаторів штатів.

«Нам потрібна ваша підтримка, щоб гарантувати, що всі системи водопостачання у вашому штаті всебічно оцінять свої поточні практики кібербезпеки», — йдеться в листі. «У багатьох випадках навіть базові запобіжні заходи щодо кібербезпеки, такі як скидання паролів за замовчуванням або оновлення програмного забезпечення для усунення відомих уразливостей, не

застосовуються, і це може означати різницю між звичайним бізнесом і руйнівною кібератакою».

За словами Малачі Вокера, радника з питань безпеки фірми з безпеки програмного забезпечення DomainTools, хакери атакували сектор водопостачання ще в 2006 році, коли система фільтрації води в Гаррісбурзі, штат Пенсільванія, була заражена шкідливим програмним забезпеченням.

«Незважаючи на ці загрози та наслідки, порівняно з енергетичним сектором, існує значно менше правил, пов'язаних з водою та водопостачанням», – сказав Вокер. «Білий дім і EPA звертають увагу на неадекватний захист цих систем від нещодавнього зростання атак на критичну інфраструктуру, що є важливим першим кроком у посиленні кіберстійкості водного сектора». ***(Chris Riotta. Water Sector Lacks Support to Meet White House Cyber Demands // Information Security Media Group, Corp. (https://www.bankinfosecurity.com/water-sector-lacks-support-to-meet-white-house-cyber-demands-a-24669). 21.03.2024).***

***

«Агентство з кібербезпеки та безпеки інфраструктури разом із ФБР і Центром обміну та аналізу інформації між штатами оновили свої вказівки щодо розподілених атак типу «відмова в обслуговуванні» (DDoSS), які спочатку були опубліковані в 2022 році.

CISA повідомила в четвер, що переглянуті інструкції під назвою «Розуміння та реагування на розподілені атаки відмови в обслуговуванні» тепер класифікують DDoS-атаки на три типи: об'ємні, протокольні та прикладні.

Об'ємна DDoS-атака прагне перевантажити доступну пропускну здатність цілі. Атака на протокол використовує вразливі місця мережевих протоколів цілі. Атака на програму спрямована на конкретні програми або служби, які запускаються ціллю.

Переглянуте керівництво також містить нові візуальні посібники та рекомендації щодо захисту від атак DDoS на основі типу.

CISA та його партнери закликали відповідні зацікавлені сторони переглянути переглянуте керівництво, щоб краще підготуватися та захиститися від загрози DDoS». ***(Jerry Petersen. Revised CISA Guidance on DDoS Offers New Attack Classifications & Threat Mitigations // Executive Mosaic (https://executivegov.com/2024/03/revised-cisa-guidance-on-ddos-offers-new-attack-classifications-and-threat-mitigations/). 22.03.2024).***

***

«12 березня 2024 року Міністерство оборони США (DoD) опублікувало остаточне правило, яке значно розширює доступ для оборонних підрядників, які бажають приєднатися до добровільної Програми кібербезпеки Міністерства оборони промислової бази («Програма DIB CS» або «Програма»). Рішення переглянути критерії прийнятності для програми DIB CS, здається, є частиною узгоджених зусиль Міністерства оборони, спрямованих на заохочення та покращення загальної участі спільноти оборонних підрядників у програмі, яка забезпечує двосторонній обмін інформацією після кіберінциденту.

Згідно з даними Федерального реєстру, остаточне правило набуде чинності 11 квітня 2024 року. Відповідно до останнього правила, усі оборонні підрядники матимуть право брати участь у Програмі кібербезпеки DIB, яка спрямована на покращення звітності про кіберзагрози та інциденти підрядниками для захисту несекретної інформації Міністерства оборони, яка зберігається та/або передається в несекретній інформаційній системі DIB через посилені заходи щодо обміну інформацією.

Мета програми DIB CS

Основна мета Програми DIB CS полягає в тому, щоб підвищити здатність оборонних підрядників захищати інформацію Міністерства оборони, яка знаходиться в несекретних інформаційних системах DIB або передається через них. Коли Програма була запущена, заявлені цілі включали наступне:

- Встановлення добровільної, взаємоприйнятної структури, спрямованої на захист державної інформації від несанкціонованого доступу

- Захист обміну конфіденційною інформацією в максимально дозволеному законодавством обсязі
- Створення довіреного середовища, призначеного для максимального захисту мережі та зусиль із відновлення шляхом обміну інформацією про кіберзагрози та звітами про інциденти між учасниками
- Надання учасникам стратегій пом'якшення та виправлення, а також аналіз зловмисного програмного забезпечення

Крім того, програма DIB CS була задумана як додатковий інструмент, спрямований на посилення договірних вимог, які висуваються до оборонних підрядників, які відповідають вимогам DIB, коли DFARS 252.204–7012 (договірне положення під назвою «Захист закритої оборонної інформації та звітування про кіберінциденти») включено до основний контракт або субпідряд.

Хоча заявлена мета була чудовою, початкова структура програми DIB CS була вузькою та обмежувала право лише на крихітну підгрупу спільноти оборонних підрядників. Нове правило є спробою вирішити цю проблему.

Що змінилося

Щойно остаточне правило набуде повної чинності, право на участь у програмі DIB CS пошириться на всіх оборонних підрядників, які підлягають обов'язковим вимогам Міністерства оборони повідомляти про інциденти кібербезпеки. Раніше програма DIB CS була доступна лише для «допущених» оборонних підрядників, які мали активні дозволи безпеки об'єктів. Міністерство оборони визначило «дозволеного» оборонного підрядника як приватну юридичну особу, яка отримала дозвіл Міністерства оборони «отримувати доступ, отримувати або зберігати секретну інформацію з метою тендеру на контракт або проведення заходів на підтримку будь-якої програми Міністерства оборони».

Це вузьке визначення означало, що менше ніж 2800 оборонних підрядників мали право брати участь у програмі DIB CS, коли вона була запущена в 2012 році. Згодом, у 2015 році, Міністерство оборони розширило право брати участь у програмі DIB CS на всіх дозволених оборонних підрядників, фактично скасувавши вимога, щоб оборонний підрядник міг захистити секретну інформацію. Ця

модифікація розширила право на участь у програмі DIB CD приблизно на 5300 додаткових підрядників із оборонної сфери, які отримали дозвіл.

Нове правило скасовує вимогу «перевірено» та відкриває програму DIB CS для всіх оборонних підрядників, які володіють або керують несекретними інформаційними системами, які обробляють, зберігають або передають закриту оборонну інформацію. Міністерство оборони вважає, що близько 68 000 додаткових оборонних підрядників матимуть право брати участь у програмі DIB CS, коли нове правило набуде чинності.

Зміни програми можуть принести користь поточним учасникам програми DIB CS

На додаток до розширення права на участь у програмі DIB CS, нове правило скасовує вимогу для учасників програми DIB CS отримати сертифікат надійності середнього рівня, який використовується для підтвердження цифрової ідентифікації підрядника та полегшення обміну зашифрованою інформацією. Щоб отримати цей сертифікат, оборонним підрядникам-учасникам довелося витрачати приблизно 175 доларів США на рік.

Згідно з новим правилом, оборонним підрядникам, які беруть участь, натомість потрібно буде зареєструватися в Procurement Integrated Enterprise Environment, головній корпоративній програмі закупівлі до оплати (P2P) для Міністерства оборони та його допоміжних агенцій.

Скасування обов’язку отримання сертифіката середньої впевненості може сприяти активізації участі оборонних підрядників, оскільки це зменшує вартість участі. У результаті менші оборонні підрядники, які, можливо, бажають брати участь, але не бажають брати на себе прямі витрати, пов’язані з добровільною програмою, тепер можуть бути більш схильні приєднатися.

Дивлячись вперед

Буде цікаво побачити, чи зміни в програмі DIB CS матимуть суттєвий вплив на оборонних підрядників-учасників. Відповідність вимогам не обов’язково означає участь. Фактично, згідно з власними оцінками Міністерства оборони, лише невеликий відсоток відповідних оборонних підрядників насправді бере участь у

програмі DIB CS. Ці оцінки можуть змінитися, коли нове правило набуде чинності 11 квітня 2024 року.

Зусилля щодо розширення відповідності та розширення участі в програмі DIB CS, здається, є частиною ширших зусиль Міністерства оборони, спрямованих на надання пріоритету кібербезпеці в сфері оборонних контрактів. Наприклад, Міністерство оборони нещодавно опублікувало запропоноване правило для впровадження своєї програми сертифікації моделі зрілості кібербезпеки (CMMC). Програма CMMC встановлює комплексний набір вимог щодо кібербезпеки для оборонних підрядників. У разі прийняття CMMC зобов'яже підрядників вжити заходів для захисту конфіденційної, несекретної державної інформації. Очікується, що Міністерство оборони включить нові вимоги кібербезпеки CMMC до положень про тендери та запровадить ці вимоги до 1 жовтня 2026 року.

Національний інститут стандартів і технологій дотримувався запропонованого правила CMMC, опублікувавши проект інструкцій, пов'язаних із захистом конфіденційної несекретної інформації, а також переглянуті кроки щодо кібербезпеки для державних контрактів – і федеральних агенцій у ширшому плані – яких необхідно вжити під час захисту уряду. даних…» ***(Patrick J. Austin, Jerry A. Miles. Defense Department Expands Access to DIB Cybersecurity Program // Woods Rogers Vandeventer Black PLC. (https://wrvblaw.com/defense-department-expands-access-to-dib-cybersecurity-program/). 21.03.2024).***

***

«…Теннессі став першим штатом США, який прийняв закон, що захищає музикантів, виконавців і художників від потенційної небезпеки, яку становить зростаюча індустрія штучного інтелекту...

Губернатор штату Теннессі Білл Лі в четвер підписав Закон про забезпечення безпеки схожості, голосу та зображень або «Закон ELVIS», який забороняє компаніям, що займаються штучним інтелектом, використовувати або відтворювати голос реальної людини, навіть якщо вона померла, без дозволу.

…прийнятий закон захищає інтелектуальну власність митців та їхню унікальність, «яка належить їм і тільки їм». Закон набуде чинності 1 липня.

Теннессі, батьківщина кантрі-музики, відомий тим, що в ньому працює найбільше людей у музичній індустрії серед усіх штатів США.

Це стало можливим завдяки унікальному законодавству штату Теннессі, яке розглядає ім'я, фотографію та зображення як об'єкти права власності, а не як суспільне надбання, що безпосередньо переходить у суспільне надбання.

Лише два інші штати мають подібні закони до Теннессі…» ***(Tennessee Passes First-Ever Law to Protect Musicians, Performers from AI Dangers // iTech Post (https://www.itechpost.com/articles/121631/20240322/tennessee-passes-first-law-protect-musicians-performers-ai-dangers.htm). 22.03.2024).***

***

Країни ЄС та Великобританія

«Європейський парламент і країни-члени ЄС досягли попередньої згоди щодо нового закону, спрямованого на посилення спроможності ЄС виявляти загрози та інциденти кібербезпеці, готуватися до них і реагувати на них.

Він також посилює механізми співпраці між країнами ЄС.

Європейська комісія, яка минулого року запропонувала Закон про кіберсолідарність, привітала цю угоду.

Заходи включають створення «системи оповіщення про кібербезпеку», яка включає національні та транскордонні кіберхаби, яка спрямована на швидке та ефективне виявлення основних загроз.

Аварійний механізм

Новий регламент також передбачає створення механізму надзвичайних ситуацій у сфері кібербезпеки для підвищення готовності та посилення можливостей реагування на інциденти в ЄС.

Він підтримуватиме:

Заходи щодо готовності, включаючи тестування суб’єктів у дуже важливих секторах, таких як охорона здоров’я, транспорт і енергетика, на потенційну вразливість,

Новий резерв кібербезпеки ЄС, що складається зі служб реагування на інциденти від приватного сектору, готових втрутитися на запит держави-члена або інституцій, органів і агентств ЄС, а також

Взаємодопомога у фінансовому плані.

Також буде діяти механізм оцінки та перегляду для оцінки ефективності дій у рамках механізму кібернадзвичайних ситуацій та використання резерву кібербезпеки.

Схеми сертифікації

Депутати Європарламенту та Рада ЄС також узгодили цільову поправку до законодавства про кібербезпеку 2019 року, яка дозволить у майбутньому прийняти європейські схеми сертифікації послуг керованої безпеки, що надаються спеціалізованими компаніями.

Це спрямовано на підвищення якості та порівнянності таких постачальників кібербезпеки.

Угода, досягнута вчора (5 березня), зараз підлягає офіційному затвердженню Європейським парламентом і Радою.

Тьєррі Бретон (комісар з питань внутрішнього ринку) назвав угоду «вирішальним кроком для створення європейського кіберщита». ***(MEPs and states agree cyber-security deal // Law Society Gazette (https://www.lawsociety.ie/gazette/top-stories/2024/march/meps-and-states-agree-cyber-security-deal). 06.03.2024).***

***

«Закон про дані ЄС набув чинності 11 січня 2024 року. Закон про дані є частиною стратегії Європейської комісії щодо даних, оприлюдненої в лютому 2020 року, і зобов'язує виробників підключених продуктів надавати дані, пов'язані з використанням, за певних обставин. Він також вимагає від постачальників послуг з обробки даних (наприклад, хмарних сервісів) полегшити

клієнтам перехід до іншого постачальника, наприклад, шляхом надання мінімальних перехідних послуг. Більшість нових правил набудуть чинності з 12 вересня 2025 року.

Зв'язані продукти та екстериторіальність

Відповідно до Закону про дані, підключені продукти охоплюють продукти, які отримують, генерують або збирають дані щодо їх використання чи середовища, і які можуть передавати ці дані за допомогою електронного зв'язку, фізичного підключення або доступу на пристрої (наприклад, пристрої Інтернету речей, наприклад, підключені побутові пристрої, медичні пристрої або транспортні засоби).

Зобов'язання відповідно до Закону про дані здебільшого покладатимуться на виробників підключених продуктів, розміщених на ринку ЄС, і постачальників пов'язаних послуг, незалежно від місця їх заснування. Від таких компаній, за винятком мікро-, малих або середніх підприємств, вимагатиметься надати користувачеві та третім сторонам доступ до даних, отриманих під час використання, за вибором користувача.

Ключові наслідки для підприємств, які розглядаються

Закон про дані вплине на виробників підключених продуктів і постачальників послуг обробки даних (включно з хмарними службами) із зазначеними нижче ключовими зобов'язаннями:

Зобов'язання для виробників пов'язаних продуктів, розміщених на ринку ЄС

Розробити продукт або послугу таким чином, щоб дані, створені під час використання, були легко доступними для користувача;

Надавати користувачеві інформацію про дані, які будуть створені під час використання продукту чи послуги, а також про те, як до них можна отримати доступ, відновити чи стерти до укладення з ним договору;

За запитом користувача надавати дані, створені під час використання, користувачеві або третій стороні, якщо ці дані недоступні безпосередньо з продукту чи пов'язаної служби;

Надавати дані третій стороні, обраній користувачем, на чесних, розумних, прозорих і недискримінаційних умовах, які мають бути оформлені в договорі. Закон про дані забороняє підприємствам в односторонньому порядку нав'язувати іншим підприємствам «несправедливі» договірні умови щодо доступу та використання даних. 1 span>. Такі положення також застосовуються, коли компанія зобов'язана надати дані іншій компанії відповідно до законодавства ЄС або держави-члена.

Виробники або постачальники пов'язаних послуг можуть у кожному конкретному випадку відмовити у наданні певних даних, визначених як комерційна таємниця. 2 Відмова в обміні даними може мати місце лише у виняткових обставинах, коли існує висока ймовірність зазнати серйозних економічних збитків від розголошення, незважаючи на технічні та організаційні заходи, вжиті користувачем. Відмова має ґрунтуватися на об'єктивних елементах (включно з характером і рівнем конфіденційності наявних даних), належним чином обґрунтованим і наданим у письмовій формі користувачеві, а також повідомленим національному компетентному органу.

Виробники або постачальники пов'язаних послуг можуть застосовувати відповідні технічні заходи захисту, зокрема розумні контракти та шифрування, щоб запобігти несанкціонованому доступу до даних. Однак розумні контракти, які використовуються для автоматизації обміну даними, підлягають певним вимогам, таким як безпечне припинення та переривання.

Користувачам і третім особам забороняється використовувати дані для розробки продуктів, які конкурують із продуктом, з якого генеруються дані, а також використовувати отримані дані для отримання інформації про економічну ситуацію, активи та методи виробництва виробника. Третім особам дозволяється використовувати дані лише для цілей і на умовах, узгоджених з користувачем.

Юридичні особи можуть бути зобов'язані надати дані, якими вони володіють, органам державного сектору за виняткових обставин, наприклад, у надзвичайних ситуаціях, коли дані не можуть бути отримані органом державного сектору інакше вчасно та ефективно.

Зобов'язання постачальників послуг обробки даних, у тому числі хмарних служб

Сприяти переходу клієнтів до інших постачальників послуг такого ж типу, що включає утримання від встановлення комерційних, технічних, договірних або організаційних перешкод для зміни постачальника. На практиці це означає, що хмарні провайдери будуть зобов'язані надавати клієнтам певні мінімальні перехідні послуги, на які поширюватимуться обмеження плати, яку провайдери можуть стягувати за свою допомогу. Такі зобов'язання не застосовуватимуться, якщо основні функції послуги створені для задоволення конкретних потреб окремого клієнта. Ці зобов'язання мають екстратериторіальне застосування та поширюються на постачальників послуг з обробки даних, незалежно від місця їх заснування, які надають послуги клієнтам у ЄС.

Вжити адекватних технічних, правових та організаційних заходів для запобігання міжнародному міжнародним урядам і урядам третіх країн, якщо така передача або доступ є незаконними відповідно до законодавства ЄС або держав-членів. доступу та передачі неособистих даних, що зберігаються в ЄС,

Штрафи

Держави-члени встановлюють правила щодо санкцій, які застосовуються до порушень Закону про дані. Штрафи, які накладаються за порушення зобов'язань щодо обміну даними, можуть сягати 20 мільйонів євро або 4% від загального світового обороту організації за попередній фінансовий рік, залежно від того, яка сума є більшою.

Наступні кроки

Більшість зобов'язань відповідно до Закону про дані застосовуватимуться з 12 вересня 2025 року. Зобов'язання, пов'язані з розробкою та виробництвом підключених продуктів, застосовуватимуться до продуктів і підключених послуг, випущених на ринок після 12 вересня 2026 року.

Що підприємства мають робити зараз

Виробникам підключених продуктів і постачальникам пов'язаних послуг рекомендується критично оцінити свою практику щодо надання даних

користувачам з огляду на вимоги Закону про дані та підготувати дорожню карту для впровадження заходів відповідності.

Постачальникам послуг з обробки даних також рекомендується розглянути необхідність будь-яких змін у своїй практиці (включаючи технічні та договірні заходи) щодо перемикання та допомоги в переході, сумісності та державного доступу та передачі неособистих даних.

Правила конфіденційності, такі як GDPR, а також правила кібербезпеки, такі як галузеві правила, що застосовуються до медичних пристроїв і підключених транспортних засобів, уже можуть застосовуватися до продуктів і послуг, які входять до сфери дії Закону про дані. Крім того, незабаром, ймовірно, будуть прийняті нові кіберправила щодо підключених пристроїв – дивіться нашу юридичну інформацію про проект Закону ЄС про кібернетостійкість від жовтня 2023 року.

Крім того, незрозуміло, як Закон про дані взаємодіятиме з іншими нещодавно прийнятими законодавчими актами, такими як Закон про цифрові ринки («DMA»). Зокрема, DMA має власні положення щодо переносимості даних у DMA, а Закон про дані забороняє «привратникам», призначеним згідно з DMA, отримувати дані користувачів. Це ілюструє, як законодавство про конкуренцію та правила, пов’язані з даними, все більше взаємопов’язані в ЄС і часто вимагають комбінованої правової оцінки.

Ці існуючі та майбутні положення слід враховувати при розробці стратегії відповідності». ***(Ana Hadnes Bruder, Benjamin Beck, Livia Crepaldi Wolf, Ondrej Hajda, Mark A. Prinsley and Aymeric de Moncuit. EU Data Act: New Rules on Data Sharing and Portability of Cloud Services Now in Force // Mayer Brown (https://www.mayerbrown.com/en/insights/publications/2024/03/eu-data-act-new-rules-on-data-sharing-and-portability-of-cloud-services-now-in-force). 08.03.2024).***

***

«Уряди в усьому світі посилюють вимоги до кібербезпеки з великою кількістю нових законів і законодавчих пропозицій, що очікують на розгляд.

ЄС не є винятком. Два найвідоміших кіберзакони ЄС, які незабаром набудуть чинності, — це Закон про цифрову операційну стійкість (DORA) і Директива про мережеві та інформаційні системи 2 (NIS2). DORA встановлює єдині вимоги до кібербезпеки для установ, що працюють у фінансовому секторі. NIS2, з іншого боку, призначений для захисту критично важливої інфраструктури та організацій у межах ЄС від кіберзагроз. У сферах, де NIS2 і DORA перетинаються, наприклад, інфраструктури банківського та фінансового ринку, Комісія нещодавно пояснила, що галузеві правила DORA мають пріоритет.

І DORA, і NIS2 чітко покладають значну частину кіберобов'язків організації на «керівний орган», причому керівний орган несе остаточну відповідальність за визначення, затвердження та моніторинг системи управління ризиками інформаційно-комунікаційних технологій («ІКТ») організації.. ІКТ включає будь-яке програмне або апаратне забезпечення в мережевих та інформаційних системах, що використовуються фінансовою організацією, наприклад стільникові телефони, комп'ютерне та мережеве обладнання та програмне забезпечення. Невиконання своїх зобов'язань може призвести до штрафів та інших заходів виправлення.

Що таке орган управління?

Відповідно до DORA та NIS2, орган управління може бути органом з управлінськими та/або наглядовими функціями. Повноваження та структура органів управління різняться в державах-членах ЄС, а управлінські та наглядові функції можуть покладатися на різні органи в організації. У країнах-членах ЄС, де органи управління мають однорівневу структуру, одна правління зазвичай виконує функції управління та нагляду. У державах-членах ЄС із дворівневою системою наглядові функції зазвичай виконуються окремою наглядовою радою без виконавчих функцій, а виконавчі функції виконуються окремою керівною радою, яка може бути відповідальною та підзвітною за щоденні -денне управління компанією.

Це означає, що залежно від національної законодавчої бази та особливостей організації компанії правління та наглядова рада можуть розглядатися, окремо чи

спільно, як «орган управління» для цілей певного зобов'язання. Подальші вказівки національних фінансових регуляторів допоможуть прояснити це.

Які кіберобов'язки мають члени органів управління?

Згідно з DORA та NIS2, керівний орган несе основну відповідальність за визначення, затвердження та нагляд за структурою управління ризиками ІКТ організації. Це означає, що, як правило, кіберобов'язки органу управління не можуть бути делеговані третій стороні.

Зобов'язання за DORA та NIS2 певною мірою відрізняються, але за своєю суттю зобов'язання схожі. На додаток до управління загальною структурою управління ризиками ІКТ, керівний орган, зокрема, зобов'язаний, серед іншого:

Політики: встановлюйте та періодично переглядайте кібердокументацію для забезпечення кібервідмовостійкості, таку як політика безперервності бізнесу ІКТ та план реагування та відновлення ІКТ, серед іншого;

Управління: визначте чіткі ролі та відповідальність для всіх функцій, пов'язаних з ІКТ, і створіть відповідні механізми управління для забезпечення ефективного та своєчасного зв'язку, співпраці та координації між цими функціями;

Належна перевірка ланцюга постачання: схвалення та періодичний перегляд використання послуг ІКТ, що надаються сторонніми постачальниками послуг ІКТ, що включає регулярний перегляд договірних угод щодо використання постачальників ІКТ.

Крім того, члени керівного органу повинні мати достатні знання та навички для розуміння та оцінки ризиків ІКТ та їхнього впливу на діяльність організації. Для цього вони повинні пройти кібернавчання.

Які наслідки невиконання зобов'язань?

DORA вимагає від держав-членів ЄС запровадити національні заходи щодо накладення адміністративних санкцій і заходів виправлення щодо членів керівного органу за певні порушення їхніх кіберзобов'язань. Наприклад, проект закону Німеччини про імплементацію DORA передбачає, що Федеральний орган фінансового нагляду Німеччини (BaFin) може застосовувати санкції за порушення DORA з боку керівного органу за допомогою наказів, які є «придатними та

відповідними» для забезпечення відповідності, наприклад, накази про припинення та відмову. Порушення DORA також може призвести до штрафу в розмірі до 5 мільйонів євро.

NIS2 вимагає від держав-членів ЄС гарантувати, що керівні органи суб'єктів дослідження можуть бути притягнуті до відповідальності за порушення своїх кіберзобов'язань. Оскільки NIS2 – як Директива – транспонується в національне законодавство кожною державою-членом ЄС, обсяг відповідальності може дещо відрізнятися від однієї країни-члена ЄС до іншої. Наприклад, проект закону Німеччини про імплементацію NIS2 передбачає, серед іншого, що члени керівного органу, які порушують свої обов'язки затвердження та нагляду, несуть відповідальність перед організацією за будь-які завдані збитки. Поняття «збитки» включає як регресні позови до організації, так і штрафи, накладені відповідними органами, які можуть бути значними. Організація не може відмовитися від будь-яких претензій щодо відшкодування збитків або врегулювати їх.

Як зазначалося вище, кіберобов'язки органу управління зазвичай не можуть бути делеговані третій стороні, що означає, що делегування навряд чи буде ефективним засобом уникнення відповідальності.

Наступні кроки та коли почнуть подаватись заявки на NIS2 і DORA?

DORA почне застосовуватися в усіх країнах-членах ЄС 17 січня 2025 року. Як Директива, NIS2 має бути перенесено в національне законодавство держав-членів, перш ніж вона набуде прямої чинності. Держави-члени мають перенести NIS2 у національне законодавство до 18 жовтня 2024 року, що означає, що більшість національного імплементаційного законодавства, ймовірно, набуде чинності в цю дату або близько неї.

До цих відповідних дат члени керівних органів організацій, які охоплюють сферу дії, повинні бути повністю обізнані про свої кіберзобов'язання згідно з цими законами та виконувати їх. Оскільки NIS2 необхідно впроваджувати окремо в кожній державі-члені ЄС, зобов'язання можуть дещо відрізнятися від однієї країни-члена ЄС до іншої. Це особливо актуально для організацій, які здійснюють діяльність більш ніж в одній державі-члені ЄС.

Оскільки обидва закони не існують у вакуумі, а деякі зобов'язання збігаються з існуючими законами, аналіз прогалин, ймовірно, буде корисним інструментом для визначення того, де DORA та NIS2 виходять за межі існуючих зобов'язань. Організації можуть отримати вигоду від заснування своїх заходів відповідності DORA / NIS2 на засобах контролю, політиках і процедурах, які вони вже діють на основі існуючих законів і правил». ***(Ana Hadnes Bruder, Benjamin Beck and Livia Crepaldi Wolf. EU Cyber Legislation Puts Emphasis on Board Responsibility // Mayer Brown (https://www.mayerbrown.com/en/insights/publications/2024/03/eu-cyber-legislation-puts-emphasis-on-board-responsibility). 07.03.2024).***

***

«Було цікаво прочитати звіт Ipsos про навички кібербезпеки на ринку праці Великобританії у 2023 році, в якому висвітлено поточні розчарування та проблеми під час найму, навчання та утримання персоналу в усіх сферах кібербезпеки. Деякі повчальні висновки:

Приблизно 739 000 підприємств (50% опитаних) потребують базових навичок. Тобто людям, відповідальним за кібербезпеку в цих компаніях, не вистачає впевненості у виконанні основних завдань, викладених у схваленій урядом схемі Cyber Essentials, і вони не отримують підтримки від зовнішніх постачальників кібербезпеки.

Приблизно 487 000 компаній (33% опитаних) мають більш просунуті прогалини в навичках, найчастіше у сфері криміналістичного аналізу порушень, архітектури безпеки, інтерпретації шкідливого коду та тестування на проникнення. 41% мають внутрішній брак навичок, коли справа доходить до реагування на інциденти та відновлення, і не мають зовнішніх ресурсів для цього аспекту кібербезпеки.

Відсутність реагування на інцидент

Найбільше тривоги викликав звіт про відсутність навичок реагування на інциденти; це неприйнятно, коли хакерство зараз є оплачуваною кар'єрою. Кінцевим результатом є зростаючий попит на кваліфікованих фахівців з

кібербезпеки, і нам потрібно визначити пріоритетність освітніх і навчальних програм, щоб заповнити ці прогалини. Крім того, ці недоліки поширюються на керівників вищої ланки та керівників на рівні правління, яким необхідно розуміти кроки, які необхідно вжити для управління інцидентом. Хоча приємно бачити, що ради директорів все більше розуміють кіберризики; очевидно, що потрібно зробити більше, щоб допомогти просвітити вище керівництво щодо їх участі в інциденті. Кіберінциденти завжди вимагали реагування бізнесу, а не просто технічного реагування. Дії на рівні старшого керівництва та ради можуть бути такими простими, як:

- Обов’язково повідомте про інцидент
- Негайно повідомте провайдера кіберстрахування
- Не йдіть на самоті; завжди шукайте сторонньої допомоги
- Призначте власника кіберінцидентів, щоб контролювати процес реагування
- Ведіть журнал дій і рішень
- Зосередьтеся на стримуванні
- Прислухайтеся до порад і кращих практик; ви не перший, кого порушили
- Будьте терплячі; боротьба з кіберзлочинами є процесом
- Допомагайте органам влади та контролюючим органам якомога більше з документацією
- Турбуйтеся про управління репутацією та контролюйте розповідь.

Кібератаки – це бізнес

IT-відділи повинні перевести кіберризики в операційні та бізнес-ризики, щоб було розуміння на рівні правління. Члени правління розуміють бізнес і кіберзлочинність — це добре організований бізнес. IT-фахівцям необхідно пояснити, що світ кіберзлочинців перетворився на екосистему, що складається з трьох різних типів груп:

Посередник доступу зосереджується на пошуку організацій із уразливими місцями, скомпрометуванні мереж і дослідженні найпростішого шляху до них, щоб продати це як пакет іншим групам.

Розробники створюють інструменти програми-вимагача як послуга (RaaS), щоб здавати в оренду.

Після придбання інформації про доступ і наймання інструментів RaaS третя група переміститься в мережу, викраде або зашифрує дані, запустить програмне забезпечення-вимагач і вимагатиме викуп.

Коротше кажучи, це стало індустрією. Групи виконують різні ролі спеціалістів, розподіляючи прибутки залежно від їхніх навичок і ризиків, пов'язаних із виконанням своєї частини угоди. Завдяки цій бізнес-моделі дослідникам важче визначити, які угруповання кіберзлочинців були залучені до кожного кіберзлочину.

Унція профілактики

Одним із найефективніших методів передачі знань є ознайомлення керівників вищого рівня зі змодельованим кіберінцидентом, щоб навчити їх ролям і обов'язкам у разі атаки. Настільні вправи з реагування на інциденти є чудовим способом забезпечити ретельну перевірку планів, посібників і команд. Тісно співпрацюючи з керівництвом вищого рівня, IT-спеціалісти можуть допомогти їм отримати уроки з кожної вправи, щоб підготувати їх до будь-яких обставин. Ця передача знань включає не лише внесок від внутрішніх юридичних, фінансових та інших бізнес-керівників і зовнішніх експертів у галузі, але й швидке визначення напрямку та визначення пріоритетів багатьох вимог, які будуть поставлені перед командою, і стимулювання без звинувачень, без культура страху.

Протягом останніх 15 років я працював з правліннями багатьох організацій, які стали жертвами руйнівних інцидентів. Я на власні очі бачив позитивний вплив ефективного керівництва та прямої участі правління на успішне проходження атаки. Хоча ми всі намагаємося зрозуміти, як залучити та навчити нових кращих талантів у нашій галузі, ми можемо допомогти собі, працюючи з нашим вищим керівництвом, щоб навчити їх про їхню роль у позитивному впливі на результат атаки». ***(James Allman-Talbot. Cybersecurity skills gap and boardroom blindness invite hacker havoc // Future US, Inc. (https://www.techradar.com/pro/cybersecurity-skills-gap-and-boardroom-blindness-invite-hacker-havoc). 14.03.2024).***

***

«Європарламент та Рада ЄС дійшли попередньої згоди навколо пропозицій Європейської комісії щодо запровадження Акту кібернетичної солідарності, покликаного підвищити кібербезпеку та стійкість європейських інституцій.

Як повідомляє Укрінформ, така інформація оприлюднена на сайті Єврокомісії.

«Європейська комісія вітає політичну угоду, досягнуту між Європейським парламентом та Радою ЄС щодо Акту кібернетичної солідарності, який був запропонований Європейською комісією у квітні 2023 року. Цей документ… зміцнить солідарність на рівні ЄС та дозволить краще виявляти, готуватися та відповідати на кібернетичні загрози й інциденти. Він приймається у критично важливі часи для кібернетичної безпеки, оскільки кількість кібернетичних загроз продовжує зростати у зв'язку із геополітичними подіями», - йдеться у повідомленні.

Акт кібернетичної солідарності ЄС передбачає координацію між країнами-членами за трьома головними напрямками.

Насамперед ідеться про створення європейської системи раннього попередження, яка складатиметься з національних та транскордонних кібернетичних хабів, оснащених сучасним обладнанням та інфраструктурою, включаючи спроможності штучного інтелекту та розвинутого аналізу баз даних. Це дозволить швидко, в режимі реального часу, ідентифікувати кібернетичні загрози й інциденти та планувати ефективні відповіді на них.

Другий напрямок передбачає створення так званого надзвичайного кібернетичного механізму, який поєднає спроможності з підвищення готовності до реагування на значні й масштабні кібернетичні інциденти. В рамках цього інструменту проводитимуться тестування стійкості кібернетичних систем захисту в ключових сферах управління та економіки, наприклад, в енергетиці та на транспорті. Також має бути створено так званий Резерв кібернетичної безпеки ЄС,

який надаватиме резервні послуги в разі серйозних порушень, на запит країн-членів, євроінституцій, або асоційованих третіх країн.

Окрім того, новий документ передбачатиме взаємну фінансову підтримку членів ЄС у разі серйозних кібернетичних інцидентів, а також надання технічної допомоги країнам, що потерпіли від них.

Дані про кожен такий інцидент будуть аналізуватися для усунення вразливостей та для зміцнення кібернетичної стійкості ЄС, його інституцій та країн-членів.

Відповідна політична угода має бути формально затверджена Європейським парламентом та Радою ЄС. Вона набуде чинності за 20 днів після оприлюднення рішення в Офіційному журналі ЄС.

Як відомо, в умовах повномасштабного російського вторгнення ЄС та його члени надають Україні суттєву політичну, економічну, фінансову, гуманітарну й військову допомогу.

На цьому тлі значно зросла кількість кібернетичних атак на установи й інституції Євросоюзу з метою дестабілізації їхньої діяльності. Особливої гостроти проблема кібербезпеки та реагування на спроби зовнішнього втручання набуває з наближенням європейських виборів, що мають відбутися у червні». ***(У ЄС погодили Акт кібернетичної солідарності для боротьби із зовнішніми впливами // Укрінформ (https://www.ukrinform.ua/rubric-technology/3836556-u-es-pogodili-akt-kiberneticnoi-solidarnosti-dla-borotbi-iz-zovnisnimi-vplivami.html). 07.03.2024).***

***

«Сьогодні держави-члени за підтримки Комісії та ENISA, Агентства ЄС з кібербезпеки, опублікували новий збірник про те, як захистити чесність виборів з точки зору кібербезпеки.

Після останніх виборів до ЄС у 2019 році ландшафт загроз погіршився, включаючи прискорення діяльності найнятих хактивістів і підвищення складності методів, які використовують суб'єкти загрози.

У той же час виборчі процеси зазнали технологічного прогресу. Таким чином, основні елементи цього видання включають: оновлену картину загроз перед виборами, нові та переглянуті тематичні дослідження, найкращі практики кібербезпеки та дослідження потенційних загроз, що походять від нових технологій, які можуть вплинути на стійкість виборів, а саме втручання в маніпулювання іноземною інформацією. (FIMI), дезінформація в соціальних мережах, ШІ та глибокі фейки.

У новому виданні Компендіуму містяться рекомендації для держав-членів, кроки, які необхідно вжити, і корисні вказівки щодо управління потенційними кіберінцидентами протягом виборчого процесу. Серед запропонованих заходів – найкращі практики щодо обміну інформацією, підвищення обізнаності та тренінгів, а також управління ризиками, підтримка кібербезпеки для кампаній, партій і кандидатів, а також технологія електронного голосування. Це видання містить основні питання кібербезпеки на кожному етапі виборчого циклу». ***(New Cybersecurity compendium on how to protect integrity of elections published // European Commission (https://digital-strategy.ec.europa.eu/en/news/new-cybersecurity-compendium-how-protect-integrity-elections-published). 06.03.2024).***

***

«Імплементація Чехією директиви ЄС щодо кібербезпеки NIS2 піддалася різкій критиці з боку операторів мобільного зв'язку, які стверджують, що чеське законодавство є одним із найсуворіших у Європі та поставить під загрозу їхній бізнес.

На думку мобільних операторів, які працюють на ринку, запропонований закон надасть занадто багато повноважень органу з кібербезпеки – Національному агентству з кібербезпеки та інформаційної безпеки (NUKIB).

Оператори мобільного зв'язку стверджують, що нове законодавство дозволить NUKIB заборонити вибраних постачальників на основі рішення агентства. Це може стосуватися, наприклад, постачальників технологій з недемократичних країн, таких як Китай.

«Буде створено суперагентство, яке самостійно визначатиме сферу регулювання у формі власного наказу, самостійно встановлюватиме критерії оцінки безпеки постачальників, проводитиме оцінку за власною методологією та самостійно прийматиме рішення про обмеження чи виключення. конкретного постачальника», – сказав Euractiv Czechia Їржі Грунд, президент Чеської асоціації постачальників мобільних послуг (APMS).

За словами Грунда, така висока концентрація влади неприпустима в демократичній правовій державі.

Віце-президент Vodafone Czech Republic Ян Клоуда також сказав Euractiv Czechia, що законопроект є набагато суворішим, ніж вимагається директивою ЄС NIS2 або рекомендаціями Європейської комісії щодо безпеки мережі 5G.

NUKIB відкидає звинувачення у створенні «суперагентства».

«NUKIB не буде оцінювати демократичний характер окремих країн», — сказав Euractiv Чехія Марек Вала, речник NUKIB. За словами Vala, потенційні обмеження щодо постачальників будуть здійснюватися у співпраці з іншими державними органами.

«Простіше кажучи, NUKIB разом з іншими партнерами перевірятиме, чи відповідає даний постачальник встановленим і необхідним параметрам безпеки для входу в системи критичної або стратегічно важливої національної інфраструктури», — пояснив Вала.

Речник Cyber Agency також відкинув твердження, що Чеська Республіка матиме більш суворі правила, ніж інші країни-члени ЄС. За його словами, проект закону підпадає під дію європейського регламенту NIS2.

Проте до критики мобільних операторів приєдналися й інші організації. Чеська спілка міст і муніципалітетів стверджує, що NUKIB не зміг підрахувати вартість нового закону.

Асоціація поскаржилася, що ця пропозиція створює «заплутану, непрозору і, отже, дуже складну ситуацію». Представники міста також заявили, що виконання всіх зобов’язань щодо безпеки буде поза їхніми фінансовими та людськими можливостями». ***(Aneta Zachová and Dávid Pásztor. Criticism mounts over Czech***

implementation of EU cyber security // EURACTIV MEDIA NETWORK BV. (https://www.euractiv.com/section/politics/news/criticism-mounts-over-czech-implementation-of-eu-cyber-security/). 14.03.2024).

***

«У вівторок парламент схвалив нові стандарти кіберстійкості для захисту всіх цифрових продуктів в ЄС від кіберзагроз.

Регламент, уже погоджений з Радою в грудні 2023 року, спрямований на те, щоб продукти з цифровими функціями були безпечними у використанні, стійкими до кіберзагроз і надавали достатньо інформації про їхні властивості безпеки.

Важливі та критично важливі продукти будуть внесені в різні списки залежно від їх критичності та рівня ризику для кібербезпеки, який вони становлять. Два списки буде запропоновано та оновлено Європейською комісією. Продукти, які вважаються такими, що становлять вищий ризик для кібербезпеки, перевірятимуться уповноваженим органом суворіше, тоді як інші можуть проходити легший процес оцінки відповідності, яким часто керують виробники.

Під час переговорів євродепутати переконалися, що такі продукти, як програмне забезпечення систем керування ідентифікацією, менеджери паролів, біометричні зчитувачі, розумні домашні помічники та приватні камери безпеки, охоплюються новими правилами. Продукти також мають автоматично встановлювати оновлення безпеки окремо від функціональних оновлень.

Депутати Європарламенту також наполягали на тіснішій участі Агентства Європейського Союзу з кібербезпеки (ENISA), коли виявляються вразливості та виникають інциденти. Агентство буде сповіщено відповідною державою-членом і отримає інформацію, щоб воно могло оцінити ситуацію та, якщо воно виявить системний ризик, повідомить інші країни-члени, щоб вони могли вжити необхідних заходів.

Щоб підкреслити важливість професійних навичок у сфері кібербезпеки, депутати Європарламенту також представили освітні та навчальні програми,

спільні ініціативи та стратегії для підвищення мобільності робочої сили в регламенті.

Цитата

Провідний депутат Європарламенту Нікола Данті (Renew, IT) сказав: «Закон про кіберстійкість посилить кібербезпеку підключених продуктів, усуваючи вразливості як в апаратному, так і в програмному забезпеченні, що зробить ЄС безпечнішим і стійкішим континентом. Парламент захистив ланцюжки поставок, гарантуючи, що ключові продукти, такі як маршрутизатори та антивіруси, є пріоритетними для кібербезпеки. Ми забезпечили підтримку мікро- та малих підприємств, покращили залучення зацікавлених сторін і звернули увагу на проблеми спільноти з відкритим кодом, залишаючись амбітними. Лише разом ми зможемо успішно впоратися з надзвичайною ситуацією у сфері кібербезпеки, яка чекає на нас у найближчі роки».

Наступні кроки

Закон було схвалено 517 голосами «за», 12 «проти» та 78 утрималися. Тепер він також має бути офіційно прийнятий Радою, щоб набути закону.

Фон

Нові технології пов’язані з новими ризиками, і вплив кібератак через цифрові продукти різко зріс за останні роки. Споживачі стали жертвами недоліків безпеки, пов’язаних із цифровими продуктами, такими як радіоняні, роботи-пилососи, маршрутизатори Wi-Fi та системи сигналізації. Для компаній важливість забезпечення безпеки цифрових продуктів у ланцюжку постачання стала ключовою, враховуючи, що троє з п’яти постачальників уже втратили гроші через прогалини в безпеці продуктів». ***(Cyber Resilience Act: MEPs adopt plans to boost security of digital products // European Parliament (https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products). 12.03.2024).***

***

«Нове дослідження показує, що деякі з найбільших роздрібних торговців Великобританії повинні активізувати свою діяльність щодо боротьби з кібербезпекою.

Дослідження Beyond Words, проведене юридичною фірмою Irwin Mitchell, проаналізувало останні річні звіти найбільших і найвідоміших роздрібних торговців у Великій Британії та виявило, що ті, хто входить до рейтингу FTSE 100, у середньому згадують про «кібербезпеку» 12,5 разів. Це порівняно з 19,7 згадуваннями на звіт у всьому FTSE 100.

Сектор не має кращих результатів, коли оцінювалися роздрібні торговці через FTSE 350*. Тут середній бал, що стосується згадок про кібербезпеку, склав 12,4.

Дослідження також порівняло останні річні звіти з попередніми виданнями та виявило, що кількість згадок була на 6,5% нижчою в останніх версіях серед роздрібних торговців FTSE 350. Для порівняння з сектором відпочинку та гостинності, де компанії, що працюють у цьому секторі, збільшили кількість згадок про кібербезпеку на 27,6% до середнього 19,8 на звіт.

Висновки стали результатом резонансних порушень кібербезпеки минулого року на WH Smith і JD Sports. У випадку з JD Sports компанія заявила, що атака могла поставити під загрозу дані, що стосуються 10 мільйонів клієнтів.

Занепокоєння Ірвіна Мітчелла підтверджено останніми статистичними даними Управління комісара з інформації (ICO). Їх інформаційна панель тенденцій інцидентів безпеки даних показує, що роздрібні торговці та виробники зазнали більше кіберінцидентів, які торкнулися понад 100 000 суб'єктів даних, у перші три квартали 2023 року, ніж за весь 2022 рік…

Кібербезпека була лише однією з сфер дослідження Ірвіна Мітчелла в цьому дослідженні. Beyond Words також досліджував інші сфери ESG**, зокрема зміну клімату, різноманітність та інклюзивність.

Що стосується навколишнього середовища, дані вказують на більш позитивні новини для сектора. Посилання на «сферу викидів 3», категорію викидів парникових газів, які є непрямими викидами в результаті діяльності організації, але

відбуваються з джерел, якими вона не володіє або не контролює, збільшилися з року в рік у FTSE 350 роздрібної торгівлі більш ніж на 70%.

Сектор роздрібної торгівлі в FTSE 100 мав такі ж результати, як і решта найбільших компаній Великобританії. Середня кількість згадок обсягу 3 у звіті в FTSE 100 становила 21,7, тоді як показник для роздрібної торгівлі був трохи нижчим – 20,4». ***(Graham Thomson and David Shirt. Largest UK Retailers Showing Signs Of Cyber Security Apathy Despite Growing Risks // Irwin Mitchell LLP (https://www.irwinmitchell.com/news-and-insights/newsandmedia/2024/march/largest-uk-retailers-showing-signs-of-cyber-security-apathy-despite-growing-risks). 12.03.2024).***

***

«Молодший міністр закордонних справ Великої Британії лорд Тарік Ахмад Вімблдонський оголосив про виділення 300 тисяч фунтів стерлінгів до спеціального фонду Міжнародного кримінального суду для зміцнення його кібербезпеки.

Про це, як пише «Європейська правда», 25 березня оголосив британський уряд.

Про внесок до спецфонду МКС лорд Тарік Ахмад Вімблдонський оголосив під час зустрічі із секретарем Суду Освальдо Савалою Гілером у Лондоні.

«Кібербезпека є спільним викликом для тих, хто захищає і підтримує міжнародну систему, засновану на правилах», – прокоментував він.

У британському уряді стверджують, що його внесок у 300 тисяч фунтів до фонду є вже п’ятим за рахунком і третім за величиною в порівнянні з іншими державами.

Спеціальний фонд Міжнародного кримінального суду є тимчасовим фондом, призначеним для надання цільових ресурсів для посилення цифрової та фізичної безпеки МКС.

Його створенню передувала масштабна кібератака на ІТ-інфраструктуру МКС у вересні 2023 року, за якою, на думку Суду, стояла спроба шпигунства.

Суд не вперше стає об’єктом міжнародного шпигунства. У 2022 році Нідерланди заявили, що запобігли проникненню до суду російського шпигуна Сергєя Черкєсова під виглядом стажера з Бразилії. У березні 2023-го йому оголосили звинувачення у США». ***(Британія передає £300 тисяч на кібербезпеку Міжнародного кримінального суду // Internetua (https://internetua.com/britaniya-peredaye-300-tisyacs-na-kiberbezpeku-mijnarodnogo-kriminalnogo-sudu). 26.03.2024).***

***

Австралія та Нова Зеландія

«Двічі на рік Управління уповноваженого з інформації Австралії (OAIC) звітує про статистичні дані та ключові знання, зібрані з відповідних повідомлень про порушення даних, отриманих відповідно до Схеми Співдружності про порушення даних, що підлягає повідомленню (Схема) протягом попередніх 6 місяців. Звіт допомагає агентствам і організаціям (суб’єктам APP), які підпадають під дію Схеми, краще зрозуміти поточні тенденції та ризики конфіденційності у сфері витоку даних.

Останній звіт охоплює повідомлення, надіслані OAIC з липня 2023 року по грудень 2023 року.

Ми узагальнюємо ключові статистичні дані, визначені в останньому звіті, а також деякі ключові висновки для організацій APP.

Основна статистика

Ключові сектори, які постраждали: першими 5 секторів, які повідомляли про порушення даних, були постачальники послуг охорони здоров’я, фінанси, страхування, роздрібна торгівля та уряд Австралії.

Кількість отриманих сповіщень: OAIC отримав 483 відповідні повідомлення про порушення даних. Це на 19% більше порівняно зі звітним періодом січень 2023 – червень 2023 року.

Джерело порушень: джерела повідомлених порушень включають:

зловмисна або злочинна атака (67%)

помилка людини (39%)

системна помилка (3%). На відміну від інших «топ-5» секторів, австралійські державні установи повідомили про більше порушень даних, спричинених помилками людини, ніж тих, спричинених зловмисними або злочинними атаками.

Інциденти кібербезпеки: 44% усіх порушень даних сталися внаслідок інцидентів кібербезпеки, таких як фішинг, скомпрометовані або вкрадені облікові дані, програми-вимагачі, хакерство, зловмисне програмне забезпечення та атаки грубою силою.

Кількість постраждалих осіб: більшість порушень (65%) торкнулися 100 або менше осіб. Порушення, які стосуються від 1 до 10 осіб, становлять 44% усіх повідомлень, як і в попередні звітні періоди. Кіберінциденти були основною причиною інцидентів, які вплинули на велику кількість осіб (тобто порушення, що вплинули на понад 5000 осіб)…

Ключові висновки

Незважаючи на те, що у Звіті визначено постачальників медичних послуг, фінанси, страхування, роздрібну торгівлю та уряд Австралії як сектори, які наразі повідомляють про найбільшу кількість порушень. Звіт має широке значення для всіх суб'єктів APP.

Останній звіт також містить важливі знання для державних установ та університетів Нового Уельсу, які з листопада 2023 року підлягають еквівалентній спеціальній схемі та зобов'язанням щодо обов'язкового звітування.

Ключові поради:

OAIC очікує, що організації APP мають налагоджені процеси для забезпечення відповідності вимогам Схеми.

Організації APP повинні мати встановлений план реагування на порушення даних, щоб забезпечити ефективну та своєчасну оцінку та сповіщення відповідно до своїх нормативних зобов'язань.

Нарешті, особа, яка постраждала від порушення, завжди має бути «в центрі» реагування. Оперативне сповіщення дає людям змогу вжити заходів і зрештою мінімізувати ризик заподіяння шкоди.

З нашого досвіду, належна практика гігієни даних завжди буде основою найкращої практики, коли йдеться про готовність до витоку даних і реагування.

«Основи» відповідності, такі як розробка та введення в дію політик і процедур обробки даних, впровадження та тестування вашого плану реагування на порушення даних, а також доповнення цих кроків регулярним навчанням персоналу, можуть бути основоположними для успіху у випадку порушення». ***(Ooma Khurana and Radhika Bhatia. What the latest OAIC Notifiable Data Breaches Report means for you // Maddocks (https://www.maddocks.com.au/insights/notifiable-data-breaches-report). 07.03.2024).***

***

Російська Федерація та країни ЄАЕС

«У сфері кібербезпеки Росії відбувається деградація — як в обладнанні та програмному забезпеченні, так і падає рівень фахівців. Про це в ефірі телеканалу FREEДОМ розповів зовнішній консультант з аналізу даних і кібербезпеки в The World Bank Group Михайло Кольцов, коментуючи операцію кіберфахівців ГУР МОУ зі зламу сервера Міністерства оборони Росії.

За його словами, такі операції завжди пов’язані зі специфікою цілі.

«Тому що одна справа, коли ви атакуєте ціль, яка вважає, що ніхто на неї не нападатиме, вона невинна, не представляє ніякого стратегічного значення. Зовсім інша, коли ви працюєте проти структури, в якій є спеціальний підрозділ кібербезпеки, окремий підрозділ інформаційної безпеки, тобто який конкретно чекає на ваш прихід. І тому в цьому випадку це дійсно дуже складна ціль, яка, втім, виявила вразливість. Ця вразливість у тому, що в них дуже сильно падає рівень кібербезпеки, насамперед через західні санкції, через те, що вони не можуть співпрацювати з провідними провайдерами, які постачають і обладнання, і програмне забезпечення у сфері кіберзахисту», — сказав Кольцов.

Він уточнив, що росіяни можуть тільки покладатися на свої рішення і на ізоляцію інтернету. Це всього два способи, які їм доступні.

«Але, як ми бачимо станом на березень, обидва способи все ще неефективні», — додав консультант.

Кольцов пояснив, що взагалі будь-яка мережа володіє сімома технологічними рівнями, а людину називають «восьмим», тому що це найбільш вразлива частина будь-якої мережі.

«У середовищі кіберфахівців людина називається восьмим рівнем мережі. Оскільки людина дуже вразлива до різних когнітивних викривлень, не кажучи вже про те, що вона чутлива до однієї з найпопулярніших технік зі злому — це фішинг. І в цьому випадку ГУР ніби натякає на те, що вони провели дуже успішну фішингову атаку. Ключі у вигляді паролів стали доступні для ГУР МОУ. У цьому випадку, я думаю, подібні типи атак продовжуватимуться, оскільки технологічна деградація в кіберзахисті в РФ, зрештою призведе до того, що ми побачимо ще більше таких зломів, виною яким буде невміння відповідного персоналу поводитися з доступом, інформацією, масивами, до яких вони мають доступ. У цьому випадку, найімовірніше, заступник міністра мав пароль на кшталт 12345, що цілком вистачило фахівцям отримати доступ до всього масиву інформації», — розповів він.

Також фахівець зробив висновки про кібербезпеку, рівні захисту в Міноборони РФ:

«Я думаю, там, напевно, стоїть чергова ікона біля сервера. Можливо, вони повернуть її в інший бік, щоб якось ефективніше взаємодіяти в цифровому полі. Але це говорить про те, що рівень фахівців, які відповідають за цей кіберзахист, неухильно падає. Не кажучи вже про обладнання та програмне забезпечення. Схоже, вони втратили доступ до критичних технологій, які їм раніше забезпечували доступ. І зараз вони сидять тільки на власних напрацюваннях, ефективність яких, як ми бачимо зі зломів, дуже складно оцінити як високу».

Він зазначив, що цифровий світ не може існувати автономно в одній країні, усі змушені взаємодіяти з іншими країнами.

«Щойно на вас накладають санкції, цифровий світ — це перше, що починає відчувати відсутність міжнародного співробітництва. І в цьому випадку відтік

фахівців, закриття доступу до технологій і обладнання ви завжди побачите на інтернеті, на зв'язку», — резюмував Михайло Кольцов». ***(У Росії дуже сильно падає рівень кібербезпеки, зломів буде більше, — фахівець // Internetua (https://internetua.com/u-rosiyi-duje-silno-padaye-riven-kiberbezpeki-zlomiv-bude-bilshe-fahivec?utm_source=news.ukrnet). 07.03.2024).***

***

Інші країни

«Уряд Кенії розвіяв побоювання щодо втручання в запропоновані правила, які дозволять державі контролювати сліди користувачів Інтернету…

Положення є частиною Закону про неправомірне використання комп'ютерів і кіберзлочини (критична інформаційна інфраструктура та управління кіберзлочинністю) від 2024 року…

Згідно з правилами, держава прагне змусити інтернет-провайдерів ділитися інформацією про веб-сайти в рамках зусиль щодо стримування тероризму.

Компанії також будуть змушені вести записи про діяльність користувачів в Інтернеті та будуть змушені надавати їх уряду.

Інтернет-провайдери та менеджери шлюзів, які не виконають вимоги, зазнають наслідків, зокрема припинення дії ліцензій.

У кожному поліцейському відділку буде створено спеціальну службу боротьби з кіберзлочинністю з навченим персоналом.

Запропоновані правила дають кенійцям право повідомляти комітету з кібербезпеки про шкідливі акаунти в соціальних мережах і скріншоти підозрілої діяльності.

Вони також можуть повідомити про переривання життєзабезпечення, включаючи постачання води, медичних послуг та енергії.

Це окрім несприятливого впливу на економіку, події, яка призведе до масових жертв або смертельних випадків, або порушення грошового ринку, а також негативного впливу на безпеку країни.

Правила також передбачають, що всі системи критичної інформаційної інфраструктури розташовані в Кенії, а будь-які винятки повинні бути схвалені комітетом…» ***(Moses Odhiambo. State allays intrusion fears as MPs hint at endorsing cyber security regulations // The Star (https://www.the-star.co.ke/news/2024-03-05-state-allays-intrusion-fears-as-mps-hint-at-endorsing-cyber-security-regulations/). 05.03.2024).***

***

«Рада з кібербезпеки ОАЕ запустила «Національну кампанію з кібербезпеки», інформаційну кампанію, орієнтовану на державні та приватні установи, а також на всіх членів суспільства, з метою підвищення обізнаності громадськості про загрози, які виходять із відкритого кіберпростору, і різні способи захистити від кібератак.

Кампанія закликає до важливості обережності та пильності, щоб не стати жертвою фішингових і шахрайських атак, які використовують технологію, щоб обманним шляхом змусити цифрових користувачів скомпрометувати їх особисту інформацію та дані.

Національна кампанія з кібербезпеки є практичним впровадженням директив мудрого керівництва ОАЕ, що випливає з його віри у важливість безпеки інформації та даних у світлі величезних цифрових розробок, свідком яких є країна.

Ці директиви наголошують на необхідності забезпечення безпечного цифрового середовища як для громадян, так і для мешканців, а також підвищення обізнаності про загрози відкритого кіберпростору та способи захисту від них.

Щотижнева кампанія, яка триває цілий рік, охоплює різні аспекти кібербезпеки, зокрема вказівки та поради щодо того, як ідентифікувати підозрілі електронні листи, важливість створення надійних паролів, а також постійне оновлення програм і додатків, а також використання захищених комунікаційних програм через інтернет.

За допомогою інформаційних кампаній і постійного спілкування з громадськістю Рада з кібербезпеки прагне підвищити обізнаність шляхом

покращення розуміння спільнотою природи електронних загроз і способів боротьби з ними. Це на додаток до надання їм знань та інструментів, необхідних для виявлення та захисту від цих атак, а також для сприяння безпечній поведінці за допомогою передового досвіду та запобіжних заходів.

Національна кампанія з кібербезпеки прагне підвищити культуру кібербезпеки в усіх секторах суспільства та підтримати безпечну цифрову трансформацію в країні. Він має на меті поширити обізнаність про загрози електронних атак, надати найкращі методи захисту від цих ризиків і забезпечити безпечне цифрове середовище для всіх.

Це також одна з найважливіших цілей Ради кібербезпеки ОАЕ та зробити кібербезпеку щоденною культурою для всіх членів суспільства ОАЕ. Він також прагне зробити кібербезпеку частиною повсякденної культури, яка включає всіх членів суспільства ОАЕ, на додаток до підвищення рівня обізнаності серед людей про те, що кіберзагрози не обмежуються лише великими установами, але також можуть вплинути на них та їхні родини.

Доктор Мохаммед Хамад Аль Кувейті, голова Ради кібербезпеки ОАЕ, зазначив, що «Національна кампанія з кібербезпеки» проводиться у світлі зростання кіберзагроз та їхнього впливу на всі аспекти нашого життя. «Це в світлі величезної цифрові розробки, свідками яких є країна, і на підтвердження зобов'язань уряду ОАЕ забезпечити безпечне цифрове середовище для всіх жителів».

Аль-Кувейті наголосив: «Рада з кібербезпеки вірить у важливість підвищення обізнаності та поширення культури пильності в суспільстві для вирішення цих проблем. Обізнаність окремих осіб та установ вважається важливою опорою для захисту суспільства ОАЕ від кібератак у світлі величезної кількості технологічний розвиток і зростання кіберзагроз, які його супроводжують».

У цьому контексті Голова Ради з кібербезпеки закликав усіх осіб та установи слідкувати за кампанією та активно взаємодіяти з нею, щоб досягти безпечнішого кіберпростору для всіх. Це ґрунтується на вірі в відповідальність, яку кожен повинен нести, протистоячи цим загрозам.

Аль-Кувейті пояснив, що Національна кампанія з кібербезпеки відповідає баченню «Ми, ОАЕ 2031», метою якого є побудова взаємопов'язаного та ефективного суспільства, здатного йти в ногу з глобальними розробками в різних сферах. Національна кампанія з кібербезпеки прагне сприяти участі всіх членів суспільства ОАЕ в створенні безпечного цифрового середовища, яке сприяє досягненню бачення процвітаючого майбутнього «Ми, ОАЕ 2031».

Аль-Кувейті додав, що кампанія не обмежується лише ОАЕ, а прагне поділитися своїм досвідом і найкращими практиками з усім світом. Це відображає усвідомлення важливості міжнародного співробітництва у сфері кібербезпеки та необхідності посилення обміну інформацією та досвідом з іншими країнами для забезпечення безпечного цифрового середовища для всіх.

Національна кампанія з кібербезпеки включає набір просвітницького контенту на різних платформах Ради з кібербезпеки ОАЕ в соціальних мережах, а також різноманітне висвітлення діяльності та зусиль Ради, включаючи семінари, майстер-класи та виставки. Він містить попередження безпеки щодо загроз і оновлення системи безпеки від Центру з метою консолідації повідомлення Ради щодо посилення кібербезпеки ОАЕ». ***(UAE Cyber Security Council launches 'National Campaign for Cybersecurity' // Gulf Today (https://www.gulftoday.ae/news/2024/03/04/uae-cyber-security-council-launches-national-campaign-for-cybersecurity). 04.03.2024).***

***

«Тайський національний комітет з кібербезпеки Таїланду («NCSC») випустив два повідомлення, які вимагають від операторів критичної інформаційної інфраструктури («CIIO») запровадити базові заходи захисту кібербезпеки у своїх даних та інформаційних системах, щоб підвищити їх стійкість до кібербезпеки.

Ці сповіщення:

Повідомлення про стандарти у визначенні категорії безпеки для даних або інформаційних систем («Повідомлення про категорію безпеки»); і

Повідомлення про базові стандарти для даних та інформаційних систем («Повідомлення про базові стандарти кібербезпеки»), які мають згадуватися як «Повідомлення».

Ці повідомлення були опубліковані в Королівському віснику Таїланду 18 січня 2024 року та набудуть чинності 18 січня 2025 року (тобто через 1 рік із дати публікації). Очікується, що CIIO відповідатимуть Повідомленням на дату набрання чинності.

Позначення CIIO

CIIO відносяться до тих організацій, які були призначені відповідним регулятором як CIIO у відповідних секторах, і загалом включають компанії, які надають або чиї функції включають «критичні послуги».

Повідомлення NCSC, опубліковане в 2021 році, містить розширений перелік конкретних послуг, які вважаються критично важливими, включно з певними послугами, пов’язаними з такими секторами: національна безпека, важливі державні послуги, банківська справа та фінанси (включаючи бізнес, пов’язаний з цінними паперами, як-от брокерські операції з цінними паперами), IT та телекомунікації, транспорт і логістика, енергетика та комунальні послуги та охорона здоров'я.

Визначаючи, які компанії є CIIO, NCSC надає кожному відповідному галузевому регуляторному органу право визначати, чи слід будь-яку з їхніх регульованих компаній/організацій вважати CIIO на основі вказівок, виданих NCSC та відповідним регулятором. Визначені компанії/організації CIIO будуть проінформовані відповідними регуляторами, оскільки список CIIO недоступний для громадськості.

Зобов'язання CIIO

Згідно з Повідомленнями, CIIO зобов’язані:

класифікувати свої дані/інформаційні системи на основі цілей кібербезпеки в один із трьох класів ризику: низький, середній або високий (відповідно до Повідомлення про категорію безпеки); і

встановити та впровадити базові заходи кібербезпеки для захисту кожного класу даних/інформаційної системи (відповідно до Повідомлення про базові стандарти кібербезпеки).

Крок 1: Класифікація даних/інформаційних систем СІІО

СІІО зобов'язані оцінити свої дані та інформаційні системи та призначити їм відповідний клас, який визначається після розгляду трьох цілей кібербезпеки: конфіденційності, цілісності та доступності.

Іншими важливими міркуваннями є потенційний вплив на (i) потенційну фінансову, майнову та репутаційну шкоду СІІО; (ii) користувачів, співробітників або представників широкого загалу, які користуються послугами СІІО; (iii) ефективність діяльності СІІО; та (iv) національна безпека та громадський порядок.

Результати класифікації необхідно переглядати принаймні один раз на три (3) роки або у разі будь-яких суттєвих змін у даних/інформаційних системах або функціях СІІО.

Крок 2. Запровадження базових заходів кібербезпеки в системах даних та інформації СІІО

Після класифікації даних/інформаційних систем за рівнем ризику СІІО повинні впровадити базові заходи кібербезпеки для кожного класу даних/інформаційних систем…» ***(Nonnabhat Paiboon, Peggy Chow, Supadith Palungteapin. Cybersecurity law update – New Thai rules mandating baseline cybersecurity requirements for critical systems // Herbert Smith Freehills (https://hsfnotes.com/cybersecurity/2024/03/11/cybersecurity-law-update-new-thai-rules-mandating-baseline-cybersecurity-requirements-for-critical-systems/). 11.03.2024).***

***

«Агентство кібербезпеки Сінгапуру (CSA) опублікувало консультаційний документ щодо запропонованого законопроекту про кібербезпеку (з поправками) (CAB), який передбачає внесення змін до Закону про кібербезпеку 2018 року (CA). CAB прагне зміцнити законодавчу базу, що

регулює підтримку національної кібербезпеки в Сінгапурі, проти гострої потреби в законодавстві для ефективного вирішення технологічного середовища, що швидко розвивається.

Фон

З моменту запровадження CA у 2018 році бізнес-ландшафт Сінгапуру зазнав подальшої цифрової трансформації, коли компанії впровадили такі технологічні інструменти, як хмарні обчислення, і запровадили нові бізнес-моделі, які все частіше залучають сторонніх постачальників послуг у ланцюг поставок.

Таким чином, швидка цифровізація створює нові ризики та міркування щодо кіберзагроз, які CAB прагне вирішити, щоб оновити та захистити безпеку кіберпростору Сінгапуру.

Ключові зміни в ООВ

1. Розширення визначення критичної інформаційної інфраструктури (KII) шляхом введення окремої категорії «ICI, що не належать провайдеру».

Наразі CA регулює CII, тобто комп'ютери або комп'ютерні системи, необхідні для безперервного надання основних послуг у Сінгапурі. ICI, як правило, належать постачальникам основних послуг, але постачальники все частіше залучають постачальників для надання обчислювальних послуг, і ці комп'ютери чи інфраструктура мають такий самий вплив на кібербезпеку, як ICI. Таким чином, CAB пропонує розширити зобов'язання, пов'язані з ICI, щоб охопити ситуації, пов'язані з «ICI, що не належить постачальнику».

Відповідальність за кібербезпеку основної послуги все ще покладається на постачальника основної послуги. Постачальник основних послуг повинен буде, серед іншого, надати Уповноваженому інформацію про ICI, що не належать провайдеру, та отримати різноманітні юридично обов'язкові зобов'язання від свого постачальника комп'ютерів, щоб гарантувати, що постачальник основних послуг зможе виконувати свої обов'язки відповідно до закону.

2. Розширення сфери звітування про інциденти

Враховуючи зростаючу складність суб'єктів загрози, які націлені на нешкідливі з'єднання для доступу до критично важливих мереж, по відношенню до

ICI, що належать провайдерам, CAB прагне накласти ширші обов'язки на провайдерів повідомляти про інциденти в будь-якій частині мережі під контролем провайдера або інциденти в повага до мережі під контролем постачальника до власника, яка взаємопов'язана або спілкується з ICI, що належить постачальнику, на відміну від інцидентів, пов'язаних саме з ICI, що належить постачальнику.

Розширений обсяг звітування про інциденти має на меті підвищити ситуаційну обізнаність CSA про ризики збою в роботі основних послуг, дозволяючи CSA завчасно виявляти та пом'якшувати такі загрози.

3. Розширте повноваження Уповноваженого з кібербезпеки за межі власників ICI, включивши три нові категорії

CAB пропонує розширити регуляторний нагляд Уповноваженого, щоб включити ключові системи кібер-екосистеми Сінгапуру, які не класифікуються як CII.

Нижче наведено три нові категорії:

Основні послуги цифрової інфраструктури (FDI)

Цифрова інфраструктура, яка сприяє доступності, затримці, пропускній здатності або безпеці цифрових послуг, у тому числі тих, що надають послуги хмарних обчислень або центрів обробки даних.

CSA може призначити постачальника послуг ПІІ «основним постачальником послуг ПІІ», якщо воно переконається, що (i) послуга надається до або з Сінгапуру, і (ii) будь-яке погіршення або втрата послуги ПІІ може призвести до збій у роботі великої кількості компаній чи організацій, які покладаються на послуги ПІІ або підтримуються ними.

Організації особливого інтересу з кібербезпеки (ESCI)

Суб'єкти, які обробляють конфіденційні дані або виконують критично важливі для Сінгапуру функції, які, як очікується, можуть завдати значної шкоди обороні, зовнішнім відносинам, економіці, охороні здоров'я, громадській безпеці чи громадському порядку Сінгапуру.

Тимчасові системи кібербезпеки (STCC)

Комп’ютерні системи, які є тимчасово критичними для інтересів Сінгапуру, але піддаються високому ризику кібератак у цей критичний період.

CSA може призначити комп’ютер або комп’ютерну систему як STCC на період до одного року, якщо він переконається, що ризик кібератаки високий і що компрометація або втрата STCC призведе до значної шкоди національній безпеці, обороні., зовнішні відносини, економіка, охорона здоров’я, громадська безпека чи громадський порядок Сінгапуру.

На три категорії послуг ПІІ, ESCI та STCC, буде покладено декілька обов’язків, які включають надання CSA інформації, пов’язаної з кібербезпекою, і повідомлення CSA про будь-які встановлені інциденти кібербезпеки. Крім того, ці системи мають відповідати подальшим вимогам звітування про інциденти та відповідним стандартам кібербезпеки.

Недотримання зобов'язань щодо послуг ПІІ та ESCI може призвести до фінансових санкцій, тоді як недотримання вимог STCC вважається правопорушенням.

4. Посилити повноваження ліцензіатів

Згідно з частиною 5 цього Закону про кібербезпеку особи, які займаються наданням ліцензованих послуг кібербезпеки (наприклад, тестування на проникнення), повинні отримати ліцензію постачальника послуг кібербезпеки, а умови та умови надання ліцензії визначаються ліцензійними особами. CAB внесе поправки до CA, щоб надати офіцерам ліцензій повноваження щодо моніторингу, наприклад, повноваження входити, перевіряти та перевіряти місцезнаходження та записи ліцензіатів.

Ключові висновки

Запропоновані поправки до CA спрямовані на те, щоб йти в ногу з розвитком технологій і галузевої практики, а також з подальшим зростанням проблем кібербезпеки. Операторам хмарних служб і центрів обробки даних може також знадобитися оцінити вплив зобов’язань, викладених у CAB. Підприємствам потрібно буде бути уважними до майбутніх подій і прийняти гнучку позицію під

час впровадження необхідних змін. Нарешті, як зазначено в CAB, CSA, ймовірно, забезпечить подальшу ясність шляхом публікації додаткових кодексів поведінки та вказівок». ***(Andy Leck Ken Chia and Ren Jun Lim. Singapore: Cyber Security Agency introduces Draft Cybersecurity (Amendment) Bill // Baker McKenzie (https://insightplus.bakermckenzie.com/bm/viewContent.action?key=Ec8teaJ9VaqYPz%2Fgv%2BeCQV7eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JMz1e2tr2Ki26bJK6KF1TgA%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true). 13.03.2024).***

***

«У все більш оцифрованому світі, де персональні дані є наріжним каменем сучасної економіки, перетин захисту споживачів і кібербезпеки стає першорядним, особливо в сфері довгострокового страхування. Цей перетин має надзвичайно важливе значення для захисту конфіденційності даних страхувальників, фундаментального аспекту довіри та чесності в страховій галузі.

У контексті Південної Африки компанії, особливо у сфері фінансових послуг, постійно інвестують у захист даних споживачів. Це позитивний прогноз як для споживачів, так і для організацій, які їх обслуговують.

У глобальному масштабі кібербезпека стала головним пріоритетом для страхових компаній, враховуючи зростання частоти та складності кіберзагроз. Страховий ландшафт Південної Африки не застрахований від цих викликів, про що свідчить зростаюча кількість кіберінцидентів, націлених на різні сектори, включаючи фінансові послуги.

Страхова галузь у Південній Африці має надати пріоритет заходам кібербезпеки, щоб ефективно захистити конфіденційність даних страхувальників. Такі кіберзагрози, як витік даних, атаки програм-вимагачів і викрадення особистих даних, створюють значні ризики як для споживачів, так і для страховиків, що підкреслює важливість надійного захисту кібербезпеки.

Щоб вирішити ці проблеми, страхові компанії Південної Африки інвестують у передові технології кібербезпеки та впроваджують комплексні стратегії

управління ризиками. Це включає протоколи шифрування, багатофакторну автентифікацію, системи виявлення вторгнень і регулярні оцінки безпеки для виявлення та пом'якшення потенційних вразливостей.

Страховики повинні активно співпрацювати з регуляторними органами, галузевими асоціаціями та іншими зацікавленими сторонами, щоб бути в курсі нових нормативних актів у сфері кібербезпеки, найкращих практик і нових загроз. Спільні зусилля можуть сприяти колективній відповіді на виклики кібербезпеки та сприяти обміну інформацією та знаннями в галузі.

Правила Південної Африки, які варто виділити

У південноафриканському контексті Закон про захист особистої інформації (PoPI) є законодавчим запобіжним заходом, спрямованим на захист особистої інформації осіб, яка обробляється як державними, так і приватними органами. Закон про PoPI наголошує на важливості відповідального поводження з даними, вимагаючи від організацій забезпечення конфіденційності, цілісності та доступності особистої інформації, яка знаходиться під їхнім контролем. Для сектору довгострокового страхування дотримання Закону про PoPI є не просто юридичним зобов'язанням, а й свідченням відданості галузі повазі прав власників полісів на конфіденційність.

Крім того, Закон про захист прав споживачів (CPA) посилює принципи прозорості, справедливості та підзвітності в угодах споживачів. Він вимагає від компаній, у тому числі постачальників страхових послуг, обробляти дані споживачів з належною обачністю, чесністю та таким чином, щоб поважати переваги споживачів щодо конфіденційності. Це узгоджується зі світовими тенденціями, що відстоюють більш жорсткі заходи захисту даних споживачів, що відображає зростаюче визнання прав людей контролювати свою особисту інформацію.

Протидія кіберзагрозам

У галузі спостерігається тенденція, за якою страховики вдосконалюють програми навчання та підвищення обізнаності співробітників, щоб сприяти розвитку культури обізнаності та пильності щодо кібербезпеки. Наділивши

співробітників знаннями та навичками, щоб розпізнавати кіберзагрози та реагувати на них, страховики можуть посилити свою загальну кібербезпеку та краще захистити конфіденційні дані страхувальників.

Компанії починають розробляти надійні плани реагування на порушення даних, щоб ефективно керувати потенційними порушеннями та пом'якшувати їх вплив. Це включає в себе процедури виявлення порушень, сповіщення постраждалих осіб, координацію з регуляторними органами та впровадження заходів щодо запобігання майбутнім інцидентам.

Загалом компанії, що надають фінансові послуги, часто покладаються на сторонніх постачальників і партнерів для надання різноманітних послуг, зокрема IT-інфраструктури, обробки даних і підтримки клієнтів. Для страховиків важливо оцінити стан кібербезпеки цих третіх сторін і переконатися, що вони дотримуються відповідних стандартів безпеки для захисту даних страхувальників.

По суті, перетин захисту прав споживачів і кібербезпеки має вирішальне значення для захисту конфіденційності даних страхувальників у страховому секторі як у Південній Африці, так і в усьому світі. Дотримуючись законодавчих рамок, таких як PoPI Act і CPA, і вживаючи активних заходів кібербезпеки, страховики можуть підтримувати довіру і впевненість своїх страхувальників, орієнтуючись у мінливому ландшафті кібербезпеки». ***(Mamsi Nkosi. The intersection of consumer protection and cybersecurity in insurance // IT News Africa (https://www.itnewsafrica.com/2024/03/the-intersection-of-consumer-protection-and-cybersecurity-in-insurance/). 14.03.2024).***

***

«Організація настільки сильна, наскільки сильна її найслабша ланка. Занепокоєння щодо кібербезпеки в Нігерії зростає прямо пропорційно технологічному прогресу Нігерії. Національна комісія з керування ідентифікаційною інформацією нещодавно оголосила, що розслідує ймовірні витоки даних у результаті інциденту кібербезпеки, який міг бути пов'язаний із субпідрядником. Загрози кібербезпеці не можуть бути ближчими. Національна

комісія з управління ідентифікацією відповідає за збір детальної особистої інформації про кожного нігерійця вдома та за кордоном і видачу нам усім національних ідентифікаційних номерів. Витік даних такого масштабу торкається кожного нігерійця.

Організаціям потрібна структурована стратегія управління ризиками, щоб полегшити оцінку ризиків, яка є систематичною, задокументованою, перегляданою та, сподіваємося, періодично переробленою, щоб забезпечити захист від випадкового розкриття даних або проникнення хакерів у їхню мережу.

Поточна та майбутня участь Нігерії в регіональній та глобальній цифровій економіці забезпечена завдяки вражаючим структурам інформаційно-комунікаційних технологій (ІКТ), створеним та постійно розширюваним місцевими експертами в цій галузі. Ми в авангарді інноваційних технологій. Наша освітня система, незважаючи на її недоліки та невдачі, сповнена прагнення, прагнення та рішучості як викладачів, так і студентів тримати нашу країну поінформованою та оснащеною, зміцнюючи наше місце в епоху інформації.

Однак чи займає кібербезпека те першочергове становище, яке вона заслуговує? Чи є захист даних пріоритетним?

У сучасному швидкоплинному середовищі з високою конкуренцією компанії стикаються з різноманітними проблемами, які вимагають їхньої уваги та значною мірою спираються на свої обмежені ресурси. Операційна ефективність і задоволення попиту клієнтів залишаються в їх центрі. Кібербезпека може дуже легко вийти з поля зору.

З найкращими намірами та інфраструктурою безпекова позиція організації завжди залишається нестабільною. Один із способів захисту організації від випадкового порушення закону чи зловмисних атак — це постійна оцінка стратегії захисту конфіденційності даних, інфраструктури кібербезпеки та реалізації політики.

Сфера, яку часто забувають, це управління ризиками третьої сторони (TPRM). Ваша організація може мати встановлені процедури та методично вимірювати ефективність. Проте ваші постачальники, постачальники, підрядники,

партнери, партнери та постачальники послуг — всі слова, що взаємозамінно використовуються для позначення постачальників підтримки, можуть бути піддані ризику — без яких ваша організація не зможе досягти своїх цілей і безперебійно надавати послуги клієнтам. Більшість організацій вважають, що вони можуть відпочити, будучи впевненими, що вони закрили цю лазівку.

Перш ніж залучити постачальника, організації зазвичай проводять поглиблену оцінку ризиків третьої сторони, щоб переконатися, що підрядник має адекватні системи для запобігання ризику для себе та своїх клієнтів. Дні, коли брали постачальника просто тому, що він добре зарекомендував себе, має перевірений довгий список задоволених клієнтів і показує значний дохід, давно минули. Оскільки всі компанії працюють на різних платформах ІКТ, вам слід дослідити, що має під капотом ваш потенційний постачальник.

Ваш підрядник з прибирання може бути тим шляхом, через який хакери проникають у вашу систему. Справжнім прикладом цього став 2014 рік, коли зламали велику мережу супермаркетів Target у США. Облікові дані мережі Target були вкрадені у субпідрядника постачальника, якого Target найняв для обслуговування її холодильників і кондиціонерів. Тут слабкою ланкою був субпідрядник, а не підрядник.

Провівши початкову оцінку ризику, зробіть крок далі, щоб забезпечити постійну оцінку підрядників, звертаючи увагу на процедури TPRM. Організації — це динамічні організми, які постійно змінюються. Постачальник може бути вільним від ризику на момент укладення контракту, але може не залишатися вільним від ризику протягом усього періоду його відносин з вашою організацією. Вони створюють нові союзи, беруть нових підрядників або розривають відносини з іншими. Без постійної оцінки та переоцінки вашого підрядника ви не помітите про ці зміни.

У той час як можна очікувати, що сектор фінансових технологій буде пильно тримати руку на пульсі свого TPRM, оператори в інших секторах можуть відстати. Постачальники медичних послуг, юридичні фірми, публічні бібліотеки,

університети, інші навчальні заклади та некомерційні організації однаково ризикують.

Збір даних клієнтів є додатковим до їх щоденних операцій; ці організації є справжніми резервуарами особистої інформації, привабливою для хакерів. Те, що їхні підрядники роблять для управління кібербезпекою, часто не є їхнім пріоритетом.

Постійні сторонні оцінки ризиків субпідрядників навряд чи скорочують їхні і без того надмірні ресурси. Якщо підрядник бере на себе слабку ланку, субпідрядника з неадекватною інфраструктурою кібербезпеки, може виникнути відповідальність згідно з Законом Нігерії про захист даних 2023 року та іншими нормативними актами. Періодичні сторонні аудити безпеки заощадять вашій організації час, гроші, збентеження та втрату клієнтів…» ***(Olufunmilola J. Oyelahan. Safeguarding against data breaches and cybersecurity risks: Finding your weakest link (Part 1 of 2) // Businessday NG (https://businessday.ng/opinion/article/safeguarding-against-data-breaches-and-cybersecurity-risks-finding-your-weakest-link-part-1-of-2/). 25.01.2024).***

***

«Зараз кібербезпека є головним пріоритетом для бізнесу в Сінгапурі, оскільки ІТ-керівники та бізнес-лідери розуміють фінансову та репутаційну шкоду, яку можуть завдати кібератаки.

Однак невпинний тиск кібератак, що постійно розвиваються, призводить до виснаження фахівців з кібербезпеки.

У нещодавньому звіті Sophos було виявлено, що 88% фахівців з кібербезпеки в Сінгапурі страждають від виснаження та втоми.

Це справжня проблема. Такий рівень втоми може призвести до зниження пильності, створюючи можливості для використання кіберзлочинцями. Фактично, 32% респондентів в опитуванні Sophos сказали, що виснаження та втома роблять їх менш старанними у своїх ролях, а 23% респондентів вважають, що це сприяє порушенню кібербезпеки.

Наслідки втрати кібербезпеки

Фахівці з кібербезпеки знаходяться під постійним тиском, щоб не відставати від постійно зростаючого обсягу та складності кіберзагроз.

Навіть команди з найкращими ресурсами засипаються попередженнями, намагаються встигати за останніми виправленнями та стикаються з невпинним тиском запобігання атакам, які можуть завдати шкоди їхнім організаціям, із пов'язаною з цим загрозою вказівки пальцем, якщо атака все-таки вдасться.

Як наслідок, у Сінгапурі спостерігається зростання плинності кадрів у секторі кібербезпеки, що свідчить про те, що безкінечне робоче навантаження стає непідйомним для фахівців з кібербезпеки.

Тим часом роботодавці борються з дефіцитом кадрів у галузі. Проблема ускладнюється тим, що деякі кваліфіковані професіонали взагалі залишають сферу діяльності, незважаючи на сильну зарплату та пакети пільг.

MSPs: прибуває кавалерія

Постачальники керованих послуг (MSP) мають чудову можливість вирішити проблему вигоряння кібербезпеки. Попит на послуги кібербезпеки не тільки великий, але й прибутковий.

Очікується, що до 2028 року глобальний ринок керованих послуг безпеки зросте майже вдвічі з 36,05 мільярда доларів США до 76,09 мільярда доларів США, причому, за даними Mordor Intelligence, ринок Азіатсько-Тихоокеанського регіону буде найшвидше зростаючим.

Можливість для MSP полягає у впровадженні систем, які можна застосовувати в багатьох організаціях для ефективного управління навантаженням із кібербезпеки. Наприклад:

Моніторинг безпеки та виявлення загроз: MSP можуть забезпечити цілодобовий моніторинг мережі організації на наявність загроз безпеці, використовуючи свій досвід і ресурси для розслідування підозрілої діяльності та потенційних загроз.

Реагування на інцидент безпеки: у разі кібератаки MSP може допомогти організації стримати порушення, усунути збитки та відновити їхні системи.

Керування виправленнями: MSP можуть автоматизувати процес виправлення вразливостей у системах організації. Це допомагає забезпечити оперативне застосування критичних оновлень безпеки.

Навчання з питань безпеки: MSP можуть проводити навчання з питань безпеки для працівників організації. Цей тренінг може допомогти співробітникам виявляти та уникати фішингу та інших атак соціальної інженерії.

Щойно клієнти MSP починають використовувати досвід MSP, їхні внутрішні команди IT-безпеки звільняються, щоб зосередитися на більш стратегічних ініціативах.

Зростання ринку керованих послуг безпеки

Очікується, що в найближчі роки ринок керованих послуг безпеки зазнає значного зростання.

Очікується, що Азіатсько-Тихоокеанський регіон стане ринком, що розвивається найшвидше, із сукупним річним темпом зростання (CAGR) у Сінгапурі понад 10% на рік…» ***(Study: Cybersecurity burnout impacts 88% of cybersecurity and IT roles in Singapore. What can you do as an MSP to help? // IDG Communications, Inc. (https://www.csoonline.com/article/2070139/study-cybersecurity-burnout-impacts-88-of-cybersecurity-and-it-roles-in-singapore-what-can-you-do-as-an-msp-to-help.html). 24.03.2024).***

***

Кіберстрахування

«У першому глобальному дослідженні управління страховими ризиками EY/Інституту міжнародних фінансів (IIF) кібербезпека була визнана найбільшою проблемою для керівників ризиків.

Опитані керівники управління ризиками (CRO) сказали, що п’ять основних типів ризиків або типів управління ризиками на наступний рік:

53% – Ризик кібербезпеки

35% – страховий ризик (наприклад, андеррайтинговий ризик, включаючи збої, катастрофічний (CAT) і ризик довголіття)

32% – зміна/трансформація бізнес-моделі

26% – Кредитний ризик (включаючи ризик країни, суверенний ризик і ризик концентрації)

24% – пов'язаний між розподілом капіталу, ризиком відсоткової ставки та технологічним ризиком (наприклад, ризик неадекватного управління або обслуговування технологічних систем, мереж, активів і програм)

Ризики людського капіталу (22%) також отримали високу оцінку в однорічному прогнозі, що відображає жорсткість ринку праці. Загалом 64% CRO-учасників сказали, що залучення талантів у довгостроковій перспективі стане дедалі складнішим. Ризик третіх сторін відображає дефіцит талантів і збільшення зв'язку галузі; все більше страховиків прагнуть отримати доступ до певних можливостей і технологій через екосистеми та альтернативні моделі постачання.

Згідно з даними опитування 68 страхових компаній у 15 країнах, занепокоєння змінюється, коли погляд розширюється до ризиків, що виникають протягом наступних трьох років. Незважаючи на те, що ризики кібербезпеки все ще очолюють список (68%) для всіх опитаних CRO, п'ятірку головних проблем замикають більш глобальні проблеми, включаючи геополітичний ризик (56%), екологічний ризик (50%), машинне навчання та штучний інтелект (43). %) та брак навичок/перекваліфікація існуючої робочої сили (41%).

Політична невизначеність у цей рік виборів у США посилює ризики, що сприяє тому, що більшість респондентів називають геополітичні ризики одними з найактуальніших у наступні три роки. Респонденти CRO бачать геополітичні ризики в основному з точки зору макроекономічного впливу (79%), посилення кібервійни (67%) і регуляторних змін (64%).

Американські респонденти опитування вдвічі частіше, ніж їхні європейські колеги, очікували, що в наступні п'ять років зосередять увагу на GenAI. Приблизно чверть компаній запровадили основні компоненти необхідних інфраструктур для усунення ризиків, пов'язаних зі штучним інтелектом. Незважаючи на залежність

від зростаючих екосистем і альянсів для підвищення ефективності (43%) і залучення нових клієнтів (59%), майже половина (46%) вважали управління сторонніми кіберризиками загрозою своїй операційній стійкості.

Незважаючи на те, що вони впевнено керують новими фінансовими та регуляторними ризиками, менше чверті (22%) респондентів заявили, що впроваджують штучний інтелект, штучний інтелект покоління та машинне навчання. Ті опитані, які впроваджують ШІ, роблять це прагматично, маючи огорожі – 50% встановлюють засоби контролю, щоб допомогти забезпечити відповідальне використання ШІ та ML під час прийняття рішень. Респонденти вказали на підвищений ризик у моделюванні (включаючи ризик галюцинацій і пояснення) 61%, конфіденційність даних 49%, а справедливість щодо споживачів і алгоритмічне упередження 37%.

Понад дві третини (69%) опитаних CRO інтегрують ESG у свою систему управління ризиками, а 87% впроваджують стандарти ESG в інвестиції. Незважаючи на те, що багато CRO впевнені в здатності своєї організації інтегрувати ESG у процес прийняття рішень, лише 3% респондентів мають повне уявлення про свій ризик зміни клімату, а трохи більше третини (36%) заявили, що кліматичний ризик є інтегрована в бізнес-стратегію – хоча позитивні дії попереду. Більше половини (53%) назвали інвестиції, пов’язані з ESG, і винагороду за позитивну поведінку ESG (34%) як провідні продукти або функції з найбільшим потенціалом для зростання.

Тим не менш, майже три чверті (72%) респондентів CRO впевнені, що вони здатні керувати змінами, пов’язаними з підвищеним ризиком, тоді як 74% бачать бюджет як найбільшу загрозу для прискорення критичних стратегій цифрової трансформації.

«Страхові CRO продовжують шукати можливості для стимулювання зростання та зниження операційного ризику, пов’язаного з цим, включно з кіберризиками третіх сторін», — сказала Ізабель Сантенак, глобальний лідер страхування EY. «З огляду на рекордні природні катастрофи в 2023 році, тиск на перевізників, щоб вирішити дедалі більшу багатомільярдну прогалину в захисті,

посилюється скороченням бюджетів і нестачею талантів для боротьби з деякими з найактуальніших кліматичних катастроф, з якими стикалося наше покоління».

За її словами, незважаючи на те, що вони діють у середовищі «пливучих пісків», «CRO суттєво інвестують в екосистеми, використовуючи штучний інтелект для боротьби зі зростанням шахрайства та пом'якшення майбутніх ризиків, закладаючи основу для залучення талантів у галузь із багатим потенціалом».

Впевненість залишається незважаючи на те, що деякі називають «полікризою».

«Зіткнувшись зі складними ризиками, стрімким технологічним прогресом і обмеженнями ресурсів і талантів, результати нашого опитування підкреслюють стійкість і адаптивність страхових CRO та їх тверду відданість цифровій трансформації», — сказала Мері Френсіс Монро, директор відділу регулювання та політики страхування в Інституті страхування. Міжнародні фінанси. «Спільнота страхових CRO також є невід'ємною частиною зусиль компаній з інтеграції ESG, які є вирішальними для вирішення проблем, пов'язаних із кліматом».

Події 2023 року пришвидшили темпи, з якими страхові перевізники прагнуть зміцнити свою лінію фронту за допомогою методів управління ризиками: 59% респондентів покращили свою політику, процедури та практику управління ліквідністю, а більше половини (56%) оновили свої зобов'язання активів управління (ALM) за останні 12 місяців. Ця позитивна тенденція продовжується: більше 90% респондентів планують оцінити або запровадити управління фінансовими (наприклад, кредитними, ринковими, ліквідними) і нефінансовими (наприклад, операційними) ризиками протягом наступних 12 місяців». ***(Jahna Jacobson. Chief Risk Officers Say Cybersecurity Most Pressing Risk: Survey // Wells Media Group, Inc. (https://amp.insurancejournal.com/news/national/2024/03/21/765793.htm). 21.03.2024).***

***

«За даними Польської армії кібероборони, Польща отримує велику кількість DDoS-атак, які походять з Росії.

За словами представника Армії кібероборони Польщі, у Польщі спостерігається збільшення DDoS-атак, що походять з Росії.

DDoS-атаки — це форма кіберзлочинності, при якій зловмисник переповнює сервер інтернет-трафіком, щоб заблокувати їм доступ до онлайн-сервісів.

Деякі веб-сайти, як-от Управління залізничного транспорту в Польщі, зазнають почастішали атак, які експерти географічно відстежують у Росії». ***(Poland experiences increase in DDoS attacks from Russia // Euronews (https://www.euronews.com/2024/03/06/poland-experiences-increase-in-ddos-attacks-from-russia). 06.03.2024).***

***

«Компанія Microsoft (MSFT.O) заявила в п'ятницю, що хакери, пов'язані з російською зовнішньою розвідкою, знову намагалися зламати її системи, використовуючи дані, викрадені з корпоративної електронної пошти в січні, щоб отримати новий доступ до технологічного гіганта, чиї продукти широко використовуються в структурі національної безпеки США.

Це розголошення стривожило деяких аналітиків, які посилалися на занепокоєння щодо безпеки систем і служб Microsoft, одного з найбільших у світі виробників програмного забезпечення, який надає цифрові послуги та інфраструктуру уряду США.

Аналітики висловлюють занепокоєння щодо ризиків для національної безпеки. Microsoft заявила, що за вторгненнями стоїть російська державна група під назвою Midnight Blizzard або Nobelium.

Російське посольство у Вашингтоні не відразу відповіло на запит прокоментувати заяву Microsoft, а також не відповіло на попередні заяви Microsoft про діяльність Midnight Blizzard.

Microsoft оприлюднила злом у січні, заявивши, що хакери намагалися зламати облікові записи корпоративної електронної пошти, включно з обліковими записами вищого керівництва компанії, а також служби кібербезпеки, юридичні та інші служби.

«Останніми тижнями ми бачили докази того, що Midnight Blizzard використовує інформацію, спочатку викрадену з наших корпоративних систем електронної пошти, щоб отримати або спробувати отримати неавторизований доступ», — заявила технічна компанія в новому блозі.

З огляду на величезну клієнтську мережу Microsoft, не дивно, що вона стала мішенню, сказав Джером Сегура, головний дослідник загроз у фірмі з кібербезпеки Malwarebytes' Threatdown Labs. Він додав, що дратує те, що атака все ще триває, незважаючи на зусилля Microsoft перешкодити доступу.

«Те, що один із найбільших постачальників програмного забезпечення сам начебто вивчає речі, трохи лякає», — сказав Сегура. «У вас немає впевненості, що якщо ви клієнт, то не відбувається чогось більшого».

Атаки також є свідченням того, наскільки агресивні хакери, додав він.

Серед даних, які хакери вкрали, був доступ до сховищ вихідного коду та внутрішніх систем, повідомила Microsoft. Компанії належить GitHub, загальнодоступне сховище програмного коду для різних додатків, повідомила Segura Malwarebytes.

«Це те, що нас дуже хвилює», — сказав Сегура. «Зловмисник хотів би використати секрети (Microsoft), щоб проникнути у виробниче середовище, а потім скомпрометувати програмне забезпечення та встановити бекдори тощо».

Раніше Microsoft заявила, що хакери зламали електронну пошту співробітників, використовуючи неактивний обліковий запис за допомогою атаки «розпилення паролів» — використовуючи той самий пароль для кількох облікових записів, доки вони не зламали один. За останніми спробами Midnight Blizzard такі атаки зросли в десять разів порівняно зі зломом у січні, повідомляє Microsoft у своєму блозі.

«Схоже, що це щось дуже цілеспрямоване, і якщо (хакери) знаходяться настільки глибоко всередині Microsoft, і Microsoft не змогла вивести їх звідти протягом двох місяців, то це викликає величезне занепокоєння», – сказав Адам Мейерс, старший заступник директора. президент фірми з кібербезпеки Crowdstrike, який відстежує хакерство національних держав.

«ТАЄМНИЦІ РІЗНОГО ВИДУ»

Згідно з різними аналітиками, які відстежують групу, відомо, що Midnight Blizzard спрямована на уряди, дипломатичні установи та неурядові організації. У своїй січневій заяві Microsoft заявила, що Midnight Blizzard, ймовірно, націлена на неї, оскільки компанія провела серйозне дослідження, щоб розгадати операції хакерської групи.

Команда Microsoft із аналізу загроз розслідує та ділиться дослідженнями щодо Nobelium принаймні з 2021 року, коли було встановлено, що група стоїть за кібератакою SolarWinds, яка скомпрометувала низку урядових установ США.

Наполегливі спроби зламати Microsoft є ознакою «постійної, значної відданості ресурсів, координації та зосередженості зловмисника», заявила компанія в п’ятницю.

«Очевидно, що Midnight Blizzard намагається використовувати секрети різних типів, які вона знайшла», — додали в ньому.

«Деякими з цих секретів клієнти та корпорація Майкрософт поділилися електронною поштою, і коли ми виявили їх у нашій викраденій електронній пошті, ми зв’язалися і продовжуємо звертатися до цих клієнтів, щоб допомогти їм у вживанні заходів пом’якшення».

Microsoft не назвала постраждалих клієнтів». ***(Zeba Siddiqui, Raphael Satter. Microsoft warns Russian hackers still trying to break into its systems // Reuters (https://www.reuters.com/technology/cybersecurity/microsoft-says-cyber-threat-actor-has-been-able-access-internal-systems-2024-03-08/). 08.03.2024).***

***

«Shanghai Zhenhua Heavy Industries (ZPMC) (600320.SS) заявив у неділю, що його крани не становлять загрози кібербезпеці, після того як комітети Конгресу США поставили під сумнів роботу китайської державної компанії над кранами, що прямують до Сполучених Штатів.

Панелі безпеки Палати представників ретельно перевіряють установку ZPMC швейцарської інженерної групи ABB (ABBN.S) обладнання на кранах типу «судно-берег», що прямують у США, у січні запросив керівників ABBN на публічні слухання, щоб з'ясувати свої стосунки з ZPMC, які, за їх словами, викликали «значне занепокоєння».

«ZPMC серйозно ставиться до занепокоєння США і вважає, що ці звіти можуть легко ввести громадськість в оману без достатньої перевірки фактів», — йдеться в заяві, посилаючись на розслідування комітетів внутрішньої безпеки та стратегічної конкуренції.

«Крани, надані ZPMC, не становлять загрози кібербезпеці для будь-яких портів», — йдеться в повідомленні.

Компанія ABBN заявила, що продала своє обладнання для управління та електрифікації багатьом виробникам кранів, включаючи китайські компанії, які, у свою чергу, продавали крани безпосередньо в порти США.

США і Китай, найбільші економіки світу, часто звинувачують один одного в кібератаках і промисловому шпигунстві. Цього року Вашингтон заявив, що перервав китайську операцію з кібершпигунства, спрямовану на інфраструктуру США, і розслідує імпорт китайських автомобілів на предмет ризиків для національної безпеки. Раніше він забороняв китайським телекомунікаційним компаніям.

ZPMC повідомила, що крани, які вона постачає, використовуються в портах по всьому світу, включаючи Сполучені Штати, і відповідають міжнародним стандартам і чинним законам і нормам.

Згідно з веб-сайтом, компанія ZPMC, зареєстрована на Шанхайській фондовій біржі, є одним із найбільших у світі виробників портового обладнання, що володіє флотом із понад 20 транспортних суден.

ABBN забезпечує 16% своїх продажів у Китаї, поступаючись лише ринку США з 24%». ***(Shanghai Zhenhua denies posing cybersecurity risk to US ports // Reuters (https://www.reuters.com/technology/cybersecurity/shanghai-zhenhua-denies-posing-cybersecurity-risk-us-ports-2024-03-10/). 10.03.2024).***

***

«США вважають, що Росія, Китай та Іран мають засоби та наміри зірвати вибори президента США в листопаді. Росія підозрює кібератаку США на її систему голосування пізніше цього тижня.

У новому щорічному звіті Офісу директора національної розвідки США, який містить огляд кіберзагроз національним інтересам США на основі даних національних шпигунських агентств, стверджується, що Китай і Росія готові підірвати США в глобальному масштабі., тоді як Іран залишається регіональною загрозою.

«Посилення конкуренції між демократичними та авторитарними формами правління, яке Китай, Росія та інші країни підживлюють шляхом просування авторитаризму та поширення дезінформації, чинить тиск на давні норми, які заохочують кооперативні підходи до глобальних благ», — йдеться у звіті.

Згідно зі звітом, Китай вважається найбільш активною та стійкою загрозою для США в багатьох аспектах, включаючи кібернетичну загрозу, яка потенційно загрожує комунікаціям із союзниками та має можливість здійснювати кібератаки на критичну інфраструктуру та військові активи.

Крім того, Китай розширює свої дії зловмисного впливу та «може спробувати на певному рівні вплинути на вибори в США у 2024 році через своє бажання відійти від критиків Китаю та посилити розбіжності в суспільстві США», — йдеться у звіті.

Росія розглядається як «стійкий і дієздатний супротивник», який зміцнює відносини з Китаєм, Іраном і Північною Кореєю, що є серйозним викликом для США та їх партнерів.

«Москва продовжуватиме використовувати всі застосовні джерела національної влади, щоб просувати свої інтереси та намагатися підірвати Сполучені Штати та їхніх союзників, але вона стикається з низкою проблем, таких як відрив від західних ринків і технологій і втеча людського капіталу», звіт показує.

Очікується, що Росія залишатиметься довгостроковою глобальною кіберзагрозою, здатною вражати критичну інфраструктуру, і продовжуватиме свої операції зловмисного впливу, зокрема спроби посіяти розбрат серед виборців у США.

«Москва розглядає вибори в США як можливість і проводила операції впливу протягом десятиліть, аж до проміжних виборів у США в 2022 році. Росія розмірковує над тим, як результати виборів у США в 2024 році можуть вплинути на підтримку України Заходом, і, ймовірно, намагатиметься певним чином вплинути на вибори які найкращим чином відповідають її інтересам і цілям», – йдеться у звіті.

Служба зовнішньої розвідки (СВР) Росії тим часом заявляє, що США планують втрутитися у власні президентські вибори, які мають відбутися 15-17 березня. За даними SVR, адміністрація Байдена вже запустила плани вразити російські виборчі системи та перешкодити підрахунку голосів, повідомляє Reuters.

СВР не надала жодних доказів на підтримку цих звинувачень, але також заявила, що будь-яке іноземне втручання у вибори вважатиметься актом агресії. Володимир Путін майже напевно переможе на президентських виборах». ***(Ionut Arghire. US, Russia Accuse Each Other of Potential Election Cyberattacks// SecurityWeek (https://www.securityweek.com/us-russia-accuse-each-other-of-potential-election-cyberattacks/). 12.03.2024).***

***

«Китайська державна компанія Shanghai Zhenhua Port Machinery Company, відома як ZPMC, заперечує, що її крани становлять загрозу кібербезпеці для портів у Сполучених Штатах.

Минулого місяця Білий дім оголосив, що витратить 20 мільярдів доларів США на заміну китайських контейнерних кранів типу «судно-берег» (STS) у портах США, посилаючись на проблеми кібербезпеки.

Минулого тижня з'явилася інформація про те, що під час розслідування Конгресом критичної вразливості безпеки інфраструктури в портах США було виявлено стільникові модеми на компонентах крана ZPMC в порту США.

«Ці комунікаційні пристрої не були частиною контрактів на обладнання, а також портові чиновники не могли визначити, чому компоненти були встановлені», — йдеться в заяві Комітету Палати представників з питань внутрішньої безпеки та Спеціального комітету Палати представників щодо Китаю.

Але китайський виробник кранів, який постачає близько 80% підйомного обладнання, що використовується в портах США, заперечує будь-які правопорушення.

«ZPMC помітила нещодавні дії, вжиті урядом США на основі проблем кібербезпеки щодо портів США, а також повідомлення ЗМІ про те, що на кранах ZPMC були встановлені «стільникові модеми», — йдеться в заяві компанії на своєму веб-сайті.

«ZPMC серйозно ставиться до цих звинувачень і вважає, що такі повідомлення без достатнього аналізу фактів можуть легко ввести громадськість в оману. Крани, надані ZPMC, не становлять загрози кібербезпеці для жодного порту».

Кранівник стверджує, що його обладнання виготовляється та постачається відповідно до міжнародних стандартів, чинного законодавства та специфікацій замовників.

У квітні минулого року Південна Корея оголосила, що перевірить усі крани, поставлені Китаєм, після того, як уряд США попередив, що крани, виготовлені ZPMC, можуть використовуватися для шпигунських цілей». ***(ZPMC denies cybersecurity threat // Forkliftaction.com (https://www.forkliftaction.com/news/zpmc-denies-cybersecurity-threat.aspx?n=28957). 14.03.2024).***

***

«Елітні хакери, пов’язані з російською розвідкою, минулого місяця атакували кілька німецьких політичних партій, щоб проникнути в їхні мережі та викрасти дані, згідно з попередженням, опублікованим німецьким агентством з кібербезпеки та дослідниками безпеки, які працюють на власника Google Alphabet (GOOGL).

У звіті, опублікованому в п'ятницю, кіберпідрозділ Alphabet Mandiant заявив, що спіймав хакерську групу, відому як APT29, яка, як стверджується західною розвідкою, діяла від імені російського зовнішнього шпигунського агентства SVR, намагаючись обманом змусити «ключових політичних діячів Німеччини» відкрити електронний лист маскуючись під запрошення на вечерю 1 березня, організовану Християнсько-демократичним союзом (ХДС), правоцентристською політичною партією Німеччини.

Попередження, розповсюджене німецьким кіберагентством BSI та переглянуте Reuters, стосується того самого інциденту, в якому говориться, що підтримувані державою кібершпигуни націлювалися на політичні партії Німеччини, намагаючись створити довгостроковий доступ і викрасти дані.

У своїй заяві ХДС зазначив, що протягом тривалого часу піддавався цифровим атакам з боку вітчизняних та іноземних гравців.

«І в цьому випадку ми отримали дуже оперативну інформацію про атаку» - йдеться в повідомленні. «Офіційної вечері ХДС 1 березня не було, захід був фіктивним».

У попередженні не надано додаткових подробиць про те, кого вважають відповідальними, ані воно, ані Mandiant не надали подробиць про те, хто саме став мішенню. BSI не відразу повернув запит на коментар. Посольство Росії у Вашингтоні також не відразу відповіло на електронний лист із проханням про коментар.

У своєму попередженні BSI стверджує, що іноземні держави особливо зацікавлені в шпигунстві за політиками в контексті «майбутніх виборів до

Європарламенту». Mandiant сказав, що націлювання відповідає зосередженості Москви на її довготривалому конфлікті з Києвом.

«Це останнє націлювання стосується не лише переслідування Німеччини чи її політиків; це частина ширших зусиль Росії, спрямованих на пошук способів підірвати європейську підтримку України», — сказав у заяві Ден Блек з Mandiant.

Німеччина є однією з західних держав, які надали військову підтримку Україні у війні з Росією. У грудні президент Росії Володимир Путін заявив, що відносини між Берліном і Москвою залишаються в основному замороженими…» ***(Christopher Bing, Raphael Satter. Elite Russian hackers targeting German politicians, Google warns // Reuters (https://www.reuters.com/technology/cybersecurity/elite-russian-hackers-are-targeting-german-political-parties-google-warns-2024-03-22/). 22.03.2024).***

***

«У понеділок представники США та Великобританії висунули звинувачення, наклали санкції та звинуватили Пекін у широкомасштабній кампанії кібершпигунства, яка нібито вразила мільйони людей, включаючи законодавців, науковців і журналістів, а також компанії, включаючи оборонних підрядників.

Влада по обидва боки Атлантики назвала хакерську групу Advanced Persistent Threat 31 або «APT31», назвавши її підрозділом Міністерства державної безпеки Китаю. Офіційні особи склали список цілей: співробітники Білого дому, сенатори США, британські парламентарі та урядовці в усьому світі, які критикували Пекін.

Деякі інші жертви були ідентифіковані по іменах, але американські чиновники заявили, що шпигунство хакерів, яке проводилося понад десятиліття, скомпрометувало оборонних підрядників, дисидентів і низку американських компаній, включаючи американські металургійні, енергетичні та швейні компанії. Серед цілей були провідні постачальники мобільного телефонного обладнання та бездротових технологій 5G. За словами офіційних осіб, мішенню стали навіть подружжя високопоставлених чиновників США та законодавців.

Метою глобальної хакерської операції було «репресувати критиків китайського режиму, скомпрометувати державні установи та викрасти комерційні таємниці», — заявила заступник генерального прокурора США Ліза Монако.

У розкритому в понеділок обвинувальному акті проти семи ймовірних китайських хакерів американські прокурори в суді заявили, що хакерство призвело до підтвердженого або потенційного зламу робочих облікових записів, особистих електронних листів, онлайн-сховища та записів телефонних дзвінків, що належать мільйонам американців. Офіційні особи в Лондоні звинуватили APT31 у зламі британських законодавців, які критикують Китай, і заявили, що друга група китайських шпигунів стоїть за зломом британської виборчої служби, яка окремо скомпрометувала дані ще мільйонів людей у Сполученому Королівстві.

Китайські дипломати у Великобританії та США відкинули звинувачення як необґрунтовані. Посольство Китаю в Лондоні назвало звинувачення «повністю сфабрикованим і злісним наклепом».

Агентству Reuters не вдалося відразу знайти контактну інформацію семи ймовірних хакерів, яким міністерство юстиції висунуло звинувачення.

Ці оголошення були зроблені після того, як Британія та США наклали санкції на фірму, яку вони назвали підставною компанією Міністерства державної безпеки, пов’язаною з хакерською діяльністю.

У заяві Міністерства фінансів США йдеться, що санкції стосуються компанії Wuhan Xiaoruizhi Science and Technology, а також двох громадян Китаю.

«Сьогоднішнє оголошення викриває безперервні та зухвалі зусилля Китаю, спрямовані на підрив кібербезпеки нашої країни та спрямовані проти американців і наших інновацій», — заявив директор ФБР Крістофер Рей.

Між Пекіном і Вашингтоном зростає напруженість через проблеми, пов’язані з кібершпигунством, оскільки західні спецслужби все частіше б’ють на сполох щодо ймовірної хакерської діяльності, яка підтримується Китаєм.

Останніми роками Китай також почав заявляти про ймовірні хакерські операції Заходу. Наприклад, минулого року Міністерство державної безпеки

заявило, що Агентство національної безпеки США неодноразово проникало в китайського телекомунікаційного гіганта Huawei Technologies.

Прокуратура США перерахувала численні неназвані жертви по всьому світу, які стали мішенню, але деякі з них виділяються в обвинувальному акті.

У 2020 році китайські хакери атакували співробітників президентської кампанії в США, написали прокурори. Розголошення збігається з публічними повідомленнями Google на той час про те, що китайські хакери надсилали шкідливі електронні листи до кампанії нинішнього президента Джо Байдена, але компрометації виявлено не було.

Інша передбачувана місія включала злом американської фірми, відомої дослідженнями громадської думки, у 2018 році, у той самий рік проміжних виборів у США.

«Політики, партії та виборчі організації є багатими джерелами розвідувальних даних, які пропонують колекціонерам все: від рідкісних геополітичних ідей до величезних скарбниць даних», — сказав Джон Халткві ст, головний аналітик американської розвідувальної фірми з кібербезпеки Mandiant, підрозділу власника Google Alphabet (GOOGL.O).

«Як ми бачили на попередніх виборчих циклах, такі актори, як APT31, звертаються до політичних організацій, щоб знайти геополітичну розвідку, яку їм доручено збирати», — сказав Хултквіст». ***(James Pearson, Raphael Satter and Christopher Bing. US, UK accuse China of cyberespionage that hit millions of people // Reuters (https://www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25/). 25.03.2024).***

***

Кіберзахист критичної інфраструктури

«Консультативна рада Білого дому рекомендує федеральному уряду створити нові програми економічного стимулювання, щоб спонукати власників і операторів критичної інфраструктури підвищити свої стандарти

кібербезпеки, розробити нові засоби захисту від відповідальності щодо обміну інформацією та спростити дедалі складніший національний режим кіберрегулювання.

Ці рекомендації є частиною звіту, схваленого в четвер Консультативним комітетом з телекомунікацій національної безпеки, який складається з представників найбільших телекомунікаційних компаній країни, а також фірм, що займаються кібербезпекою. У звіті було зосереджено увагу на тому, чому так багато організацій, які надають критично важливі послуги країні, часто намагаються застосувати найкращі практики або інвестувати достатні ресурси в свої операції з кібербезпеки.

Було зроблено висновок, що ринкових сил самих по собі «недостатньо», щоб спонукати приватні компанії надавати пріоритет кібербезпеці на рівнях, необхідних для захисту національної безпеки.

У звіті також виявлено, що зацікавлені сторони в критичній інфраструктурі загалом не знають про технічну допомогу та програми, які вже пропонує федеральний уряд для покращення кібербезпеки, і стикаються з дедалі складнішим тягарем відповідності, оскільки адміністрація Байдена намагається змінити свої регуляторні повноваження, щоб підвищити панель кібербезпеки в різних секторах.

Щоб усунути ці перешкоди, комітет рекомендував Офісу національного кібердиректора співпрацювати з галуззю, щоб вивчити ряд нових фінансових стимулів, таких як податкові відрахування та федеральні гранти, щоб допомогти закрити прогалину в інвестиціях у кібербезпеку. Він також рекомендував, щоб ONCD працював з іншими федеральними агентствами над загальнонаціональним поштовхом до навчання власників і операторів щодо безкоштовних федеральних послуг, таких як Служба кібергігієни CISA, Центр кіберспівробітництва АНБ і Національний центр передового досвіду кібербезпеки NIST, які не використовуються ефективно.

Комітет також запропонував ONCD взяти на себе провідну роль у розробці стратегії, яка забезпечує «однозначну мову», яка передбачає захист від відповідальності та безпечну гавань для компаній, щоб більш вільно обмінюватися

інформацією про кіберзагрози та вразливості, які можуть вплинути на один або декілька промислових секторів.

Національний кібердиректор Гаррі Кокер зробив короткі зауваження під час зустрічі, подякувавши комітету та зазначивши рекомендації у звіті: «Я вже переглянув їх, і вони мені подобаються».

Метью Деш, генеральний директор Iridium Communications і співголова підкомітету, який створив звіт, сказав, що висновки були зроблені на основі більш ніж 50 брифінгів, проведених членами NSTAC з постачальниками критичної інфраструктури, постачальниками хмарних і технологічних послуг, консультантами, торговими асоціаціями та експертами. танки.

«Відсутність послідовного прийняття та впровадження найкращих кіберпрактик і стандартів є особливо проблематичною, оскільки об'єкти критичної інфраструктури США стикаються зі значно підвищеною загрозою, і тим більше з огляду на поточний геополітичний клімат», – сказав Деш.

Рекомендації у звіті були схвалені незабаром після того, як офіційні особи США попередили в січні, що хакерська група, пов'язана з китайським урядом, відома як Volt Typhoon, роками ховається в системах і мережах американських постачальників критичної інфраструктури. Брендон Уейлз, виконавчий директор CISA, сказав, що «метою групи є проникнення в нашу критичну інфраструктуру з метою проведення руйнівних або руйнівних атак». ***(Derek B. Johnson. White House advisory group says market forces 'insufficient' to drive cybersecurity in critical infrastructure // cyberscoop (https://cyberscoop.com/nstac-white-house-advisory-group-critical-infrastructure/?utm_source=flipboard&utm_content=barryrgreene%2Fmagazine%2FSURFING+CYBERSECURITY). 07.03.2024).***

***

«У міру того як організації критичної інфраструктури стають все більш оцифрованими, однорідними та пов'язаними, ризик кібератак з боку як

державних, так і злочинних хакерів зростатиме, попередив у середу Роберт М. Лі, генеральний директор і засновник фірми промислової кібербезпеки Dragos.

«Ви подивіться на багато наших систем водопостачання в Сполучених Штатах. Є багато застарілих, старих систем, які не є цифровими та не підключеними», — сказав Лі на конференції з безпеки S4x24, присвяченій ICS, у Маямі. «У міру того, як ці системи будуть оновлені протягом наступних трьох-п'яти років, ви почнете бачити значно більш зв'язаний і значно більш однорідний водний сектор, ніж будь-коли раніше».

Лі стверджував, що ця розробка відтворить те, як інші галузі переходили від аналогових до підключених цифрових систем — лише для того, щоб побачити, що вони є об'єктом широкомасштабних кібератак. У пошуках ефективності виробничий сектор був одним із перших, хто оцифрував, і сьогодні це сектор, який найбільше постраждав від атак програм-вимагачів, згідно з нещодавнім оглядом Dragos за рік.

Більша цифровізація також принесла більшу однорідність, і це незабаром можна буде побачити в інших секторах критичної інфраструктури, що, у свою чергу, збільшить як кількість атак програм-вимагачів, так і їхній вплив, попередив Лі.

«Заводу з виробництва інсуліну не потрібно було бути однорідним з чимось іншим у світі. Це була автономна рослина», — сказав Лі. «Але зараз ми це бачимо».

Однорідність також полегшить хакерам повторне використання можливостей, які традиційно були лише в IT-системах, які мають подібні стеки технологій. Лі попередив, що невдовзі злочинні хакери зрозуміють, що вони можуть повторно використовувати можливості на багатьох об'єктах і мати більший вплив на операції.

Це особливо хвилює галузі, які історично мало інвестували в кібербезпеку. Виступаючи на слуханнях у січні, Рік Джеффарес, президент Асоціації сільського водопостачання Джорджії, сказав законодавцям Палати представників, що багато невеликих водопровідних підприємств у Джорджії використовують обмежені

системи SCADA і часто не підключені до Інтернету. Тому для деяких із цих водопровідних служб кібербезпека просто не є нагальною проблемою.

Потенційний вплив посиленого зв'язку та однорідності нещодавно проілюстрував відносно нехитрий напад на пристрій, виготовлений ізраїльською фірмою Unitronics, який здійснила група під назвою Cyber Av3ngers, група хакерів, пов'язана з Корпусом вартових Ісламської революції Ірану.

За словами Dragos, націлившись на один пристрій, екіпаж зміг спричинити збій у кількох об'єктах водопостачання, пивоварні, а також у хімічному та виробничому секторах. Підключивши пристрої до Інтернету та покладаючись на стандартний пароль, адміністратори стали легкою мішенню». ***(Christian Vasquez. Dragos CEO: Digitization in critical infrastructure will spur attacks // cyberscoop (https://cyberscoop.com/water-digitization-critical-infrastructure-attacks/?utm_source=flipboard&utm_content=other). 06.03.2024).***

***

Кіберзахист закладів охорони здоров'я

«Управління з громадянських прав (OCR) Міністерства охорони здоров'я та соціальних служб США оголосило про своє перше врегулювання справи HIPAA (Health Insurance Portability and Accountability Act — є актом про мобільність та підзвітність медичного страхування, що прийнятий 21 серпня 1996), пов'язаної з фішинговою кібератакою. У травні 2021 року компанія Lafourche Medical Group, LLC подала повідомлення про порушення HIPAA в OCR, заявивши, що хакер отримав електронну інформацію про здоров'я пацієнтів (ePHI) за допомогою фішингової кібератаки. У прес-релізі OCR йдеться: «Фішинг — це тип атаки на кібербезпеку, який використовується для того, щоб оманою змусити людей розкрити конфіденційну інформацію за допомогою електронного зв'язку, наприклад електронної пошти, видаючи себе за надійне джерело». Ця кібератака є найпоширенішим способом доступу хакерів до систем охорони здоров'я для отримання інформації про пацієнтів.

Після розслідування порушення OCR встановив, що Lafourche не зміг провести аналіз ризиків правил безпеки або запровадити процедури для регулярного перегляду записів про діяльність інформаційної системи. HIPAA вимагає, щоб охоплені організації, включаючи Lafourche, виконували ці дії.

Угода про вирішення проблеми вимагає, щоб Lafourche сплатила компенсацію в розмірі 480 000 доларів США та дотримувалася плану коригувальних дій (CAP), який OCR контролюватиме протягом наступних двох років. CAP зобов'язує Lafourche вживати наступних заходів для дотримання вимог:

Створити та реалізувати план управління ризиками;

Проводити щорічну оцінку ризиків для виявлення ризиків і вразливостей до ePHI у всій групі;

Створювати, впроваджувати та поширювати політики та процедури, зокрема:

Процес регулярного перегляду всіх записів інформаційної діяльності, які збирає група; і

Метод оцінки того, коли збір нової або іншої інформації слід включити в процес перегляду;

Повідомити HHS, якщо співробітник не дотримується групових політик і процедур щодо конфіденційності або безпеки PHI;

Навчіть співробітників, які мають доступ до PHI, щодо конфіденційності, безпеки та відповідних політик і процедур;

Вести облік проходження персоналом навчання; і

Переглядайте та оновлюйте навчання щороку на основі змін законодавства або проблем, що виникають під час перевірок чи перевірок». ***(HHS' Office for Civil Rights Reaches Settlement of First Phishing Cyberattack Under HIPAA // Hall Benefits Law (https://hallbenefitslaw.com/hhs-office-for-civil-rights-reaches-settlement-of-first-phishing-cyberattack-under-hipaa/). 08.03.2024).***

***

«У той час як багато хто з нас зайняті торгівлею валютами, активами, колекційними картками та іншими цінними предметами, кіберзлочинці торгують даними. Маючи дані, кіберзлочинці можуть відкривати інші двері, і коли ці дані надходять від компанії, ці двері можуть призвести до незаконного прибутку.

У той час як витоки даних і крадіжки з боку великих компаній часто потрапляють у заголовки, кіберзлочинці також націлені на малі та середні підприємства (МСП). Це має сенс, оскільки з тактичної точки зору малих підприємств більше, ніж великих. За даними Світового банку, 90 відсотків підприємств класифікуються як МСП. Це величезний ігровий майданчик для кіберзлочинців.

Що викликає занепокоєння, це те, що малі та середні підприємства, здається, не сприймають загрозу кіберзлочинності серйозно.

У своєму звіті про загрози за 2024 рік Sophos підкреслив цифрові небезпеки, з якими стикаються МСП, а також те, наскільки поширеними є атаки на малі підприємства.

Фірма з кібербезпеки стверджує, що у 2023 році 75 відсотків випадків реагування на інциденти клієнтів, переданих її службою X-Ops Incident Response, були від малого бізнесу.

Аналізуючи дані, зібрані в цих випадках, Sophos відзначив кілька тенденцій. Найпоширенішим було використання зловмисного програмного забезпечення, призначеного для крадіжки інформації, або інфокрадії.

Ця шкідлива програма може збирати паролі та реєструвати натискання клавіш, надсилаючи їх до віддаленої бази даних.

Кіберзлочинці порівнюють ці дані, а потім продають їх тому, хто запропонує найвищу ціну. Маючи бізнес-реєстраційні дані, кіберзлочинці часто можуть отримати доступ до інших сервісів і навіть інших частин бізнесу. За даними Sophos,

90 відсотків кібератак, про які їй повідомили в 2023 році, стосувалися крадіжки даних або облікових даних.

«Цінність «даних» як валюти експоненціально зросла серед кіберзлочинців, і це особливо вірно для малих і середніх підприємств, які, як правило, використовують одну послугу або програмне забезпечення для кожної функції для всієї своєї діяльності.

Наприклад, скажімо, зловмисники розгортають інфокрадію в мережі своєї цілі, щоб викрасти облікові дані, а потім отримати пароль для бухгалтерського програмного забезпечення компанії. Потім зловмисники можуть отримати доступ до фінансових даних цільової компанії та мати можливість перерахувати кошти на власні рахунки», – сказав Крістофер Бадд, директор дослідження Sophos X-Ops у Sophos.

Незважаючи на те, що інфокрадії набувають популярності серед кіберзлочинців, програмне забезпечення-вимагач все ще використовується та залишається помітною загрозою для МСП.

Програмне забезпечення-вимагач du jour на 2023 рік було створено бандою програм-вимагачів LockBit. На щастя, головні сервери банди були захоплені, а двоє чоловіків були заарештовані за причетність до нападів.

Програми-вимагачі групи були відповідальними за більшість – 27,59 відсотка – атак програм-вимагачів, розслідуваних Sophos минулого року з програмами-вимагачами від Akira (15,52 відсотка) та BlackCat (13,79 відсотка), які слідували за ними.

Sophos зазначає, що з 2023 роком вона відзначила збільшення кількості дистанційного виконання програм-вимагачів за допомогою незахищених пристроїв у мережі фірми. Сервери, персональні пристрої, пристрої Інтернету речей навіть принтери можуть бути скомпрометовані та поширювати програми-вимагачі та інші проблеми на інші пристрої в мережі. Оскільки багато з цих пристроїв мають незмінні паролі за замовчуванням, які можна легко знайти в Інтернеті або зламати, їх легко підібрати для кіберзлочинців, які хочуть виманити бізнес.

Згідно зі звітом Sophos, соціальна інженерія все ще є серйозною загрозою, як і компрометація бізнес-електронної пошти.

Здатність кіберзлочинців маніпулювати мішенню, щоб вона передала інформацію, яку вони зазвичай не мали б, лише посилена завдяки великим мовним моделям. Однак Sophos зазначає, що шахраї стали неймовірно нахабними у своїй тактиці, зайшовши настільки далеко, що називають мішенями.

«Минулого року команда безпеки обміну повідомленнями Sophos натрапила на безліч нових трюків і методів соціальної інженерії, призначених для ухилення від традиційного контролю електронної пошти. Повідомлення, у яких зловмисник несподівано надсилає вкладення або посилання, тепер перестали бути видаленими: ефективніші спамери з більшою ймовірністю спочатку розпочнуть розмову, а потім перейдуть до вбивства у наступних електронних листах», — пише компанія.

«Ми спостерігали цю методологію в атаках, під час яких спамери, видаючи себе за працівників служби доставки, дзвонили корпоративним клієнтам по телефону та просили їх відкрити збройний електронний лист. Ми також спостерігали, як спамери спочатку надсилали електронною поштою прохання до бізнесу або скаргу під час атак, спрямованих на різні галузі у 2023 році, після чого надсилали посилання для завантаження замаскованого, збройного файлу після того, як компанія відповіла на перший електронний лист», – додали в ньому.

Фірма додає, що спамери також знаходять способи обійти захист електронної пошти. Це може приймати форму заміни тексту зображеннями, включно із зображеннями, схожими на рахунки-фактури. Ці рахунки-фактури можуть містити номери, яким пропонується зателефонувати. Це може вселити у співробітника впевненість у тому, що рахунок-фактура законний, або спонукати його до ненавмисного завантаження зловмисного програмного забезпечення.

Це лише приклади загроз, з якими зіткнулися МСП у 2023 році, і ви можете бути впевнені, що тактика та загрози стануть лише більш серйозними у 2024 році…» ***(Brendyn Lotz. Cybercriminals love that you aren't taking cybersecurity seriously // Hypertext (https://htxt.co.za/2024/03/cybercriminals-love-that-you-arent-taking-cybersecurity-seriously/). 13.03.2024).***

***

«Конфіденційну інформацію, що належить десяткам тисяч клієнтів Fidelity Investments Life Insurance, було викрадено, як повідомляється, завдяки атаці на ланцюжок поставок, яка сталася у 2023 році.

Страховий гігант подав повідомлення про порушення даних до офісу генерального прокурора штату Мен, у якому він заявив, що 28 268 його клієнтів отримали витік особистих даних після витоку даних у Infosys McCamish Systems LLC – американській дочірній компанії індійського гіганта технічних послуг Infosys.

Порушення, яке сталося в листопаді 2023 року, призвело до викрадення імен людей, номерів соціального страхування, штатів проживання, банківських рахунків і маршрутних номерів або номерів кредитних/дебетових карток у поєднанні з кодом доступу, паролем і PIN-кодом для облікового запису і дати народження.

Участь LockBit

Ця база даних є справжньою скарбницею для кожного хакера, оскільки вона надає достатньо інформації для здійснення неймовірно правдоподібних фішингових атак, крадіжок особистих даних, видавання себе за іншу особу, шахрайства з використанням електронного зв'язку та цілої низки подібних шахрайств.

Невдовзі після того, як з'явилася новина про злам, оператори програм-вимагачів LockBit взяли на себе відповідальність. LockBit є одним із найбільших і найнебезпечніших у світі операторів програм-вимагачів як послуг, афілійовані особи якого стоять за одними з найруйнівніших атак програм-вимагачів у нові часи.

LockBit також був об'єктом операції Cronos, великої правоохоронної операції під керівництвом NCA Великобританії, яка відбулася на початку цього року. Під час операції було вилучено десятки серверів LockBit, вилучено викрадені дані, зіпсовано веб-сайти та отримано інформацію про майже 200 афілійованих осіб.

Однак, оскільки ніхто не був арештований, LockBit швидко повернувся, підтримуючи нову інфраструктуру та веб-сайти менш ніж за тиждень. На веб-сайті одразу з'явилося п'ять нових жертв». ***(Sead Fadilpašić. Insurance giant Fidelity hit by data breach — thousands of customers may have had data stolen // Future US, Inc. (https://www.techradar.com/pro/security/insurance-giant-fidelity-hit-by-data-breach-thousands-of-customers-may-have-had-data-stolen?utm_source=flipboard&utm_content=AWC%2Fmagazine%2FOur+Electronic+%26+Digital+Lives.). 06.03.2024).***

***

«Французька державна служба зайнятості France Travail постраждала від кібератаки, яка скомпрометувала персональні дані близько 43 млн громадян країни.

Про це пише The Register.

Нинішній інцидент з France Travail поки що не пов'язують з кремлем. Однак атаки відбулися через кілька днів після того, як президент Франції Еммануель Макрон публічно підтвердив непохитну підтримку Києва у російсько-українській війні.

За даними відомства, зловмисникам вдалося отримати доступ до масиву конфіденційних даних, які накопичувалися протягом останніх 20 років. Серед викраденої інформації — імена, дати народження, номери соцстрахування, електронні адреси, поштові адреси та номери телефонів

Відомство проінформувало Національну службу захисту даних (CNIL) про інцидент і попередило, що зловмисники можуть об'єднати викрадені дані з іншими для створення потужних баз даних про громадян. На щастя, паролі та банківські реквізити не постраждали.

Розслідуванням витоку, який відбувся між 6 лютого по 5 березня, наразі займається бригада по боротьбі з кіберзлочинністю Департаменту судової поліції Парижа. Громадян закликають бути пильними до можливих спроб фішингу та перевірити захищеність своїх паролів.

Фахівці радять France Travail невідкладно вжити заходів для посилення кібербезпеки та інформувати постраждалих громадян про ситуацію.

Хто стоїть за кібератакою на уряд Франції

Це вже другий масштабний витік даних у Франції за останні кілька місяців. У березні цього року зловмисники отримали доступ до даних понад 33 млн осіб внаслідок атак на медичні та страхові компанії.

Як сталася нинішня кібератака наразі не повідомляється. Відомо, що зловмисники представлялися членами Cap Emploi — відділу опіки над людьми з інвалідністю, які шукають роботу…» ***(Богдан Камінський. Кібератака на уряд Франції розкрила дані до 43 млн громадян // SPEKA (https://speka.media/kiberataka-na-uryad-franciyi-rozkrila-dani-do-43-mln-gromadyan-9wnw01). 15.03.2024).***

***

«AT&T стверджує, що величезна кількість даних, що впливають на 71 мільйон людей, не походить з її систем після того, як хакер вилив їх на форумі кіберзлочинців і заявив, що їх було вкрадено під час злому в компанії в 2021 році.

Хоча BleepingComputer не зміг підтвердити легітимність усіх даних у базі даних, ми підтвердили, що деякі записи є точними, включно з тими, чиї дані не є загальнодоступними для збирання.

Дані отримано від передбачуваного витоку даних AT&T у 2021 році, який загрозливий актор, відомий як ShinyHunters, намагався продати на форумі крадіжки даних RaidForums за початкову ціну в 200 000 доларів США та додаткові пропозиції в 30 000 доларів США. Хакер заявив, що негайно продасть його за 1 мільйон доларів.

Тоді AT&T повідомила BleepingComputer, що дані не походять від них і що їх системи не були зламані.

«Виходячи з нашого сьогоднішнього розслідування, інформація, яка з’явилася в кімнаті інтернет-чату, схоже, не надійшла з наших систем», — повідомила AT&T BleepingComputer у 2021 році.

Коли ми повідомили ShinyHunters, що AT&T каже, що ці дані походять не від них, вони відповіли: «Мене не хвилює, якщо вони не визнають. Я просто продаю».

Сьогодні AT&T продовжує повідомляти BleepingComputer, що вони все ще не бачать доказів зламу в їхніх системах і все ще вважають, що ці дані походять не від них.

BleepingComputer запитав AT&T, чи можливо, дані надійшли від стороннього постачальника послуг або постачальника, але наразі не отримав відповіді.

Передбачувані дані AT&T просочилися через два роки

Сьогодні інший загрозливий діяч, відомий як MajorNelson, безкоштовно злив дані про передбачувану витоку даних 2021 року на хакерському форумі, стверджуючи, що це дані, які ShinyHunters намагалися продати у 2021 році.

Ці дані включають імена, адреси, номери мобільних телефонів, зашифровану дату народження, зашифровані номери соціального страхування та іншу внутрішню інформацію.

Проте зловмисники розшифрували дати народження та номери соціального страхування та додали їх до іншого файлу, що витікає, зробивши їх також доступними.

BleepingComputer переглянув дані, і хоча ми не можемо підтвердити, що всі 73 мільйони рядків точні, ми перевірили, що деякі дані містять правильну інформацію, включаючи номери соціального страхування, адреси, дати народження та номери телефонів.

Це було зроблено шляхом підтвердження витоку даних з людьми, яких я знаю, на яких це вплинуло, і перевіркою того, що багато з перерахованих користувачів мають онлайн-акаунти AT&T.

Крім того, інші дослідники кібербезпеки, такі як Dark Web Informer, який першим повідомив BleepingComputer про витік даних, і VX-Underground також підтвердили, що деякі дані точні.

У той же час BleepingComputer не зміг знайти дані про людей, які, як відомо, були клієнтами AT&T у 2021 році та раніше. Однак це не було б чимось незвичайним, оскільки їх загальна база мобільних клієнтів на кінець 2021 року становила 201,8 мільйона абонентів, що означає, що якщо цей дамп законний, то це лише частковий дамп.

На даний момент залишається загадкою, звідки взялися дані. Проте, незалежно від того, звідки вони походять, усі ознаки вказують на те, що це дані клієнтів AT&T.

Таким чином, якщо ви були клієнтом AT&T до та до 2021 року, безпечніше припустити, що ваші дані були розкриті та можуть бути використані в цілеспрямованих атаках, включаючи фішингові атаки через SMS і електронну пошту, а також атаки під час заміни SIM-карти.

Якщо ви отримуєте SMS-повідомлення або фішингові електронні листи, нібито від AT&T, будьте дуже обережні, надаючи будь-яку інформацію. Натомість зверніться безпосередньо до AT&T, щоб підтвердити, що вони намагалися зв'язатися з вами». ***(Lawrence Abrams. AT&T says leaked data of 70 million people is not from its systems // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70-million-people-is-not-from-its-systems/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 17.03.2024).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Корпорація Microsoft планує випустити 1 квітня інструменти штучного інтелекту, які допоможуть працівникам кібербезпеки створювати зведення про підозрілі інциденти та виявляти хитрі методи, які використовують хакери, щоб приховати свої наміри.

Корпорація Майкрософт представила свій Copilot for Security приблизно рік тому і відтоді тестує його з корпоративними клієнтами. За словами Ендрю Конвея, віце-президента Microsoft із маркетингу безпеки, тестувальники включають BP Plc і Dow Chemical Co., і зараз вони налічують «сотні партнерів і клієнтів». Клієнти сплачуватимуть плату залежно від використання, так само як і з хмарними службами Azure компанії.

Copilot безпеки є частиною постійних зусиль Microsoft, спрямованих на те, щоб наповнити свої основні лінійки продуктів інструментами штучного інтелекту від партнера OpenAI і переконати корпоративних клієнтів купувати підписки.

Хоча штучний інтелект може допомогти створювати вміст і синтезувати корпоративні дані, він також допускає помилки, які можуть бути дорогими або незручними. Оскільки комп'ютерна безпека є надзвичайно важливою, а ризики настільки високими, Конвей сказав, що гігант програмного забезпечення приділяв особливу увагу цьому Copilot. Програмне забезпечення поєднує потужність моделі OpenAI із величезним набором інформації про безпеку, яку збирає Microsoft.

«Враховуючи серйозність варіанту використання, ми робимо ряд речей, щоб усунути [ризики]», — сказав він, зокрема шукати постійний відгук про продукт і про те, де він не відповідає вимогам. «З огляду на все це, безпека все ще є місцем, де продукти безпеки створюють помилкові спрацьовування та генерують помилкові негативи. Це просто природа простору».

Copilot працює з усім програмним забезпеченням безпеки та конфіденційності Microsoft, пропонуючи панель помічника, яка може створювати підсумки та відповідати на запитання. Наприклад, одна з програм безпеки компанії вже збирає різноманітні сповіщення безпеки та об'єднує пов'язані з ними в один інцидент. Тепер, коли користувач натискає на кожен інцидент, Copilot може узагальнювати дані та писати звіт, що зазвичай займає багато часу. Часто під час атаки хакери використовують складні сценарії програмування, щоб приховати те, що вони намагаються зробити, що ускладнює відстеження. Копілот призначений для пояснення мети зловмисника.

Програмне забезпечення звільнить досвідчених спеціалістів із кібербезпеки для більш складних завдань і допоможе новим швидше навчитися, а також доповнить свої навички, сказав Конвей. У своїх тестах Microsoft заявила, що нові системи безпеки працюють на 26% швидше та на 35% точніше. Це корисно, оскільки галузь кібербезпеки страждає від хронічної нестачі робочої сили.

Microsoft заявила, що програма штучного інтелекту також може зв'язуватися з програмним забезпеченням безпеки від конкуруючих компаній, а не лише від Microsoft.

Від 20 до 30 співробітників BP тестували Copilot, сказав Чіп Калхун, віце-президент з кіберзахисту нафтового гіганта. За його словами, щоб налаштувати його, знадобилося лише один або два клацання миші, але знадобилося кілька місяців, щоб його спеціалісти з безпеки справді звикли користуватися інструментом. Деякі члени його команди використовують Copilot для пошуку загроз, покладаючись на штучний інтелект для швидкого сканування масивів даних і попереджень на наявність доказів порушення безпеки.

Досвідченіші аналітики можуть задавати інструменту запитання — говоріть простою англійською мовою, доповненою захистом, ШІ навчений розуміти. Наприклад, аналітик може попросити надати докази того, що хакер переміщається через системи BP, використовуючи «методи живого за рахунок землі», тип атаки, яка використовує власні інструменти мережі для уникнення засобів захисту. Такі вторгнення популярні серед пов'язаних з Росією та Китаєм хакерів.

«Погані хлопці стають швидшими, і ми також маємо ставати швидшими, тому такі інструменти справді допомагають нам», — сказав Калхун, чия команда також створює власні індивідуальні інструменти штучного інтелекту на основі загальнодоступних моделей. «Це ще не ідеально. Це буде ідеально». ***(Dina Bass. Microsoft to Release Security AI Product to Help Clients Track Hackers // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2024-03-13/microsoft-to-release-security-ai-product-to-help-clients-track-hackers). 13.03.2024).***

***

«…Унікальна здатність штучного інтелекту аналізувати величезну кількість даних, вчитися на них і швидко адаптуватися робить його незамінним активом у виявленні кіберзагроз і реагуванні на них. Здатність технології розпізнавати закономірності та аномалії в режимі реального часу, які можуть вислизати від аналітиків, значно підвищує рівень безпеки компаній.

За даними MarketsandMarkets, у 2023 році світовий ринок штучного інтелекту в сфері кібербезпеки оцінювався в приголомшливі 22,4 мільярда доларів. Ця цифра є свідченням зростаючого визнання потенціалу штучного інтелекту в посиленні заходів кібербезпеки.

Згідно з прогнозами, цей ринок буде експоненціально розширюватися, досягнувши 60,6 мільярдів доларів до 2028 року. Ця траєкторія зростання підкреслює зростаючу залежність від ШІ як основного механізму захисту від складних кіберзагроз.

Інтеграція штучного інтелекту в захист кібербезпеки може помітно посилити різні аспекти кіберзахисту. Ось ключові приклади ШІ в кібербезпеці та його переваги в різних випадках використання.

1. Виявлення та запобігання загрозам

Використовуючи алгоритми штучного інтелекту, дослідники безпеки аналізують величезні обсяги даних, виявляючи шаблони та аномалії, які можуть завчасно сигналізувати про потенційні загрози.

Моделі машинного навчання покращують запобігання загрозам. Вони вивчають дані про історичні атаки, адаптуються до нових векторів атак і забезпечують постійне вдосконалення безпеки.

2. Поведінковий аналіз

AI відстежує поведінку користувачів і системи, виявляючи аномалії, щоб запобігти внутрішнім загрозам. Сповіщення викликаються незвичними діями, такими як неавторизований доступ або нетипова передача даних.

Цей проактивний підхід покращує безпеку, ефективно виявляючи відхилення від нормальних моделей.

3. Автоматизоване реагування на інциденти

Автоматизація на основі штучного інтелекту змінює правила реагування на інциденти безпеки. Він швидко ізолює скомпрометовані системи, блокує зловмисний трафік і ініціює кроки для відновлення.

Ця автоматизація зменшує ручне втручання, забезпечуючи швидку та ефективну реакцію безпеки на події.

4. Розширена автентифікація

AI покращує автентифікацію, аналізуючи поведінку користувачів, біометричні та контекстні дані.

Адаптивна автентифікація регулює рівні безпеки відповідно до факторів ризику, забезпечуючи надійну безпеку та безперебійну роботу користувача.

5. Прогнозна аналітика

Моделі ШІ можуть передбачати потенційні загрози безпеці на основі історичних даних і поточних тенденцій.

Цей проактивний підхід допомагає запобігти атакам до того, як вони відбудуться, і може допомогти запобігти атакам на ланцюг поставок.

6. Виявлення зловмисного програмного забезпечення та попередження

Інструменти захисту від вірусів і зловмисного програмного забезпечення на базі штучного інтелекту можуть виявляти нові та нові загрози. Поведінковий аналіз може виявити атаки нульового дня та поліморфне шкідливе програмне забезпечення.

7. Безпека мережі

AI може контролювати мережевий трафік на наявність підозрілої активності, включаючи спроби вторгнень і викрадання даних. Він може динамічно налаштовувати правила брандмауера наступного покоління та засоби контролю доступу.

8. Управління вразливістю

ШІ може визначати пріоритети вразливостей на основі ризику та впливу. Він допомагає керувати виправленнями та зменшує вплив відомих уразливостей.

9. Розвідка загроз

ШІ може обробляти канали розвідки про загрози та співвідносити їх із внутрішніми даними. Це забезпечує контекст для команд безпеки та допомагає їм приймати обґрунтовані рішення.

10. Зменшення помилкових спрацьовувань

Алгоритми штучного інтелекту можуть відфільтровувати помилкові спрацьовування, мінімізуючи втому від сповіщень для аналітиків безпеки. Щоб забезпечити оптимальну кібербезпеку, вкрай важливо впровадити кілька основних основних заходів.

Регулярне оновлення та виправлення систем є обов’язковими, оскільки це допомагає усунути будь-які щойно виявлені вразливості.

Крім того, підтримувати надійний контроль доступу. для запобігання несанкціонованому проникненню важливо

Нарешті, безперервний моніторинг і журналювання забезпечують видимість системних дій у режимі реального часу, забезпечуючи швидке виявлення та реагування на підозрілу поведінку.

Кіберзлочинці, включно з національними державними загрозами, все частіше використовують технології ШІ. Ці зловмисники, які часто володіють значними ресурсами, можуть зловмисно отримати доступ до передових інструментів ШІ та використовувати їх.

Ця тенденція підкреслює нагальну потребу в надійних заходах кібербезпеки. Кіберзлочинці використовують штучний інтелект, щоб підвищити ефективність атак, уникнути захисту та завдати значної шкоди організаціям.

Платформа для співпраці AI/ML Hugging Face нещодавно виявила 101 шкідливу модель AI/ML завдяки наполегливим зусиллям дослідницької групи безпеки JFrog. Під час завантаження файлу pickle ці моделі можуть ініціювати неавторизоване виконання коду, потенційно дозволяючи зловмисникам проникати в системи та встановлювати бекдори, щоб отримати повний контроль.

Ця вразливість має глобальні наслідки, впливаючи на численні нічого не підозрюють жертви. Це викликає серйозне занепокоєння в спільноті кібербезпеки, підкреслюючи важливість пильності та надійних заходів безпеки.

Ось деякі інші сфери, де зловмисники використовують ШІ:

1. Атаки соціальної інженерії

За допомогою штучного інтелекту кіберзлочинці можуть масштабувати та вдосконалювати атаки соціальної інженерії, вивчаючи та імітуючи моделі поведінки. Таким чином вони переконливо видають себе за законних осіб у різних формах, таких як відео, телефонні дзвінки чи електронні листи. Жертви несвідомо ризикують скомпрометувати мережі та розкрити конфіденційні дані.

2. Автоматизовані фішингові кампанії

ШІ-боти швидко створюють і розповсюджують фішингові електронні листи з неперевершеною швидкістю. Оцінюючи дії одержувачів, ШІ підвищує ефективність спроб фішингу. Ця передова тенденція створює значні проблеми для систем безпеки електронної пошти.

3. Створення та адаптація шкідливих програм

Generative AI налаштовує варіанти зловмисного програмного забезпечення, пристосовуючи поведінку до цільового середовища для уникнення виявлення. Поліморфне зловмисне програмне забезпечення змінює структуру свого коду, щоб перешкоджати захисту на основі сигнатур. Динамічні загрози з підтримкою ШІ постійно розвиваються.

4. Внесення облікових даних і атаки грубою силою

Штучний інтелект автоматизує додавання облікових даних для викрадення облікових даних користувача з різних сайтів і покращує атаки грубої сили за допомогою передбачення пароля.

5. Автоматичне сканування вразливостей

Системи штучного інтелекту шукають уразливості, виявляючи слабкі місця, які кіберзлочинці використовують для несанкціонованого доступу.

6. Ухилення від заходів безпеки

AI оцінює протоколи безпеки, розробляє тактику ухилення, щоб перевершити CAPTCHA, системи виявлення вторгнень і брандмауери. Його можливості кидають виклик традиційним механізмам захисту, підкреслюючи необхідність адаптивних заходів безпеки.

7. Змагальні атаки на системи ШІ

Кіберзлочинці використовують вразливості штучного інтелекту, впроваджуючи оманливі приклади змагання. Ці незначні модифікації змушують системи штучного інтелекту приймати неправильні рішення.

8. Автоматизоване вилучення даних

AI автоматично визначає цінні мережеві дані, спрощуючи вилучення. Зводячи до мінімуму людські зусилля, ця автоматизація полегшує викрадання даних, позначаючи значну загрозу мережевим процесам і безпеці.

9. Динамічна поведінка зловмисного програмного забезпечення

AI динамічно змінює поведінку зловмисного програмного забезпечення, відстежуючи дані в реальному часі. Він ухиляється від перевірок пісочниці та підлаштовується під протоколи безпеки, створюючи загрози. Ця адаптивність кидає виклик традиційним системам захисту.

10. Автоматизовані ботнети

Штучний інтелект ефективно керує бот-мережами для виконання DDoS-атак, надсилаючи сервери, щоб порушувати служби. Ці ботнети здійснюють масові атаки, викликаючи перебої в роботі сервісів.

Майбутнє штучного інтелекту в кібербезпеці

Проблеми та недоліки ШІ в кібербезпеці

ШІ має величезний потенціал для посилення заходів кібербезпеки, але також створює нові вразливості та перешкоди.

Одним із поширених занепокоєнь є поява кібератак на основі ШІ. Зловмисники все частіше використовують штучний інтелект для оптимізації та посилення атак, що ускладнює їх ідентифікацію та протидію. Це може проявлятися в різних формах, від складних схем фішингу до автоматизованих спроб злому пароля.

Компрометація систем ШІ створює ще одну критичну проблему. Припустімо, що модель штучного інтелекту підроблено, як у випадку злому платформи Hugging Face, згаданого вище. У такому випадку він може надати помилкові або оманливі

дані, що призведе до фальшивих сповіщень системи безпеки та помилкової оцінки ризиків, що потенційно відкриває шлях до серйозних порушень безпеки.

ШІ став невід'ємною частиною хмарних технологій, SOAR і рішень аналізу загроз. Однак розгортання штучного інтелекту в рамках кібербезпеки викликає етичні міркування та міркування конфіденційності.

Оскільки системи штучного інтелекту зазвичай покладаються на масивні набори даних, що містять конфіденційну інформацію, забезпечення відповідального використання та надійного захисту таких даних стає серйозною проблемою.

Оскільки штучний інтелект стає все більш поширеним, спеціалісти з кібербезпеки повинні пройти навчання технологіям штучного інтелекту, щоб захищатися від загроз, створених штучним інтелектом. Інакше швидкий розвиток технології штучного інтелекту може призвести до нестачі навичок у кадрах із кібербезпеки.

Штучний інтелект зміцнює стійкість, протидіючи тактиці суперництва, але він вимагає цілісного розуміння, суворих механізмів захисту та стратегічного підвищення кваліфікації, щоб створити надійний щит захисту від поточних і майбутніх цифрових загроз.

Під час інтеграції штучного інтелекту в стратегії безпеки організації повинні збалансувати ці фактори.

Обґрунтовані рішення вимагають розуміння потенціалу та обмежень ШІ. Варто пам'ятати, що ШІ може підвищити кібербезпеку, але це не універсальне рішення. Врахування витрат, навичок і етичного використання має вирішальне значення для успішної інтеграції ШІ.

Останні розробки в галузі кібербезпеки ШІ

Переваги штучного інтелекту в кібербезпеці є величезними: усунення за допомогою ШІ збільшує час реагування на загрози та зменшує наслідки кіберінцидентів.

Генеративні моделі штучного інтелекту імітують сценарії атак, посилюючи аналіз загроз.

Великі мовні моделі (LLM), як-от GPT-4, аналізують шаблони паролів, сприяючи більш надійним методам паролів.

Методи обману, керовані ШІ, створюють мережі-приманки, вводячи в оману зловмисників і захищаючи критичні активи.

Інструменти штучного інтелекту допомагають розробникам писати безпечний код, визначати вразливості та автоматизувати керування виправленнями.

AI також автоматизував тестування на проникнення та оцінку ризиків, активно усуваючи прогалини в безпеці та ефективно розподіляючи ресурси.

Ці досягнення підкреслюють зростаючу роль штучного інтелекту в посиленні заходів кібербезпеки.

Висновки

Джон Маккарті ввів термін «штучний інтелект» у 1956 році для опису систем, що імітують людський інтелект, які сьогодні забезпечують такі досягнення, як виявлення вторгнень і аналіз поведінки.

Незважаючи на його переваги, власники бізнесу повинні використовувати ШІ обережно та пам’ятати про ризики кібербезпеки. Інтеграція штучного інтелекту в практику кібербезпеки дає значні переваги, але вимагає етичних міркувань, оскільки його неправильне використання створює загрози.

Майбутнє бачить безліч рішень на основі штучного інтелекту, які революціонізують цю сферу. Важливо пам’ятати, що штучний інтелект, хоч і розширює можливості захисників, може також підтримувати зловмисників». ***(John Meah. AI and Cybersecurity: Accelerate Your Defenses in 2024 // Techopedia (https://www.techopedia.com/ai-and-cybersecurity-benefits-and-threats). 13.03.2024).***

***

«Безпека є пріоритетом для всіх підключених пристроїв і рішень. Виробники пристроїв, компанії, що встановлюють Інтернет речей (IoT), і постачальники рішень повинні прийняти всеосяжний 360-градусний підхід до захисту своїх продуктів і послуг від багатьох кіберзагроз, з якими вони стикаються.

Структура безпеки, яка включає заходи захисту, виявлення та реагування, пропонує надійний підхід, який компаніям слід доповнювати репетицією та постійним вдосконаленням, щоб поставити їх у найсильнішу позицію для пом'якшення ризиків безпеки IoT.

Зростання кібератак IoT

Згідно зі звітом SonicWall про кіберзагрози, у першій половині 2023 року в усьому світі було зафіксовано понад 77 мільйонів атак зловмисного програмного забезпечення IoT, що на 37% більше з початку року. Тим часом у звіті Всесвітнього економічного форуму «Стан підключеного світу» за 2023 рік, який розглядає прогалини в управлінні Інтернетом речей і пов'язаними технологіями, визначено кібербезпеку як «другу за величиною прогалину в управлінні».

Усі пристрої та рішення IoT, незалежно від того, чи вони збирають дані про навколишнє середовище, записують і обмінюються даними інтелектуальних лічильників або здійснюють будь-яку іншу діяльність IoT, стикаються з загрозами безпеці. До них належать програми-вимагачі, зловмисне програмне забезпечення, підробка пристроїв і атаки типу «людина посередині».

Компанії повинні захищати свої пристрої та рішення, щоб зменшити ризик атаки або злому, а також операційну, фінансову та репутаційну шкоду, яку вони можуть завдати.

Тому безпека є головним пріоритетом в IoT, але 96% респондентів у звіті Keyfactor кажуть, що їм важко захистити свій IoT і підключені продукти.

Заходи безпеки IoT, які ви повинні вжити

Безпека Інтернету речей повинна використовувати комплексний підхід для захисту рішень, виявлення будь-яких інцидентів безпеки та реагування на них. Цей цілісний підхід до безпеки Інтернету речей має включати процеси та людей, а також технології, і поширюватися на вибір партнерів із міцною репутацією та обліковими записами безпеки.

Захищати

Це починається із захисту, який починається із запобігання несанкціонованому доступу до пристроїв, хмарної інфраструктури та даних. У

цьому IoT SAFE відіграє центральну роль. Це сумісний загальногалузевий стандарт безпеки SIM-карти для унікальної ідентифікації пристроїв для автентифікації. Заходи захисту також повинні включати безпечний зв'язок, стійкість до збоїв, оновлення програмного забезпечення, політики безпеки даних і дотримання ринкових і галузевих норм.

Якщо 360-градусна безпека Інтернету речей — це кругова діаграма, захист — це найбільший шматочок, тоді як решта однаково відводиться для виявлення та реагування.

Виявляти

Виявлення має важливе значення, оскільки незалежно від того, наскільки надійними є заходи захисту, компанії все одно повинні стежити за поведінкою пристроїв, аналізувати мережевий трафік і використовувати аналітику для прийняття обґрунтованих рішень. Ці заходи необхідні для виявлення будь-яких потенційних порушень, аномальних дій або незвичайної поведінки. Попереджувальними ознаками можуть бути змінені цільові URL-адреси або використання даних, яке є нестандартним.

Реагувати

Якщо заходи виявлення виявлять будь-які тривожні прапорці, компанії повинні відреагувати, використовуючи заздалегідь сплановані контрзаходи, деякі з яких можуть бути автоматизованими. Дія може включати розміщення на карантині й очищення уражених пристроїв, а також застосування коригувальних дій у всіх системах. Повідомлення про порушення та аномалії також підпадають під заходи реагування.

«Захищати, виявляти та реагувати» разом складають 360-градусну структуру безпеки IoT, але є четверта дія, яку компанії також повинні зробити: репетиція. Репетиція дає змогу компаніям швидко почати діяти, якщо цього вимагає ситуація, оскільки вони це спланували та знають, що робити. Репетиції також мають ще одну перевагу – вони можуть допомогти виявити будь-які слабкі місця або прогалини в безпеці, які потрібно усунути.

Компанії можуть скористатися інструментами та методами, які допоможуть їм відпрацювати сценарії безпеки. До них належать віртуальні представлення «цифрових близнюків» для моделювання загроз і «що, якщо?» семінари, які покроково оброблюють сценарії.

Яке законодавство щодо безпеки Інтернету речей існує?

Відповідність нормативним вимогам, звичайно, є важливою та є частиною стратегії захисту безпеки Інтернету речей.

Компанії повинні бути обізнані про чинне та незавершене законодавство та розуміти, що воно для них означає. Окрім законодавства про безпеку для певного сектору, це включає Закон Великої Британії про безпеку продуктів та телекомунікаційну інфраструктуру (PSTI), Закон ЄС про кібер-стійкість і Закон США про покращення кібербезпеки IoT (для пристроїв, які використовуються федеральним урядом).

Режим PSTI (Product Security), який набуває чинності 29 квітня цього року, регулює споживчі товари, такі як маршрутизатори, веб-камери та підключені холодильники. Він зобов'язує продукти, на які впливає, не використовувати паролі за замовчуванням, мати політику розкриття вразливостей і бути прозорими щодо періодів підтримки оновлень.

Великі розгортання IoT часто є міжнародними або глобальними, і компанії повинні дотримуватися відповідних нормативних актів, які, ймовірно, відрізнятимуться в усіх регіонах.

Низка існуючих галузевих стандартів, як-от стандарт EN 303 645 Європейського інституту телекомунікаційних стандартів (ETSI), IEC 62443 4-2 і ISO/SAE 21434, є важливими ресурсами, на які розробники рішень IoT можуть спиратися для вказівок щодо вирішення проблем кібербезпеки.

Ефективна безпека IoT потребує постійних циклів вдосконалення

Компанії з продуктами та послугами Інтернету речей, виробники пристроїв і постачальники рішень повинні забезпечити безпеку розгортання Інтернету речей. Для цього їм потрібна комплексна безпека на 360 градусів із заходами захисту, виявлення та реагування. Крім того, вони повинні регулярно перевіряти безпеку та

повертати інформацію про цикли розробки, щоб постійно покращувати свою безпеку. Загрози для IoT цілком реальні, і жодна компанія не хоче страждати від операційного, фінансового та репутаційного впливу збою безпеки». ***(Harry Fowle. How to improve your IoT security in a world of rising cyber attacks // Electronic Specifier (https://www.electronicspecifier.com/products/iot/how-to-improve-your-iot-security-in-a-world-of-rising-cyber-attacks). 20.02.2024).***

***

«Тіньові IT – використання програмного забезпечення, апаратного забезпечення, систем і послуг, які не були схвалені відділами IT/IT-техніки організації – були проблемою протягом останніх кількох десятиліть, і для IT-лідерів важко керувати ними ефективно.

Подібно до тіньових IT, тіньовий ШІ стосується всіх продуктів і платформ із підтримкою штучного інтелекту, які використовуються у вашій організації, про які ці відділи не знають. Хоча особисте використання програми штучного інтелекту можна вважати нешкідливим і низьким ризиком, Samsung (наприклад) миттєво постраждав від наслідків, коли використання ChatGPT її співробітниками призвело до витоку конфіденційної інтелектуальної власності в Інтернеті.

Але ризик тіньового ШІ є потрійним:

1) Введення даних або вмісту в ці програми може поставити інтелектуальну власність під загрозу

2) Зі збільшенням кількості додатків із підтримкою штучного інтелекту зростає ймовірність неправомірного використання, причому ключовими міркуваннями є такі аспекти, як керування даними та правила, такі як GDPR

3) Існує репутаційний ризик, пов’язаний із неперевіреним виходом ШІ. Маючи значні наслідки, пов’язані з порушеннями нормативних документів, це створює значні головні болі для IT-команд у спробах відстежити це

Зменшення ризиків, які створює тіньовий штучний інтелект

Є чотири кроки, які слід зробити, щоб пом’якшити загрозу, якою є тіньовий ШІ. Усі вони взаємозалежні, і відсутність будь-якого з чотирьох залишить прогалину в пом’якшенні:

1. Класифікуйте використання ШІ

Створення матриці ризиків для використання штучного інтелекту у вашій організації та визначення способу його використання дозволить вам вести продуктивні розмови щодо використання штучного інтелекту для всього бізнесу.

Ризик можна розглядати в континуумі: від низького ризику використання GenAI як «віртуального помічника», до програм «другого пілота» та до областей підвищеного ризику, таких як вбудовування ШІ у ваші власні продукти.

Категоризація на основі потенційної схильності до ризику для бізнесу дозволить вам визначити, які програми з підтримкою ШІ можна схвалити для використання у вашій організації. Це матиме вирішальне значення, коли ви розробляєте свою політику прийнятного використання, навчання та процеси виявлення.

2. Створіть політику прийнятного використання

Після класифікації вашого використання штучного інтелекту потрібно розробити прийнятну політику використання для всієї вашої організації, щоб переконатися, що всі співробітники точно знають, що вони можуть, а що не можуть робити під час взаємодії з затвердженими програмами з підтримкою штучного інтелекту.

Роз’яснення того, що є прийнятним використанням, є ключовим для забезпечення безпеки ваших даних і дозволить вам у разі потреби вжити примусових заходів.

3. Створіть навчання для співробітників на основі вашої політики використання ШІ та прийнятного використання та переконайтеся, що всі співробітники пройшли навчання

Генеративний штучний інтелект є таким же фундаментальним, як і впровадження Інтернету на робочому місці. Навчання потрібно починати з нуля,

щоб переконатися, що працівники знають, що вони використовують і як це використовувати ефективно та безпечно.

Трансформаційна технологія завжди потребує навчання, і люди не можуть залишатися напризволяще, коли ці навички настільки важливі. Інвестування зараз у здатність ваших співробітників безпечно використовувати генеративний штучний інтелект допоможе підвищити продуктивність вашої організації та допоможе зменшити зловживання даними.

4. Наявність правильних інструментів виявлення для моніторингу активного використання ШІ у вашій організації

Інструменти IT Asset Management (ITAM) працювали над можливостями виявлення ШІ ще до того, як ChatGPT потрапив у заголовки газет минулого року. Організації можуть керувати лише тим, що вони можуть бачити, і це подвоюється для програм із підтримкою штучного інтелекту, оскільки багато програм із підтримкою штучного інтелекту є безкоштовними, і їх неможливо відстежувати за допомогою традиційних засобів, таких як квитанції про витрати чи замовлення на покупку.

Це особливо важливо для інструментів, які мають вбудований ШІ, де користувач не обов'язково знає, що використовується ШІ. Багато співробітників не розуміють наслідків інтелектуальної власності в цих обставинах, і активний контроль є критично важливим для рішення ITAM, яке має виявлення активів програмного забезпечення для інструментів ШІ.

Сильна безпека вимагає виконання всіх чотирьох цих кроків; без усіх чотирьох частин у вашій тіньовій системі захисту ШІ є діра.

Висновок

Хоча жодна окрема галузь не є більш сприйнятливою до ризику тіньового штучного інтелекту, ніж інша, більші організації або відомі бренди, як правило, швидше за все зазнають великої репутаційної шкоди через його наслідки, тому їм слід застосовувати більш обережний підхід.

Галузі та компанії будь-якого розміру повинні використовувати переваги ШІ. Однак наявність правильних процедур і вказівок у рамках інтегрованої стратегії

кібербезпеки є важливою частиною впровадження цієї трансформаційної технології.

Штучний інтелект вже вніс постійні зміни в те, як працюють організації, і прийняття цих змін допоможе компаніям досягти успіху в майбутньому…» ***(Steve Tait. Shadow AI is the latest cybersecurity threat you need to prepare for // Help Net Security (https://www.helpnetsecurity.com/2024/03/22/shadow-ai-risks/). 22.03.2024).***

***

«Стрімкий розвиток інструментів штучного інтелекту передбачає збільшення їх використання кіберзлочинцями та кібероператорами національних держав, попереджають чиновники з кібербезпеки та страхові експерти.

Протягом наступних 12-24 місяців «імовірно, що частота, серйозність і різноманітність кібервтрат меншого масштабу зросте» через використання зловмисниками все більш ефективного генеративного штучного інтелекту та великих мовних моделей, «за якими настане плато. оскільки технології безпеки та оборони наздоганяють противагу», — йдеться в нещодавньому звіті лондонського Lloyd's.

Ринок страхування та перестрахування очікує, що штучний інтелект покоління та LLM змінять «ландшафт кіберризиків» як для зловмисників, так і для захисників, і каже, що практики стійкості бізнесу повинні адаптуватися.

«Проблеми кіберстійкості ставатимуть гострішими в міру розвитку технології», — йдеться в січневому звіті, опублікованому Британським національним центром кібербезпеки, який є частиною розвідувального агентства GCHQ. NCSC стверджує, що зловмисники будь-якої масті – від малокваліфікованих кіберзлочинців до складних груп національних держав – «різною мірою» вже використовують ШІ.

Експерти кажуть, що інтерес злочинців і національних держав до таких інструментів високий, що базується на підпільних балаканинах і спробах використовувати та вдосконалювати інструменти в зловмисних цілях.

«Ми спостерігаємо це у фішингових електронних листах — мова та граматика використовуються кращі; електронний лист складений краще; і менш очевидно, що відправник не є носієм мови», — Ден Кеплін, керівник британської консалтингової компанії S-RM’s European. практика реагування на інциденти, йдеться в дописі в блозі юридичної фірми Pinsent Masons. «Це підвищує ймовірність того, що одержувачі виконають дію, яку вони хочуть, наприклад, розкриють дані або натиснуть посилання на шкідливе програмне забезпечення».

Майбутні ризики

NCSC прогнозує, що генеруючі вдосконалення AI та LLM протягом наступних дев’яти місяців «ускладнять для всіх, незалежно від їхнього рівня розуміння кібербезпеки, оцінити, чи є запит на скидання електронної пошти чи пароля справжнім, або виявити фішинг, спуфінг або соціальні мережі. інженерні спроби».

NCSC очікує, що більша автоматизація штучного інтелекту прискорить здатність зловмисників знаходити невиправлене програмне забезпечення та використовувати його протягом періоду між випуском виправлення та його встановленням. Також очікується покращення в розвідці та ексфільтрації, оскільки зловмисники використовують штучний інтелект «для виявлення цінних активів для перевірки та ексфільтрації, підвищуючи цінність і вплив кібератак», у тому числі програм-вимагачів.

У звіті Lloyd's детально описані майбутні потенційні кіберризики:

Автоматизоване виявлення вразливостей: враховуючи потенційну вигоду від однієї вразливості нульового дня або широко розповсюдженої, але погано виправленої помилки, «інструменти для створення загроз, ймовірно, випереджатимуть захисні інструменти, створені індустрією безпеки через асиметричні стимули» не лише для програмного забезпечення, а й для мікропрограм., драйвери пристроїв та інші «домени, які є дуже складними для людей».

Ворожі кібероперації: якщо ШІ покращить можливості груп національних держав, очікуйте більш ефективних шпигунських і диверсійних кампаній.

Нижчі бар’єри для входу: кращі інструменти можуть мати ефект сніжного кома, спонукаючи більш досвідчених зловмисників використовувати їх, а також «знижуючи бар’єр для входу» для менш досвідчених злочинців.

Оптимізація фішингової кампанії: більш автоматизоване виявлення цілей може призвести до більшої кількості складніших кампаній, що проводяться зловмисниками, дозволяючи їм краще вдосконалювати підручники та вражати бажані цілі з меншими витратами та з більшою частотою.

Окремі точки збою: переривання або компрометація послуг, заснованих на LLM або тісно інтегрованих з ними, може мати непередбачені наслідки, такі як «великі випадки знеструмлення, кіберфізична шкода, порушення даних або збої ринку».

Зміна ризику та винагороди: нові можливості можуть спонукати зловмисників бути сміливішими, особливо якщо інструменти штучного інтелекту зможуть краще приховувати цифрові криміналістичні докази, такі як зв’язки з діяльністю груп національних держав.

Хоча більш складні та добре фінансовані хакерські групи національних держав спочатку матимуть перевагу, NCSC очікує, що екосистема кіберзлочинності швидко наздожене згаяне, що «майже напевно збільшить обсяг і вплив кібератак, включно з програмами-вимагачами».

Більш досвідчені злочинці, швидше за все, передадуть ці можливості іншим за певну ціну. «Комерціалізація можливостей боротьби з кіберзлочинністю, наприклад, бізнес-моделей «як послуга», робить майже впевненим, що спроможні групи монетизуватимуть кіберінструменти з підтримкою штучного інтелекту, роблячи покращені можливості доступними для будь-кого, хто готовий платити», — заявили в NCSC.

Багато інструментів на основі штучного інтелекту також за своєю суттю розроблені таким чином, що менш просунуті користувачі можуть їх використовувати. «Сервіси штучного інтелекту знижують бар’єри для входу, збільшуючи кількість кіберзлочинців, і підвищать їхні можливості за рахунок покращення масштабу, швидкості та ефективності існуючих методів атак», —

нещодавно попередив Джеймс Беббідж, генеральний директор із загроз Національного агентства Британії з боротьби зі злочинністю.

«Шахрайство та сексуальне насильство над дітьми також можуть постраждати особливо», - сказав він.

У довгостроковій перспективі, оскільки «ШІ знижує бар'єр для початківців кіберзлочинців», NCSC заявив, що очікує, що «початківці кіберзлочинці, наймані хакери та хактивісти» будуть проводити більш «ефективніші операції доступу та збору інформації».

Бар'єри, що зникають

Поки що зловмисне використання штучного інтелекту стикається з численними перешкодами, включно з «ефективністю управління моделлю штучного інтелекту, витратами та апаратними бар'єрами, а також захистом вмісту», – йдеться у звіті Lloyd's.

Microsoft заявила, що, виходячи з роботи з OpenAI, інтерес національної держави залишається високим, хоча «наше дослідження з OpenAI не виявило значних атак із використанням LLM, за якими ми уважно стежимо».

У той же час технологічний гігант минулого місяця повідомив про масштабні експерименти передових постійних груп загроз, пов'язаних з Китаєм, Росією, Північною Кореєю та Іраном, і повідомив, що облікові записи, пов'язані з такою діяльністю, були заблоковані.

Схоже, що групи тестували використання LLM для різних цілей, наприклад для розвідки, в тому числі російською групою для підтримки вторгнення країни в Україну. Здається, деякі також шукали допомоги в розробці шкідливого коду - Microsoft заявила, що вбудовані етичні гарантії блокують такі запити - а також допомоги з перекладами, ймовірно, для підтримки атак соціальної інженерії.

Поточні вдосконалення означають, що існуючі перешкоди для незаконного використання можуть незабаром зникнути, особливо коли зловмисники отримають доступ до альтернатив таким варіантам хмарних чат-ботів, як ChatGPT-4 від OpenAI, Copilot від Microsoft, Gemini та PaLM від Google, у тому числі через опції з відкритим кодом, такі як Мета LLaMA.

«Випуск необмежених граничних моделей, а також нещодавні відкриття алгоритмічної ефективності, є ключовим провалом в управлінні штучним інтелектом», — сказав Lloyd's. «Зараз існує багато загальнодоступних моделей, які можуть створювати явно шкідливий вміст, і тепер їх можна дешево запускати на звичайному апаратному забезпеченні».

Коротше кажучи, більш складні інструменти ШІ покоління та LLM стають все більш доступними для всіх, незалежно від їхнього призначення». ***(Mathew J. Schwartz. Experts Warn of Cyber Risk Due to Rapid AI Tool Evolution // Information Security Media Group, Corp. (https://www.bankinfosecurity.com/experts-warn-cyber-risk-due-to-rapid-ai-tool-evolution-a-24668). 22.03.2024).***

***

Федеральна комісія зі зв'язку (FCC) запровадить добровільну програму маркування кібербезпеки для продуктів бездротового споживчого Інтернету речей, щоб допомогти споживачам враховувати стандарти безпеки під час купівлі розумних пристроїв.

У четвер FCC повідомила, що запровадить нову позначку під назвою «Знак кібердовіри США» на сертифікованих пристроях, які відповідають стандартам і вимогам кібербезпеки, щоб дозволити громадськості визначати функції безпеки бездротових продуктів IoT.

Етикетка супроводжуватиметься QR-кодом для легкого доступу до детальної інформації, такої як виправлення програмного забезпечення та оновлення безпеки.

Згідно з програмою, FCC забезпечить нагляд і затвердить сторонніх адміністраторів маркування для оцінки заявок на продукт, дозволу на використання етикетки та навчання споживачів новому знаку.

Федеральна комісія зв'язку США (FCC) просить надати галузь інформацію про потенційні вимоги до розкриття інформації, включно з тим, чи програмне забезпечення або мікропрограму продукту вироблено в країні, що становить загрозу національній безпеці». ***(Naomi Cooper. FCC Approves Voluntary Cybersecurity Labeling Program for Wireless IoT Devices // Executive Mosaic***

(https://executivegov.com/2024/03/fcc-approves-voluntary-cybersecurity-labeling-program-for-wireless-iot-devices/). 18.03.2024).

***

«Швидкий розвиток штучного інтелекту (ШІ) змінює ландшафт кібербезпеки, представляючи як потужний захист від кіберзагроз, так і нові вразливості. Ця двостороння природа технології штучного інтелекту стала центром уваги як для експертів з кібербезпеки, так і для зловмисників, що призвело до гонки озброєнь у кіберпросторі, де інновації та адаптивність є ключовими.

Ключові моменти:

Генеративні технології штучного інтелекту революціонізують практики кібербезпеки, особливо в ідентифікації загроз, але вони створюють значні проблеми через конфіденційний характер даних безпеки.

Дефіцит фахівців з кібербезпеки посилює ризики, пов'язані з кіберзлочинністю через ШІ, що підкреслює необхідність відповідального та безпечного розгортання інструментів ШІ.

Фішингові атаки та атаки зловмисного програмного забезпечення з підтримкою штучного інтелекту стають усе більш витонченими, використовуючи поточні події та людську психологію, щоб обійти традиційні заходи безпеки.

Найпопулярніші загрози кібербезпеці 2023 року, створені на базі штучного інтелекту, включають складні схеми фішингу, зловмисне програмне забезпечення, яке адаптується, щоб уникнути виявлення, і атаки, які використовують складність і швидкі зміни в цифровому середовищі.

Розширення ролі ШІ в кібератаках

Вплив штучного інтелекту на кібербезпеку є глибоким і багатогранним, що відображає його потенціал як для посилення заходів безпеки, так і для сприяння новим формам кібератак. Розробка генеративного штучного інтелекту на основі великих мовних моделей (LLM) запровадила нові можливості в операціях з кібербезпеки, зокрема у виявленні загроз. Компанії все більше покладаються на генеративний штучний інтелект для виявлення загроз, використовуючи його

здатність швидко аналізувати та інтерпретувати величезні набори даних для виявлення потенційних вразливостей і атак.

Однак цей прогрес супроводжується значними проблемами. Властива конфіденційність і відокремленість даних безпеки ускладнює створення комплексних високоякісних наборів даних, необхідних для навчання та вдосконалення моделей ШІ. Незважаючи на ці перешкоди, потенціал штучного інтелекту щодо вдосконалення ідентифікації загроз і реагування на них незаперечний, пропонуючи більш динамічний і автоматизований підхід до кібербезпеки.

Водночас зростаюче занепокоєння викликає зростання кількості кібератак із підтримкою ШІ. Зловмисники використовують технології штучного інтелекту для створення складних фішингових кампаній і кампаній зловмисного програмного забезпечення, які дедалі важче виявити та протидіяти. Ці атаки часто використовують поточні події та тактику соціальної інженерії для маніпулювання жертвами. Ця стратегія довела ефективність в епоху віддаленої роботи та цифрового зв'язку.

Двосічний меч штучного інтелекту в кібербезпеці

Подвійне використання штучного інтелекту в кібербезпеці підкреслює критичний парадокс: оскільки технології штучного інтелекту стають все більш складними та невід'ємними для операцій безпеки, вони також пропонують зловмисникам потужні інструменти для розробки більш складних і оманливих атак. Ця реальність вимагає ретельного балансу при розгортанні ШІ, гарантуючи, що його переваги у виявленні загроз і реагуванні на них не будуть затьмарені вразливими місцями, які він створює.

Погляд у майбутнє: орієнтування в ландшафті кібербезпеки на основі ШІ

По мірі просування вперед роль штучного інтелекту в кібербезпеці, безсумнівно, продовжуватиме розвиватися, що керуватиметься як технологічним прогресом, так і зміною природи кіберзагроз. Постійна розробка інструментів штучного інтелекту пропонує багатообіцяючі шляхи для покращення заходів безпеки, зокрема у сферах виявлення загроз та реагування на них. Проте зростаюча

складність кібератак із підтримкою штучного інтелекту підкреслює необхідність пильності, постійних інновацій і тонкого розуміння можливостей і обмежень штучного інтелекту в кібербезпеці.

Розширення ролі штучного інтелекту в кібератаках і захисті є свідченням трансформаційного потенціалу технології в епоху цифрових технологій. Оскільки ландшафт кібербезпеки продовжує розвиватися, взаємодія між можливостями штучного інтелекту та проблемами залишатиметься критичною сферою уваги як для професіоналів, так і для організацій, що підкреслює необхідність стратегічних, обґрунтованих підходів до використання штучного інтелекту в поточній боротьбі з кіберзагрозами». ***(Brandon Martin. The Role of AI in Cybersecurity and Cyber Attacks: An Evolving Landscape // Inferse.com (https://www.inferse.com/855063/the-role-of-ai-in-cybersecurity-and-cyber-attacks-an-evolving-landscape/). 19.03.2024).***

***

«В епоху, позначену невпинними інноваціями, автомобільна промисловість переживає зміну парадигми, вирушаючи на незвідані території підключення та програмно-визначених функцій. Поява хмарних додатків започаткувала нову еру управління транспортними засобами, обіцяючи користувачам неперевершену зручність і ефективність роботи. Однак, коли галузь приймає цю трансформацію, вона стикається з гострою проблемою – необхідністю захистити транспортні засоби від наростаючої хвилі загроз кібербезпеці.

Революція в управлінні автомобілями за допомогою хмарних додатків

Основною особливістю цієї автомобільної революції є безперебійне підключення, яке дозволяє користувачам дистанційно керувати функціями автомобіля за допомогою хмарних програм на своїх смартфонах. Це включає в себе можливість завести автомобіль, відімкнути його двері або навіть встановити температуру в салоні за допомогою кількох дотиків на мобільному пристрої. Це стрибок у зручності, який переосмислює спосіб взаємодії користувачів зі своїми транспортними засобами та покращує загальний досвід.

Цей зв’язок, який сприяють API, є двосічним мечем. З одного боку, це надає користувачам безпрецедентний контроль і гнучкість. З іншого боку, це відкриває головоломку вразливостей кібербезпеки, оскільки великі дані, створені за допомогою програмних функцій автомобіля, зберігаються в хмарному озері даних.

Дилема даних: баланс між інноваціями та кібербезпекою

У міру того, як транспортні засоби стають все більш програмно визначеними, галузь отримує переваги від збільшення модульності та масштабованості. Діагностика транспортних засобів і прогнозне технічне обслуговування, які колись виконувалися вручну, тепер бездоганно інтегровані в цифрову сферу. Однак цей перехід викликає занепокоєння щодо безпеки даних, створених і збережених у хмарі.

Завдяки величезному сховищу інформації – від показників продуктивності автомобіля до налаштувань користувачів – це також несе з собою потенціал для кібератак. Саме підключення, яке покращує взаємодію з користувачем, стає вразливим місцем, вимагаючи від галузі досягнення тонкого балансу між інноваціями та кібербезпекою.

Визначені програмним забезпеченням переваги та вразливості

Привабливість програмно-визначених функцій автомобіля полягає в їх адаптованості до вподобань користувача та розвитку автомобільного ландшафту, представляючи технологічне диво, яке підвищує ефективність роботи. Однак ця зручність також створює значні ризики, починаючи від викрадення транспортного засобу і закінчуючи несанкціонованим керуванням, прикладом чого є реальна загроза дистанційного керування під час руху. Поле битви за підключені автомобілі є свідками битви за кібербезпеку, де хакери атакують внутрішні мережі та поступово захоплюють електронні блоки керування (ECU). Цей ризик виходить за межі порушення конфіденційності даних водія, створює загрозу життю та смерті безпеці підключених автомобілів і ускладнює шлях галузі до автономних транспортних засобів. Оскільки поточна архітектура автомобіля надає перевагу практичним з’єднанням, а не безпеці, можливі порушення можуть надати хакерам

доступ до життєво важливих систем, загрожуючи безпеці водія та серйозним наслідкам для галузі.

Вирішення проблем безпеки в підключених автомобілях вимагає багатогранного підходу, який охоплює такі проблеми, як обробка конфіденційних даних, пом'якшення ризиків у бездротовому зв'язку, визначення пріоритетів розробки безпечного програмного забезпечення та посилення контролю доступу. Подолання цих складнощів має вирішальне значення для забезпечення цілісності та безпеки всієї автомобільної екосистеми.

Регулювання завтрашнього дня: вимога до суворих стандартів кібербезпеки

Враховуючи серйозність ситуації, для автомобільної промисловості вкрай необхідно активно вирішувати проблеми кібербезпеки. Для виробників оригінального обладнання (OEM) процес вибору та інтеграції рішень кібербезпеки для кожної підсистеми автомобіля вимагає комплексного підходу. Це передбачає оцінку прийнятних профілів ризику та виявлення вразливостей з точки зору клієнтів, компанії та регуляторних органів. Розуміння кіберризиків виявляє прогалини в організаційних процесах і можливостях, зокрема щодо стійкості продукту. Процес прийняття рішень зважує потенційні рішення з такими факторами, як вартість, час виходу на ринок, досвід користувача та інновації. Формулювання стратегії впровадження включає розробку дорожніх карт, придбання можливостей і управління відносинами із зацікавленими сторонами. Ця цілісна методологія гарантує, що OEM-виробники орієнтуються в складному ландшафті кібербезпеки, захищаючи транспортні засоби від нових загроз, узгоджуючи їх із ширшими бізнес-цілями.

З точки зору уряду, необхідність ухвалення нормативних актів, що встановлюють суворі стандарти кібербезпеки, має вирішальне значення для того, щоб OEM-виробники, виробники автомобілів і постачальники послуг у межах підключеної екосистеми транспортних засобів дотримувалися надійних заходів безпеки. Нещодавно уряд Індії зобов'язало автовиробників впроваджувати систему управління кібербезпекою як у пасажирських, так і в вантажних перевізниках, щоб убезпечити транспортні засоби від потенційних кібератак. Акцент на вдосконаленні

цих правил кібербезпеки підкреслює колективне зобов'язання захистити динамічний ландшафт підключених транспортних технологій. У міру того, як галузь рухається в майбутнє, зацікавлені сторони повинні приймати та впроваджувати стандарти кібербезпеки, які зменшують ризики, пов'язані з цією технологічною метаморфозою.

У двох словах, автомобільна промисловість стоїть на роздоріжжі, балансуючи між обіцянками інновацій та необхідністю кібербезпеки. Перехід до хмарних додатків і програмно-визначених функцій віщує нову еру в управлінні автомобілями, але вимагає пильного підходу до захисту даних і функцій, які визначають наше пов'язане майбутнє. Галузеві експерти повинні відстоювати заходи кібербезпеки, щоб гарантувати, що рух у майбутнє буде не просто плавним, але й безпечним для всіх зацікавлених сторін». ***(Driving the future: Automotive cybersecurity in the era of connected vehicles // The Indian Express [P] Ltd. (https://www.financialexpress.com/business/express-mobility/driving-the-future-automotive-cybersecurity-in-the-era-of-connected-vehicles/3434859/). 24.03.2024).***

***

«У цифровому середовищі, яке швидко розвивається, де звичайні механізми кіберзахисту не витримують складних загроз, стратегії на основі ШІ започаткували нову еру стійкості кібербезпеки. Ініціатором цієї трансформаційної подорожі є Томер Вайнгартен, далекоглядний засновник і генеральний директор SentinelOne, чия новаторська робота змінила галузеві стандарти.

Революція в кібербезпеці завдяки інтеграції ШІ

Усвідомлюючи неадекватність традиційних методів виявлення динамічних шкідливих програм і багатоваріантних атак, Вайнгартен розпочав місію з розробки системи, здатної завчасно запобігати кіберзагрозам, а не просто реагувати на них. Це призвело до заснування SentinelOne, компанії, яка глибоко вкорінена у використанні штучного інтелекту та технологій машинного навчання для революції в кібербезпеці.

Відданість SentinelOne інтеграції штучного інтелекту з нуля виділяє її серед конкурентів, позиціонуючи компанію як першопроходця. Віддаючи пріоритет проактивним, прогностичним моделям безпеки надміру реактивним заходам, SentinelOne уособлює зміну парадигми у філософії кібербезпеки. Концепція поведінкових алгоритмів ШІ, здатних автономно оцінювати діяльність машини в режимі реального часу, втілює цей новий підхід.

Розширене виявлення та реагування (XDR) як свідчення інтеграції

Прикладом переходу галузі до більш інтегрованого, цілісного підходу до безпеки є поява розширеного виявлення та реагування (XDR). Об'єднуючи дані з різних джерел в уніфіковану платформу, XDR пропонує панорамне уявлення про загрози, уможливлюючи попереджувальне пом'якшення вразливості. Це означає відхід від ізольованих, реактивних заходів до єдиної, проактивної стратегії безпеки.

Стів Макдауелл, головний аналітик і генеральний директор NAND Research, підкреслив Стів Макдауелл, що орієнтований на клієнта платформний підхід до корпоративної кібербезпеки. Цей зручний підхід підкреслює прагнення SentinelOne надавати комплексні рішення безпеки, адаптовані до сучасних викликів кібербезпеки.

Незважаючи на трансформаційний потенціал штучного інтелекту в кібербезпеці, проблеми залишаються. Обмеження сучасних технологій штучного інтелекту, складність визначення кіберзлочинів і регуляторні наслідки вимагають постійного діалогу та інновацій. Акцент SentinelOne на розробці потужного й автономного захисту відображає глибоке розуміння ландшафту загроз, що розвивається.

Навігація в майбутньому кібербезпеки

Оскільки інтеграція штучного інтелекту продовжує змінювати ландшафт кібербезпеки, галузь має бути пильною, адаптуючись до нових загроз. Робота таких візіонерів, як Томер Вайнгартен, слугує дороговказом, спрямовуючи галузь у майбутнє, де загрози передбачувані та нейтралізовані завчасно». ***(Benson Mawira. From Reactive to Proactive: The Evolution of Cybersecurity // Microsoft***

(https://www.msn.com/en-us/news/technology/from-reactive-to-proactive-the-evolution-of-cybersecurity/ar-BB1kiNA3). 21.03.2024).

***

Кіберзлочинність та кібертероризм

«Національні державні групи кіберзагроз знову звертаються до USB, щоб скомпрометувати суворо охоронювані урядові організації та об'єкти критичної інфраструктури.

Вийшовши з моди на деякий час і, звичайно, не сприяючи блокуванням через COVID, USB знову доводить ефективний спосіб для високорівневих загроз фізично обходити безпеку в особливо чутливих організаціях.

У основній доповіді цього тижня на CPX 2024 у Лас-Вегасі Майя Горовіц, віце-президент із досліджень у Check Point, зазначила, що USB є основним вектором зараження принаймні трьох різних основних груп загроз у 2023 році: китайського Camaro Dragon (він же Mustang Panda)., Бронзовий Президент, Прета Землі, Світлая моль, Червона Дельта, Величний Телець); Російський Gamaredon (він же Primitive Bear, UNC530, ACTINIUM, Shuckworm, UAC-0010, Aqua Blizzard) і загрозливі актори за Raspberry Robin.

«Протягом багатьох років ми нічого не чули про USB — усе це були кібератаки через Інтернет», — розповідає Горовіц Dark Reading. «Але зазвичай існують моди з акторами-загрозами — одна атака є успішною, тому інші копіюють її. Я думаю, що це те, що ми починаємо бачити з USB-накопичувачами, відновлюючи цей вектор атаки».

Відродження загрози USB

Як часто ви відчиняли двері, бачили на вітальному килимку пакунок Amazon і забували, що насправді замовляли два дні тому?

«Нещодавно ми працювали з енергетичною компанією, де один із співробітників отримав коробку Amazon із стрічкою Amazon», — згадав Деніел Вайлі, керівник відділу управління загрозами Check Point, у пресі в середу.

«Всередині був запечатаний USB-накопичувач SanDisk — абсолютно новий. Він думав, що його замовила його дружина. Тож він відкрив його, підключив. Усе інше було ланцюговою реакцією. Він зміг зламати їхній VPN. Скажімо так. енергетична компанія була не в хорошому місці».

Те, що це був співробітник енергетичної компанії, не було випадковістю — критична галузь часто розділяє IT-мережі від OT-мереж повітряними проміжками або односпрямованими шлюзами, через які не можуть проходити атаки через Інтернет. USB є мостом через цю прогалину, як Stuxnet продемонстрував більше десяти років тому.

USB-атаки також можуть бути корисними без цього обмеження повітряного зазору. Розглянемо працівника британської лікарні, який нещодавно відвідав конференцію в Азії. Під час конференції він поділився своєю презентацією з іншими учасниками через USB-накопичувач. На жаль, один із його колег був заражений шкідливим програмним забезпеченням Camaro Dragon, яке потім спіймав працівник лікарні та привіз із собою до Великобританії, заразивши всю корпоративну мережу лікарні.

Як згадувала Горовіц у своїй доповіді, зловмисне програмне забезпечення відкрило бекдор до щойно заражених машин, але також діяло як хробак, передаючи дані на будь-які нові пристрої, які контактували через USB. Це дозволило йому поширитися за межі Західної Європи в такі країни, як Індія, М’янма, Росія та Південна Корея.

Raspberry Robin поширюється приблизно таким же шляхом, надаючи можливість розповсюджувати програми-вимагачі по всьому світу. USB-модеми Gamaredon доставили черв’яка LitterDrifter до таких різноманітних країн, як Чилі, Німеччина, Польща, Південна Корея, Україна, США та В’єтнам.

Що робити з цими надокучливими USB

Існують прості кроки, які організації можуть вжити, щоб захиститися від більшості загроз, пов’язаних з USB, як-от завжди відокремлювати особисті та робочі пристрої та дбайливіше ставитися до останніх.

«Деякі організації сканують лише файли, завантажені з Інтернету», - сказав Горовіц. «Це неправильно, тому що або особи, які загрожують, або співробітники, які хочуть завдати шкоди, можуть мати свій власний USB-накопичувач, щоб обійти цей захист, збережений для файлів, які завантажуються з Інтернету».

Галузі критичної інфраструктури повинні піти далі: каналізаційні станції, сувора політика щодо знімних пристроїв і плівка через USB-порт можуть зробити трюк у крайньому випадку.

Для організацій, які не хочуть — або не можуть собі дозволити — відмовлятися від знімних носіїв, «Принесіть свій власний пристрій (BYOD) — це добре, ви можете це зробити, але це означає, що вам потрібно більше рівнів безпеки», Горовіц розповідає Dark Reading.

І найголовніше: «Перевірте свої замовлення на Amazon, перш ніж їх відкривати», — іронізував Вайлі». ***(Nate Nelson. 'The Weirdest Trend in Cybersecurity': Nation-States Returning to USBs // Informa PLC (https://www.darkreading.com/ics-ot-security/weirdest-trend-cybersecurity-nation-states-usb?utm_source=flipboard&utm_content=dnic2013%2Fmagazine%2FIn+The+News). 07.03.2024).***

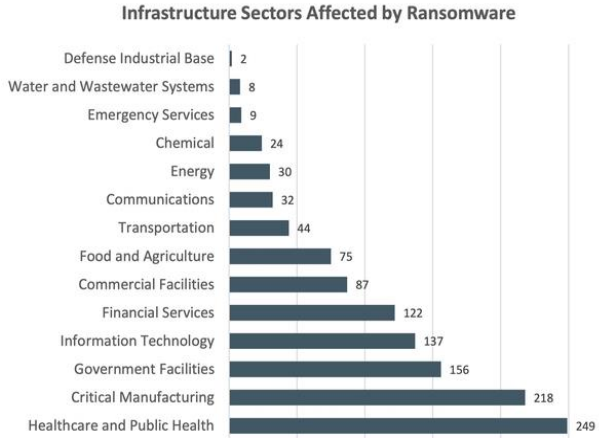
***

«…Щойно був опублікований останній щорічний звіт Центру скарг на інтернет-злочинність ФБР (IC3), і він викликає похмурі асоціації.

Згідно зі звітом IC3, онлайн-шахрайство досягло рекордних збитків у 2023 році: американська громадськість повідомила про 12,5 мільярдів доларів США, що на 22% більше, ніж роком раніше. Однак це враховує лише злочини, про які було повідомлено ФБР. Справжня цифра, швидше за все, буде набагато, набагато вищою.

…кількість зареєстрованих вторгнень програм-вимагачів зросла на 18% до 2825 (приблизно 8 на день), а заявлені збитки зросли на 74% до 59,6 мільйонів доларів США.

У статистику IC3 включено 1193 скарги від організацій критичної інфраструктури, причому найбільше постраждали охорона здоров'я та громадське здоров'я.



Як повідомляв IC3, п'ятьма найпопулярнішими варіантами програм-вимагачів у 2023 році були LockBit, ALPHV/BlackCat, Akira, Royal і Black Basta.

Нещодавні дії правоохоронних органів могли порушити роботу деяких груп програм-вимагачів, але ймовірно, що на їхнє місце прийдуть інші угруповання кіберзлочинців.

Тисячі людей також стали жертвами шахрайства, коли шахрай вдавав, що працює в службі підтримки клієнтів або державній установі, зазвичай націлюючись на людей похилого віку та викрадаючи понад 1,3 мільярда доларів США.

IC3 каже, що 40% отриманих скарг на цей тип шахрайства надходять від осіб старше 60 років, що становить понад 700 мільйонів доларів США збитків. Деякі жертви опинилися без грошей після того, як втратили свої заощадження.

	Complaints	Losses	Trend
Government Impersonation	14,190	$394,050,518	▲63%
Tech and Customer Support	37,560	$924,512,658	▲15%
TOTAL	51,750	$1,318,563,176	

Звіт показує, що через шахрайство з інвестиціями втрачається більше грошей, ніж будь-яка інша категорія кіберзлочинів.

У період з 2022 по 2023 рік інвестиційне шахрайство зросло на 38% з 3,3 мільярда доларів США до 4,57 мільярда доларів США, що робить його причиною

більших зареєстрованих збитків, ніж компрометація бізнес-електронної пошти, програми-вимагачі або шахрайство з технічною підтримкою.

By Complaint Loss			
Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

З шахрайства з інвестиціями на суму 4,57 мільярда доларів США приголомшливі 3,94 мільярда доларів пов’язані з криптовалютою (зростання з 2,57 мільярда доларів у 2022 році).

Ця наростаюча хвиля шахрайства з криптовалютою відбувається, незважаючи на попередження ФБР щодо методів, які використовують злочинці, щоб обманом змусити необережних зробити нерозумні інвестиції…» ***(Graham Cluley. $12.5 billion lost to cybercrime, amid tidal wave of crypto investment fraud // Fortra, LLC (https://www.tripwire.com/state-of-security/125-billion-lost-cybercrime-amid-tidal-wave-crypto-investment-fraud?utm_source=flipboard&utm_content=other). 07.03.2024).***

***

«Було виявлено зловмисників, які зловживали платформою гіпервізора з відкритим кодом QEMU як інструментом тунелювання під час кібератаки на велику компанію.

QEMU — це безкоштовний емулятор і гіпервізор, який дозволяє запускати інші операційні системи на комп’ютері як гостьові.

У рамках атаки зловмисники використовували QEMU для створення віртуальних мережевих інтерфейсів і мережевого пристрою сокетного типу для підключення до віддаленого сервера. Це дозволило зловмисникам створити

мережевий тунель від системи жертви до сервера зловмисника з незначним впливом на продуктивність системи.

Цей незвичайний випадок, який підкреслює різноманітні методи, які зловмисники використовують, щоб залишатися непомітними, виявили аналітики Касперського, які були викликані для розслідування підозрілої активності в системах зламаної компанії.

Приховані мережеві тунелі

Хакери створюють мережеві тунелі, щоб встановити прихований і безпечний канал зв'язку між ними та скомпрометованою системою.

Як правило, ці тунелі шифрують мережевий трафік, щоб допомогти обійти брандмауери, системи виявлення вторгнень та інші заходи безпеки.

Kaspersky каже, що в 10% випадків, які він розслідував за останні три роки, хакери використовували утиліти FRP і ngrok для створення тунелів. Інші інструменти тунелювання, які використовуються в атаках, включають тунелі CloudFlare, Stowaway, ligolo, 3proxy, dog-tunnel, chisel, gs-netcat, plink, iox і nps.

Через те, що кіберзлочинці часто зловживають ними, захисники та засоби моніторингу ставляться до них з підозрою.

У цьому незвичайному випадку, пов'язаному з QEMU, зловмисники вирішили використати менш звичайний інструмент для створення мережевих тунелів, які навряд чи викликатимуть тривогу, навіть якщо це означатиме відмову від шифрування трафіку.

Крім того, QEMU пропонує унікальні можливості, такі як емуляція широкого спектру апаратного забезпечення та віртуальних мереж, дозволяючи зловмисним діям поєднуватися з безпечним трафіком віртуалізації та з'єднуючи сегментовані частини мережі через стратегічно налаштовані опорні точки віртуальної машини.

Легкий бекдор

Під час атаки, яку побачив Kaspersky, хакери використовували «Angry IP Scanner» для сканування мережі, «mimikatz» для крадіжки облікових даних і QEMU для створення складної настройки мережевого тунелювання, яка сприяла прихованому каналу зв'язку.

Зловмисники намагалися мінімізувати свій слід, виділивши створеній ними віртуальній машині лише 1 МБ оперативної пам’яті, що значно зменшило ймовірність виявлення через споживання ресурсів.

Конфігурація віртуальної машини, яка була запущена без використання LiveCD або образу диска, містить такі аргументи:

-netdev user,id=lan,restrict=off: налаштовує серверну мережу під назвою «lan» у режимі користувача, дозволяючи необмежений доступ до мережі через мережевий стек хоста.

-netdev socket,id=sock,connect=<IP>:443: встановлює з’єднання через сокет із вказаною IP-адресою на порту 443, створюючи пряме мережеве з’єднання для серверного «sock».

-netdev hubport,id=port-lan,hubid=0,netdev=lan/sock: З’єднує мережевий пристрій (LAN або Sock) із віртуальним концентратором hubid=0, полегшуючи мережеве з’єднання між різними серверними модулями.

-nographic: запускає QEMU без графічного інтерфейсу, вибираючи лише взаємодію з командним рядком, зменшуючи його видимість і обсяг ресурсів.

Kaspersky провів імітаційні тести, щоб відтворити специфічне використання QEMU зловмисниками, дійшовши висновку, що налаштування виглядало так, як на діаграмі нижче.

Використовуючи QEMU, зловмисники встановили мережевий тунель від цільового внутрішнього хоста, який не мав доступу до Інтернету, до основного хосту з доступом до Інтернету, який, у свою чергу, підключається до сервера зловмисника в хмарі, де працює віртуальна машина Kali Linux.

Здатність віртуальних машин QEMU безперебійно з’єднуватися та об’єднувати сегментовані мережеві компоненти є ключовою в обході заходів безпеки, а також може використовуватися для посилення зламу збоку.

Kaspersky каже, що підприємству слід запровадити багаторівневий захист для виявлення використання законних інструментів, подібних до цього, включаючи цілодобовий моніторинг мережі, який може бути поза ціною для багатьох малих підприємств.

«Це додатково підтримує концепцію багаторівневого захисту, яка охоплює як надійний захист кінцевих точок, так і спеціалізовані рішення для виявлення та захисту від складних і цілеспрямованих атак, у тому числі атак, керованих людиною», — підсумував Касперський.

«Лише комплексна безпека, яка включає цілодобовий моніторинг мережі (NDR, NGFW) і кінцевих точок (EDR, EPP), зокрема експертами SOC, може вчасно виявити аномалії та заблокувати атаку на початковій стадії». ***(Bill Toulas. Hackers abuse QEMU to covertly tunnel network traffic in cyberattacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-abuse-qemu-to-covertly-tunnel-network-traffic-in-cyberattacks/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 05.03.2024).***

***

«Поширення програмованих логічних контролерів (PLC) із вбудованими в них веб-серверами дало зловмисникам можливість запускати потенційно катастрофічні дистанційні атаки на оперативні технології (OT) для промислових систем управління (ICS) у секторах критичної інфраструктури.

Щоб висвітлити загрозу, група дослідників з Технологічного інституту Джорджії розробила зловмисне програмне забезпечення, яке зловмисник може використовувати для віддаленого доступу до вбудованого веб-сервера в PLC і атакувати базову фізичну систему. За словами дослідників, зловмисник може використовувати зловмисне програмне забезпечення для маніпулювання вихідними сигналами для приводів, фальсифікації показань датчиків, відключення систем безпеки та виконання інших дій, які можуть викликати потенційно руйнівні наслідки, включаючи навіть втрату життя.

PLC — це компоненти ICS, які контролюють роботу фізичних процесів і обладнання в різних виробничих, промислових і критичних налаштуваннях інфраструктури. PLC отримує вхідні дані від різних підключених датчиків та інших джерел вхідних даних і використовує дані для надсилання команд фізичним

системам на основі попередньо запрограмованої керованої логіки. Мета зловмисного програмного забезпечення PLC загалом полягає в тому, щоб вплинути на вихідні дані таким чином, щоб порушити або саботувати фізичний процес, яким може керувати PLC.

Зловмисне програмне забезпечення для PLC, схоже на Stuxnet

Часто зловмисне програмне забезпечення, націлене на PLC та системи ICS, вимагало від зловмисників певного попереднього фізичного або мережевого доступу до цільового середовища, і часто було специфічним для платформи та легко видалялося за допомогою відновлення заводських налаштувань. У статті дослідники Georgia Tech Раян Пікрен, Тохід Шекарі, Саман Зонуз і Рахім Бейя описали своє веб-зловмисне програмне забезпечення PLC як принципово інше.

Більшість шкідливих програм для PLC зазвичай заражають мікропрограму або логіку управління контролерів, тоді як нове веб-шкідливе програмне забезпечення атакує інтерфейсний веб-рівень PLC за допомогою шкідливого JavaScript, усуваючи деякі обмеження, з якими такий шкідливий код стикався в минулому.

«Цей підхід має значні переваги над існуючими методами шкідливих програм для PLC (логіка управління і мікропрограми), такі як незалежність від платформи, простота розгортання і більш високий рівень стійкості», - зазначають дослідники.

Але результати кібератаки нового штаму такі ж самі, як і в інших успішних атаках на PLC. Наприклад, у кампанії Stuxnet вартістю 1 мільярд доларів, яку дехто приписує урядам США та Ізраїлю, зловмисники націлилися на PLC Siemens, щоб змусити високошвидкісні центрифуги на іранському заводі зі збагачення урану в Натанзі обертатися так швидко, що вони, по суті, розірвали себе на частини.

З того часу було здійснено ще кілька атак, які продемонстрували, якої шкоди можуть завдати зловмисники системам, що контролюють фізичні процеси. Яскравими прикладами є шкідливе програмне забезпечення BlackEnergy, яке російські зловмисники використали для виведення з ладу української енергосистеми в 2016 році; атака Triton/Trisis на систему безпеки Schneider на нафтохімічному заводі в Саудівській Аравії; а також INCONTROLLER - набір

інструментів шкідливого програмного забезпечення, націленого на PLC від Schneider і Omron.

Кібератака PoC: простіше в розгортанні та більш стійка

Веб-атака, яку розробили дослідники, в основному включала тестовий сценарій, у якому загрозливий суб'єкт виконує атаку, подібну до Stuxnet, на широко використовуваний PLC, який у цьому випадку керував промисловим двигуном, подібним до двигуна, який використовується для живлення центрифуг під час збагачення урану. Як і багато сучасних PLC, той, який дослідники використовували для дослідника, мав веб-інтерфейс для віддаленого моніторингу, програмування та налаштування.

Для тестового сценарію дослідники припустили, що об'єкт, де розташований PLC, мав інженерні робочі станції, підключені як до бізнес-мережі, так і до промислової мережі. Дослідники також припустили, що зловмисник мав певні базові знання про фізичний процес, яким керував тестовий PLC, і деякі інші неспецифічні деталі середовища.

У своїй статті дослідники описали, як зловмисник може отримати початковий доступ до PLC, віддалено впровадивши шкідливий код на веб-сервер різними способами, а потім використавши його законні інтерфейси прикладного програмування (API), щоб порушити роботу основного механізму. Один із тестових сценаріїв передбачав, що зловмисник обманним шляхом змушує оператора ICS відвідати шкідливу веб-сторінку, яка автоматично завантажує зловмисне програмне забезпечення PLC у веб-додаток PLC, об'єднуючи три окремі вразливості нульового дня, які дослідники виявили у веб-додатку.

Серед іншого, розроблене дослідниками зловмисне програмне забезпечення для PLC на базі Інтернету (WB PLC) могло б дозволити зловмиснику фізично пошкодити промисловий двигун, яким він керував, зловживати налаштуваннями адміністратора для подальшої компрометації та викрасти дані з метою промислового шпигунства.

«Наше зловмисне програмне забезпечення для веб- PLC знаходиться в пам'яті PLC, але в кінцевому підсумку виконується на стороні клієнта різними

пристроями, оснащеними браузером, у всьому середовищі ICS», — зазначили дослідники. «Звідси зловмисне програмне забезпечення використовує облікові дані на основі навколишнього браузера для взаємодії з законними веб-інтерфейсами API PLC для атаки на базову машину реального світу». За їхніми словами, цей тип шкідливого програмного забезпечення легше розгортати, і він здебільшого не залежить від платформи». ***(Jai Vijayan. Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure // Informa PLC (https://www.darkreading.com/ics-ot-security/improved-stuxnet-like-plc-malware-disrupt-critical-infrastructure?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FFLIPBOARD%0AMAGAZINE+OF%0AA.+NISHIHARA). 05.03.2024).***

***

«Орган, відповідальний за реєстрацію та захист прав бізнесу в Південній Африці, Комісія з компаній та інтелектуальної власності (CIPC), яка підпорядковується Міністерству торгівлі, промисловості та конкуренції, зазнав кібератаки.

У заяві для ЗМІ, опублікованій 29 лютого, CIPC заявив, що помітив, що її база даних зазнала «спроби» порушення безпеки, націленої на особисту інформацію її клієнтів і співробітників. Однак у реєстрі не повідомляється, скільки інформації було скомпрометовано.

«Через потужні брандмауери та системи захисту даних у CIPC наші спеціалісти з ІКТ були попереджені про можливу компрометацію безпеки, і в результаті певні системи CIPC були негайно вимкнені, щоб зменшити будь-який можливий збиток», — йдеться в повідомленні. йдеться в комюніке.

Створений у 2008 році CIPC аналізує мільйони південноафриканських компаній, як приватних, державних, так і закритих установ. Окрім реєстрації фірм і контролю за дотриманням вітчизняними організаціями законодавства про компанії та інтелектуальну власність, агентство існує, щоб полегшити ведення бізнесу.

Хоча комісія не повідомляє, чому сталася кібератака або хто несе відповідальність, вочевидь, ситуацію не вдалося запобігти достатньо рано, щоб запобігти розкриттю даних.

Імена, адреси та контактні номери директорів/власників підприємств, а також власників патентів і торгових марок залишаються на відкритому повітрі.

«На жаль, до певної особистої інформації наших клієнтів і співробітників CIPC було незаконно отримано доступ і було розкрито. Клієнтів CIPC закликають бути пильними під час моніторингу транзакцій кредитних карток і ЛИШЕ схвалювати/авторизувати відомі та дійсні запити на транзакції. Ступінь викриття залежить розслідується і буде повідомлено якнайшвидше", - йдеться в повідомленні.

«CIPC визнає важливість стабільної доступності наших систем і захисту інформації, яка не є загальнодоступним, і активно працює над мінімізацією впливу на клієнтів і співробітників CIPC», — вважають у CIPC.

Це вже вкотре уряд піддається кібернаступу. Минулого року Міністерство оборони, парламент провінції Західна Капська провінція (WCPP), Рада наукових і промислових досліджень і навіть президент Сиріл Рамафоса були причетні до подібних злому.

З появою пандемії коронавірусу на Півдні спостерігається зростання кіберзлочинності. Країна Африки, яка є найбільш цільовою атакою, за останні кілька років більше половини її місцевих підприємств постраждали від програм-вимагачів». ***(Andrew Christian. Hackers infiltrate South Africa's business registry // Benjamindada.com (https://www.benjamindada.com/south-africa-cipc-hacked/). 02.03.2024).***

***

«Національний центр кібербезпеки (NCSC) взяв на себе відповідальність за управління інцидентами у Федеральній адміністрації після хакерської атаки на Xplain, основного постачальника IT-послуг для національних і кантональних органів влади. Частина його діяльності включала аналіз даних, які

зловмисники публікували в даркнеті. Сьогодні NCSC опублікував звіт, в якому пояснює свій аналіз і надає інформацію про те, які типи даних зазнали впливу, і проблеми, пов'язані з аналізом даних. У звіті не оцінюється зміст даних і не аналізується, чому стався витік певних даних. Останнє питання буде з'ясовано в рамках адміністративного розслідування, яке триває.

У рамках атаки програм-вимагачів на Xplain хакерська група, відома як Play, викрала дані та опублікувала в даркнеті те, що, імовірно, було повним пакетом даних. Це включало секретну інформацію та конфіденційні особисті дані Федеральної адміністрації. Національний центр кібербезпеки (NCSC) очолив реагування на інцидент, визначив заходи для відновлення безпеки систем і провів комплексний аналіз опублікованих даних.

Зараз NCSC публікує звіт про процедуру та результати аналізу даних у рамках процесу управління інцидентом і забезпечення максимальної прозорості. Мета полягає в тому, щоб надати огляд типів даних, на які це впливає, і окреслити проблеми, пов'язані з аналізом даних.

Релевантність опублікованого обсягу даних

Пакет даних, опублікований у даркнеті, складався з близько 1,3 мільйона файлів. Після того, як дані були завантажені, NCSC взяв на себе ініціативу в систематичній категоризації та сортуванні всіх документів, що стосуються Федеральної адміністрації. Результати показали, що обсяг даних, які мають відношення до Федеральної адміністрації, склав близько 65 000 документів, або приблизно 5% від загального опублікованого набору даних. Більшість цих файлів належала Xplain (47 413) із часткою понад 70%; близько 14% (9040) належали до Федеральної адміністрації. Близько 95% файлів Федеральної адміністрації належали адміністративним підрозділам Федерального департаменту юстиції та поліції (FDJP): Федеральному відомству юстиції, Федеральному відомству поліції, Державному секретаріату з питань міграції та внутрішньому центру IT-сервісу ISC-FDJP. Маючи трохи більше 3% даних, Федеральний департамент оборони, цивільного захисту та спорту (DDPS) постраждав незначно, а інші департаменти лише незначно постраждали з точки зору обсягу.

Частка конфіденційних даних

Делікатний вміст, такий як особисті дані, технічна інформація, секретна інформація та паролі, було знайдено приблизно в половині файлів Федеральної адміністрації (5182). Особисті дані, такі як імена, адреси електронної пошти, номери телефонів і поштові адреси, були знайдені в 4779 з цих файлів. Крім того, 278 файлів містили технічну інформацію, таку як документація про IT-системи, документи з вимогами до програмного забезпечення або архітектурні описи, 121 об'єкт було класифіковано відповідно до Указу про захист інформації, а 4 об'єкти містили читабельні паролі.

Проблеми аналізу

Значний обсяг аналізу був потрібен, щоб визначити, скільки даних витік і власників витоку даних. Потрібні були відповідні інструменти, щоб обробити неструктуровані записи даних і зробити їхній вміст читабельним. Об'єкти, визначені як релевантні, потрібно було вручну переглянути та класифікувати. Різні федеральні відомства та постачальники послуг, які були залучені, тісно співпрацювали під керівництвом NCSC, щоб врегулювати інцидент безпеки. Це дозволило всім сторонам використовувати синергію, ефективно використовувати ресурси та економити дорогоцінний час.

Адміністративне розслідування

28 червня 2023 року Федеральна рада уповноважила сформувати кризову групу політичної стратегії щодо витоків даних (PSC-D) і 23 серпня 2023 року наказала провести адміністративне розслідування, щоб повністю зрозуміти витік даних у Xplain. Адміністративне розслідування має бути завершено до кінця березня 2024 року. Після цього Федеральна рада буде проінформована про результати та рекомендації, щоб вона могла вирішити, як діяти далі». ***(Hacker attack on Xplain: National Cyber Security Centre publishes data analysis report // The Federal Council (https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-100315.html). 07.03.2024).***

***

«Управління інформаційної системи Естонії прогнозує збільшення атак розподіленої відмови в обслуговуванні (DDoS) в Естонії та ширше використання Інтернету речей (IoT) для посилення інтенсивності цих атак.

Під час атаки розподіленої відмови в обслуговуванні (DDoS) служби, розташовані в мережі, перевантажуються вхідним трафіком. Подібна ситуація виникає, наприклад, при поданні податкової декларації онлайн, коли через надмірне навантаження люди не можуть отримати доступ до сайту.

5 березня 163 DDoS-атаки на естонські веб-сайти та служби були спрямовані на інформаційно-комунікаційний сектор. Щодня в Естонії здійснюється в середньому близько десяти DDoS-атак.

За даними Управління інформаційної системи Естонії (RIA), із 163 атак, які сталися 5 березня, 160 були спрямовані на одну телекомунікаційну компанію і можуть розглядатися як один інцидент. У RIA оцінюють, що приводів для занепокоєння немає, оскільки в цьому випадку не було впливу на функціонування сервісів та інформаційних систем.

Остання серйозна кібератака, яка потрапила в ЗМІ, сталася в п'ятницю, коли компанію AS Hansab, що надає рішення для безпеки та обслуговує банкомати, зазнала атаки, і їй довелося відключитися від зовнішньої мережі. За словами генерального директора Крісто Тімберга, вони відносно добре перенесли атаку. «Мережі та сервіси поступово відновлювалися, сервіси продовжувалися, хоча деякі речі доводилося робити інакше та вручну», — сказав Тімберг.

Тімберг зазначив, що раніше в історії компанії були технічні та інші інциденти, але нічого не можна порівняти з тим, що сталося в п'ятницю. «Те, як це сталося сьогодні, також є першим для нас. Але, на щастя, у нас є готові плани відновлення. Ми перевірили наші системи і готові запустити альтернативні рішення та діяти відповідно до наших процедур», — заявив Тімберг.

«Атаки типу «відмова в обслуговуванні» відбуваються постійно, щодня. Наш сектор сьогодні все частіше зазнає атаки, а завтра це може бути інший сектор. А що стосується інформаційно-комунікаційного сектору, то вони цілком звикли до атак і готові до них», — сказав Хендре.

У підсумку минулого року RIA зазначило, що порівняно з 2022 роком DDoS-атаки стали більш цілеспрямованими та краще підготовленими. «Більше уваги приділяється тому, на кого націлюватися і яким технічним способом здійснювати атаки. Зловмисники також зрозуміли, що багато сервісів і сайтів вже запровадили певні захисні заходи. Вони намагаються їх обійти», — зазначив Хендре.

За даними RIA, багато DDoS-атак в останні роки були здійснені ідеологічними хактивістами. Переважно це дружні до Кремля хакери, які DDoS-атаками намагаються покарати країни, які підтримують Україну.

RIA прогнозує, що політично вмотивовані DDoS-атаки триватимуть і цього року. Крім того, підключені до Інтернету домашні пристрої, такі як роботизовані пилососи та камери безпеки, дозволяють зловмисникам підвищувати інтенсивність DDoS-атак.

«Злочинці, так би мовити, заволодіють цілим набором пристроїв і атакують якийсь сервіс чи веб-сайт. Це називається створенням ботнету. Світова тенденція полягає в тому, що пристрої IoT використовуються для кібератак», — сказав Хендре.

У 2023 році RIA зареєструвала 484 значні DDoS-атаки, що на 60 відсотків більше, ніж у 2022 році. З них 139 вражаючих атак, коли веб-сайт або інший сервіс не працював або працював повільніше, ніж зазвичай». ***(Valner Väino, Reene Leas. Watchdog forecasts uptick in cyberattacks in Estonia // Eesti Rahvusringhääling (https://news.err.ee/1609273686/watchdog-forecasts-uptick-in-cyberattacks-in-estonia). 06.03.2024).***

***

«Французький уряд заявив у понеділок, що кілька його сервісів зазнали кібератак «безпрецедентної інтенсивності», і для відновлення онлайн-сервісів був активований спеціальний кризовий центр.

Офіс прем'єр-міністра Габріеля Аттала заявив у заяві, що атаки почалися в неділю ввечері та вразили кілька урядових міністерств, без надання подробиць. До

обіду понеділка, як сказано, «вплив атак було зменшено для більшості сервісів, а доступ до урядових сайтів відновлено».

Відповідальність за атаки на дописи в Інтернеті взяла на себе група хакерів під назвою Anonymous Sudan, яку експерти з кібербезпеки вважають проросійською. Офіс прем'єр-міністра Франції та агентство з цифрової безпеки не коментували цю заяву та не надавали подробиць того, що було ціллю чи якої шкоди могло бути завдано.

Французький чиновник сказав, що це були атаки на відмову в обслуговуванні, поширений тип кібератак, який передбачає заповнення сайту даними з метою його перевантаження та виведення з ладу.

Уряд Франції зробив поштовх до покращення кіберзахисту перед Олімпійськими іграми в Парижі цього літа та після згубних атак програм-вимагачів за останні роки, зокрема на лікарні у 2021 році.

Французький уряд звинуватив Росію в веденні тривалої онлайн-кампанії маніпуляцій проти західних прихильників України, в тому числі шляхом дублювання веб-сайту МЗС Франції серед інших методів. Президент Еммануель Макрон займає дедалі жорсткішу позицію щодо Москви та війни, яку президент Росії Володимир Путін розпочав в Україні». ***(The French Government Says It's Being Targeted by Unusual Intense Cyberattacks // SecurityWeek (https://www.securityweek.com/the-french-government-says-its-being-targeted-by-unusual-intense-cyberattacks/). 11.03.2024).***

***

«…китайські злочинці все частіше тримаються невідомо на загальнодоступних форумах і покладаються на Telegram та інші зашифровані іноземні додатки для обміну повідомленнями, щоб непомітно координувати дії та продавати товари.

Кіберзлочинці, які діють у Китаї з надзвичайною обачністю, не повинні дивувати. З 2018 року Пекін ініціював численні репресії проти кіберзлочинних груп і сайтів, підкріплюючись драконівськими законами, які «створили атмосферу

самоцензури серед великих і незначних операторів веб-сайтів, а також користувачів хакерських форумів і блогів у країні, перешкоджаючи відкритій діяльності кіберзлочинців на платформах», - йдеться у звіті Kela, який вивчає кримінальний ландшафт Китаю.

Китай також намагався ускладнити анонімне використання Інтернету, в тому числі шляхом придушення використання VPN і криптовалюти. Принаймні деякі китайські кіберзлочинні групи, схоже, перемістили свою базу операцій за межі країни.

У порівнянні з російсько- та англомовним кіберзлочинним підпіллям, за словами дослідників, китайська екосистема має набагато менше підпільних форумів, присвячених дискусіям про хакерство або продажу інструментів злому, вкрадених даних чи інших незаконних матеріалів. Форуми, які існують, не мають надто багатослівної бази користувачів, але вони, здається, є прелюдією для спілкування через прямі повідомлення або зашифровану програму чату, йдеться у звіті.

«Дотримуючись свого стриманого підходу, вміст, яким китайськомовні кіберзлочинці діляться на різних платформах, здебільшого зосереджений на послугах і пропозиціях, а не на обговореннях, і часто використовує закодовану мову або загальний огляд замість конкретних пропозицій», — йдеться в документі.

На форумах китайської екосистеми щодо кіберзлочинності також не вистачає ряду типових функцій, таких як «системи чіткої репутації» для оцінки покупців, продавців і товарів, «що вимагає додаткових зусиль у аналізі пропозицій і дослідженні конкретних учасників», – повідомили дослідники Kela Information Security Media Group.

Значна частина цієї діяльності, схоже, відбувається в каналах Telegram, і групи займаються такими речами, як «послуги тестування на проникнення» та продаж викрадених баз даних (китайські та іноземні карткові дані завжди продаються через різні групи), а також відмивання грошей, створення послуги підробленої ідентифікації та обходу, які можуть дозволити користувачам купувати криптовалюту або іноземні SIM-карти. За словами дослідників, це відбувається

паралельно з тим, що спільноти кіберзлочинців по всьому світу постійно використовують Telegram та інші зашифровані програми для чату.

Наскільки цей рівень китайських кіберзлочинців, що використовують ці форуми та інструменти обміну повідомленнями, може допомогти державі, кажуть експерти, залишається незрозумілим, хоча, здається, між спільнотами існує певний ступінь перехресності. «Розмита межа між спонсорованими державою суб'єктами, які зазвичай мають на меті шпигунство, та фінансово мотивованими суб'єктами в Китаї дозволяє обмінюватися ресурсами та досвідом між двома групами», — сказав Кела.

Kela сказав, що підтримувані національною державою передові стійкі хакерські групи, ймовірно, «мають широкий доступ як до китайськомовної, так і до ширшої екосистеми кіберзлочинності», що підтверджується використанням ними багатьох тих самих китайських розробників з відкритим вихідним кодом і готових продуктів. інструментів у своїх атаках.

На відміну від тих, кого Пекін міг би класифікувати як «китайських кіберзлочинців», у країні, схоже, також є процвітаючий сектор професійних наступальних хакерських операцій, який регулярно допомагає уряду за контрактом. Минулого місяця на GitHub просочилася частина документів — очевидно, отриманих із шанхайської iSoon — показала, як приватна компанія підтримує урядові хакерські операції». ***(Mathew J. Schwartz. Chinese Cybercrime: Discretion Is the Better Part of Valor // Information Security Media Group, Corp. (https://www.databreachtoday.com/chinese-cybercrime-discretion-better-part-valor-a-24592). 13.03.2024).***

***

«Комісія з інформаційних і комунікаційних технологій (ICTC) у Танзанії закликала до узгоджених зусиль для розробки ефективних систем боротьби з кіберзлочинністю в країні.

Генеральний директор ICTC д-р Мкундве Мвасага подзвонив у середу під час розмови з журналістами, назвавши п'ять ключових питань, які комісія збирається

розглянути під час дводенної конференції з кібербезпеки, запланованої на 4-5 квітня 2024 року в Аруші.

У зустрічі візьмуть участь як місцеві, так і міжнародні зацікавлені сторони та експерти з технологій. Прагнучи сприяти інклюзивності, комісія планує спонсорувати відвідування конференції 100 жінок, які працюють у сферах, пов'язаних із технологіями, у Танзанії, у тому числі студенток університетів.

«Оскільки зараз технології відіграють ключову роль у багатьох сферах, таких як освіта, медицина, сільське господарство, платіжні системи, бізнес та багато інших, кіберзахист є найважливішим компонентом, який необхідно розглянути, маючи на увазі, що якщо когось обдурять через Інтернет, вони втрачають довіру до мереж», – зазначив доктор Мвасага.

Він висловив зобов'язання комісії контролювати питання кібербезпеки під час здійснення комплексної цифрової трансформації.

«Ми знаємо, що кібербезпека змінюється, і люди постійно змінюють тактику, тому ми повинні продовжувати вчитися цьому, щоб переконатися, що ситуація покращується», — сказав він.

Він сказав, що питання, які будуть обговорюватися під час запланованої зустрічі, включають розгляд того, як заходи кібербезпеки можуть сприяти підвищенню стійкості економічного сектора. За його словами, для обговорення буде винесено захист кіберпростору в нових технологіях, таких як штучний інтелект, і забезпечення безпечного способу ефективного використання нових технологій.

«Ми знаємо, що деякі державні установи почали використовувати штучний інтелект, тому ми обговоримо аспект кібербезпеки, який включає ці нові технології», — сказав доктор Мвасага.

Крім того, він сказав, що конференція має на меті обговорити належне сприяння безпечному, стійкому та інклюзивному кіберпростору.

За словами Мвасаги, ключовим є підвищення обізнаності звичайних громадян про те, як правильно користуватися мережами. У нас будуть різні

експерти під час зустрічі, і ми отримаємо досвід інших країн», – додав доктор Мвасага.

Д-р Мвасага наголосив на важливості інвестування в цифрову трансформацію для підтримки економічного зростання. Він зазначив, що під час пандемії Covid-19 багато країн зазнали економічного спаду, але лише деяким вдалося відновитися завдяки інвестиціям у цифрову трансформацію.

У успішній цифровій трансформації д-р Мвасага згадав п’ять стовпів, включаючи передачу цифрових навичок усім танзанійцям, забезпечення безпеки для всіх людей, сприяння інклюзивним комунікаційним послугам і сприяння цифровим інноваціям і дослідженням.

Відповідно до щоквартального звіту Управління зв’язку Танзанії (TCRA), опублікованого за грудень минулого року, було зафіксовано 21 788 випадків шахрайства порівняно з 12 603 випадками, зареєстрованими за той самий період у 2022 році». ***(Wilson Malima. ICTC: It’s time to team up against cybercrime // Tanzania Standard Newspapers Limited (https://dailynews.co.tz/ictc-its-time-to-team-up-against-cybercrime/). 15.03.2024).***

***

«Зловмисники перетворили сотні зламаних сайтів із програмним забезпеченням WordPress на командно-контрольні сервери, які змушують браузери відвідувачів виконувати атаки для злому паролів.

Веб-пошук JavaScript, який виконує атаку, показав, що він був розміщений на 708 сайтах на момент публікації цього допису на Ars, порівняно з 500 два дні тому. Денис Синегубко, дослідник, який помітив цю кампанію, сказав тоді, що він бачив тисячі комп’ютерів відвідувачів, на яких запускався сценарій, який змушував їх звертатися до тисяч доменів, намагаючись вгадати паролі імен користувачів з обліковими записами на них.

Відвідувачі мимоволі набираються

«Таким чином тисячі відвідувачів сотень заражених веб-сайтів несвідомо й одночасно намагаються брутфорсувати тисячі інших сторонніх сайтів WordPress»,

— написав Синєгубко. «А оскільки запити надходять із браузерів реальних відвідувачів, ви можете собі уявити, що фільтрувати та блокувати такі запити — це складно».

Подібно до зламаних веб-сайтів, на яких розміщено шкідливий JavaScript, усі цільові домени працюють із системою керування вмістом WordPress. Сценарій — розміром лише 3 кілобіти — звертається до керованого зловмисником getTaskURL, який, у свою чергу, надає ім’я конкретного користувача на певному сайті WordPress разом із 100 типовими паролями. Коли ці дані надходять у браузер, який відвідує зламаний сайт, він намагається увійти в цільовий обліковий запис користувача за допомогою потенційних паролів. JavaScript працює в циклі, запитуючи завдання з getTaskURL, повідомляючи результати на completeTaskURL, а потім виконуючи кроки знову і знову…

Маючи 418 пакетів паролів станом на вівторок, Синегубко дійшов висновку, що зловмисники намагаються ввести 41 800 паролів для кожного цільового сайту.

Синегубко написав:

Етапи атаки та життєвий цикл

Атака складається з п’яти ключових етапів, які дозволяють зловмисникам використовувати вже скомпрометовані веб-сайти для проведення розподілених атак грубої сили проти тисяч інших потенційних сайтів-жертв.

Етап 1: Отримайте URL-адреси сайтів WordPress. Зловмисники або самостійно сканують Інтернет, або використовують різні пошукові системи та бази даних, щоб отримати списки цільових сайтів WordPress.

Етап 2: Витягніть імена користувачів авторів. Потім зловмисники сканують цільові сайти, вилучаючи справжні імена користувачів авторів, які публікують на цих доменах.

Етап 3: ін’єкція шкідливих сценаріїв. Потім зловмисники впроваджують свій сценарій dynamic-linx[.]com/chx.js на веб-сайти, які вони вже зламали.

Етап 4: облікові дані грубої сили. Коли звичайні відвідувачі сайту відкривають заражені веб-сторінки, завантажується шкідливий сценарій. За

лаштунками браузери відвідувачів проводять розподілену атаку грубої сили на тисячі цільових сайтів без будь-якої активної участі зловмисників.

Етап 5: Перевірте скомпрометовані облікові дані. Зловмисники перевіряють облікові дані грубим шляхом і отримують неавторизований доступ до сайтів, націлених на етапі 1.

Отже, як зловмисники насправді здійснюють розподілену атаку грубої сили з браузерів абсолютно невинних і нічого не підозрюючих відвідувачів веб-сайту? Розглянемо етап 4 докладніше.

Кроки розподіленої атаки грубої сили:

Коли відвідувач сайту відкриває заражену веб-сторінку, браузер користувача запитує завдання з URL-адреси hxxps://dynamic-linx[.]com/getTask.php.

Якщо завдання існує, воно аналізує дані та отримує URL-адресу сайту для атаки, а також дійсне ім’я користувача та список із 100 паролів для спроби.

Для кожного пароля в списку браузер відвідувача надсилає запит wp.uploadFile XML-RPC API, щоб завантажити файл із зашифрованими обліковими даними, які використовувалися для автентифікації цього конкретного запиту. Це 100 запитів API для кожного завдання! Якщо автентифікація проходить успішно, у каталозі завантажень WordPress створюється невеликий текстовий файл із дійсними обліковими даними.

Коли всі паролі перевірено, сценарій надсилає сповіщення на hxxps://dynamic-linx[.]com/completeTask.php про те, що завдання з певним taskId (ймовірно, унікальний сайт) і checkId (пароль) було виконано.

Нарешті, сценарій запитує наступне завдання та обробляє новий пакет паролів. І так до нескінченності, поки відкрита заражена сторінка.

Станом на вівторок дослідник спостерігав «десятки тисяч запитів» до тисяч унікальних доменів, які перевіряли файли, завантажені браузерами відвідувачів. Більшість файлів повідомили про веб-помилки 404, що свідчить про те, що вхід із вгаданим паролем не вдалося. Приблизно 0,5 відсотка випадків повернули код відповіді 200, залишаючи відкритою ймовірність того, що вгадування пароля могло бути успішним. Під час подальшої перевірки лише один із сайтів був

скомпрометований. Інші використовували нестандартні конфігурації, які повертали відповідь 200, навіть для сторінок, які були недоступні.

За чотири дні, що закінчилися у вівторок, Синєгубко зафіксував понад 1200 унікальних IP-адрес, які намагалися завантажити файл облікових даних. З них на п’ять адрес припадало понад 85 відсотків запитів:

IP	%	ASN
146.70.199.169	34.37%	M247, RO
138.199.60.23	28.13%	CDNEXT, ГБ
138.199.60.32	10.96%	CDNEXT, ГБ
138.199.60.19	6.54%	CDNEXT, ГБ
87.121.87.178	5.94%	СОУЗА-АС, БР

Минулого місяця дослідник помітив, що одна з адрес — 87.121.87.178 — містить URL-адресу, яка використовується в атаці криптозлому. Однією з можливостей зміни є те, що попередня кампанія провалилася, оскільки шкідлива URL-адреса, на яку вона спиралася, не була розміщена на достатньо зламаних сайтах, і у відповідь той самий зловмисник використовує сценарій злому паролів, намагаючись залучити більше сайтів.

Як зазначає Синєгубко, нещодавня кампанія є важливою, оскільки вона використовує комп’ютери та Інтернет-з’єднання мимовільних відвідувачів, які нічого поганого не зробили. Один із способів зупинити це – використовувати NoScript або інший інструмент, який блокує запуск JavaScript на невідомих сайтах. NoScript зламує достатньо сайтів, тому він не підходить для менш досвідчених користувачів, і навіть ті, хто має більше досвіду, часто вважають, що клопоти не варті вигоди. Ще один можливий засіб – використовувати певні блокувальники реклами». ***(Dan Goodin. Attack wrangles thousands of web users into a password-cracking botnet // Condé Nast (https://arstechnica.com/security/2024/03/attack-wrangles-thousands-of-web-users-into-a-password-cracking-botnet/?utm_source=flipboard&utm_content=user%2FArsTechnica). 08.03.2024).***

***

«У вересні 2023 року стався сімдесят один інцидент і 3 808 687 191 зламаних записів. У всьому світі загальна кількість порушених рекордів за 2023 рік наразі становить понад 4,5 мільярда. Відповідно до Orange Cyberdefense Security Navigator 2023, типи атак переважно включають зловмисне програмне забезпечення, соціальну інженерію, порушення політики, системні аномалії та аномалії мережі та додатків.

Програми-вимагачі залишаються однією з найпоширеніших загроз. Відповідно до звіту Sophos State of Ransomware 2023, 27% платежів за програми-вимагачі у 2023 році становили від одного до п’яти мільйонів, а відновлення даних коштує компаніям у середньому 1,82 мільйона доларів США. Однак ця форма атаки відходить від свого коріння шифрування до підходу, заснованого на здирництві, який кіберзлочинці вважають набагато вигіднішим і ефективнішим. Замість того, щоб шифрувати файли – процес, для організації якого потрібен час і терпіння – вони просто викрадають дані та вимагають викупу, погрожуючи продати або передати їх тому, хто запропонує найвищу ціну.

Це крок, який показує, наскільки добре програмне забезпечення-вимагач виконує свою роботу. Інструменти, які використовуються для здійснення атак програм-вимагачів, стають дедалі складнішими, націлюючись на більші організації, використовуючи інструменти, вдосконалені штучним інтелектом (ШІ) та інвестиції для захоплення даних і виманювання дедалі більших сум грошей. Програмне забезпечення-вимагач як послуга також відіграє певну роль у постійному успіху цього шкідливого програмного забезпечення. Коммерційне, воно оптимізоване для надання послуг тим, хто купує та користується ним.

Зловмисне програмне забезпечення для мобільних пристроїв, руйнівне шкідливе програмне забезпечення, очищувачі дисків і вразливості нульового дня також вважаються серед загроз, що зростають у 2023 році, причому хмарні атаки сторонніх розробників також набувають поширення. Хмарні обчислення можуть принести значні переваги південноафриканським підприємствам, але вони також створюють вразливі місця. Кіберзлочинці постійно шукають нові способи використання хмари, а націлювання на сторонніх постачальників послуг стає

популярним шляхом усередині підприємства. Дискові склоочисники викликають ще одне занепокоєння: за даними Fortinet, до кінця 2022 року кількість склоочисників зросла на 53%, і вони залишаються всеосяжною загрозою.

Однак саме використання вразливостей залишається справжньою проблемою., зловмисники Згідно з дослідженням в 327 разів частіше використовують уразливості, а кількість унікальних виявлень експлойтів зросла на 68%. Крім того, звісно, є вразливості нульового дня, на які хакери стрибають на швидкості. Ці широко відкриті двері — це легкий шлях до бізнесу, особливо тому, що багато компаній не виправляють свої платформи так швидко, як мали б, коли ці вразливості були виявлені.

Усі ці загрози та виклики складають один досить простий крок вперед. Настав час організації стати мисливцем, а не полюваним. Інвестувати в інструменти та методології, які повертають безпеку в руки бізнесу. Дослідження PwC Global Digital Trust Insights за 2024 рік показало, що 5% компаній стикаються з меншою кількістю зломів і менш дорогими атаками, оскільки вони зосередилися на оптимізації своєї безпеки. Ці компанії більш продуктивні та демонструють прискорене зростання, тому що вони можуть скористатися перевагами нових технологій і інвестувати в нові способи роботи з більшою впевненістю.

Що це означає? Це означає, що вони поставили безпеку в центр організації, дозволяючи інноваціям і зростанню виходити з технологій, які захищають їх, а не навпаки. Це інвестиції в технології та партнерів, які дозволяють організації процвітати та рости, незважаючи на загрози, які знаходяться поза її стінами. Якщо компанія має надійну систему безпеки, яка здатна швидко адаптуватися до загроз, вона може впевнено просувати свої інновації та інвестиції.

Спостерігайте, реагуйте, полюйте та захищайте. Це чотири стовпи надійної системи безпеки, які забезпечують безпеку мережі, електронної пошти та ідентифікаційних даних разом із керованим виявленням і реагуванням (MDR), моніторингом і аналізом, а також розвідувальними даними та пошуком загроз. Центр виявлення загроз BCX використовує підходи передового досвіду разом із провідними ринковими технологіями виявлення та пом’якшення загроз для

швидкого реагування на ризики всередині організації, гарантуючи, що вона залишається такою ж складною та гнучкою, як і самі загрози.

Кібербезпека – це більше, ніж просто технології. Це менталітет і методологія, прийняті організаціями, які хочуть віддати пріоритет розвитку з партнером, який має правильні інструменти та досвід». ***(Redefining security in the age of cyber-threats // Daily Maverick (https://www.dailymaverick.co.za/article/2024-03-19-redefining-security-in-the-age-of-cyber-threats/). 19.04.2024).***

***

«Міжнародний валютний фонд (МВФ) нещодавно зіткнувся з кіберінцидентом, який було виявлено 16 лютого 2024 року.

Подальше розслідування за участю незалежних експертів з кібербезпеки визначило характер порушення та було вжито заходів щодо усунення.

Розслідування встановило, що одинадцять (11) облікових записів електронної пошти МВФ були зламані. Уражені облікові записи електронної пошти було повторно захищено. На даний момент ми не маємо ознак подальшого компрометування за межами цих облікових записів електронної пошти. Розслідування цього інциденту триває.

МВФ дуже серйозно ставиться до запобігання кіберінцидентам і захисту від них і, як і всі організації, діє, виходячи з припущення, що кіберінциденти, на жаль, траплятимуться. МВФ має надійну програму кібербезпеки, щоб швидко та ефективно реагувати на такі інциденти». ***(IMF Investigates Cyber-Security Incident // International Monetary Fund (https://www.imf.org/en/News/Articles/2024/03/15/pr2488-imf-investigates-cyber-security-incident). 15.03.2024).***

***

«…Інтерфейси прикладного програмування (API) давно визнані основою цифрової економіки, і останні дані показують, що більшість усього інтернет-трафіку зараз спрямовується через API.

Відсутність заходів щодо порушень API

Повсюдне поширення API означає, що вони стали одними з улюблених шлюзів кіберзлочинців для атак захоплення облікових записів. У нещодавньому опитуванні Fastly 84% респондентів визнали, що не мають розширеної безпеки API.

Відсутність заходів щодо порушень API виникає, незважаючи на те, що переважна більшість осіб, які приймають рішення, знають про наявність проблеми. 95% респондентів, опитаних Fastly, сказали, що вони стикалися з проблемами безпеки API протягом останніх дванадцяти місяців.

79% відклали розгортання або інтеграцію нової програми через проблеми безпеки API. Крім того, 79% стверджують, що надають безпеці API «високий або дуже високий» рівень важливості. На запитання, чому нічого з цього не було втілено в життя, найчастіше називали «недостатній бюджет» і «брак досвіду».

«Результати нашого опитування показують, що особи, які приймають рішення, знають, що підвищена залежність від API створює ризик серйозних кібератак. Але поки що вони роблять для цього недостатньо. Це дивно, враховуючи, що експлуатаційні та репутаційні витрати від злому значно перевищують ціну розгортання консолідованої веб-програми та рішення безпеки API від одного постачальника», — сказав Джей Колі, старший архітектор безпеки в Fastly.

Компанії з усіх сил намагаються виявити атаки API

Відповідаючи на запитання, які атрибути платформи безпеки API будуть найважливішими для їхньої компанії, респонденти сказали, що першим місцем буде визначення того, які API розкривають особисті або конфіденційні дані (43%). Інші основні проблеми включали ідентифікацію всіх API, у тому числі незадокументованих (40%), а також ведення журналів і моніторинг (28%).

Однак компанії все більше намагаються виявити атаки API через величезну кількість сповіщень, які вони отримують, використовуючи застарілі рішення безпеки.

Згідно з досвідом Fastly, підкидання облікових даних, зловживання бізнес-логікою та DDoS-атаки – це лише деякі зловмисних автоматизованих атак ботів, які

застосовуються для захоплення облікових записів і крадіжки особистих даних і шахрайства. Доступні сценарії та інструменти спрощують організацію атак API, а застарілі методи захисту від ботів важко виявляють ці потенційно руйнівні вторгнення.

Одним із рішень складності API-ландшафту може стати нове покоління систем кібербезпеки на базі штучного інтелекту, але Fastly виявив, що наразі це мало ентузіазму. Лише 14% опитаних компаній вважали пріоритетом використання технологій ШІ в безпеці API. При цьому 58% очікують, що генеративний ШІ матиме «великий або дуже великий» вплив на безпеку API протягом приблизно 2-3 років.

62% компаній очікують, що штучний інтелект матиме високий або дуже високий ступінь впливу на зростання нових виявлених уразливостей API.

C-suite надає пріоритет безпеці API

Одним з аспектів опитування, що викликає занепокоєння, є те, що жорстко регульовані сектори, які мають справу з конфіденційними даними, є одними з найгірших винуватців, коли справа доходить до бездіяльності API. Лише 80% респондентів у сфері фінансових послуг надають високого або дуже високого рівня важливості безпеці API. Це порівняно з 89% в оптовій, роздрібній торгівлі та електронній комерції.

З точки зору регіональних відмінностей, важливість безпеки API була високо оцінена у Великобританії (86%) порівняно з міжнародним середнім показником у 79%. Zombie API та збирання даних були названі британськими компаніями пріоритетними. Незважаючи на це, у Великій Британії все ще існувала тенденція не перетворювати думки на дії.

«79% учасників у Великій Британії сказали, що їхня безпека API не є високою, — зазначає Колі, — у порівнянні з 84% загалом. Це величезна ціль для все більш досвідчених кіберзлочинців».

Одне інтригуюче розуміння — це прірва в ставленні в ієрархії компанії. 91% експертів із керівництва та відповідності надають безпеці API «високий або дуже високий» рівень важливості, але лише 74% внутрішніх спеціалістів із безпеки

вважають так само. Наслідком, можливо, є те, що когорта безпеки недооцінює масштаб загрози – або це, або вони щодня піддаються більш широкому спектру загроз». ***(95% of companies face API security problems // Help Net Security (https://www.helpnetsecurity.com/2024/03/22/api-security-importance-for-businesses/). 22.03.2024).***

***

«Відповідно до нового звіту Recorded Future, кіберзлочинці, ймовірно, незабаром націляться на служби передачі файлів, спробують скомпрометувати ланцюг постачання програмного забезпечення та запустять нові стратегії фішингу.

У новому звіті прогнозуються найпоширеніші загрози кібербезпеці на 2024 рік, зазначаючи, що в цьому році може спостерігатися еволюція стратегій фішингу, зосередження уваги на ланцюжку постачання програмного забезпечення та використання більш широко використовуваного корпоративного програмного забезпечення, такого як MOVEit.

Цей звіт був опублікований у четвер Recorded Future, і він аналізує тенденції загроз кібербезпеці 2023 року, щоб передбачити, як вони поширяться на 2024 рік.

«Ми передбачаємо, що принаймні одна група програм-вимагачів здійснить успішну компрометацію сотень цілей, використовуючи вразливість у корпоративних сторонніх рішеннях для передачі файлів», — сказала Меггі Коулман із Recorded Future.

Якщо це звучить знайомо, це так. Це нагадує нещодавні проблеми з кібербезпекою з MOVEit. Цей тип служби передачі файлів передає конфіденційні дані, які потрібні зловмисникам. Зловмисники також можуть націлитися на IT, які підтримують віддалену та гібридну роботу, наприклад VPN, хмарне сховище та інструменти багатофакторної автентифікації (MFA).

Захисники можуть підготуватися, створивши або повторно перевіривши плани реагування на інциденти, а також прямі лінії зв’язку з відповідними постачальниками, сказав Коулман. Організаціям потрібне чітке розуміння рішень,

які вони використовують, і способів їх впровадження, а також їм потрібно знати, хто відповідає за виправлення — вони чи постачальник. Крім того, організації повинні відстежувати розвідувальні канали, щоб бути в курсі нещодавно виявлених або широко використовуваних уразливостей.

Захисникам потрібен не лише доступ до програмного забезпечення, а й до ланцюга постачання програмного забезпечення.

За словами Коулман, зловмисники публікують сховища зловмисників під нешкідливими назвами на платформах з відкритим кодом, таких як GitHub. Хакери сподіваються, що розробники ПЗ або завантажать шкідливий код, або включать його в програмні рішення. Крім того, особлива ціль – менеджери пакетів даних npm і PyPI.

У 2023 році фішинг був основним способом доступу зловмисників до системи. Деякі зловмисники передавали шкідливі файли за допомогою архіву та форматів HTML, щоб уникнути виявлення програмним забезпеченням безпеки електронної пошти. Фішери також почали розповсюджувати зловмисне програмне забезпечення або посилання на шкідливі сайти за допомогою тексту, QR-кодів або корпоративних систем обміну повідомленнями, таких як Skype і Teams. Збільшене використання багатофакторної автентифікації захисниками призвело до того, що зловмисники намагаються зловживати втомою від MFA або проводити атаки противника посередині, під час яких вони перехоплюють комунікації.

Все більше організацій відходять від паролів до методів доступу до облікових записів, які менш вразливі до крадіжки. До них належать чарівні посилання та методи автентифікації на основі телефону. Ймовірно, біометрична аутентифікація також стане більш популярною. Таке посилення, швидше за все, спонукає зловмисників до еволюції, і вони надсилатимуть підроблені шкідливі магічні посилання. Вони також можуть використовувати генеративний штучний інтелект, щоб допомогти у фішингу. У деяких випадках шахраї можуть переходити від спроб захоплення облікового запису до спроб нового шахрайства.

Хакери впроваджують інновації й в інші способи. У 2023 році більше хакерів використовували мови програмування, які дозволяли зловмисному програмному

забезпеченню зламати кілька операційних систем. Як наслідок, користувачі macOS і Linux захочуть бути пильними, оскільки, хоча зловмисне програмне забезпечення традиційно зосереджено на Windows, деякі хакери створюють варіанти, націлені на інші операційні системи.

Наприклад, сумно відома банда програм-вимагачів LockBit, здається, експериментувала з варіантом програми-вимагача macOS у квітні, хоча цей варіант не зустрічався в дикій природі.

У всьому світі 2023 рік також став стиранням меж між ідеологічно орієнтованими хактивістами та кіберзлочинцями, які керуються прибутком. Хактивісти часто прагнуть привернути увагу за свої атаки, які можуть створити хаос, на якому деякі кіберзлочинці користуються, сказала Коулман. Злочинці можуть здійснювати власні атаки, які можна сплутати з хактивістською діяльністю. В інших випадках хактивісти, які потребують фінансової підтримки, можуть продавати експлойти або послуги розподіленої відмови в обслуговуванні за наймом.

Політичні мотиви також, ймовірно, стимулюють операції впливу навколо цьогорічних виборів. Очікується, що Росія та Китай спробують завдати шкоди кандидатам, які підтримують Україну та Тайвань, йдеться у звіті. Для цього їхні кампанії можуть посилити політичну поляризацію США та «підірвати демократичний процес». ***(Jule Pattison-Gordon. Report Predicts Top Cybersecurity Threats for 2024 // e.Republic LLC (https://www.govtech.com/security/report-predicts-top-cybersecurity-threats-for-2024). 21.03.2024).***

***

«Поліція Гонконгу попередила компанії про посилення безпеки після того, як минулого року зросла кількість кібератак, порадивши їм постійно оновлювати програмне забезпечення та запобігати злому хакерам у їхні системи.

Минулого року було 37 повідомлень про кібератаки на підприємства, що на 54 відсотки більше, ніж у 24 випадках у 2022 році. Заявлені збитки зросли втричі до

2,1 мільйона гонконгських доларів (268 400 доларів США) з 700 000 гонконгських доларів у 2022 році.

Під час п’ятимісячного онлайн-тралення з вересня минулого року по минулий місяць поліція знайшла та вилучила понад 210 000 пристроїв із серйозними порушеннями безпеки в Інтернеті та шахрайськими веб-сайтами. Вони включали сервери та комп’ютери як корпоративних, так і індивідуальних користувачів.

У вас є запитання про найпопулярніші теми та тенденції з усього світу? Отримайте відповіді за допомогою SCMP Knowledge, нашої нової платформи підібраного вмісту з поясненнями, поширеними запитаннями, аналізом та інфографікою, наданими нашою нагородженою командою.

«Виявивши ці загрози безпеці під час нашого розслідування, сили зв’язалися з 80 місцевими інтернет-провайдерами, щоб усунути лазівки», — сказав ЗМІ на брифінгу минулої середи Джо Лау Нго-Чунг, головний інспектор відділу кібербезпеки сил.

Кілька статутних органів і відомих компаній були серед тих, хто став жертвою хакерів минулого року.

У Cyberport, технологічному центрі міста, понад 400 ГБ даних, включаючи інформацію про банківські рахунки та копії посвідчень співробітників, було викрадено під час атаки програм-вимагачів минулого вересня.

Хакери вимагали 300 000 доларів США як викуп, погрожуючи оприлюднити інформацію в темній мережі, де злочинці купують і продають дані для використання в шахрайствах та інших незаконних цілях. Викуп не був сплачений.

Генеральний директор гонконзького Cyberport йде у відставку, викликаючи пошуки нового боса

Через тиждень після цієї атаки хакери атакували Раду споживачів, забравши особисті дані понад 25 000 співробітників, колишніх співробітників, передплатників внутрішнього журналу та учасників попередніх заходів. Хакери вимагали викуп у розмірі 500 000 доларів США, але споживча служба не заплатила.

Виконувач обов’язків старшого суперінтенданта Барон Чан Шун-чінг з відділу кібербезпеки та технологічних злочинів сказав, що збитки від кібератак різко зросли минулого року через кілька справ, пов’язаних із великими сумами.

У найбільшому випадку чоловік нібито вкрав 710 000 гонконгських доларів у свого колишнього роботодавця протягом 14 місяців через несанкціонований доступ до внутрішніх систем фірми.

Компанія повідомила в поліцію, і справа все ще розслідується, сказав Чан.

Під час п’ятимісячного онлайн-перевірки під кодовою назвою «Operation Strongfighter» поліція виявила 175 970 пристроїв із серйозними лазівками в безпеці в Інтернеті після аналізу понад 3 мільйонів фрагментів даних, які свідчать про вразливість елементів до злому.

Серед них 100 000 пультів дистанційного керування для точок підключення до мережі з високим ризиком, майже 63 000 комп’ютерних систем, які більше не підтримувалися, і понад 4 800 застарілих мереж, підключених до пристроїв зберігання даних.

Рада споживачів Гонконгу стала жертвою хакерів через місяць після атаки на техноцентр

Було виявлено та видалено майже 40 000 інших інтернет-загроз, більшість із яких були фішинговими веб-сайтами, які використовувалися для того, щоб обманом змусити жертв розкрити свою конфіденційну інформацію. Решта — 60 комп’ютерів, які контролювали мережі ботів, і 4006 комп’ютерів, захоплених хакерами.

Поліція також взяла участь у міжнародних навчаннях, організованих Інтерполом у період з вересня по минулий місяць проти фішингових веб-сайтів, шкідливих програм і програм-вимагачів.

Поліція Гонконгу посіла перше місце серед 55 країн і регіонів за кількістю арештів, видаливши 153 шкідливі програми та фішингові сайти.

Пол Цанг Чеунг-фай, системний інженер-директор Sangfor Technologies, сказав, що хакери зазвичай починали з пошуку цілей у соціальних мережах,

пошукових системах або онлайн-скануваннях портів на предмет вразливих адрес Інтернет-протоколу (IP).

Після ідентифікації цільової адреси хакери спробують вгадати пароль, щоб отримати доступ до даних у комп'ютеризованому пристрої, перш ніж пропонувати викрадені дані для продажу в темній мережі.

Цанг сказав, що як тільки хакери дізнаються пароль жертви, вони отримають перевагу.

«Вони можуть проводити більш глибокі атаки, такі як встановлення бекдор-програми, і після встановлення програми вони можуть здійснювати подальші дії, такі як керування камерою пристрою», — сказав він.

Старший інспектор Лау закликав підприємства постійно оновлювати свої системи та використовувати надійні паролі.

Він сказав, що стикався з компаніями, які використовували слабкі, інтуїтивно зрозумілі паролі, такі як «Адміністратор», для своїх облікових записів веб-адміністраторів, тоді як інші ігнорували попередження про ризики від сканування безпеки на своїх власних системах, наражаючи їх на можливі кібератаки.

«Хакери спочатку шукають широко відомі лазівки у своїх скануваннях», — сказав він. «Якщо підприємства не оновили своє програмне забезпечення та системи, кібератакники можуть використати їх для подальших атак». ***(Jess Ma. Hong Kong police tell businesses to tighten cybersecurity as more fall victim to hackers // Microsoft (https://www.msn.com/en-xl/news/other/hong-kong-police-tell-businesses-to-tighten-cybersecurity-as-more-fall-victim-to-hackers/ar-BB1kstJr). 25.03.2024).***

***

«Частота та складність кібератак, скоєних проти підприємств і галузей усіх рівнів, експоненціально зросла у зв'язку з тим, що ці організації покладаються на цифрові технології для підтримки свого бізнесу та операцій. Це призвело до незліченних трильйонів доларів у вигляді збитків і доходів, а також до перебоїв у наданні послуг компаніям і організаціям по всьому світу. Про інциденти з кібербезпекою повідомляли відомі гіганти галузі, такі як Apple, Meta,

Sony, Twitter тощо, але на кожну з цих резонансних розголошених атак є незліченна кількість нападів на менші компанії, служби та мережі, які так само вразливі, якщо не більше, до цих загроз.

Це робить кібербезпеку зростаючою проблемою не лише для великих корпорацій з багатомільярдною оцінкою та критично важливою державною інфраструктурою, але й для всіх видів малих і середніх підприємств, муніципалітетів, лікарень та будь-яких організацій, які покладаються на цифрові мережі та технології, які: у 2024 році — це всі вони в тій чи іншій якості.

Зміна технологічних послуг стимулює більше атак

Найлогічніша причина нещодавнього стрімкого зростання кількості кібератак є також найочевиднішою. Оскільки все більше компаній і послуг розміщуються в цифрових мережах, цілком зрозуміло, що зростатиме кількість інцидентів зловмисних груп, які намагаються використовувати слабкі сторони цих мереж. Незважаючи на те, що розвиток і впровадження цифрових технологій збільшили потужність і можливості компаній і організацій у всьому світі, те саме можна сказати про хакерські групи та банди програм-вимагачів. Прогрес у таких технологіях, як штучний інтелект, полегшив кібертерористам виявлення та злам уразливостей мережі з більшою швидкістю та ефективністю, і ці технології розгортаються цілодобово, щоб досліджувати та атакувати вразливості, де б вони не були виявлені. Отже, хоча так, кількість кібератак зростає через цифрову трансформацію нашого суспільства, справа в тому, що ці хакерські групи також, безсумнівно, стають кращими в цьому.

Різноманітність мотивацій для цих хакерських угруповань і кібертерористів є важливим фактором, що спричинило такий постійний ріст цих атак. Найбільш очевидною є фінансова мотивація. Простіше кажучи, це платить. Коли одна з цих груп може отримати доступ до мережі та витік конфіденційної інформації або тримати дані та служби в заручниках, вони часто отримують чималий викуп.

Хоча найбільш розголошеними цілями для цих банд програм-вимагачів є великі компанії та критична інфраструктура, малі та середні підприємства є кращими цілями для цих організацій, на які припадає майже 70% зареєстрованих

атак. Хоча цим малим підприємствам і організаціям місцевого рівня може не вистачати бездонних кишень, яких жадають хакери, їм також не вистачає ресурсів, які мають у своєму розпорядженні більші організації, щоб захистити себе, що робить їх незначними плодами для кіберзлочинців.

Геополітичні мотиви

Інша мотивація кіберзлочинців і хакерських груп була політично та ідеологічно заряджена. Із зростанням геополітичної напруженості та спалахом глобальних конфліктів багато країн використовують групи кібертерористів, щоб завдати удару по економічних і соціальних структурах своїх ворогів. Це можна побачити в зусиллях Росії дестабілізувати Україну, у війні Ізраїлю та ХАМАСу та в зусиллях Китаю зруйнувати та послабити західні країни. Кіберзлочинність стала продовженням військового потенціалу розвинених країн у всьому світі і часто є одним із найефективніших інструментів для диверсій і шпигунства.

На масовому рівні більш екстремістські групи активістів звертаються до кіберзлочинності як до засобу прямого удару по компаніях, галузях і політичних партіях. Випадки «хактивізму» зростають, оскільки громадянська непокора зазнає цифрової трансформації разом із агентствами та організаціями, проти яких багато хто з цих груп протистоять.

Витрати перевищують долари

Кібербезпека – це не просто стаття на балансі. Збитки від цих атак, безумовно, можна виміряти в доларах і центах, втратах доходів і сплачених викупах, але вони також можуть завдати незліченних збитків тканині нашого суспільства та життям його людей. Для багатьох компаній це не тимчасовий збій. Багато компаній після порушення не існують більше шести місяців. Тривожною тенденцією є те, що кібертерористи нападають на лікарні та медичні установи. Що станеться, коли вартість цих атак перестане вимірюватися у фінансовому вимірі?

Села та міста також все частіше стають мішенями кіберзлочинців. Що відбувається, коли їхня здатність реагувати на надзвичайні ситуації скомпрометована триваючою кібератакою? І це лише приклади на місцевому рівні. Що станеться, коли критично важлива інфраструктура федеральних агентств і

організацій недоступна, а життєво важливі послуги недоступні для людей, які їх потребують?

Протоколи кібербезпеки повинні розроблятися та впроваджуватися з тією ж швидкістю та ефективністю, що й ті, хто шукає шляхи проникнення в них. Нам потрібно краще розуміти ризики безпеці та найефективніші відповіді та стратегії для розгортання в разі кібератаки. Навчання та освіта в поєднанні з останніми розробленими платформами та протоколами є життєво важливими для стримування цієї ескалації кібератак і забезпечення захисту наших мереж і систем від загроз злому. Однак ми настільки сильні, наскільки сильна наша найслабша ланка.

Недостатньо розробити найповнішу кібербезпеку, якщо вона залишається або недоступною, або недостатньо використовується. Більше компаній, організацій і підприємств на всіх рівнях повинні знати про свою поточну вразливість до кібератак і вживати профілактичних заходів, щоб запобігти таким атакам. Остання причина того, що хакери щодня здійснюють більше таких атак — і єдина, на яку ми можемо вплинути — це найпростіша причина. Це тому, що вони можуть». ***(Charles Regan. Cybersecurity is not just an enterprise-level risk // Endeavor Business Media, LLC. (https://www.securityinfowatch.com/cybersecurity/article/53099862/cybersecurity-is-not-just-an-enterprise-level-risk). 22.03.2024).***

***

«Задовго до настання ери Інтернету в комп'ютерах були виявлені недоліки безпеки, які використовувалися – спочатку шляхом атак на дані в самому комп'ютері, а невдовзі – на комп'ютери, підключені до мережі. Історично загрози кібербезпеці йшли в ногу з розвитком інформаційних технологій і засобів захисту кібербезпеки, як-от антивірусне програмне забезпечення. Коли комп'ютери були підключені до Інтернету та почали обмінюватися даними, кіберзлочини суттєво змінилися, а також механізми їх запобігання.

У 1988 році аспірант інформатики Корнельського університету запустив комп’ютерний хробак в Інтернеті, заразивши приблизно 6000 мейнфреймів, міні-комп’ютерів і робочих станцій, під’єднаних до Інтернету, шкідливим кодом, який знизив продуктивність комп’ютера до повзання. Пізніше він зізнався, що його мотивом було «продемонструвати неадекватність поточних заходів безпеки в комп’ютерних мережах, використовуючи виявлені ним дефекти безпеки».

Цей відносно нешкідливий кіберзлочин, оглядаючись назад, був провісником майбутньої широкомасштабної кіберзлочинної діяльності, оскільки Інтернет і цифрові перетворення, що відбуваються в усіх сферах життя, породили хитро продумані кібератаки у формі шкідливих вірусів, мережевих вторгнень, шкідливих програм, програм-вимагачів., витоку даних тощо.

На початку зв’язаного світу кіберзлочинці атакували комп’ютерні інформаційні системи, мережі та персональні комп’ютерні пристрої, щоб викрасти такі дані, як паролі та облікові дані для входу, кредитні картки та фінансові дані та навіть особисту медичну інформацію. Деякі з найбільш розголосних інцидентів включають Stuxnet у 2010 році, який був першою кіберзброєю, яка мала завдати фізичної шкоди. У цьому випадку вважалося, що Stuxnet знищила 20 відсотків центрифуг, які використовувалися в Ірані для створення свого ядерного арсеналу.

Атака програми-вимагача 2017 року WannaCry вразила приблизно 200 000 комп’ютерів у 150 країнах, тоді як атака NotPetya, яка почалася в Україні, знищила тисячі комп’ютерів у 60 країнах. NotPetya також торкнулася промисловості, коли Mondelez, багатонаціональна компанія з виробництва продуктів харчування та напоїв, втратила тисячі комп’ютерів у результаті атаки, що вплинуло на виробничі потужності по всьому світу, а також на здатність компанії виконувати замовлення клієнтів.

Вплив виробництва

Хоча кібератаки поширені майже в усіх галузях, виробничі процеси, зокрема, є основними цілями для таких загроз, тому виробникам необхідно усвідомити ризики, пов’язані з кібератаками, і зрозуміти доступні засоби захисту.

Згідно з опитуванням, проведеним компанією Barracuda Networks у 2022 році [6], понад 90 відсотків визнали, що минулого року вони зазнали інциденту безпеки, який суттєво вплинув на їхню організацію. Повідомлені інциденти включали широкий спектр атак, причому найпоширенішими були веб-додатки, зловмисне зовнішнє обладнання/змінні носії та розподілені атаки на відмову в обслуговуванні.

З масштабними цифровими трансформаціями, що відбуваються у виробничому секторі, площа кіберзагроз експоненціально розширилася. Це робить кібербезпеку надзвичайно важливою для виробників будь-якого розміру, незалежно від рівня цифрової трансформації, яку пройшла компанія.

Вибухове зростання цифрової трансформації в промисловому секторі, що характеризується терміном «Індустрія 4.0», є основою обговорення кібербезпеки для підключених розумних виробників і цифрових мереж постачання. Ці розумні системи запрограмовані на збір і обмін даними, прийняття рішень, які ініціюють дії, і незалежний контроль процесів. Крім того, нова інтеграція штучного інтелекту та технологій машинного навчання в додатки промислового Інтернету речей, такі як машинне зір, робототехніка та прогнозне технічне обслуговування, робить уразливими все більшу кількість критично важливих даних і ставить промислові процеси під загрозу.

Наприклад, процеси адитивного виробництва починають інтегрувати різні алгоритми на основі штучного інтелекту та машинного навчання, щоб використовувати весь потенціал 3D-технології. Навчена модель друку, яка виростає в процесі машинного навчання, стає інтелектуальною власністю виробника та має бути захищена від ненавмисних модифікацій або навіть навмисних атак. Можуть існувати фальшивомонетники, які намагаються створювати подібні системи, зловживаючи власністю оригінального виробника, або можуть бути навіть відверті саботажники, які хочуть маніпулювати тим, що система може виробляти на практиці.

Ще більш зловмисною атакою на лінію серійного виробництва є маніпуляція самими результатами. Наприклад, дистанційний хакер може маніпулювати налаштуваннями в робототехнічному процесі виробництва, щоб утримувати одні

болти вільними, а інші надмірно закручувати в готовому продукті. Як наслідок, небезпечні продукти можуть вийти на ринок із потребою дорогого відкликання та загрозою судового розгляду.

Оскільки технології Індустрії 4.0 продовжують розвиватися, стиратимуться межі між оперативними та інформаційними технологіями. Оскільки критично важливі виробничі дані виходять за межі традиційної фабрики, правами доступу та політиками потрібно буде керувати в усій організації, що обов'язково призведе до більш тісно узгодженого середовища IT та OT.

Конвергенція IT/OT систем і процесів, забезпечуючи нові рівні ефективності виробництва та продуктивності на виробництві, залучить нових зацікавлених сторін у середовище безпеки. Групи та процеси IT-безпеки тепер повинні включати різноманітні вимоги розподілених промислових середовищ у реальному часі.

Немає сумніву, що IT/OT технології продовжуватимуть розвиватися, так само як і природа та механізми кіберзлочинів, незалежно від того, чи це буде крадіжка IP, зрив операцій або спричинення хаосу іншими способами. Технології кібербезпеки та запобіжні заходи також повинні розвиватися, не просто реагуючи на проблеми, що виникають, а радше забезпечуватись завдяки вбудованому підходу кібербезпеки за проектом до нових інновацій Індустрії 4.0». ***(Marcellus Buchheit. Cybersecurity-by-Design for Industry 4.0 // manufacturing.net (https://www.manufacturing.net/cybersecurity/blog/22890925/cybersecuritybydesign-for-industry-40). 21.03.2024).***

***

«Дослідники з Університету штату Колорадо опублікували нову статтю, в якій детально описуються вразливості в системах комерційних вантажних перевезень, які можуть дозволити хакерам отримати контроль над цілими автопарками, викрасти з них або навіть порушити роботу цілих автопарків, непомітно поширюючи зловмисне програмне забезпечення між транспортними засобами.

Отримані дані підкреслюють прогалини в кібербезпеці в галузі вантажних перевезень за допомогою електронних пристроїв реєстрації, або ELD — федерально затвердженої додаткової системи, яка використовується для відстеження відповідності годин обслуговування та інших показників для подальшої перевірки, яка тісно пов'язана з системами керування в автомобілі. Ці пристрої наразі не зобов'язані мати запобіжні заходи, і в статті показано, як ними можна бездротово керувати з дороги, щоб, наприклад, змусити вантажівки зупинитися.

Висновки були представлені на симпозіумі з безпеки мереж і розподілених систем 2024 року, де дослідження зайняло друге місце в категорії найкращих статей. Доцент Джеремі Дейлі керував роботою відділу системної інженерії Інженерного коледжу Вальтера Скотта-молодшого. Основними авторами статті були аспіранти системної інженерії Джейк Джепсон і Рік Чаттерджі.

Висновки загалом стосуються більш ніж 14 мільйонів вантажівок середньої та великої вантажопідйомності, які утворюють ядро судноплавної галузі США, повідомляє Daily.

«Це дослідження доповнює минулу роботу, яку ми виконали щодо кібербезпеки важкої техніки, як-от вантажівок, човнів і тракторів, спільно з Національною асоціацією автомобільних вантажних перевезень, а також через наші практичні заходи Cyber Challenge зі студентами в університетському містечку», — сказав Daily. «Це нові та складні проблеми безпеки, які вимагають польових випробувань на додаток до розширеної співпраці з усіма зацікавленими сторонами».

Пристрої електронного журналу відстежують години роботи двигуна, дані про рух автомобіля та пройдену відстань. Регулятори та правоохоронні органи потім використовують ці журнали для відстеження безпечних практик експлуатації, наприклад забезпечення достатнього відпочинку водіїв. Команда CSU перевірила кілька моделей для своєї роботи над ELD, які часто встановлюються «готово» з налаштуваннями за замовчуванням. Через це — і через їх взаємозв'язок із

ключовими системами — вони представляють унікальний набір уразливостей, які, ймовірно, не обмежуються одним виробником.

У статті команда CSU демонструє, як до цих систем можна отримати доступ по повітрю через системи Bluetooth або Wi-Fi, щоб порушити роботу. Команда також продемонструвала, як зловмисне програмне забезпечення можна завантажити на одну вантажівку, а потім поширити на інші, навіть коли воно рухається по шосе або під час паркування та очікування на транспортних вузлах і зупинках для вантажівок.

Джепсон був першим автором статті та сказав, що команда працювала безпосередньо з виробниками та Агентством кібербезпеки та безпеки інфраструктури США, щоб вирішити проблеми, перш ніж поділитися висновками. Агентство є частиною Міністерства внутрішньої безпеки США.

«Проблеми, висвітлені в нашій статті, є суттєвими, і ми виявили кілька критичних вразливостей у конкретній моделі ELD, яка становить значну частку існуючого ринку», — сказав Джепсон. «Виробник зараз працює над оновленням мікропрограми, але ми підозрюємо, що ці проблеми можуть бути звичайними і потенційно не обмежуватися одним пристроєм чи примірником».

Daily сказав, що ці висновки, очевидно, важливі для галузі вантажних перевезень, але вони також інформують про деякі ширші потенційні вразливості, оскільки різні активи та елементи інфраструктури стають взаємопов’язаними.

«Наша група продовжуватиме розробляти адаптивні заходи безпеки, оцінки та моделі, які можна легко інтегрувати в існуючі операції», — сказав він. «Ці шаблони проектування безпеки також можна використовувати протягом життєвого циклу вантажівки, від концептуального проектування до виведення системи з експлуатації». ***(Josh Rhoten. Researchers highlight potential cybersecurity threats to trucking industry, supply chain // Microsoft (https://www.msn.com/en-us/news/technology/researchers-highlight-potential-cybersecurity-threats-to-trucking-industry-supply-chain/ar-BB1kjaX6). 21.03.2024).***

***

«Хакери, підтримані урядом Північної Кореї, здобули серйозну перемогу, коли Microsoft не виправляла Windows zero-day протягом шести місяців після того, як дізналася, що її активно експлуатують.

Навіть після того, як Microsoft виправила вразливість минулого місяця, компанія не згадала, що північнокорейська група загроз Lazarus використовувала вразливість принаймні з серпня для встановлення прихованого руткіта на вразливі комп'ютери. Ця вразливість забезпечувала легкий та прихований спосіб для зловмисного програмного забезпечення, яке вже отримало права адміністратора системи, щоб взаємодіяти з ядром Windows. Лазарус використовував вразливість саме для цього. Незважаючи на це, корпорація Майкрософт уже давно заявляє, що таке підвищення прав адміністратора до ядра не є перетином кордону безпеки, можливим поясненням часу, який знадобився корпорації Майкрософт для усунення вразливості.

Руткіт «святий Грааль»

«Коли мова заходить про безпеку Windows, існує тонка грань між адміністратором і ядром», — пояснив минулого тижня Ян Войтешек, дослідник фірми безпеки Avast. Microsoft « Критерії обслуговування безпеки вже давно стверджують, що «адміністратор-ядро не є межею безпеки», що означає, що Microsoft залишає за собою право виправляти вразливості адміністратора-ядра на власний розсуд. Як наслідок, модель безпеки Windows не гарантує, що вона завадить зловмисникам на рівні адміністратора отримати прямий доступ до ядра».

Політика Microsoft виявилася благом для Lazarus у встановленні «FudModule», спеціального руткіта, який, за словами Avast, був надзвичайно прихованим і просунутим. Руткіти — це зловмисне програмне забезпечення, яке має здатність приховувати свої файли, процеси та іншу внутрішню роботу від самої операційної системи та водночас контролювати найглибші рівні операційної системи. Щоб працювати, вони повинні спочатку отримати адміністративні привілеї — головне досягнення для будь-якого зловмисного програмного забезпечення, що заражає сучасну ОС. Потім вони повинні подолати ще одну

перешкоду: безпосередньо взаємодіяти з ядром, найпотаємнішим куточком ОС, зарезервованим для найбільш чутливих функцій.

У минулі роки Lazarus та інші групи загроз досягли цього останнього порогу, в основному використовуючи системні драйвери сторонніх виробників, які за визначенням уже мають доступ до ядра. Щоб працювати з підтримуваними версіями Windows, драйвери сторонніх виробників повинні мати цифровий підпис Microsoft, щоб підтвердити, що вони надійні та відповідають вимогам безпеки. У випадку, якщо Lazarus або інший загрозливий суб'єкт уже подолав перешкоди адміністратора та виявив уразливість у схваленому драйвері, вони можуть встановити його та використати вразливість для отримання доступу до ядра Windows. Ця техніка, відома як BYOVD (принесіть власного вразливого драйвера), однак коштує дорого, оскільки вона надає захисникам широкі можливості для виявлення атаки.

Уразливість, яку використовував Lazarus, відстежувана як CVE-2024-21338, пропонувала значно більше скритності, ніж BYOVD, оскільки використовувала appid.sys, драйвер, що вмикає службу Windows AppLocker, попередньо встановлену в ОС Microsoft. Avast сказав, що такі вразливості є «святим Граалем» порівняно з BYOVD.

У серпні дослідники Avast надіслали Microsoft опис нульового дня разом із кодом для підтвердження концепції, який демонстрував, що він робив у разі експлуатації. Microsoft не виправляла вразливість до минулого місяця. Навіть тоді розкриття активної експлуатації CVE-2024-21338 і подробиці руткіта Lazarus надійшли не від Microsoft у лютому, а від Avast через 15 днів. Через день Microsoft оновила свій бюлетень виправлень, щоб відзначити використання.

Незрозуміло, що спричинило затримку або початкову відсутність розкриття інформації. Microsoft не відразу отримала відповіді на запитання, надіслані електронною поштою.

Якою б не була причина, шестимісячне очікування дало Lazarus набагато більш ефективний і прихований спосіб встановлення FudModule. Потрапивши на місце, руткіт дозволив Lazarus обійти ключові засоби захисту Windows, такі як

виявлення та реагування кінцевих точок, індикатор захищених процесів, призначений для запобігання втручанню в процеси захисту кінцевих точок, а також запобігання читанню пам’яті та впровадженню коду незахищеними процесами. Войтешек з Avast пояснив:

З точки зору зловмисника, перехід від адміністратора до ядра відкриває цілу нову сферу можливостей. З доступом на рівні ядра зловмисник може порушити роботу програмного забезпечення безпеки, приховати індикатори зараження (включно з файлами, мережевою активністю, процесами тощо), вимкнути телеметрію в режимі ядра, вимкнути засоби захисту тощо. Крім того, оскільки безпека PPL (Protected Process Light) залежить від межі між адміністратором і ядром, наш гіпотетичний зловмисник також отримує можливість підробити захищені процеси або додати захист до довільного процесу. Це може бути особливо потужним, якщо lsass захищено за допомогою RunAsPPL, оскільки обхід PPL може дозволити зловмиснику скинути недоступні облікові дані.

Далі дослідник писав:

Якщо зловмиснику, незважаючи на всі ці перешкоди, вдасться використати вразливість нульового дня у вбудованому драйвері, він отримає рівень скритності, який неможливо порівняти зі стандартним використанням BYOVD. Використовуючи таку вразливість, зловмисник у певному сенсі живе за рахунок землі, не потребуючи приносити, видаляти чи завантажувати будь-які спеціальні драйвери, що робить можливим, щоб атака на ядро була справді безфайловою. Це не тільки дозволяє уникнути більшості механізмів виявлення, але й уможливлює атаку на системи, де діє білий список драйверів (що може здатися трохи іронічним, враховуючи, що CVE-2024-21338 стосується драйвера AppLocker).

Хоча ми можемо лише здогадуватися про мотивацію Lazarus для вибору цього третього підходу для перетину межі між адміністратором і ядром, ми вважаємо, що їх основною мотивацією була скритність. Враховуючи рівень їхньої слави, їм доведеться міняти вразливості щоразу, коли хтось спалює їх техніку BYOVD, яка зараз використовується. Можливо, вони також міркували, що,

вийшовши за межі BYOVD, вони могли мінімізувати потребу в обміні, залишаючись непоміченими довше.

Не всі дослідники настільки критичні. В онлайн-інтерв'ю Вілл Дорманн, старший аналітик уразливостей у фірмі безпеки Analygence та постійний критик Microsoft, сказав:

Вони могли мати дуже вагомі причини, чому це могло бути складнішим і потребувало більше часу інженерів для виправлення. З іншого боку, він міг просто стати пріоритетним для інших більш актуальних виправлень безпеки. І, можливо, у грі є власна публічна позиція Microsoft про те, що зв'язок адміністратора з ядром *не* є межею безпеки, тож вони могли б цілком законно відмовитися від вирішення проблеми, якби хотіли.

Далі він сказав, що шестимісячне очікування для усунення вразливостей є «звичайним явищем», навіть якщо такі затримки можуть бути «прийнятними».

Оскільки корпорація Майкрософт не пояснює причини того, як вона обробила виправлення CVE-2024-21338, світ, ймовірно, ніколи не дізнається. Ясна річ: тепер, коли вразливість стала загальнодоступною, ризик її більш широкого використання зріс. Користувачі Windows, які ще не встановили виправлення, мають зробити це пріоритетним». ***(Dan Goodin. Hackers exploited Windows 0-day for 6 months after Microsoft knew of it // Condé Nast (https://arstechnica.com/security/2024/03/hackers-exploited-windows-0-day-for-6-months-after-microsoft-knew-of-it/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 05.03.2024).***

***

«Сумно відомий російський хакерський колектив, відомий як APT28, тепер використовує законну функцію Microsoft Windows для розгортання інформаційних крадіжок та іншого шкідливого програмного забезпечення для своїх жертв.

У новому документі кібербезпеки IBM відділу, X-Force, стверджується, що кампанія була активною з листопада минулого року по лютий цього року.

Згідно зі звітом, зловмисники (також відомі як Fancy Bear, Forest Blizzard або ITG05) видають себе за урядові та неурядові організації в Європі, на Південному Кавказі, в Центральній Азії, а також у Північній і Південній Америці, звертаючись до своїх жертв електронною поштою. Електронні листи містять збройні PDF-файли.

Викрадення конфіденційної інформації

PDF-файли містять URL-адреси, які ведуть до скомпрометованих веб-сайтів, які можуть зловживати обробником протоколу URI «search-ms:», а також протоколом програми «search:». Обробник дозволяє програмам і HTML-посиланням запускати користувацькі локальні пошуки на пристрої, а протокол Whale служить механізмом для виклику програми пошуку на робочому столі в Windows.

У результаті жертви зрештою виконують пошук на контрольованому зловмисником сервері та виявляють зловмисне програмне забезпечення, яке відображається в Windows Explorer. Це зловмисне програмне забезпечення маскується під PDF-файл, який жертвам пропонується завантажити та запустити.

Зловмисне програмне забезпечення розміщено на серверах WebDAV, які, швидше за все, розміщені на скомпрометованих маршрутизаторах Ubiquiti. Ці маршрутизатори були частиною ботнету, який, очевидно, був ліквідований урядом США минулого місяця, повідомляє The Hacker News.

Ми не знаємо, хто жертви, але можна з упевненістю припустити, що вони з тих самих країн, що й урядові та неурядові організації, яких видають за напади: Аргентина, Україна, Грузія, Білорусь, Казахстан, Польща, Вірменія, Азербайджан, і США

Ті, хто потрапив на цей трюк, зрештою встановили MASEPIE, OCEANMAP і STEELHOOK, зловмисне програмне забезпечення, призначене для викрадання файлів, виконання довільних команд і крадіжки даних браузера. «ITG05 залишається адаптованим до змін у можливостях, надаючи нові методології

зараження та використовуючи комерційно доступну інфраструктуру, одночасно постійно розвиваючи можливості шкідливого програмного забезпечення», — підсумували дослідники». ***(Sead Fadilpašić. Russian hacker group exploits Microsoft Windows feature in worldwide phishing attack // Future US, Inc. (https://www.techradar.com/pro/security/russian-hacker-group-exploits-microsoft-windows-feature-in-worldwide-phishing-attack?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 18.03.2024).***

***

Вірусне та інше шкідливе програмне забезпечення

«Фахівці з кібербезпеки створили хробака Morris II для чат-ботів зі штучним інтелектом. Використання цієї шкідливої програми може призвести до викрадення даних та поширення спаму.

Група дослідників стверджує, що створена ними програма, ймовірно, є першим у світі хробаком для генеративного штучного інтелекту. Хробак здатний поширюватися від однієї системи до іншої, потенційно викрадаючи дані або розгортаючи зловмисне програмне забезпечення, пише WIRED.

«Це фактично означає, що тепер у вас є можливість здійснити новий вид кібератак, якого раніше не було», — каже керівник дослідження Бен Нассі з Cornell Tech.

У новій статті вчені показали, як здійснюють атаки за допомогою цього хробака та помічників для електронної пошти з метою викрасти дані з листів і розсилати спам. Для демонстрації дослідники створили систему електронної пошти, яка може надсилати та отримувати повідомлення за допомогою генеративного штучного інтелекту, підключаючись до ChatGPT, Gemini та LLM з відкритим кодом LLaVA.

В одному випадку дослідники, діючи як зловмисники, написали електронний лист, який «отруює» базу даних ШІ-помічника електронної пошти,

використовуючи пошуково-розширену генерацію (RAG). Коли RAG отримує електронний лист у відповідь на запит користувача та надсилає його GPT-4 або Gemini Pro для створення відповіді, він, кажуть дослідники, «зламує службу генеративного ШІ» і зрештою викрадає дані з електронних листів. Це можуть бути імена, номери телефонів, номери кредитних карток та будь-яка інша конфіденційна інформація.

«Згенерована відповідь, що містить конфіденційні дані користувача, коли вона використовується для відповіді на електронний лист, пізніше заражає нові хости», — говорить Нассі.

У другому методі, кажуть вчені, використовується зображення з вбудованою зловмисною підказкою, яке змушує помічника електронної пошти пересилати повідомлення іншим.

«Після кодування самовідтворюваної підказки будь-яке зображення, що містить спам, образливий матеріал або навіть пропаганду, може бути перенаправлено новим клієнтам», — пояснює Нассі.

Дослідники очікують на появу хробаків для генеративного штучного інтелекту в «диких» умовах вже у найближчі два-три роки. Також творці нового вірусу наголошують, що їхня робота є попередженням про недосконаліть архітектури екосистем зі штучним інтелектом. Вони повідомили про свої висновки Google й OpenAI…» ***(Створено вірус, здатний використовувати ChatGPT чи Gemini для викрадання даних // ТОВ «ІНФОРМАЦІЙНЕ АГЕНТСТВО „НЬЮЗ ФЛЕШ“» (https://ua.news/ua/technologies/stvoreno-virus-zdatnyj-vykorystovuvaty-chatgpt-chy-gemini-dlya-vykradannya-danyh). 05.03.2024).***

***

«Зловмисники ховають зловмисне програмне забезпечення у файлах зображень SVG, щоб уникнути виявлення та розповсюджувати програмне забезпечення-вимагач, завантажувати банківський троян і поширювати шкідливе програмне забезпечення.

У січні дослідники Cofense Intelligence спостерігали за двомісячною кампанією, яка використовувала файли SVG для доставки зловмисних програм Agent Tesla Keylogger і XWorm RAT. Дослідники радять командам безпеки нагадувати користувачам стежити за неочікуваними завантаженнями після відкриття файлу SVG, що є ознакою компромісу.

Файловий формат Scalable Vector Graphic використовує математичні рівняння для опису зображень, що дає змогу масштабувати їх без втрати якості зображення та робить їх придатними для різноманітних дизайнерських програм.

AutoSmuggle, інструмент із відкритим вихідним кодом, випущений у травні 2022 року, дозволяє суб'єктам загрози вставляти шкідливі файли у вміст SVG або HTML, обходячи заходи безпеки, такі як безпечні шлюзи електронної пошти, і збільшуючи шанси успішної доставки зловмисного програмного забезпечення.

Використання файлів SVG для доставки зловмисного програмного забезпечення вперше було помічено в 2015 році, але дослідники сказали, що хакери вдосконалили свою тактику, щоб обійти заходи безпеки та успішно поширювати шкідливі корисні дані. Файли SVG поширювали зловмисне програмне забезпечення Ursnif у 2017 році та використовувалися для контрабанди.zipархіви, що містять зловмисне програмне забезпечення QakBot 2022.

У кампаніях Agent Tesla Keylogger у грудні 2023 року та січні 2024 року електронні листи містили вкладені файли SVG, які під час відкриття доставлялися вбудованими.zipархіви. Ці архіви ініціювали серію завантажень корисного навантаження, кульмінацією яких стало виконання програми Agent Tesla Keylogger. Зловмисники модифікували файли SVG, згенеровані AutoSmuggle, щоб покращити свої можливості введення в оману.

Кампанії XWorm RAT включали різні ланцюжки зараження. Деякі використовували вбудовані посилання, що вели до файлів SVG, а інші використовували безпосередньо вкладені файли SVG.

Ці файли ініціювали завантаження.zipархіви, що містять корисні дані для виконання XWorm RAT. Файлам SVG, які використовувалися в цих кампаніях,

бракувало вишуканості, яка спостерігається в кампаніях Agent Tesla Keylogger, і вони містили порожні сторінки після відкриття.

Дослідники рекомендують надійні стратегії пом'якшення загроз зловмисного програмного забезпечення на основі SVG. Традиційні засоби захисту, які покладаються на розширення файлів, є недостатніми перед обличчям тактики розвитку шкідливих програм». ***(Prajeet Nair. Hackers Hiding Keylogger, RAT Malware in SVG Image Files // Information Security Media Group, Corp. (https://www.databreachtoday.com/hackers-hiding-keylogger-rat-malware-in-svg-image-files-a-24598?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 13.03.2024).***

***

«Японський технологічний гігант Fujitsu виявив, що кілька його систем заражені шкідливим програмним забезпеченням, і попереджає, що хакери вкрали дані клієнтів.

Fujitsu є шостим у світі постачальником IT-послуг, у якому працює 124 000 людей і має річний дохід 23,9 мільярда доларів. Його портфоліо включає комп'ютерні продукти, такі як сервери та системи зберігання даних, програмне забезпечення, телекомунікаційне обладнання та ряд послуг, включаючи хмарні рішення, системну інтеграцію та IT-консультаційні послуги.

Компанія має потужну присутність на світовому ринку, працюючи в понад 100 країнах. Він також підтримує багатогранні стосунки з урядом Японії, реалізуючи проекти в державному секторі, беручи участь у фінансованих державою науково-дослідних проектах і відіграючи вирішальну роль у національній безпеці країни.

Оголошення, опубліковане наприкінці минулого тижня на новинному порталі фірми, розкриває серйозний інцидент із кібербезпекою, який поставив під загрозу системи та дані, включаючи конфіденційну інформацію клієнтів.

«Ми підтвердили наявність зловмисного програмного забезпечення на кількох наших бізнес-комп’ютерах, і в результаті нашого внутрішнього розслідування було виявлено, що файли, що містять особисту інформацію та інформацію, пов’язану з нашими клієнтами, можуть бути незаконно видалені», — йдеться в повідомленні Fujitsu.

«Після підтвердження наявності зловмисного програмного забезпечення ми негайно ізолювали уражені бізнес-комп’ютери та вжили заходів, наприклад, посилили моніторинг інших бізнес-комп’ютерів».

Fujitsu каже, що продовжить розслідування того, як зловмисне програмне забезпечення потрапило в бізнес-системи та які дані воно викрало.

Хоча фірма заявляє, що не отримувала повідомлень про неправомірне використання даних клієнтів, вона повідомила про інцидент Комісію із захисту персональних даних і наразі готує індивідуальні повідомлення для постраждалих клієнтів.

BleepingComputer зв’язався з Fujitsu, щоб дізнатися, чи вплине витік даних на корпоративних клієнтів або споживачів, і дізнатися про кількість постраждалих фізичних/юридичних осіб, але коментар не був доступний.

Злом Fujitsu 2021

У травні 2021 року інструмент обміну інформацією Fujitsu ProjectWEB було використано для проникнення в офіси кількох японських державних установ, дозволивши отримати несанкціонований доступ і викрасти 76 000 адрес електронної пошти та конфіденційних даних.

Викрадені дані включали конфіденційну інформацію з урядових систем і потенційно дані управління повітряним рухом з міжнародного аеропорту Наріта.

Подальші розслідування, завершені в грудні 2021 року, показали, що хакери використовували вкрадені облікові дані ProjectWEB для виявлення злому.

Розслідування також виявило кілька вразливостей у ProjectWEB, який було припинено та пізніше замінено новим інструментом обміну інформацією, що включає заходи безпеки з нульовою довірою». ***(Bill Toulas. Fujitsu found malware on IT systems, confirms data breach // Bleeping Computer® LLC***

(https://www.bleepingcomputer.com/news/security/fujitsu-found-malware-on-it-systems-confirms-data-breach/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 18.03.2024).

***

«Бекдор WINELOADER, який використовувався в останніх кібератаках на дипломатичні установи з використанням фішингових приманок для дегустації вина, вважається роботою хакерської групи, пов'язаної зі Службою зовнішньої розвідки (СЗР) Росії, яка відповідала за злом SolarWinds і Microsoft.

Висновки надійшли від Mandiant, яка повідомила, що Midnight Blizzard (також відома як APT29, BlueBravo або Cosy Bear) використовувала зловмисне програмне забезпечення, щоб націлити на німецькі політичні партії фішингові електронні листи з логотипом Християнсько-демократичного союзу (ХДС) приблизно 26 лютого 2024 року.

«Це перший раз, коли ми бачимо, як цей кластер APT29 націлений на політичні партії, що вказує на можливу сферу оперативного фокусування, що виходить за межі типового націлювання на дипломатичні представництва дослідники Люк Дженкінс і Ден Блек», — заявили.

WINELOADER був вперше оприлюднений Zscaler ThreatLabz минулого місяця як частина кампанії кібершпигунства, яка, як вважають, триває принаймні з липня 2023 року. Вона приписувала діяльність кластеру під назвою SPIKEDWINE.

Мережі атак використовують фішингові електронні листи з німецькомовним вмістом-приманкою, який нібито є запрошенням на вечерю, щоб обманом змусити одержувачів натиснути фальшиве посилання та завантажити файл фальшивого HTML-додатку (HTA), початкового дроппера під назвою ROOTSAW (він же EnvyScout), який діє як канал для доставки WINELOADER з віддаленого сервера.

«Німецькомовний документ-приманка містить фішингове посилання, яке спрямовує жертв на шкідливий ZIP-файл, що містить програму ROOTSAW,

розміщену на скомпрометованому веб-сайті, контрольованому актором», — повідомили дослідники. «ROOTSAW надав другу стадію документа про приваблення CDU та наступну стадію корисного навантаження WINELOADER».

WINELOADER, викликаний за допомогою техніки під назвою DLL side-loading з використанням законного sqldumper.exe, оснащений можливостями зв'язуватися з сервером, яким керує актор, і отримувати додаткові модулі для виконання на скомпрометованих хостах.

Кажуть, що він має спільні риси з відомими сімействами шкідливих програм APT29, такими як BURNTBATTER, MUSKYBEAT і BEATDROP, що свідчить про роботу спільного розробника.

WINELOADER, відповідно до дочірньої компанії Google Cloud, також брав участь в операції проти дипломатичних установ у Чехії, Німеччині, Індії, Італії, Латвії та Перу наприкінці січня 2024 року.

«ROOTSAW продовжує залишатися центральним компонентом початкових зусиль APT29 щодо доступу до збору іноземної політичної розвідки», - заявили в компанії.

«Розширене використання зловмисного ПЗ на першому етапі для націлювання на політичні партії Німеччини є помітним відхиленням від типової дипломатичної спрямованості цього підкластера APT29 і майже напевно відображає зацікавленість SVR у зборі інформації від політичних партій та інших аспектів громадянського суспільства, яка могла б просувати Москву. геополітичні інтереси».

Ця подія сталася після того, як німецька прокуратура висунула звинувачення військовому офіцеру на ім'я Томас Х. у шпигунстві після того, як він нібито був спійманий у шпигунстві від імені російських спецслужб і передачі невизначеної конфіденційної інформації. Його затримали у серпні 2023 року.

«З травня 2023 року він кілька разів з власної ініціативи звертався до генконсульства Росії в Бонні та посольства РФ у Берліні та пропонував співпрацю», – повідомили в офісі федерального прокурора. «Одного разу він передав інформацію, отриману в ході професійної діяльності, для передачі російській

розвідці». ***(Russian Hackers Use 'WINELOADER' Malware to Target German Political Parties // The Hacker News (https://thehackernews.com/2024/03/russian-hackers-use-wineloader-malware.html). 23.03.2024).***

***

Програми-вимагачі

«Група програм-вимагачів, відповідальна за два тижні стримування ринку ліків, що відпускаються за рецептом, раптово пішла нанівець, лише через кілька днів після того, як отримала платіж у розмірі 22 мільйонів доларів і була звинувачена в шахрайстві у шахрайстві афілійованої особи, яка відібрала свою частку здобичі.

Події стосуються AlphV, групи програм-вимагачів, також відомої як BlackCat. Два тижні тому він ліквідував Change Healthcare, найбільшу компанію з обробки платежів у сфері охорони здоров'я в США, змусивши аптеки, постачальників медичних послуг і пацієнтів з усіх сил виписувати рецепти на ліки. У п'ятницю, як показує бухгалтерська книга біткойнів, група отримала майже 22 мільйони доларів у криптовалюті, викликаючи підозри, що депозит був сплачений Change Healthcare в обмін на те, що AlphV розшифрує його дані та пообіцяє їх видалити.

Представники Optum, материнської компанії, відмовилися повідомити, чи виплатила компанія AlphV.

Честь серед злодіїв

У неділю, через два дні після платежу, сторона, яка стверджує, що є філією AlphV, заявила на кримінальному онлайн-форумі, що платіж у розмірі майже 22 мільйонів доларів був пов'язаний зі зломом Change Healthcare. Партія також заявила, що члени AlphV обдурили афілійовану компанію щодо узгодженого скорочення платежу. У відповідь афілійована компанія заявила, що не видалила отримані дані Change Healthcare.

У вівторок — через чотири дні після того, як було здійснено платіж у біткойнах, і через два дні після того, як афілійована особа заявила про те, що її обманом відмовили — на загальнодоступному темному веб-сайті AlphV почало відображатися повідомлення про те, що його вилучило ФБР відповідно до міжнародного права. виконавчі дії.

Національне агентство зі злочинності Великої Британії, одне з агентств, яке, як повідомляється в повідомленні про конфіскацію, бере участь у вилученні, заявило, що агентство не бере участі в будь-якій подібній дії. ФБР, тим часом, відмовилося від коментарів. Спростування NCA, а також докази того, що повідомлення про конфіскацію було скопійовано з іншого сайту та вставлено в AlphV, змусили багатьох дослідників зробити висновок, що група програм-вимагачів інсценувала видалення та забрала собі всю суму в розмірі 22 мільйонів доларів.

«Оскільки люди продовжують піддаватися прикриттю ALPHV/BlackCat: ALPHV/BlackCat не було конфісковано», — написав у соцмережах Фабіан Восар, керівник відділу дослідження програм-вимагачів у фірмі безпеки Emsisoft. «Вони обманюють своїх філій. Це явно очевидно, коли ви перевіряєте вихідний код нового повідомлення про видалення».

Восар супроводив свій пост зображенням, на якому показано джерело сторінки, використане для рендерингу ймовірно конфіскованої домашньої сторінки AlphV. Джерело вказало, що зображення в повідомленні про арешт було скопійовано за допомогою команди «Файл» > «Зберегти сторінку як» у браузері Tor. У грудні ФБР і партнери з правоохоронних органів у всьому світі фактично закрили багато серверів, які використовував AlphV, і деякий час на сайті AlphV відображалося зображення, ідентичне тому, що з’явилося на сайті, який AlphV з’явився після видалення. Восар та інші дослідники припустили, що учасники AlphV просто скопіювали зображення зі старішого сайту та вставили його на новий.

На момент публікації цього допису на Ars здавалося, що джерело конфіскованого сайту було змінено, щоб видалити докази, які були скопійовані з інших місць.

Вихід зліва

Низка подій свідчить про те, що після отримання 22 мільйонів доларів AlphV вирішила піти на пенсію або принаймні піти на тимчасову перерву перед реформуванням у нову групу, що є звичайним кроком серед груп програм-вимагачів, коли вони потрапляють у поле зору правоохоронних органів. Замість того, щоб платити філії, AlphV вирішив залишити всю суму. Потім, замість того, щоб бути прозорим щодо виходу, AlphV опублікував підроблене повідомлення про вилучення, щоб створити враження, що його закривають правоохоронні органи.

Якщо припущення правильні, то найбільш значущою подією у всій низці подій є претензія, яку афілійована особа висунула на кримінальному форумі. Це означає, що хтось виклав 22 мільйони доларів в обмін на його дані та обіцянку, що вони будуть видалені третіми особами. «Notchy», ім’я якого використовує особа, яка називає себе афілійованою особою, стверджує, що володіє 4 терабайтами «критичних» даних Change Healthcare.

Вперше AlphV було помічено наприкінці 2021 року, коли він з’явився з ніколи раніше не баченим шифрувальником, який працював як у Windows, так і в Linux. Він примушував жертв до платежів, використовуючи модель потрійного вимагання, яка (1) шифрувала дані, (2) погрожувала оприлюднити їх і (3) здійснювала розподілені атаки на інфраструктуру жертви. Як і більшість аналогів, AlphV працює за моделлю програм-вимагачів як послуги, у якій основна група надає програмне забезпечення-вимагач та інфраструктуру та звертається до афілійованих осіб для фактичного злому жертв. Тоді обидві сторони отримують частину будь-яких доходів.

ФБР заявило, що кілька членів AlphV мають зв’язки з DarkSide, групою програм-вимагачів, яка раптово припинила роботу після зламу Colonial Pipeline, одного з найбільших постачальників бензину в США. Багато дослідників вважають, що DarkSide призупинила роботу після того, як атака на Colonial Pipeline

привернула занадто багато уваги з боку правоохоронних органів. Потім, деякий час залишаючись бездіяльною, група перейменувала себе в AlphV/BlackCat.

Вихід AlphV у цей момент має сенс. Минулого місяця ФБР завдало серйозного удару іншій групі програм-вимагачів, відомій як Lockbit. Ступінь збою, включно з повною компрометацією веб-сайту Lockbit і десятків його серверів, можливо, викликав достатнє занепокоєння на ринку програм-вимагачів у цілому, і AlphV вирішила, що зараз саме час заховатися.

Хоча призупинення однієї з найпотужніших груп програм-вимагачів може бути хорошою новиною для багатьох, це менш актуально для афілійованої компанії та ще гірше для Change Healthcare». ***(Dan Goodin. After collecting $22 million, AlphV ransomware group stages FBI takedown // Condé Nast (https://arstechnica.com/security/2024/03/alphv-ransomware-site-claims-it-was-seized-by-fbi-researchers-suspect-22m-scam/?utm_source=flipboard&utm_content=user%2FArsTechnica). 06.03.2024).***

***

«Атака програми-вимагача, спрямована на медичну компанію Change Healthcare, була однією з найруйнівніших за останні роки, завдавши шкоди аптекам у США, включно з лікарнями, і призвела до серйозних збоїв у доставці ліків, що відпускаються за рецептом, по всій країні протягом 10 днів і далі. Тепер суперечка в кримінальному підпіллі виявила новий розвиток цієї катастрофи: один із партнерів хакерів, які стоять за атакою, зазначає, що ці хакери, група, відома як AlphV або BlackCat, отримали транзакцію на 22 мільйони доларів, яка виглядає дуже дуже схоже на великий викуп.

1 березня біткойн-адреса, підключена до AlphV, отримала 350 біткойнів за одну транзакцію, або близько 22 мільйонів доларів США за курсом обміну на той час. Потім, через два дні, хтось, назвавши себе філією AlphV — один із хакерів, які працюють з групою, щоб проникнути в мережі жертв, — написав на підпільному форумі кіберзлочинців RAMP, що AlphV обманом позбавила їх частки викупу

Change Healthcare., вказуючи на загальнодоступну транзакцію на 22 мільйони доларів у блокчейні біткойна як доказ.

За словами Дмитра Смілянця, дослідника охоронної фірми Recorded Future, який першим помітив публікацію, це свідчить про те, що Change Healthcare, ймовірно, заплатила викуп AlphV. «Ви можете побачити кількість монет, які туди впали. Таку трансакцію не так часто побачиш», – каже Смілянець. «Є докази потрапляння великої суми в біткойн-гаманець, контрольований AlphV. І ця афілійована особа пов'язує цю адресу з атакою на Change Healthcare. Тож цілком ймовірно, що жертва заплатила викуп».

Представник Change Healthcare, яка належить UnitedHealth Group, відмовився відповісти, чи заплатила вона викуп AlphV, сказавши WIRED лише, що «ми зараз зосереджені на розслідуванні».

І Recorded Future, і TRM Labs, фірма з аналізу блокчейнів, пов'язують біткойн-адресу, на яку надійшов платіж у розмірі 22 мільйонів доларів, із хакерами AlphV. TRM Labs каже, що може пов'язати адресу з платежами від двох інших жертв AlphV у січні.

Якщо Change Healthcare справді заплатить викуп у розмірі 22 мільйонів доларів, це стане не лише величезною зарплатою для AlphV, але й стане небезпечним прецедентом для галузі охорони здоров'я, стверджує Бретт Каллоу, дослідник програм-вимагачів із фірми безпеки Emsisoft. Кожен платіж за програму-вимагач, каже він, одночасно фінансує майбутні атаки відповідальної групи та пропонує іншим хижакам-вимагачам спробувати ту саму ігру — у цьому випадку атакувати послуги охорони здоров'я, від яких залежать пацієнти.

«Якщо Change платив, це проблематично», — каже Каллоу. «Це підкреслює прибутковість атак на сектор охорони здоров'я. Угруповання програм-вимагачів — це нічого, якщо не передбачити: якщо вони знайдуть певний сектор прибутковим, вони атакуватимуть його знову і знову, промиватимуть і повторять».

Філія AlphV, яка сама себе назвала філією, яка першою опублікувала докази платежу на RAMP і яка носить ім'я «notchy», поскаржилася, що AlphV, очевидно, отримала викуп у розмірі 22 мільйонів доларів від Change Healthcare, а потім

залишила всю суму, замість того, щоб поділитися нею. прибуток зі своїм партнером-хакером, як вони нібито домовилися. «Будьте обережні та припиніть справу з ALPHV», — написав Нотчі.

Цей афілійований хакер також написав, що під час проникнення в мережу Change Healthcare вони отримали доступ до даних багатьох інших медичних фірм, які є партнерами компанії. Якщо це твердження правдиве, зазначає Смілянець із Recorded Future, це створює додатковий ризик того, що афілійований хакер все ще володіє конфіденційною медичною інформацією. Навіть якби Change Healthcare платила AlphV, афілійована хакерська компанія все одно могла вимагати додаткову оплату або витік даних самостійно.

«Філії досі мають ці дані, і вони бісляться, що не отримали ці гроші», — каже Смілянець. «Це хороший урок для всіх. Ви не можете довіряти злочинцям; їхнє слово нічого не варте».

З огляду на виплати програм-вимагачів, 22 мільйони доларів становлять надзвичайно прибуткову оцінку для AlphV. Лише відносно невелика кількість викупів в історії програм-вимагачів, як-от платіж у розмірі 40 мільйонів доларів, здійснений фінансовою компанією CNA хакерам, відомим як Evil Corp, була настільки великою, каже Каллоу з Emsisoft. «Це не без прецедентів, але це, безумовно, дуже незвично», — каже він.

Незалежно від того, чи підтверджено, що Change Healthcare сплатила цей викуп, атака показує, що AlphV здійснив тривожне повернення: у грудні він був об’єктом операції ФБР, яка захопила його темні веб-сайти та оприлюднила ключі дешифрування, які завадили його атакам. на сотні жертв. Всього через два місяці вона здійснила кібератаку, яка паралізувала Change Healthcare, спровокувавши збій, який вплинув на аптеки та їхніх пацієнтів уже більше тижня. Станом на минулий вівторок AlphV перелічила 28 компаній на темному веб-сайті, який використовує для вимагання своїх жертв, не враховуючи Change Healthcare.

Зараз цей сайт вимкнено. Станом на вівторок вранці на ньому містилося те, що було схоже на повідомлення про вилучення правоохоронними органами, але дослідник безпеки Фабіан Восар зазначає, що повідомлення, здається, було

скопійоване з останнього видалення AlphV. Причина зникнення групи — чи через іншу операцію правоохоронних органів, чи через спроби AlphV ухилитися від власних ошуканих афілійованих осіб — незрозуміла. Трекери програм-вимагачів кажуть, що AlphV уже кілька разів зникав і змінював бренд. Дослідники безпеки відзначають, що попередні втілення під назвами BlackCat, BlackMatter і Darkside були більш-менш однією групою.

Насправді хакери, які працювали під керівництвом Darkside, відповідальні за атаку програми-вимагача Colonial Pipeline у 2021 році, яка призвела до припинення транспортування газу через східне узбережжя США та призвела до короткочасної нестачі палива в деяких містах східного узбережжя. У цьому випадку також жертви заплатили хакерам викуп. «Це було найважче рішення, яке я приймав», — заявив генеральний директор Colonial Джозеф Блаунт пізніше на слуханнях у Конгресі США.

Тепер, здається, деякі з тих самих хакерів, можливо, змусили іншу компанію прийняти таке ж важке рішення». ***(Andy Greenberg. Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment // Condé Nast (https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/?utm_source=flipboard&utm_content=lks2017%2Fmagazine%2FInet+Scams%2FComputing+Tips%2FTech+Updates%2FInteresting+Snippets+from+the+Ether). 04.03.2024).***

***

«У четвер Агентство з кібербезпеки та безпеки інфраструктури опублікувало консультаційне попередження про відомі методи кібератак і ознаки компрометації, щоб допомогти організаціям державного сектору краще захистити себе від програм-вимагачів, зокрема від загрозливого актора Фобоса.

У повідомленні йдеться, що з 2019 року Phobos, постачальник програм-вимагачів як послуг, націлив на ІТ-системи муніципальних і окружних органів влади, екстрених служб, навчальних закладів, систем охорони здоров’я та іншої

критичної інфраструктури. Програмне забезпечення-вимагач як послуга, або RaaS, дозволяє тим, хто має мінімальний технічний досвід, запускати атаки програм-вимагачів за допомогою попередньо розроблених інструментів.

Ренді Роуз, віце-президент із операцій із забезпечення безпеки та розвідки в Центрі безпеки в Інтернеті, некомерційній організації штату Нью-Йорк, яка керує Міждержавним центром обміну та аналізу інформації, який фінансується федеральним бюджетом, сказав, що він спостерігав зростання частоти кібератак RaaS у державному секторі в В останні роки.

«Phobos — досить стандартна програма-вимагач», — сказала Роуз StateScoop. «Ми бачимо їх у [державному, місцевому, племінному та територіальному] секторі, що є однією з причин, чому ми приділяємо їм багато уваги».

Хоча CISA та інші федеральні агентства радять не здійснювати платежі за програми-вимагачі, оскільки вони не гарантують, що дані, отримані хакерами, більше не будуть скомпрометовані або призведуть до відновлення служб і даних, CISA каже, що Фобос отримав кілька мільйонів доларів США у вигляді платежів за програми-вимагачі. його жертви.

Згідно зі звітом Міністерства охорони здоров'я та соціальних служб США за 2021 рік, середній платіж за програму-вимагач Phobos становить приблизно 38 100 доларів США.

«Інциденти з програмами-вимагачами Phobos, які впливають на державні, місцеві, племінні та територіальні органи влади, регулярно повідомляються в [Міждержавний центр обміну та аналізу інформації]», — йдеться в повідомленні, хоча незрозуміло, скільки випадків програм-вимагачів Phobos може претендувати.

У 2023 році Служба безпеки повідомила, що «експерти приписують групі 67 атак у травні 2023 року», причому більшість жертв перебувають у США чи Бразилії.

Методи програм-вимагачів

У повідомленні CISA сказано, що програма-вимагач Phobos використовує два основні методи отримання доступу до системи. Одна з них – це фішинг, практика викрадення даних для входу в обліковий запис шляхом обману, щоб люди

відкривали шкідливі вкладення електронної пошти. Інший – отримання прямого доступу за допомогою протоколу віддаленого робочого столу, мережевого інструменту Microsoft, який дозволяє користувачам віддалено керувати комп'ютерами.

Роуз сказав, що фішингові кампанії, подібні до програм-вимагачів Phobos, є, безумовно, найпоширенішою та найефективнішою тактикою, яка використовується в кібератаках, не тому, що їх найпростіше розгорнути, а тому, що вони використовують людські слабкості.

«Фішинг — це атака соціальної інженерії, чи не так? Ми любимо натискати на речі, [тому що] ми цікаві люди, ми цікаві створіння. І нами також легко маніпулювати», – сказала Роуз. «Ось чому фокусники досі дурять людей, менталістів, ілюзіоністів і людей, які розмовляють із мертвими, ніби ми хочемо вірити в такі речі».

Він також сказав, що фішингові листи стає все важче і важче виявити, частково через генеративний штучний інтелект.

«Generate AI може допомогти вам написати надзвичайно переконливий фішинговий електронний лист», — сказав Роуз. «Я не думаю, що ми побачимо кінець фішингу як обраного вектора вторгнення для цих учасників просто тому, що він настільки ефективний. І тому що тепер у нас є ці інструменти, які, по суті, роблять його ефективнішим».

Генеративний ШІ для захисту від програм-вимагачів

Роуз вважає, що генеративний штучний інтелект також можна використовувати для боротьби з більш складними фішинговими кампаніями.

«Я думаю, що штучний інтелект суттєво допоможе нам у захисті», — сказав Роуз. «Ми зможемо бачити речі, які ніхто інший, жодна людина не зможе виявити самостійно, і ми використовуватимемо штучний інтелект, щоб допомогти виявити та запобігти цьому».

Щойно Phobos отримує доступ, йдеться в повідомленні, програма-вимагач встановлюється в ключові місця, такі як папка запуску Windows, і створює нові ключі реєстру в операційній системі. Потім він націлює локальні користувацькі

файли та мережеві спільні файли та відстежує нові файли, які відповідають вимогам шифрування, включаючи документи, часто використовувані папки та інші носії. Потім зловмисник вимагає від своїх жертв викуп в обмін на ключ дешифрування.

Оскільки не існує жодного дешифратора Phobos, окрім тих, які є у розробників програм-вимагачів, CISA рекомендує захистити протокол віддаленого робочого столу, використовувати надійні паролі та політику блокування облікових записів, використовувати багатофакторну автентифікацію, використовувати віртуальні приватні мережі та регулярне оновлення програмного забезпечення — все це найкращі практики, які давно визнані. в інформаційній безпеці». ***(Sophia Fox-Sowell. CISA warns state, local government about Phobos ransomware // statescoop (https://statescoop.com/cisa-phobos-ransomware-state-local-government/?utm_source=flipboard&utm_content=untangledcj%2Fmagazine%2FMSP1337+Cybersecurity+News). 01.03.2024).***

***

«LockBit є однією з найактивніших груп програм-вимагачів у світі, відповідальних за значну частку глобальних кібератак і витоків даних з моменту свого дебюту в кінці 2019 року. LockBit працює як «програмне забезпечення-вимагач як послуга» (RaaS), за допомогою якого найняті філії можуть використовувати програмне забезпечення-вимагач LockBit для націлювання на організації в різних секторах і юрисдикціях.

LockBit продає своє програмне забезпечення-вимагач (або його варіанти) афілійованим особам, беручи 20% будь-якої виплати викупу, а як організація RaaS вони надають своїм афілійованим особам індивідуальні шифрувальники, доступ до сайту витоку темної мережі LockBit, а іноді допомагають у переговорах щодо викупні платежі.

За останні чотири роки LockBit нібито спричинив глобальні збитки на мільярди (£) через виплати викупу та втрати від відновлення бізнесу. Через широкий спектр міжнародних афілійованих осіб LockBit часто важко передбачити

їхню тактику, методи та процедури (TTP) для кожного окремого кіберінциденту, тому правоохоронним органам непросто відстежити LockBit і спробувати знищити їх інфраструктура.

Операція Кронос

19 лютого 2024 року Національне агентство з боротьби зі злочинністю Великої Британії (NCA) та ФБР разом з дев'ятьма іншими міжнародними агентствами координували операцію «Cronos», яка передбачала конфіскацію сайту витоку LockBit у темній мережі та «безпрецедентний» доступ до систем та інфраструктури LockBit.

Після захоплення інфраструктури та серверів LockBit ці агентства змогли переробити аспекти сторінки, щоб відобразити конфісковані елементи роботи LockBit (подібно до того, як поліція демонструє наркотики чи зброю). Це включало:

Випуск інструменту дешифрування, який допоможе організаціям, які зараз або раніше були жертвами варіанту програм-вимагачів LockBit.

Вилучення біткоін-гаманців, пов’язаних із виплатою викупу.

Виготовлення списку всіх відомих афілійованих осіб LockBit і введення проти них різних санкцій, звинувачень і арештів.

Наведення доказів того, що LockBit зберігав дані жертв після сплати викупу.

Дешифратори

Правоохоронним органам вдалося отримати та оприлюднити понад 1000 ключів дешифратора, які дозволять організаціям, які стали жертвами атаки програм-вимагачів LockBit, потенційно відновити свої системи та розшифрувати дані та/або пристрої, які колись вважалися неможливими для відновлення. Детальніше про вплив дешифраторів нижче.

Bitcoin

Правоохоронним органам вдалося заморозити приблизно 200 біткойн-гаманців і виявити, що з липня 2022 року по лютий 2024 року понад 126 мільйонів доларів США в біткойнах було переведено через 30 000 облікових записів, пов’язаних з LockBit.

Приблизно 114 мільйонів доларів США в біткойнах залишилися недоторканими на рахунках LockBit, які складалися з платежів викупу та комісій партнерів LockBit.

Арешти, звинувачення та санкції щодо афілійованих осіб LockBit

Правоохоронні органи оприлюднили особи понад 190 афілійованих осіб LockBit та їхні псевдоніми. Афілійовані особи – це організації або окремі особи, які працюють безпосередньо з LockBit для цільових організацій по всьому світу.

Українські та польські органи влади змогли заарештувати трьох філій LockBit, розташованих у Польщі та Україні, а Міністерство юстиції США висунуло звинувачення та застосувало санкції до двох росіян, які пов'язані з LockBit.

Крім того, NCA виявило, що LockBitSupp, очевидний лідер LockBit, спілкувався з правоохоронними органами, і NCA оголосило, що їм відомо про його особу, де він живе та скільки він коштує.

LockBit «видаляє» дані після виплати викупу

Тактика вимагання LockBit включала крадіжку та витік даних жертви, якщо викуп не був сплачений. І навпаки, LockBit «пообіцяв» видалити всі викрадені дані після отримання платежу викупу. Правоохоронним органам вдалося виявити, що LockBit зберігав викрадені дані від жертв, які платили викупи через сайти спільного використання, такі як mega.nz, або на власних серверах LockBit.

Звичайно, ніколи немає впевненості щодо того, виконав загрозливий суб'єкт обіцянку видалити дані чи ні. Новина про те, що LockBit не виконав своїх обіцянок, підкреслить, що такі обіцянки суб'єктів загрози є ненадійними.

LockBit повертається на поверхню

Через кілька днів після того, як операція Cronos знищила діяльність LockBit, зловмисники знову з'явилися на поверхні, перейшовши на новий темний веб-сайт і назвавши більше жертв.

LockBit оголосив про активацію своєї інфраструктури та нових афілійованих доменів, але для відновлення їхньої афілійованої мережі потрібен час. У заяві, опублікованій на їхній новій темній веб-сторінці, вони зазначили, що деякі з їхніх

конкурентів також можуть бути скомпрометовані, і що вони доручили своїм філіям розпочати націлювання на урядові установи США.

Відродження LockBit не було несподіваним. Декілька коментаторів публічно применшували значення операції «Кронос», зазначивши, що зусилля правоохоронних органів із ліквідації є еквівалентом «удару по кроту», коли суб'єкти загрози просто знову з'являються в іншому місці.

Проте те, що LockBit знову з'явився, не означає, що операція Cronos стала невдалою, і це не означає, що вона була марною. Дійсно, ми підозрюємо, що правоохоронні органи очікували, що LockBit знову з'явиться в інших місцях. Дії проти LockBit не просто ліквідували сайт витоку LockBit, а й демонструють той факт, що правоохоронні органи змогли отримати дешифратори, заморозити криптоактиви, виявити афілійованих осіб і застосувати серйозні санкції до окремих осіб. Він встановлює, що групи суб'єктів загрози не діють безкарно, мають власні вразливі місця та мають що втрачати.

Що це означає для організацій?

Полегшення для організацій

З випуском інструментів дешифрування, клієнти та/або власники полісів, які все ще можуть мати незашифровані дані та системи від попередніх або поточних атак LockBit, тепер можуть покладатися на випущений дешифратор для відновлення своїх систем без необхідності виплачувати викуп або взагалі вести переговори. Ми знаємо, що ФБР, NCA та інші правоохоронні органи активно зверталися до жертв, щоб запропонувати свою допомогу, надавши дешифратор і сприяючи його впровадженню.

Зберігання зашифрованих даних

Отримання інструменту дешифрування також викликає у клієнтів питання: як довго організація повинна зберігати зашифровані дані чи пристрої в надії, що дешифратор може стати доступним у майбутньому? З успіхом операції «Кронос» стає очевидним, що правоохоронні органи можуть скоординовано знищувати групи загроз і отримати один із найважливіших інструментів, необхідних організаціям, — дешифратор. Крім того, наслідки операції «Кронос» і майбутні операції

відкривають дискусію про те, чи буде вказівкою та/або хорошою практикою для організацій зберігати свої зашифровані дані/пристрої, щоб потенційно зменшити регуляторні дії. Однак, якщо організації зберігають достатньо резервних копій, судові слідчі можуть проявити обережність, перебудувавши мережу жертви та знищивши/повторно використавши зашифровані диски чи пристрої, а не залишаючи їх у бездіяльному стані, щоб швидко й ефективно налагодити роботу організації.

Регулятори

Буде цікаво подивитися, як регуляторні органи у Великій Британії та інших юрисдикціях змінять свої погляди на те, що є безповоротною втратою даних під час перегляду регуляторних заходів після інциденту LockBit, враховуючи, що правоохоронні органи надали розширені інструменти дешифрування, які інакше були недоступні в аналогічному масштабі.

Судово-медичні докази

Загальноприйнято стверджувати, що «не було доступних судово-медичних доказів», які організація могла б розкрити зацікавленим сторонам у результаті шифрування. Однак з випуском комплексних дешифраторів для колишніх і поточних жертв це може змінити зручний історичний висновок щодо порушень LockBit.

Звітність

Оскільки NCA разом із ФБР очолює операцію Cronos, це показує обнадійливий і чіткий приклад того, чому сповіщення та залучення Action Fraud, Національного центру кібербезпеки та NCA з першого дня може призвести до обнадійливих результатів. Очевидно, що підтримка практиками посиленого звітування державним установам може лише допомогти майбутнім жертвам кібератак». ***(Hans Allnutt and Pavan Trivedi. Lockbit: Locked down // DAC Beachcroft (https://www.dacbeachcroft.com/en/What-we-think/LockBit-Locked-down). 08.03.2024).***

***

«Більше ніж через два місяці після атаки програм-вимагачів, які залишили веб-сайт, каталог і внутрішню мережу в автономному режимі на кілька тижнів, представники Лондонської публічної бібліотеки кажуть, що їм вдалося в основному повернути все до нормального стану.

Проте деталі інциденту все ще невідомі, зокрема, хто за ним стоїть, скільки даних було зібрано та загальна вартість усунення збитків.

«Я вважаю, що веб-сайт — єдина загальнодоступна річ, яку нам не вдалося повністю відновити. Але здебільшого ми майже повністю відновилися», — сказав Майкл Чікконе, генеральний директор бібліотеки та головний бібліотекар.

«Ми просто маємо деякі проблеми, завершуємо деякі деталі кодування, але, сподіваюся, це повернеться відносно скоро».

Кібератака 13 грудня спричинила масові збої в системі бібліотеки, змусивши її тимчасово закрити деякі філії та надати безкоштовний кредитний моніторинг співробітникам після того, як стало відомо, що особисту інформацію деяких співробітників було зламано.

Досі не зрозуміло, хто стоїть за атакою програм-вимагачів, і чи була спеціально спрямована бібліотека. Більшість атак програм-вимагачів здійснюються випадковим чином за допомогою фішингових кампаній або використання невиправлених уразливостей мережі.

Офіційні особи бібліотеки не скажуть, як програмне забезпечення-вимагач заразило їхню мережу, лише те, що це не був фішинговий інцидент і що її каталог і веб-сайт не винні.

Вони також додають, що це не було результатом зламу стороннього постачальника чи організації спільного обслуговування, як у випадку з програмою-вимагачем, яка вразила п’ять лікарень на південному заході Онтаріо в жовтні.

Доступ до онлайн-каталогу бібліотеки та до веб-порталу для відвідувачів бібліотеки було відновлено в середині січня разом з іншими цифровими послугами, такими як доступ до OverDrive та платформ аудіокниг, згідно з веб-сайтом бібліотеки.

Кібератака змусила бібліотеку посилити свою IT-інфраструктуру, над чим, за словами Чікконе, вона працювала.

«У нас були плани, просто через те, що у нас немає зіркового бюджету, нам довелося повільно розвивати цю кібербезпеку, і це, ймовірно, зрештою зашкодило нашій можливості справді запобігти цьому», — сказав він. сказав.

«Ми вели розмови, я думаю, майже щомісяця, про це, і наш IT-директор повідомляв нам про те, що він планує робити. Ми не встигли».

Цього тижня електронні системи Лондонської публічної бібліотеки були вимкнені через «кіберінцидент». Чарльз Фінлей, виконавчий директор Rogers CyberSecure Catalyst з Університету Торонто Метрополітен, приєднався до London Morning, щоб поговорити про те, чому бібліотечні системи стають все більш мішенню та чому державні установи не витрачають достатньо, щоб зупинити це.

Бібліотека не заплатила викупу, щоб відновити роботу своїх систем, і повний обсяг вкрадених даних ще не відомий, але він був «невеликим», сказав Чікконе. Вони також не знають, чи було це опубліковано в так званій темній мережі.

За його словами, організація співпрацювала з поліцією для розслідування інциденту та виконала свої зобов’язання перед уповноваженим з питань інформації та конфіденційності Онтаріо.

Залишається з’ясувати, скільки бібліотеці довелося витратити на пом’якшення наслідків атак програм-вимагачів і посилення захисту від майбутніх атак. Чікконе знає лише те, що «це було недешево».

«Експертиза недешева. Є юридичні аспекти, які недешеві. Це, звичайно, не близько мільйона, але це досить дорого», - сказав він.

«Я не хочу спекулювати, доки не отримаю всі цифри... Нам довелося зробити деякі оновлення, які, ймовірно, коштують значних грошей».

Відновлення після програм-вимагачів – це дороге завдання. Минулого року Сент-Мерік, Онтаріо. повідомила про витрати щонайменше 1,3 мільйона доларів на розслідування та відновлення після атаки програм-вимагачів, з якою зіткнулася минулого літа.

Інцидент із кібербезпекою в лондонській бібліотеці стався через два місяці після того, як системи публічної бібліотеки Торонто були пошкоджені серйозною атакою програм-вимагачів, від якої вони все ще оговтуються.

Представники бібліотеки в Торонто раніше заявляли, що в результаті інциденту, ймовірно, було виявлено імена, номери соціального страхування, державні ідентифікаційні документи та адреси співробітників, починаючи з 1998 року». **(Matthew Trevithick. London library 'almost fully recovered' from ransomware attack, CEO says // CBC/Radio-Canada (https://www.cbc.ca/news/canada/london/london-library-ransomware-almost-recovered-1.7131984). 07.03.2024).**

***

«Сумно відоме угруповання програм-вимагачів Lockbit все ще активно та передало дані про п’ять кібератак цього тижня, незважаючи на глобальне проникнення правоохоронних органів минулого місяця.

За даними фірми з кібербезпеки Falcon Feeds, у четвер Lockbit нібито опублікував дані п’яти нових жертв на своєму темному веб-сайті. Жертвами виявилися дві американські виробничі фірми, американська інженерна інфраструктурна компанія, канадська нафтова та енергетична компанія та британська бухгалтерська фірма.

Але Бретт Каллоу, аналітик загроз Emsisoft, повідомляє PCMag електронною поштою, що Lockbit представляє дані як нові атаки, тоді як насправді група програм-вимагачів просто пропонує нові дані. «Жодна з нових публікацій Lockbit, здається, не стосується нових інцидентів. Вони публікують дані про старі атаки, ймовірно, намагаючись відновити свою репутацію та переконати афілійованих осіб та інших ділових партнерів, що все добре (а це не так)» Каллоу каже.

«Оскільки компанії часто не оприлюднюють подробиці інцидентів, неможливо сказати напевно, але донедавна здавалося, що вони публікували дані про старі інциденти», — продовжив Каллоу.

Міністерство юстиції США, ФБР, а також Національне агентство зі злочинності Великобританії (NCA) та інші залучені агентства раніше заявили, що скомпрометували операції Lockbit. ФБР вилучило сервери Lockbit, правоохоронні органи вилучили приблизно 1000 ключів дешифрування, а NCA заявило, що «зламало хакерів».

Але протягом тижня після новин хакери програм-вимагачів Lockbit повернулися в мережу, стверджуючи, що змогли зберегти свої сервери резервного копіювання, які не використовували PHP, який, як повідомляється, був засобом доступу урядових установ.

Минулого місяця в Україні було заарештовано двох передбачуваних філій Lockbit, а США ідентифікували двох росіян, які ймовірно пов'язані з групою програм-вимагачів, і закликали до їх арешту. Цього місяця ще одного раніше заарештованого російсько-канадського учасника Lockbit засудили до чотирьох років ув'язнення за зараження понад 1000 жертв програмним забезпеченням-вимагачем Lockbit.

Але діяльність групи, схоже, триває. Передбачуваний анонімний керівник Lockbit заявив в інтерв'ю виданню The Record цього тижня, що вони продовжують атакувати жертв і що хоча деякі члени Lockbit «злякалися», «більшість» все ще працюють над розгортанням атак програм-вимагачів.

«ФБР не змогло повністю знищити мою інфраструктуру», — сказав керівник Lockbit.

Раніше NCA повідомило PCMag, що очікує, що Lockbit спробує відродитися, і заявило, що продовжить працювати над ліквідацією групи.

Програмне забезпечення Lockbit використовувалося для атак на Boeing, стоматологічні страхові компанії та Subway. Комп'ютери Apple Silicon Mac теж не застраховані». ***(Kate Irwin. Lockbit Strikes Back After FBI Takedown With New Ransomware Attack Details // Ziff Davis, LLC. (https://au.pcmag.com/security/104399/lockbit-strikes-back-after-fbi-takedown-with-new-ransomware-attack-***

details?utm_source=flipboard&utm_content=LeBui2014%2Fmagazine%2FSecuCybe). 16.03.2024).

***

«Програмне забезпечення-вимагач залишається постійною загрозою, незважаючи на дії правоохоронних органів, спрямовані на знищення інфраструктури загроз, на яку покладаються суб'єкти для здійснення своїх атак, згідно з останньою щорічною оцінкою загроз Управлінням директора національної розвідки.

«Транснаціональні організовані злочинці, задіяні в операціях з програми-вимагачами, вдосконалюють свої атаки, вимагають кошти, порушують роботу критично важливих служб і розкривають конфіденційні дані», — йдеться у звіті, опублікованому в понеділок. «Важливі служби та критична інфраструктура США, такі як охорона здоров'я, школи та виробництво, продовжують зазнавати атак програм-вимагачів».

Керівники національної розвідки попередили, що проблема програм-вимагачів загострюється, і боротися з нею стає все важче.

Керівники розвідувальних агенцій уряду США, включаючи ЦРУ, ФБР, Агентство національної безпеки, Державний департамент, Розвідувальне управління Міністерства оборони США та ODNI, дали свідчення в понеділок на слуханнях у Спеціальному комітеті Сенату США з розвідки, одночасно з публікацією звіту.

Зловмисники використовують децентралізовану та недорогу інфраструктуру, яка дозволяє анонімно поширювати спеціалізоване програмне забезпечення-вимагач, йдеться у звіті. «Ця взаємопов'язана система підвищила ефективність і складність атак програм-вимагачів, а також знизила технічну планку для входу нових учасників».

Федеральна влада визнала наявність обмежень або обмежених можливостей, які перешкоджають більш тривалому впливу дій правоохоронних органів проти операторів програм-вимагачів.

У той час як деякі глобальні злочинні синдикати тимчасово припиняють діяльність після дій правоохоронних органів, оператори програм-вимагачів та їхні філії часто знаходять способи ребрендингу та відновлення своєї діяльності, йдеться у звіті влади.

Участь AlphV у дуже шкідливій атаці програм-вимагачів проти Change Healthcare є особливо поганою подією після глобальних дій правоохоронних органів у грудні, які закрили інфраструктуру групи програм-вимагачів, також відомої як BlackCat. AlphV з'явився протягом кількох годин після демонтажу та залишається активним.

LockBit, ще одне програмне забезпечення-вимагач як сервісна група, яка відновила роботу протягом декількох днів після глобальних зусиль правоохоронних органів, які демонтували інфраструктуру групи, залишається найпліднішою злочинною групою в цій галузі.

«За відсутності спільних правоохоронних органів з боку Росії чи інших країн, які надають кіберзлочинцям притулок або сприятливе середовище, зусилля щодо пом'якшення наслідків залишаться обмеженими», — йдеться у звіті». ***(Matt Kapko. Ransomware festers as a top security challenge, US intel leaders say // Industry Dive (https://www.cybersecuritydive.com/news/ransomware-festers-intel-leaders-warn/710022/). 12.03.2024).***

***

«Зростання атак програм-вимагачів продовжує зростати, причому кількість компаній-жертв за минулий рік зросла на 27%, згідно з висновками, представленими у звіті Thales про загрози даним за 2024 рік. Дослідження також показує, що тривожні 8% цільових організацій відчували себе змушеними заплатити вимаганий викуп.

У звіті, заснованому на опитуванні 3000 фахівців з IT та безпеки з 18 країн і 37 окремих галузей, виявлено, що 93% IT-персоналу зараз вважають, що загрози безпеці зростають або в масштабах, або в серйозності. Ця цифра є значним стрибком порівняно з минулорічними 47%.

Дослідження 2024 року, проведене 451 Research, оприлюднило кілька інших ключових ідей. Майже половина всіх підприємств (43%) не пройшли аудит відповідності протягом минулого року. Виявилося, що ці банкротні підприємства мають у 10 разів більше шансів постраждати від витоку даних, ніж їхні аналоги. Зловмисне програмне забезпечення стало найбільшою загрозою 2024 року, жертвами якої стали 41% підприємств. Фішинг і програми-вимагачі слідували за ними. Опитування також показало, що хмарні активи, включаючи додатки SaaS, хмарне сховище та керування хмарною інфраструктурою, були головним джерелом таких атак.

Рік поспіль у звіті головною причиною витоку даних є людська помилка, оскільки 31% організацій пояснюють витоки даних головним чином цією помилкою. Себастьєн Кано, старший віце-президент Thales Cloud Protection and Licensing, підкреслив важливість сучасного розуміння всіх систем, програм і пов’язаних із ними ризиків через постійно змінювані нормативні та загрозливі ландшафти, щоб залишатися у відповідності з глобальними даними. правила конфіденційності.

Відповідність стала наріжним каменем безпеки даних. Минулого року понад дві п’ятих (43%) підприємств не пройшли аудит відповідності. Організації, які не пройшли аудит відповідності, мали 31% ймовірність зіткнутися з витоком даних у тому ж році, порівняно з лише 3% імовірністю для тих, хто успішно пройшов аудит.

Крім того, підтримання оперативного контролю над даними залишається недосяжною метою для багатьох компаній. Лише третина (33%) зуміла повністю класифікувати всі свої дані, тоді як тривожні 16% класифікували дуже мало або взагалі не класифікували свої дані. Примітно, що лише 5,4% респондентів повідомили про використання п’яти або більше ключових систем управління, порівняно з 5,6% минулого року.

Що стосується нових технологій, 57% фахівців з IT і безпеки визнали штучний інтелект (AI) серйозною проблемою, трохи більше, ніж Інтернет речей (IoT) і постквантову криптографію. Попри побоювання, бізнес також схвильований

потенціалом цих технологій, оскільки понад п’ятий (22%) планує включити Generative AI у свої продукти та послуги безпеки протягом наступного року». ***(Shannon Williams. Ransomware attacks against companies rise by 27% in 2024 // TechDay (https://securitybrief.co.nz/story/ransomware-attacks-against-companies-rise-by-27-in-2024). 21.03.2024).***

***

Фішингові атаки

«Хакерська група, відома як TA577, нещодавно змінила тактику, використовуючи фішингові електронні листи для викрадення хешів автентифікації NT LAN Manager (NTLM) для викрадення облікових записів.

TA577 вважається посередником початкового доступу (IAB), раніше пов’язаним із Qbot і пов’язаним із зараженням програм-вимагачів Black Basta.

Фірма безпеки електронної пошти Proofpoint повідомляє сьогодні, що хоча нещодавно вона помітила, що TA577 віддає перевагу розгортанню Pikabot, дві останні хвилі атак демонструють іншу тактику.

Окремі кампанії TA577, запущені 26 і 27 лютого 2024 року, розповсюдили тисячі повідомлень сотням організацій по всьому світу, орієнтуючись на хеші NTLM співробітників.

Хеші NTLM використовуються в Windows для автентифікації та безпеки сеансу та можуть бути захоплені для офлайн-злому паролів для отримання простого текстового пароля.

Крім того, їх можна використовувати в атаках «передачі хешу», які взагалі не передбачають злому, коли зловмисники використовують хеш як він є для автентифікації на віддаленому сервері чи службі.

Викрадені хеші можуть, за певних обставин і залежно від застосованих заходів безпеки, дозволити зловмисникам підвищити свої привілеї, захопити облікові записи, отримати доступ до конфіденційної інформації, уникнути продуктів безпеки та пересуватися в межах зламаної мережі.

Використання фішингу для викрадення хешів NTLM

Нова кампанія почалася з фішингових електронних листів, які, здається, є відповідями на попереднє обговорення цільової групи, метод, відомий як викрадення потоку.

До електронних листів додаються унікальні (на жертву) ZIP-архіви, що містять HTML-файли, які використовують HTML-теги META refresh для запуску автоматичного підключення до текстового файлу на зовнішньому сервері блокування повідомлень сервера (SMB).

Коли пристрій Windows підключається до сервера, він автоматично намагатиметься виконати запит/відповідь NTLMv2, дозволяючи віддаленому серверу, керованому зловмисником, викрасти хеші автентифікації NTLM.

«Примітно, що TA577 доставив шкідливий HTML у zip-архів для створення локального файлу на хості», — йдеться у звіті Proofpoint.

«Якщо URI схеми файлу було надіслано безпосередньо в тілі електронної пошти, атака не працюватиме на поштових клієнтах Outlook, виправлених з липня 2023 року».

Proofpoint каже, що ці URL-адреси не доставляли шкідливих програм, тому їх основною метою є захоплення хешів NTLM.

Proofpoint згадує певні артефакти, присутні на серверах SMB, які загалом є нестандартними, як-от набір інструментів із відкритим вихідним кодом Impacket, що свідчить про те, що ці сервери використовуються для фішингових атак.

Фахівець із кібербезпеки Брайан із Піттсбурга зазначає, що для того, щоб зловмисники могли використовувати ці викрадені хеші для зламу мереж, багатофакторна автентифікація має бути вимкнена в облікових записах.

Дослідник уразливостей Вілл Дорманн припускає, що можливо хеші викрадають не для зламу в мережі, а як форму розвідки для пошуку цінних цілей.

«Я міг уявити, що комбінація імені домену, імені користувача та імені хоста може викликати деякі соковиті цілі?», — написав Дорманн у Twitter.

Proofpoint каже, що лише обмеження гостьового доступу до SMB-серверів не пом’якшує атаку TA577, оскільки воно використовує автоматичну автентифікацію на зовнішньому сервері, яка обходить гостьовий доступ.

Потенційно ефективним заходом може бути налаштування брандмауера для блокування всіх вихідних з’єднань SMB (як правило, порти 445 і 139), припинення надсилання хешів NTLM.

Іншим захисним заходом було б впровадження фільтрації електронної пошти, яка блокує повідомлення, що містять заархівовані файли HTML, оскільки вони можуть ініціювати підключення до небезпечних кінцевих точок після запуску.

Також можна налаштувати групову політику Windows «Безпека мережі: обмежити NTLM: вихідний трафік NTLM до віддалених серверів», щоб запобігти надсиланню хешів NTLM. Однак це може призвести до проблем автентифікації на законних серверах.

Для організацій, які використовують Windows 11, Microsoft представила додаткову функцію безпеки для користувачів Windows 11, щоб блокувати атаки на основі NTLM на SMBs, що було б ефективним рішенням». ***(Bill Toulas. Hackers steal Windows NTLM authentication hashes in phishing attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-steal-windows-ntlm-authentication-hashes-in-phishing-attacks/?utm_source=flipboard&utm_content=AWC%2Fmagazine%2FOur+Electronic+%26+Digital+Lives). 04.03.2024).***

***

«Дослідники з кібербезпеки виявили нову хвилю фішингових атак, спрямованих на розповсюдження викрадача інформації, що постійно розвивається, під назвою StrelaStealer.

Кампанії впливають на понад 100 організацій у ЄС та США, заявили дослідники Palo Alto Networks Unit 42 у новому звіті, опублікованому сьогодні.

«Ці кампанії відбуваються у формі спаму з вкладеннями, які зрештою запускають корисне навантаження DLL StrelaStealer», — повідомили дослідники

Бенджамін Чанг, Гоутам Тріпаті, Пранай Кумар Чхапарвал, Анмол Маурія та Вішва Тотатрі.

«Намагаючись уникнути виявлення, зловмисники змінюють початковий формат вкладеного файлу електронної пошти від однієї кампанії до наступної, щоб запобігти виявленню за попередньо згенерованим підписом або шаблонами».

Вперше оприлюднений у листопаді 2022 року, StrelaStealer здатний перекачувати дані електронної пошти для входу з відомих поштових клієнтів і передавати їх на контрольований зловмисником сервер.

Відтоді в листопаді 2023 року та січні 2024 року було виявлено дві масштабні кампанії з використанням зловмисного програмного забезпечення, націлені на високі технології, фінанси, професійну та юридичну галузі, виробництво, уряд, енергетику, страхування та будівництво в ЄС і США.

Ці атаки також спрямовані на надання нового варіанту викрадача, який містить кращі методи обфускації та антианалізу, поширюючи його через електронні листи на тему рахунків-фактур із вкладеними файлами ZIP, що свідчить про відхід від файлів ISO.

У ZIP-архіві присутній файл JavaScript, який видаляє пакетний файл, який, у свою чергу, запускає корисне навантаження DLL-викрадача за допомогою rundll32.exe, законного компонента Windows, відповідального за запуск 32-розрядних бібліотек динамічного компонування.

Зловмисне програмне забезпечення-викрадач також покладається на низку трюків обфускації, щоб ускладнити аналіз у пісочному середовищі.

«З кожною новою хвилею електронних кампаній зловмисники оновлюють як вкладення електронної пошти, яке ініціює ланцюг зараження, так і саму корисну бібліотеку DLL», — кажуть дослідники.

Це сталося після того, як Symantec, що належить Broadcom, виявила, що підроблені інсталятори для відомих програм або зламаного програмного забезпечення, розміщеного на GitHub, Mega або Dropbox, служать каналом для зловмисного програмного забезпечення, відомого як Stealc.

Також було виявлено фішингові кампанії, які доставляли Revenge RAT і Remcos RAT (він же Rescoms), причому останній доставлявся за допомогою крипторів як послуги (CaaS) під назвою AceCryptor, згідно з ESET.

«Протягом другої половини [2023] Rescoms став найпоширенішим сімейством зловмисних програм, упакованих AceCryptor», — повідомила компанія з кібербезпеки, посилаючись на дані телеметрії. «Понад половина цих спроб сталася в Польщі, за нею йдуть Сербія, Іспанія, Болгарія та Словаччина».

Серед інших відомих готових зловмисних програм, запакованих у AceCryptor у другій половині 2023 року, є SmokeLoader, STOP-вимагач, RanumBot, Vidar, RedLine, Tofsee, Fareit, Pitou та Stealc. Варто зазначити, що багато з цих штамів зловмисного програмного забезпечення також поширюються через PrivateLoader.

Інше шахрайство із соціальною інженерією, за яким спостерігала Secureworks, було виявлено, що він націлений на людей, які шукають інформацію про нещодавно померлих осіб у пошукових системах, за допомогою підроблених повідомлень про некрологи, розміщених на фіктивних веб-сайтах, спрямовуючи трафік на сайти через пошукову оптимізацію (SEO) для того, щоб зрештою проштовхнути рекламне ПЗ та інші небажані програми.

«Відвідувачі цих сайтів перенаправляються на веб-сайти електронних знайомств або розваг для дорослих або одразу отримують підказки CAPTCHA, які встановлюють веб-повідомлення або спливаючу рекламу після натискання», — повідомили в компанії.

«Повідомлення відображають помилкові попередження про віруси від відомих антивірусних програм, таких як McAfee і Windows Defender, і вони зберігаються в браузері, навіть якщо жертва натискає одну з кнопок».

«Кнопки посилаються на законні цільові сторінки для антивірусних програм на основі підписки, а ідентифікатор філії, вбудований у гіперпосилання, винагороджує суб’єктів загрози за нові підписки або поновлення».

Хоча підробка наразі обмежується наповненням скарбниці шахраїв через партнерські програми для антивірусного програмного забезпечення, ланцюжки

атак можна легко перепрофілювати для доставки викрадачів інформації та інших шкідливих програм, що зробить їх більш потужною загрозою.

Розробка також послідувала за відкриттям нового кластера активності, відстежуваного як Fluffy Wolf, який використовує фішингові електронні листи, що містять виконуваний вкладений файл, щоб доставити коктейль загроз, таких як MetaStealer, Warzone RAT, майнер XMRig і законний інструмент віддаленого робочого столу під назвою Remote Utilities.

Ця кампанія є ознакою того, що навіть некваліфіковані загрозливі особи можуть використовувати схеми зловмисного програмного забезпечення як послуги (MaaS) для проведення успішних масштабних атак і викрадення конфіденційної інформації, яку потім можна монетизувати для отримання прибутку.

«Хоча ці посередники з точки зору технічних навичок, ці суб'єкти загрози досягають своїх цілей, використовуючи лише два набори інструментів: законні служби віддаленого доступу та недороге шкідливе програмне забезпечення», — зазначає BI.ZONE». ***(New StrelaStealer Phishing Attacks Hit Over 100 Organizations in E.U. and U.S. // The Hacker News (https://thehackernews.com/2024/03/new-strelastealer-phishing-attacks-hit.html). 22.03.2024).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Міністерство юстиції США висунуло обвинувачення іранському громадянину Алірезе Шафі Насабу. За даними слідства, чоловік упродовж кількох років керував масштабною кібероперацією, яка скомпрометувала сотні тисяч облікових записів. Кібератака була спрямована на проникнення у комп'ютерні системи оборонних підрядників США, а також держвідомств.

Насаб і його спільники діяли під прикриттям вигаданої компанії з кібербезпеки Mahak Rayan Afraz. Використовуючи фішингові розсилки, методи

соціальної інженерії та розроблене на замовлення шкідливе ПЗ, вони компрометували американські цілі в період із 2016 по квітень 2021 року.

«Насаб був учасником кібероперації, під час якої через фішинг та інші хакерські хитрощі було зламано понад 200 000 пристроїв, багато з яких містили секретну оборонну інформацію», — заявив прокурор Південного округу Нью-Йорка Деміан Вільямс.

Головними мішенями Насаба були організації, пов'язані з Пентагоном. А проте, постраждали й аудиторські фірми, готелі Нью-Йорка, а також Держдепартамент, Міністерство фінансів США та одна неназвана іноземна держава.

Діяльність компанії Mahak Rayan Afraz раніше вже привертала увагу фахівців з кібербезпеки. Так у 2021 році Facebook «вжила заходів» проти іранської хакерської групи Tortoiseshell, що мала зв'язки з Mahak Rayan Afraz. Згідно з інформацією Facebook, частину шкідливого ПЗ, яке використовували Tortoiseshell, також розробили спільники Насаба. Зазначимо, що зловмисне ПЗ американська влада також пов'язує з Корпусом вартових ісламської революції.

Насабу висунуто звинувачення у змові з метою комп'ютерного шахрайства, шахрайстві з використанням електронних засобів зв'язку, а також крадіжці персональних даних. Йому загрожує до 47 років тюремного ув'язнення.

Однак затримання Насаба, який є громадянином Ірану, може виявитися непростим завданням. Наразі його оголошено у міжнародний розшук. Держдепартамент США призначив винагороду в 10 мільйонів доларів за інформацію, яка допоможе встановити його місцеперебування». ***(За хакера, який зламав Пентагон, оголошено винагороду у $ 10 мільйонів // Internetua (https://internetua.com/za-hakera-yakii-zlamav-pentagon-ogolosheno-vinagorodu-u-10-milioniv?utm_source=news.ukrnet). 09.03.2024).***

***

«Федеральний суд США засудив співадміністратора незаконного онлайн-майданчика до 42 місяців тюремного ув'язнення після того, як визнав

себе винним за двома пунктами звинувачення, які могли посадити його у в'язницю на 15 років.

31-річний Санду Борис Дьякону допоміг розробити та адмініструвати ринок E-Root, який з грудня 2016 року по лютий 2020 року заробив близько 1 мільйона доларів США. Відомий своєю високоякісною підтримкою клієнтів – він мав політику обміну та гарантії на викрадені облікові дані. - ринок працював, поки влада не вилучила його в кінці 2020 року. Незаконний ринок спеціалізувався на продажу облікових даних протоколу віддаленого робочого стола та оболонки безпечного сокета.

Громадянин Молдови визнав себе винним 1 грудня 2023 року в залі федерального суду міста Тампа, штат Флорида, згідно з угодою про визнання провини, яка обмежувала його злочинність одним пунктом змови з метою шахрайства з комп'ютером і пристроєм доступу та одним пунктом володіння принаймні 15 пристроїв несанкціонованого доступу. Прокурори заявили, що вимагатимуть значно меншого покарання, ніж максимальне, в обмін на співпрацю Дьякону.

Прокуратура заявила, що на ринку E-Root, ймовірно, виставлено понад 350 000 облікових даних для продажу. Клієнти могли переглядати облікові дані, що продаються, за такими критеріями, як країна, регіон або поштовий індекс зламаного сервера або базової операційної системи.

Спочатку Дьякону не визнав себе винним під час свого першого поста перед судом після його екстрадиції зі Сполученого Королівства 13 жовтня 2023 року. Британська влада заарештувала Дьякону, коли він намагався покинути країну в травні 2021 року. Він боровся з екстрадицією до Сполучених Штатів до вересня 2023 року. Міністерство юстиції США. повідомило тоді

Клієнти використовували облікові дані для широкого кола злочинних дій, включаючи атаки програм-вимагачів, шахрайські електронні перекази та податкове шахрайство. Незаконний ринок працював у розподіленій мережі та набув популярності завдяки заходам із приховування особи покупців і продавців. Він використовував систему онлайн-платежів під назвою Perfect Money і пропонував

окремий незаконний сервіс обміну криптовалюти для конвертації біткойнів у Perfect Money і навпаки. Влада заарештувала біржу у 2020 році». ***(Mihir Bagwe. Illicit Credentials Marketplace Admin Gets 42-Month Sentence // Information Security Media Group, Corp. (https://www.databreachtoday.com/illicit-credentials-marketplace-admin-gets-42-month-sentence-a-24620). 15.03.2024).***

***

Технічні аспекти кібербезпеки

«Дослідники з Національної лабораторії Оук-Рідж Департаменту енергетики продемонстрували, що передову квантову кібербезпеку можна реалізувати в розгорнутому оптоволоконному каналі.

Їхні результати, опубліковані в CLEO 2023, підтверджують попередній лабораторний експеримент із підтвердженням принципу, проведений вченими ORNL у 2015 році.

Команда передала квантовий сигнал для розподілу квантового ключа — безпечний підхід до обміну секретним ключем — за допомогою справжнього гетеродина. Гетеродин гасить вплив шуму, розсіяного від інших даних, що передаються в тій самій волоконно-оптичній мережі, і робота продемонструвала співіснування між квантовими та звичайними сигналами даних.

Сигнал проходив через волоконно-оптичну мережу ORNL, закодований у безперервних змінних, які описували властивості легких частинок, або фотонів, в амплітуді та фазі. Використання безперервних змінних фотонів для кодування дозволяє майже нескінченну кількість налаштувань для розподілу випадковості, які можна використовувати для кібербезпеки та забезпечує сумісність з існуючими класичними системами зв’язку.

Експеримент команди ORNL не тільки заклав нову основу в інформаційній безпеці, але й використав існуючу волоконно-оптичну інфраструктуру, що забезпечить дешевше та легше впровадження.

За словами Ніколаса Пітерса, голови відділу квантової інформаційної науки ORNL і головного дослідника, експеримент усунув основні перешкоди на шляху впровадження квантового розподілу ключів, одночасно підвищивши безпеку.

«Квантовий розподіл ключів — це криптографічний протокол, за допомогою якого дві сторони можуть створити безпечний ключ, який знають лише вони», — сказав Пітерс. «У цьому експерименті це робиться за допомогою лазерів для генерації слабких оптичних імпульсів між двома точками, які зазвичай називають Алісою та Бобом».

Коли приймаюча сторона вимірює пульс, вимірювання можуть виявити, чи перехопив та зіпсував повідомлення перехоплювач. У минулих експериментах без справжнього гетеродина цей оптичний імпульс передавався разом із гетеродином. Попередні методи створювали потенціал для вразливостей, які не розглядалися в поточних найкращих практиках, визначених базовою концепцією безпеки. Новий метод базується на оптичних сигналах, які генеруються незалежними лазерами в точках передачі та прийому.

«По суті, ми розглядаємо перешкоди», — сказав Браян Вільямс, провідний автор дослідження та вчений з квантових досліджень ORNL. «Це як кинути камінь в озеро та створити брижі. Це схоже на хвилеподібну природу фотона, на який ми дивимося. Якщо кинути два камені, вони створять дивні візерунки у воді. Ми робимо подібне втручання вимірювання на основі цього квантового сигналу, але виявляється лише та частина, яка збігається з лазером. Для цього потрібна дуже вузька енергетична роздільна здатність».

Надлишок шуму знижує швидкість ключа, який можна розповсюдити. Занадто багато шуму, і частка потенційного ключа споживається для захисту конфіденційності.

«Мета полягає в тому, щоб отримати найкраще співвідношення сигнал/шум», — сказав Вільямс. «Використовуючи вузький енергетичний лазер як гетеродин, він діє як фільтр для фонового шуму та покращує співвідношення сигнал/шум».

Подальші зусилля будуть зосереджені на відтворенні результатів експерименту в більш широкому діапазоні мережевих сценаріїв». ***(Reece Brown.***

Researchers achieve quantum key distribution for cybersecurity in novel experiment // Phys.org (https://phys.org/news/2024-03-quantum-key-cybersecurity.html). 13.03.2024).

***

Виявлені вразливості технічних засобів та програмного забезпечення

«За підсумками 2023 року компанія Google виплатила етичним хакерам, які брали участь у програмі пошуку вразливостей у різних продуктах IT-гіганта, $ 10 млн. Інформація про це з'явилася в блозі компанії.

Винагороду від Google у сфері інформаційної безпеки минулого року отримали 632 дослідники з 68 країн світу. Вони займалися пошуком уразливостей у різних продуктах компанії, таких як операційні системи Android та Wear OS. Розмір найбільшої одиничної виплати за звіт про виявлену вразливість становив $ 113 337, а лише з моменту запуску програми у 2010 році Google виплатила дослідникам $ 59 млн.

Минулого року Google розширила свою програму пошуку вразливостей, додавши до неї сервіси на основі генеративних нейромереж, таких як Gemini. Протягом усього року у цьому сегменті було виявлено 35 помилок, а загальна сума винагороди становила $ 87 000. За виявлені вразливості в Android та апаратних продуктах Google сума виплат становила $ 3,4 млн.

Помилки, які були виявлені у Wear OS та Android Automotive, принесли дослідникам $ 70 000. У браузері Chrome за рік було виявлено 359 вразливостей, які принесли дослідникам близько $ 2,1 млн. Ознайомитися з детальнішою інформацією з цього питання можна у блозі Google». ***(Хакери, які зламали Google, отримали $ 10 мільйонів винагороди від техногіганта // Internetua (https://internetua.com/hakeri-yaki-zlamali-google-otrimali-10-milioniv-vinagorodi-vid-tehnogiganta?utm_source=news.ukrnet). 15.03.2024).***

***

«Пов’язаний з Китаєм кластер загроз використовував недоліки безпеки в програмному забезпеченні Connectwise ScreenConnect і F5 BIG-IP, щоб розмістити спеціальне шкідливе програмне забезпечення, здатне створювати додаткові бекдори на скомпрометованих хостах Linux у рамках «агресивної» кампанії.

Mandiant, що належить Google, відстежує діяльність під своїм некатегоризованим псевдонімом UNC5174 (він же Uteus або Uetus), описуючи його як «колишнього члена китайських хакерських колективів, який з тих пір показав ознаки того, що діє як підрядник Міністерства державної безпеки Китаю (MSS) зосереджено на виконанні операцій доступу».

Вважається, що зловмисник організував широкомасштабні атаки на дослідницькі та освітні установи Південно-Східної Азії та США, підприємства Гонконгу, благодійні та неурядові організації (НУО), а також урядові організації США та Великої Британії в період з жовтня по листопад 2023 року та знову в лютому. 2024 за допомогою помилки ScreenConnect.

Початковий доступ до цільових середовищ полегшується завдяки використанню відомих недоліків безпеки в Atlassian Confluence (CVE-2023-22518), ConnectWise ScreenConnect (CVE-2024-1709), F5 BIG-IP (CVE-2023-46747), ядрі Linux (CVE-2022-0185) і Zyxel (CVE-2022-3052).

Успішне закріплення супроводжується широкомасштабною розвідкою та скануванням систем, що підключаються до Інтернету, на наявність уразливостей безпеки, при цьому UNC5174 також створює облікові записи адміністраторів для виконання зловмисних дій із підвищеними привілеями, включаючи видалення завантажувача ELF на основі C під назвою SNOWLIGHT.

SNOWLIGHT призначений для завантаження корисного навантаження наступного етапу, обфускованого бекдору Golang під назвою GOREVERSE, з віддаленої URL-адреси та обміну даними з SUPERSHELL, системою керування (C2) з відкритим вихідним кодом, яка дозволяє зловмисникам встановлювати

зворотний SSH-тунель і запускати інтерактивні сеанси оболонки для виконання довільного коду.

Зловмисник також використовує тунельний інструмент на базі Golang, відомий як GOHEAVY, який, імовірно, використовується для полегшення бокового переміщення в зламаних мережах, а також інші програми, такі як afrog, DirBuster, Metasploit, Sliver і sqlmap.

В одному незвичайному випадку, поміченому компанією з розвідки загроз, було виявлено, що суб'єкти загрози застосували засоби пом'якшення CVE-2023-46747, ймовірно, намагаючись перешкодити іншим непов'язаним супротивникам використати ту саму лазівку для отримання доступу.

«UNC5174 (він же Uteus) раніше був учасником китайських хактивістських колективів «Dawn Calvary» і співпрацював з «Genesis Day» / «Xiaoqiying» і «Teng Snake», – оцінив Mandiant. «Схоже, що ця особа покинула ці групи в середині 2023 року і з тих пір зосередилася на виконанні операцій доступу з наміром посередництва в доступі до скомпрометованих середовищ».

Є дані, які свідчать про те, що загроза може бути початковим посередником доступу та має підтримку MSS, враховуючи їхні ймовірні заяви на форумах темної мережі. Це підтверджується тим фактом, що деякі з оборонних установ США та уряду Великої Британії були одночасно мішенню іншого посередника доступу під назвою UNC302.

Отримані дані китайських державних угруповань ще раз підкреслюють постійні зусилля зламати периферійні пристрої шляхом швидкого кооптування нульових днів і нещодавно розкритих уразливостей у свій арсенал для проведення масштабних операцій кібершпигунства.

«Наприкінці 2023 року після використання CVE-2023-46747 було помічено спробу UNC5174 продати доступ до обладнання американських оборонних підрядників, державних установ Великобританії та установ в Азії», — повідомили дослідники Mandiant.

«Існує подібність між UNC5174 і UNC302, що свідчить про те, що вони працюють у середовищі посередника початкового доступу до MSS. Ці подібності

вказують на можливі спільні експлойти та операційні пріоритети між цими суб'єктами загрози, хоча для остаточного визначення авторства потрібне подальше дослідження».

Це повідомлення сталося після того, як MSS попередило, що неназвана іноземна хакерська група проникла в «сотні» китайських ділових і державних організацій, використовуючи фішингові електронні листи та відомі помилки безпеки для зламу мереж. Ім'я чи походження загрозливого актора не повідомляється». ***(China-Linked Group Breaches Networks via Connectwise, F5 Software Flaws // The Hacker News (https://thehackernews.com/2024/03/china-linked-group-breaches-networks.html).*** 22.03.2024).

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Microsoft (MSFT.O) розширить доступність свого інструменту на основі штучного інтелекту для професіоналів з кібербезпеки з 1 квітня та запровадить стратегію «оплата за використанням» для помічника, повідомила компанія в середу.

«Security Copilot», запущений минулого року, дозволяє аналітикам запускати запити через просте вікно підказок, щоб допомогти з такими завданнями, як узагальнення інцидентів, аналіз вразливостей і обмін інформацією з колегами на дошці.

Приблизно 300 клієнтів зараз використовують цей інструмент, повідомив представник Microsoft на заході в Сан-Франциско.

Технічний гігант планує стягувати з клієнтів плату за те, скільки вони користуються продуктом, а не на основі передплати, оскільки він «хотів зменшити бар'єри входу», повідомив журналістам корпоративний віце-президент Microsoft Васу Джаккал». ***(Microsoft expands availability of its AI-powered cybersecurity***

assistant // Reuters (https://www.reuters.com/technology/microsoft-expands-availability-its-ai-powered-cybersecurity-assistant-2024-03-13/). 13.03.2024).

***