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

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 5 (травень)

Київ – 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.– №5 (травень) . – 316 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

«Міністерство закордонних справ активно працює над розробкою Стратегії кібердипломатії України для своєчасного та якісного реагування на виклики цифрової епохи.

Про це заявив заступник міністра закордонних справ з питань цифрового розвитку, цифрових трансформацій і цифровізації Антон Демьохін під час онлайн-виступу на першій науково-практичній міжнародній конференції з питань кібердипломатії, повідомляє кореспондент Укрінформу.

«Для своєчасного та якісного реагування на виклики цифрової епохи МЗС розбудовує напрямок кібердипломатії. Для цього минулого року було створено виокремлений підрозділ з кібердипломатії, ведеться активна робота над Стратегією кібердипломатії України», - сказав Демьохін.

За його словами, діяльність сучасного МЗС неможлива без запровадження сучасних цифрових технологій для підвищення ефективності роботи дипломатів.

У цьому контексті Демьохін поінформував, що зовнішньополітичне відомство активно розбудовує систему цифрових спроможностей. Зокрема це включає створення технічної бази з використанням сучасних технічних та програмних засобів, розбудову мережевої інфраструктури, підготовку кадрів для використання новітніх технологій, а також розбудову цифрових послуг, які міністерство надає громадянам, та цифровізацію процесів, пов’язаних із щоденною діяльністю дипломатичної служби.

Як повідомляв Укрінформ, Міністерство закордонних справ України 1 травня вперше в історії створило з використанням технологій штучного інтелекту цифрову особу, яка офіційно коментуватиме консульську інформацію для ЗМІ. Представниця МЗС з консульських питань Вікторія Ші створена на основі реальної людини — української співачки та інфлюенсерки Розалі Номбре, яка погодилася pro bono взяти участь у проєкті МЗС і виступити прототипом для представниці.

У Києві проходить перша науково-практична міжнародна конференція з питань кібердипломатії». ***(МЗС розробляє Стратегію кібердипломатії України - заступник міністра // Укрінформ (https://www.ukrinform.ua/rubric-***

polytics/3863944-mzs-rozroblae-strategiu-kiberdiplomatii-ukraini-zastupnik-ministra.html). 15.05.2024).

***

Кібервійна проти України

«Після повномасштабного вторгнення Росії в Україну кіберпростір став вкрай вразливим. Наприклад, за 2023 рік було зафіксовано 1105 кіберінцидентів, що на 62,5% більше, ніж у 2022 році.

Один із способів захиститися від кібератак — зберігати інформацію у хмарних середовищах. Якщо ви готові до переходу в хмару, ця стаття допоможе зрозуміти основні принципи роботи хмарної інфраструктури, усі переваги та недоліки.

Як резервна копія у хмарі захистить бізнес від кібератаки

Лише за 2022 рік середні витрати на подолання наслідків витоку даних склали 4,35 мільйона доларів. Найбільш поширеним кіберзлочином залишаються DDoS-атаки — це спроба порушити нормальний інтернет-трафік та намагання зупинити роботу сервера.

DDoS-атаки на бізнес можуть організовуватися з декількох причин. Наприклад, нечесна конкуренція, вимагання грошей, звичайний кібервандалізм задля шкоди, а в деяких випадках DDoS-атаку використовують спосіб відвернути увагу від іншого злочину.

Допомогти розв'язати це питання можуть хмарні технології. Це своєрідне середовище для зберігання інформації в мережі Інтернет. Хмари охоплюють такі віртуальні послуги: SaaS (програмне забезпечення), PaaS (платформа), IaaS (інфраструктура) тощо.

Внаслідок атаки на «Київстар» повне відновлення роботи усіх сервісів зайняло кілька днів. Компанія залучила до допомоги фахівців з СБУ, Мінцифри та Держспецзв’язку. Керівники наголошували, що завдяки системам, в яких зберігаються дані клієнтів, вони залишилися неушкодженими після атаки.

Тож кількість хакерських атак щороку лише збільшується, а самі атаки стають дедалі небезпечнішими. І передбачити повністю їх неможливо, проте можна запобігти. Нові технології, допомога від провідних ІТ-спеціалістів можуть значно полегшити життя і зберегти бізнес від непередбачуваних наслідків. З іншого боку, важлива підтримка держави та її політика безпеки.

Наприклад, у березні 2023 року в США презентували нову стратегію кібербезпеки. В її основі закладений принцип "нульової довіри". Тобто апріорі всі мережі вважаються скомпрометованими й вимагають безперервної перевірки користувачів та пристроїв.

Одна з переваг «нульової довіри» — використання співробітниками платформ, де є необхідна інформація й нічого більше. Тобто діє принцип «рівно стільки, скільки необхідно». Розділити цю інформацію на платформи можна з легкістю у хмарних середовищах і таким чином мінімізувати ризики втратити все. Ця модель могла б допомогти й українському бізнесу.

Але для початку варто переглянути систему зберігання та копіювання даних. І не економити на нових технологіях, які будь-якої миті можуть врятувати компанію.

Хмара — це безпечно?

Компанії, які надають послуги резервного копіювання до хмарних репозитаріїв, називаються хмарними операторами. Їхня робота полягає в тому, щоб захищати ваші дані від зловмисників, тому безпека є одним із ключових факторів для таких компаній. Хмарні оператори регулярно проходять перевірки й аудити від незалежних організацій і держави.

В результаті вони отримують відповідні документи, які свідчать про те, що їм можна довіряти. Саме на ці документи варто звертати увагу в першу чергу, коли ви обираєте хмарний сервіс. Зазвичай такі атестати викладають на офіційних сайтах.

Ось які методи захисту для ваших даних пропонують хмарні оператори:

Шифрування даних — один з основних методів захисту даних у хмарних середовищах, який дозволяє перетворити інформацію в незрозумілий для сторонніх формат, забезпечуючи її конфіденційність. При передачі та зберіганні даних у

хмарі важливо використовувати сильне шифрування для захисту інформації від несанкціонованого доступу.

Багатофакторна аутентифікація — встановлюється для запобігання несанкціонованому доступу до даних. Ці ефективні механізми можуть передбачати використання паролів, біометричних методів або подвійної аутентифікації. Надійна аутентифікація дозволяє переконатися, що лише уповноважені користувачі мають доступ до даних.

Моніторинг доступу — допомагає вчасно виявляти та реагувати на потенційні загрози безпеки. Спеціальні системи моніторингу дозволяють відстежувати активності користувачів, виявляти підозрілі дії та вживати заходів для їх запобігання.

Загальний підхід щодо захисту даних у хмарних середовищах полягає в комбінації цих методів, а також постійному вдосконаленні та оновленні заходів безпеки для відповіді на кіберзагрози, які чимдалі зростають.

Переваги хмарних сховищ

Хмарні сервіси пропонують кілька ключових переваг, які можуть підвищити рівень захисту даних. Основна з них — економічна та екологічна ефективність. Компанії уникають великих витрат на дороге локальне обладнання, яке потребує певного місця для розміщення та обслуговування.

Крім того, використання хмарних технологій сприяє зменшенню вуглецевого викиду, що робить бізнес більш екологічним.

Іншою важливою перевагою є просте масштабування хмарних середовищ. Компанії можуть легко розширювати або зменшувати обсяги використання ресурсів відповідно до своїх потреб.

Гнучкість хмарних технологій полягає в здатності бізнесу надавати нові ресурси, розгортати нові програми та послуги відповідно до змін потреб ринку. Це підвищує комунікацію онлайн та сприяє покращенню продуктивності.

Забезпечення високого рівня безпеки даних — це ще одна перевага хмарних технологій. Постачальники хмарних послуг мають великий досвід у сфері кібербезпеки й надають своїм клієнтам новітні заходи захисту.

На вибір хмарних технологій також впливають співпраця й підвищення продуктивності. Співробітники компанії можуть легко та швидко обмінюватися документами, а це додає їхній роботі ефективності.

За допомогою хмарних сервісів можливо збільшити потужності, щоб мати швидший доступ до файлів у будь-якому місці, що також позитивно впливає на збільшення продуктивності працівників.

Крім цього, хмарні середовища мають можливість аварійного відновлення. Ця перевага дозволяє швидко відновити роботу усієї компанії після потенційних атак або випадків непередбачуваних обставин.

Недоліки хмарних технологій

Хмарні технології вимагають безперервного доступу до інтернету. Це може стати проблемою, оскільки відсутність з'єднання може призвести до тимчасової втрати доступу до важливих даних та послуг.

Важливим також є питання приватності та безпеки даних. Існує ризик несанкціонованого доступу до конфіденційної інформації, а також можливість втрати контролю над даними. А це може призвести до серйозних наслідків для бізнесу.

Однак ця проблема стосується лише тих хмарних сервісів, які не достатньо добре дбають про безпеку. Найкращі гравці на ринку ставлять дорожчий цінник за свої послуги, але є надійнішими.

Врахувати варто також і вартість послуги. Економічна ефективність, яку ви отримуєте одразу, згодом може змінитися через витрати на підписку та збільшення обсягів використання сховища.

Отже, бізнесам варто ретельно зважувати всі за й проти перш ніж прийняттям рішення щодо використання хмарних технологій. Важливо розробити стратегію безпеки та план аварійного відновлення для забезпечення найвищого рівня захисту даних та бізнес-процесів». ***(Данило Бєлов. Хмарні технології як рецепт порятунку бізнесу від кібератак // Економічна правда (https://www.epravda.com.ua/columns/2024/05/13/713584/). 13.05.2024).***

***

«Кіберфахівцям Головного управління розвідки Міноборони України вдалося вивести з ладу російські онлайн-сервіси компанії 1С.

Як передає Укрінформ, цю інформацію повідомили Суспільному джерела у спецслужбах.

Зазначається, що компанія 1С спеціалізується на підтримці й розробці комп'ютерних програм для ведення ділових баз даних.

«Масштабна кібератака почалася 7 травня. Окрім онлайн-ресурсів 1С, атакою вивели з ладу ресурси корпоративного хмарного провайдера Cloud4y та сервер віддаленої роботи 1С – Scloud» — уточнили джерела.

Наразі росіяни масово скаржаться на відсутність доступу до онлайн-інструментів та серверів, а також у мережах активно пишуть про неспроможність служб підтримки відновити доступ до оплачених ресурсів.

При цьому за даними ГУР, адміністратори публічних сторінок видаляють негативні коментарі». ***(Кіберфахівці ГУР вивели з ладу російські онлайн-сервіси компанії 1С // Укрінформ (https://www.ukrinform.ua/rubric-ato/3861148-kiberfahivci-gur-viveli-z-ladu-rosijski-onlajnservisi-kompanii-1s.html). 07.05.2024).***

***

«Кіберфахівці Головного управління розвідки Міноборони атакують інтернет-провайдерів і сайти місцевої влади Бєлгородської області.

Цю інформацію Укрінформу підтвердили джерела у спецслужбі.

«Ми можемо підтвердити цю інформацію», - заявили співрозмовники агентства.

Вони не уточнили, скільки інтернет-мереж там було виведено з ладу.

За інформацією ЗМІ, станом на 13 травня виведено з ладу такі ресурси: основного інтернет-провайдера «Лучше.Нет»; вебсайт місцевої влади та уряду Бєлгорода, Регіонального порталу державних та муніципальних послуг, Газпрому Міжрегіонгаз Бєлгород, Міністерства фінансів та бюджетної політики.

Місцеві користувачі соцмереж скаржаться на відсутність доступу до мережі Інтернет, неробочий мобільний інтернет та відсутність зв'язку зі службами підтримки атакованих провайдерів. Водночас провайдери повідомляють про "аварійну ситуацію" та зазначають, що змушені припинити доступ до іноземних вебресурсів.

Джерела в ГУР МО зазначають, що DDoS-атака на російські сервіси триває». ***(ГУР атакує інтернет-провайдерів Бєлгородської області – джерела // Укрінформ (https://www.ukrinform.ua/rubric-ato/3863233-gur-atakue-internetprovajderiv-belgorodskoi-oblasti-dzerela.html). 13.05.2024).***

***

«Росіяни зламали супутниковий ефір каналів груп StarLight Media та «Інтер» і запустили трансляцію параду в Москві на Червоній площі.

Про це свідчать відео, які почали з’являтися в телеграм-каналах.

Цю ж інформацію підтвердили «Детектору медіа» і в Національній раді з питань телебачення та радіомовлення.

Українські провайдери переходять на IPTV-сигнал, фахівці працюють над відбиттям хакерської атаки.

Оновлення: У пресслужбі Inter Media Group повідомили, що на «Інтері» не було трансляції параду у Москві. «Згідно з інформацією, яку ми отримали від супутникового оператора SES Astra AB, 9 травня 2024 року трансляції через супутник Astra 4A зазнавали інтерференції від потужного зовнішнього радіосигналу: згідно з даними моніторингу, телеканали «Інтер», К1, «Мега», НТН, «Піксель TV» та «Enter-фільм» зазнали перерви у трансляції тривалістю 17 секунд — із 11:09:48 до 11:10:05. Після цього інтерференція не спостерігалася. Жодних змін у контенті зазначених каналів не зафіксовано. Все обладнання космічного апарата Astra-4A та наземна інфраструктура SES працювали під час цих інцидентів і працюють наразі у штатному режимі».

Нагадаємо, що 9 травня низка українських каналів зазнала хакерських атак з боку російських зловмисників, які намагалися глушити сигнал на супутнику. Про це повідомляли представники телеканалів.

Зокрема, атаки зазнали канали медіагруп StarLight Media, «Інтер», Суспільний мовник, канал «Дім» та «Апостроф ТВ», «Ми-Україна», «Еспресо». Втручання відбулось на супутнику Astra. Згодом сигнал відновили». ***(Андрій Богданович. Російські хакери зламали супутниковий сигнал StarLight Media та «Інтера» і транслюють парад у Москві // Інтернет-видання «Детектор медіа» (https://detector.media/infospace/article/226574/2024-05-09-rosiyski-khakery-zlamaly-suputnykovyy-sygnal-starlight-media-ta-intera-i-translyuyut-parad-u-moskvi/). 09.05.2024).***

***

«Зламати систему застосунку «Резерв+» і отримати бази даних з нього неможливо, бо вони там не зберігаються.

Про це в коментарі Укрінформу повідомила заступниця міністра оборони з питань цифрового розвитку, цифрових трансформацій і цифровізації Катерина Черногоренко.

За її словами, застосунок надійно захищений.

«Застосунок «Резерв+ отримав атестат відповідності КСЗІ (комплексної системи захисту інформації). Над застосунком працювали найкращі команди з кібербезпеки та використовували найкращі успішні практики зі створення державних застосунків. Можемо запевнити, що зламати систему застосунку та отримати дані з неї неможливо, бо вона не зберігає їх», - сказала Черногоренко.

Вона пояснила, що застосунок працює за принципом Дії та отримує дані за запитом з реєстру в зашифрованому вигляді. «Ті компрометації, що вже гуляють в мережі, – фейк та намагання зірвати мобілізаційні процеси і підірвати довіру до державних застосунків», - заявила Черногоренко…» ***(Зламати Резерв+ та отримати дані із застосунку неможливо – Міноборони // Укрінформ***

(https://www.ukrinform.ua/rubric-society/3868297-zlamati-rezerv-ta-otrimati-dani-iz-zastosunku-nemozlivo-minoboroni.html). 27.05.2024).

***

«CERT-UA, яка діє при Держспецзв'язку, попереджає про значне зростання кількості кібератак, пов'язаних з діяльністю фінансово мотивованого угруповання UAC-0006.

З 20 травня 2024 року фахівці CERT-UA зафіксували дві масштабні кампанії з розповсюдження шкідливого програмного забезпечення SMOKELOADER.

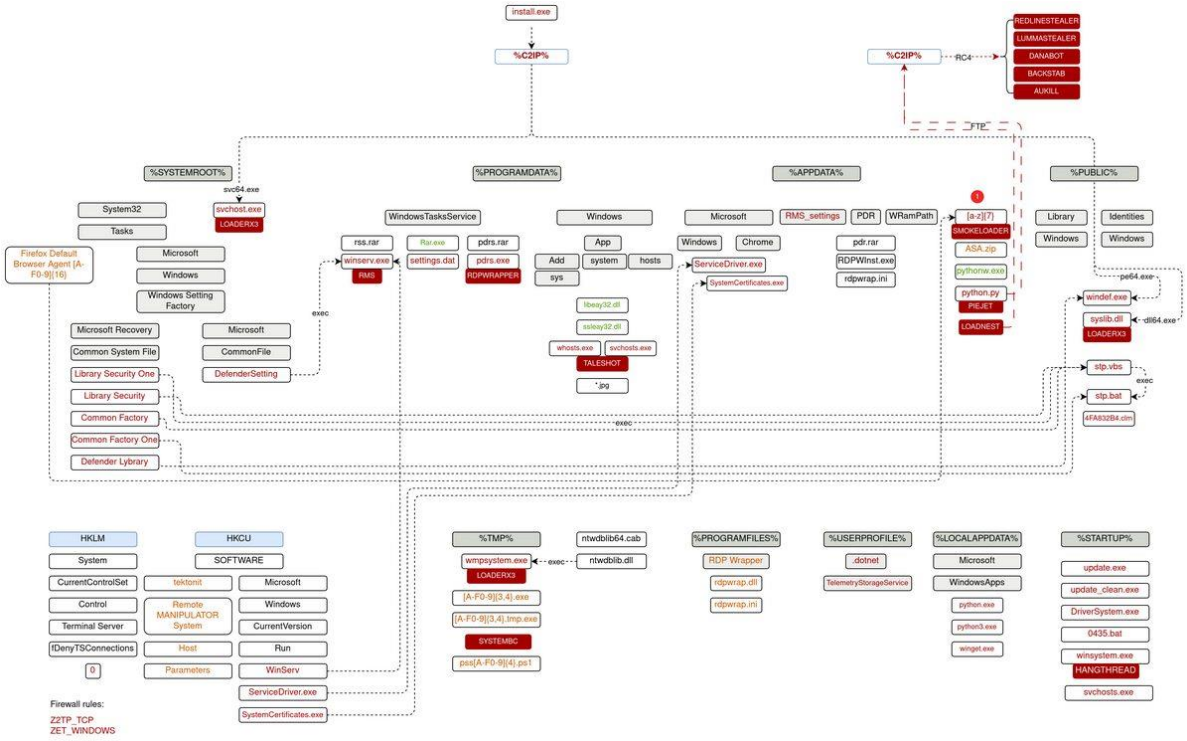
Як відбувається зараження

Зловмисники розсилають електронні листи, які містять ZIP-архіви з небезпечним вмістом:

- IMG-файли, в яких містяться EXE-файли зі шкідливим кодом;
- ACCDB-документи (Microsoft Access) з макросами, які виконують PowerShell-команди для завантаження та запуску EXE-файлів.

Після зараження на комп'ютер довантажуються інші шкідливі програми, такі як TALESHOT та RMS.

Наразі бот-мережа UAC-0006 налічує декілька сотень заражених комп'ютерів. Існує висока ймовірність, що найближчим часом зловмисники активізують шахрайські схеми з використанням систем дистанційного банківського обслуговування.



Що робити

CERT-UA закликає керівників підприємств вжити термінових заходів для підвищення кібербезпеки автоматизованих робочих місць бухгалтерів:

- перевірте комп’ютери на наявність індикаторів компрометації;
- упровадьте необхідні політики та механізми захисту…». ***(Герман Богапов. CERT-UA попереджає про ріст кібератак проти бухгалтерів // HiTech.Expert (https://expert.com.ua/182948-cert-ua-poperedzhaye-pro-rist-kiberatak-proty-buhgalteriv.html). 22.05.2024).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Естонія, у рамках роботи ІТ-коаліції, передасть Україні засоби для підсилення кіберпростору, – повідомляє прессслужба Міноборони.

«Заступниця міністра оборони України Катерина Черногоренко зустрілась із заступником командувача Кіберкомандування Сил оборони Естонії Міхкелем Тікком та керівницею департаменту кіберполітики і координаторкою ІТ коаліції з боку Міністерства оборони Естонії Лаурою Оолуп у Києві. Сторони обговорили

подальшу співпрацю щодо впровадження проєктів в межах коаліцій», – ідеться в повідомленні.

Черногоренко зазначила, що Естонія є стратегічним партнером для України і «завдяки спільній роботі Україна значно посилює можливості кіберфахівців».

У межах візиту естонська делегація провела низку зустрічей з кіберфахівцями Міністерства оборони України та Збройних сил України. Партнери окремо відзначили професійність українських фахівців та підтвердили готовність і надалі надавати експертну допомогу з питань кібербезпеки. Своєю чергою керівниця департаменту кіберполітики Міністерства оборони Естонії Лаура Оолуп відзначила високий рівень українських фахівців.

«Рівень технологічної експертизи України вражаюче високий, особливо завдяки набутому досвіду в ході повномасштабної війни проти Росії. Окрім кінетичних загроз, російська агресія охоплює також і кіберпростір. Ми готові колективно підтримати Україну необхідними засобами для отримання переваги на полі бою та обміну досвідом в межах нашого стратегічного партнерства», – зазначила Оолуп.

ІТ-коаліція – це спеціальна група держав у межах Контактної групи з питань оборони України («формат Рамштайн») під керівництвом Естонії та Люксембургу, яка зосереджена на наданні підтримки Міністерству оборони України та Збройним силам України у сфері ІТ, зв’язку та кібербезпеки.

У межах ІТ-коаліції вже вдалося зібрати фінансових та матеріальних внесків на понад 36 млн євро. Внески у розмірі понад 23 млн євро ще очікуються». ***(Іванна Капустянська. Естонія передасть Україні засоби для підсилення кіберпростору // LB.ua (https://lb.ua/world/2024/05/13/613073_estoniya_peredast_ukraini_zasobi.html).*** 13.05.2024).

***

«Корпорація Майкрософт переглядає свою практику безпеки та впроваджує ключові федеральні рекомендації після серії нещодавніх гучних порушень, які викликали занепокоєння щодо кіберпозиції глобальної корпорації.

Чарлі Белл, виконавчий віце-президент із безпеки Microsoft, заявив у п'ятницю в блозі, що компанія розширить свою ініціативу Secure Future Initiative для боротьби з ескалацією кібератак, посилення захисту конфіденційності та захисту мереж Microsoft.

«Microsoft відіграє центральну роль у світовій цифровій екосистемі, і це пов'язано з критичною відповідальністю за завоювання та збереження довіри», — сказав Белл. «Ми повинні і будемо робити більше».

Microsoft запустила свою ініціативу Secure Future Initiative у листопаді 2023 року, коли запровадила нові засоби захисту особистих даних, вимоги до розробки програмного забезпечення та швидший підхід до виявлення вразливостей і реагування на них.

Відтоді компанія стала об'єктом численних хакерських атак. Російські хакери скомпрометували його сховища вихідного коду та внутрішні системи в результаті зламу, вперше оприлюдненого в січні, а китайський загрозливий актор, відомий як Storm-0558, отримав доступ до систем Microsoft Outlook у липні, викравши електронні листи від 25 організацій.

Рада з огляду кібербезпеки у федеральному складі провела семимісячний огляд практик безпеки Microsoft після нещодавніх хакерських атак і звинуватила «корпоративну культуру компанії, яка позбавила пріоритету інвестиції в корпоративну безпеку» у тому, що вона допускала порушення безпеки, яким можна було б запобігти.

Правління рекомендувало постачальникам хмарних послуг підвищити прозорість навколо інцидентів безпеки, покращити захист цифрової ідентифікації, прийняти стандарти журналювання аудиту та сповіщати жертв про майбутні порушення.

«Вкрай важливо, щоб постачальники хмарних послуг віддавали пріоритет безпеці та створювали її за проектом», — заявив у той час у своїй заяві заступник міністра політики DHS та голова CSRB Роберт Сілверс.

У оголошенні говориться, що Microsoft «прийме більш детальний розподіл ключів підпису ідентифікаційної інформації та ключів платформи» після нещодавніх компромісів безпеки, одночасно працюючи над тим, щоб системи ідентифікації та інфраструктури відкритих ключів «готові до світу постквантової криптографії».

У блозі йдеться, що Microsoft також почне пов’язувати винагороду керівників із прогресом у досягненні певних етапів безпеки, і включатиме ці цілі як складову своїх рішень щодо найму. За словами Белла, розширена ініціатива керуватиметься трьома всеосяжними принципами безпеки: безпечний за проектом, безпечний за замовчуванням і безпечні операції.

У рамках своєї розширеної ініціативи Secure Future Initiative корпорація Майкрософт усуне повну передачу ідентифікаційних даних між орендарями, середовищами та хмарними мережами. Компанія заявила, що надалі забезпечуватиме безперервний доступ із найменшими привілеями до всіх своїх програм і користувачів і гарантуватиме, що лише «захищені, керовані, справні пристрої» зможуть отримати доступ до клієнтів Microsoft.

У оголошенні також зазначено, що Microsoft створюватиме та підтримуватиме описи програмного забезпечення для всіх активів програмного забезпечення, які використовуються для розгортання та експлуатації її продуктів і послуг. Усі журнали безпеки зберігатимуться щонайменше два роки та шість місяців і будуть доступні з центрального банку даних, «щоб забезпечити ефективне та ефективне розслідування безпеки та полювання на загрози».

На додаток до розширеної ініціативи, Microsoft заявила, що також буде впроваджувати нову структуру управління безпекою, розроблену її головним спеціалістом з інформаційної безпеки, яка включає спільні партнерства із заступниками CISO та командами інженерів.

«Зрештою, Microsoft працює на довірі, і цю довіру потрібно заслужити та підтримувати», — сказав Белл. «Ми обіцяємо постійно вдосконалюватись і адаптуватися до мінливих потреб кібербезпеки. Це робота номер один для нас». ***(Chris Riotta. Microsoft Overhauls Security Practices After Major Breaches // Information Security Media Group, Corp. (https://www.databreachtoday.com/microsoft-overhauls-security-practices-after-major-breaches-a-25130?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 06.05.2024).***

***

«…Оскільки у 2024 році в понад 70 країнах проводяться національні вибори, зараз чудовий час підвести підсумки нашого підходу до цифрової та кібернетостійкості та того, що ми маємо зробити, щоб вивести його на новий рівень.

В останньому звіті NCC Group — «Цифровий світанок: політика кібербезпеки на хвилі політичних змін» — ми використали інформацію від урядових радників, обраних посадових осіб, громадської думки, а також нашу власну роботу та дослідження, щоб визначити проблеми політики кібербезпеки в цьому бампері. рік виборів.

Якщо ви приймаєте бізнес-рішення, наш звіт показує, що ви повинні розуміти, що розподіл відповідальності за кібербезпеку змінюється. Обов’язок гарантувати вбудовану безпеку покладатиметься на постачальників. Якщо ви володієте чи керуєте критично важливою інфраструктурою, очікуйте посилення примусових заходів.

Якщо ви приймаєте політичні рішення, вам потрібно стати на передню ногу та випередити гру – те, як ви думаєте про цифрову та кіберстійкість, має налаштувати вас на довгостроковий успіх. Ми визначили п’ять ключових напрямків політики, які, на нашу думку, нові та існуючі уряди мають визначити пріоритетними для досягнення цього на практиці:

1) Прийняти кіберзакони 21 століття, які визначають обов’язки, гармонізують правила та підкріплюються належним дотриманням

Уряди повинні встановити чітку політику, законодавчу та нормативну базу, яка:

(Повторно) визначте обов’язки в межах загальної реакції суспільства вашої країни.

Поява консенсусу щодо розподілу відповідальності за кібербезпеку є величезним позитивним моментом. Але це або ще не відображено, або лише частково відображено в національній політиці, законодавчій та нормативній базах.

Уряди мають чітко визначити ролі та обов’язки всіх зацікавлених сторін у кіберекосистемі – від державних послуг, постачальників технологій та критичної інфраструктури до малого бізнесу, наукових кіл та громадян. Потім вони повинні переконатися, що цей погляд на підхід «усього суспільства» відображається в його політиці, законах і постановах.

Гармонізація правил у галузях і регіонах.

Незалежно від того, чи йдеться про стандартизацію вимог між державними кордонами, державними департаментами та секторами чи узгодження правил за міжнародними кордонами, підприємствам потрібна ясність щодо правил дорожнього руху.

Постійна відсутність узгодженості лише створюватиме дедалі складнішу мережу правил і норм. Це, ймовірно, буде контрпродуктивним для забезпечення кращої кіберстійкості та сприятиме тому, що проблема дотримання вимог кібербезпеки стане справою «галочки».

Виконуються/підлягають виконанню.

Ми закликаємо уряди запроваджувати нові правила лише там, де вони можуть ефективно та суттєво контролюватись та застосовуватися. Якщо цього не зробити, ймовірно, ті, хто ігнорував стандарти кібербезпеки, коли вони були добровільними, продовжуватимуть ігнорувати їх, коли це буде доручено.

2) Забезпечте цифрові мережі безпеки для невеликих організацій, одночасно впроваджуючи безпеку в цифрові продукти та послуги, на які вони покладаються

Наші співбесіди сказали нам, що нереалістично очікувати, що малі та середні організації дотримуватимуться тих самих стандартів кіберстійкості, що й великі компанії, і інвестуватимуть у них, залишаючи значну частину економіки вразливою до кібератак.

Натомість ми рекомендуємо урядам:

Працюйте з постачальниками технологій, щоб впроваджувати принципи безпеки за проектом і безпеки за замовчуванням у їхніх продуктах, особливо тих, на які найбільше покладаються малі підприємства.

Підтримуйте реагування невеликих організацій і відновлення після кібератак за допомогою служб «першого реагування», які надають пропорційну (безкоштовну у місці використання) підтримку малим підприємствам, які стали жертвами кібератак. Це може включати первинні послуги реагування на інциденти та сортування подальших кроків, наприклад, де жертви можуть отримати найбільш ефективну допомогу. Нещодавно уряд Австралії оголосив про Службу стійкості кібербезпеки малого бізнесу, яка може стати початком такої ініціативи.

NCC Group вважає, що ці кроки допоможуть певною мірою усунути фактори, які спричинили загальну недостатню кіберстійкість у невеликих фірмах, наприклад відсутність повернення інвестицій для консультантів з кібербезпеки, щоб надати свої послуги цьому кінці ринку. або обмеженість ресурсів і можливостей, доступних малим фірмам.

3) Зміцніть свій власний захист, інвестуючи в кіберстійкість державного сектору, зміцнюючи довіру до державних служб і показуючи приклад

Уряди повинні виконувати те, що вони проповідують, коли йдеться про кібербезпеку.

Ми визнаємо, що надання комплексних державних послуг може відвернути увагу та бюджети від кібербезпеки. Але нездатність побудувати стійкі до цифрових технологій державні служби ризикує підірвати довіру як до державних установ, так і до здатності урядових лідерів встановлювати кіберправила для інших секторів.

4) Створіть кіберстійке населення – просування кіберграмотності, розвиток кіберпрофесіоналів та оновлення кіберзаконів

Кібернавички – це не лише вирішення проблеми значного браку навичок у кіберіндустрії (хоча це є важливою частиною цього). Йдеться також про те, щоб надати людям – в організаціях будь-якого розміру та на всіх рівнях старшинства – кіберграмотність, необхідну їм для прийняття рішень щодо їх особистої, організаційної та навіть національної кіберстійкості.

З більш чітким визначенням відповідальності за кібербезпеку відповідно до підходу «всього суспільства» (див. рекомендацію 1 вище) і, незважаючи на очікуване перенесення відповідальності на тих, хто має найширші плечі, уряди повинні вжити подальших кроків, щоб дозволити окремим особам і організаціям брати активну участь в цифровій економіці.

Це має включати інноваційні заходи залучення громадян для впровадження кібербезпеки на всіх рівнях населення та вбудовування заходів гігієни кібербезпеки в психіку націй, а також зробити кіберкомпетентність (або безпечну та захищену поведінку в Інтернеті) обов'язковими елементами навчальних програм.

У той же час нам і надалі будуть потрібні як технічні, так і нетехнічні кіберпрофесіонали, щоб захищати суспільство та економіку в кіберпросторі.

Оскільки населення має більші кіберкваліфікації, потрібно зробити ще більше для заохочення талантів до кіберпрофесії, особливо тих, хто має різноманітне та недостатньо представлене середовище, а також тих, хто має наскрізні навички (наприклад, ті, які поєднують кібербезпеку та суміжні дисципліни, як-от техніка та безпека).

Це має включати зобов'язання щодо вимірювання тенденцій у частці кандидатів, які приходять у кіберпрофесію з нетрадиційного середовища та нетрадиційними шляхами, створення національних інститутів подальшої освіти для винятково обдарованих у кіберпространстві для формування національних кадрів досконалості та розробка наскрізних освітніх програм.

Вкрай важливо, щоб уряди наслідували приклад Бельгії та Німеччини в реформуванні застарілих національних комп'ютерних законів, таких як Закон Великої Британії про неправомірне використання комп'ютерів 1990 року та Закон США про комп'ютерне шахрайство та зловживання, щоб гарантувати, що

кіберпрофесіонали, які виконують законну роботу з кібербезпеки, не будуть криміналізовані.

5) Створити довгострокові, засновані на фактах структури формування політики

У розробці кіберполітики за останні кілька років можна взяти багато позитиву, включаючи надійні національні стратегії та відчутні успіхи глобальної співпраці.

Однак розробка кіберполітики часто може бути фрагментованою та розподіленою між урядами, їй важко йти в ногу з технологічними та суспільними змінами, і вона може програвати більш сприятливим для споживачів сферам політики з точки зору привернення необхідної уваги з боку політиків.

Хоча це може не бути переможцем голосування, ключовим способом вирішення багатьох із цих проблем буде створення належної інфраструктури формування політики.

В основному ми бачимо три аспекти цього:

Лідерство та міжурядова координація: Незважаючи на те, що кібербезпека й надалі залишатиметься наскрізною проблемою, яка потребуватиме уваги багатьох державних керівників і відомств, новим урядам слід подумати про те, хто в кінцевому підсумку керуватиме впровадженням їхніх національних кіберстратегій і як це буде координуватися між установами та відомствами.

Вимірність: Хороша політика базується на доказах і піддається вимірюванню. Однак у багатьох країнах немає єдиного чіткого механізму вимірювання успіху чи невдачі політики, законів і правил кібербезпеки. Тому ми підтримуємо концепцію «кібернетики як науки», розробляючи кіберметрику та кількісну оцінку ризику на основі встановленої базової лінії, щоб дозволити надійно виміряти та виразити ризик у інформований спосіб. Підхід, заснований на даних і фактах, допоможе урядам оцінити ефективність їхньої політики щодо зниження кіберризику. На практиці це може включати створення Бюро кіберстатистики, як запропоновано Комісією з кіберпростору.

Горизонтальне сканування: Централізоване урядове сканування горизонтів має зіставляти безліч існуючих ініціатив сканування горизонтів у державному секторі, приватному секторі та академічних колах, а також офіційно використовувати зворотний зв'язок у процесах розробки політики». ***(Digital Dawn: Cyber Security Policy in the Wake of Political Change // techUK (https://www.techuk.org/resource/digital-dawn-cyber-security-policy-in-the-wake-of-political-change.html). 10.05.2024).***

***

«Хоча ми знаємо, що кіберготовність важлива, компаніям може бути важко оцінити, чи достатньо вони роблять. До речі, уряд Великобританії нещодавно опублікував результати двох кіберопитувань, які можуть дати організаціям корисну інформацію про ринкову практику та те, як їхні конкуренти борються з кіберзагрозами:

«Третя хвиля» довгострокового дослідження кібербезпеки збирала дані від одних і тих же організацій за останні три роки, щоб оцінити зміни в їх кіберпрактикі з часом; і

Дослідження порушень кібербезпеки за 2024 рік, дев'ята частина цього поточного щорічного опитування уряду, надає «моментальний знімок» кібернетостійкості ринку за певний рік.

Кіберзагрози продовжують зростати

Залишається істиною те, що кіберзагрози лише зростають. За останні 12 місяців 74% великих компаній зазнали злому чи атаки (порівняно з 69% роком раніше), причому фішингові атаки були найбільш руйнівним видом (91% інцидентів).

Незважаючи на це, багатьом організаціям важко встигати за темпами змін у сфері кібербезпеки. Третя хвиля Longitudinal Survey виявила, що після початкових покращень між першою та другою хвилями кіберготовність деяких підприємств є стабільною або погіршується. Незважаючи на те, що більшість компаній все ще вважають кіберпроблеми пріоритетними (і існують помірні тенденції до зростання

кіберстійкості на ринку в цілому), зміна пріоритетів, бюджетні обмеження та економічні умови, здається, стримують кіберінвестиції.

Прихований ризик ланцюжка поставок

Обидва опитування підтверджують, що управління ризиками в ланцюзі поставок є критичним фактором кіберготовності та «основною сферою вдосконалення» для великих організацій.

Дослідження порушень показало, що лише 28% середніх і 48% великих підприємств перевіряють кіберризики, пов'язані зі своїми безпосередніми постачальниками, і лише 15% і 23% з них (відповідно) оцінюють свої ширші ланцюжки поставок. Лонгітюдне дослідження показало подібні результати, причому ці цифри майже не змінилися протягом трирічного дослідження. Очевидно, що ризик ланцюга постачання залишається основною сліпою плямою для багатьох компаній.

Наприклад, обидва опитування підтверджують, що деякі підприємства не надають пріоритету кібербезпеці при виборі постачальників цифрових послуг, таких як хмарні постачальники (DSP). Деякі покладаються на свої DSP для управління кіберризиками, відчуваючи, що у них «немає іншого вибору, окрім як довіряти» DSP із «сучасним захистом кібербезпеки». Заради чесності щодо таких клієнтів, це також може вказувати на те, що великі (особливо хмарні) постачальники можуть бути нездатними (або не бажають) змінювати свої методи безпеки відповідно до індивідуальних вимог клієнтів.

Однак резонансні порушення ланцюга постачання (такі як Capita) показують, що навіть великі постачальники можуть бути вразливими. Недавні попередження від NCSC та інших також свідчать про те, що хмарні провайдери стають дедалі більшою мішенню для деяких загроз (див. наш нещодавній блог), оскільки поширення хмарних технологій зростає. Тому важливо, щоб клієнти враховували та, де можливо, активно керували кіберризиками протягом усього життєвого циклу ланцюжка поставок. Перегляньте нашу статтю, щоб отримати кілька вказівок.

Дошки повинні керувати кораблем

Не дивно, що 98% великих компаній повідомляють, що кібернетика є пріоритетом для їх вищого керівництва. Однак, незважаючи на те, що «ради директорів визнають важливість кібербезпеки... їхня участь відносно невелика».

Наприклад, лише 30% усіх компаній мають члена правління, який безпосередньо відповідає за управління кібербезпекою, хоча цей показник зростає до 63% для великих компаній.

Важливо відзначити, що опитування показують, що сильна взаємодія з радою директорів — це не просто вправа для встановлення галочок, а й дає вимірні зміни. Продовжнє дослідження показує сильну кореляцію між кіберпредставництвом у правлінні та впровадженням критично важливих технічних засобів контролю в бізнесі, а також, можливо, вказує на те, що «організації, чиї ради директорів більше залучені до кібербезпеки, з більшою ймовірністю будуть контролювати свої системи та виявляти порушення».

Тому вкрай важливо, щоб компанії продовжували залучати свої ради директорів до кібернетики. Наша стаття містить більше інформації про кіберуправління, і (для 67% компаній, які повідомили, що не знали про це), набір інструментів правління NCSC також є чудовим ресурсом.

Кібербезпека не «встановив і забув»

Підсумовуючи зворушливе спостереження з опитувань, кіберстійкість не обов'язково є лінійною висхідною тенденцією. Незважаючи на деякі помірні покращення на ринку в цілому, кіберстійкість деяких організацій стагнує або навіть погіршується з часом, незважаючи на зростаючий кіберризик. Організації та, зокрема, ради директорів, повинні залишатися активними в управлінні ризиками кіберзагроз і йти в ногу з поточною практикою кібербезпеки (див., наприклад, останню систему 3.2 Cyber Assessment Framework NSCS, інструкції для генеральних директорів) і ризиками, що розвиваються». ***(Christopher Burns. How are your competitors managing cyber risk? Latest UK Government research on cyber published // Slaughter and May***

(https://thelens.slaughterandmay.com/post/102j6vo/how-are-your-competitors-managing-cyber-risk-latest-uk-government-research-on-cy#page=1). 03.05.2024).

***

«Близько половини (44%) фахівців з кібербезпеки стикаються з дотриманням законодавства про кібербезпеку через його складність і витрати часу, показало дослідження Infosecurity Europe.

Опитування 200 осіб, які приймають рішення в галузі IT-безпеки, проаналізувало погляди на 12 нормативних актів, пов'язаних із кібербезпекою, які діють або незабаром будуть введені в дію, включаючи Закон Сарбейнса-Оксли США (SOX) і директиву ЄС NIS2.

Такі нормативні акти, як SOX, вважають «дуже складними» для дотримання 41% респондентів.

Крім того, три чверті сказали, що Закон Великобританії про захист даних (DPA), NIS/NIS2 і Закон ЄС про кібербезпеку є «дещо складними».

Лише завдяки SOX і Закону ЄС про кібербезпеку понад 50% організацій досягли повної відповідності, що підкреслює труднощі, з якими стикаються, щоб не відставати від зростаючих нормативних зобов'язань.

Лише 0,50% респондентів сказали, що жодне з 12 правил не стосується їхньої організації.

Відповідність є ключовим фокусом Infosecurity Europe 2024

Цьогорічна європейська конференція Infosecurity приверне увагу до критичних проблем відповідності та регулювання, а також запропонує найкращі практичні поради щодо того, як випереджати цей ландшафт, що розвивається.

У програму буде включено виступ Рохана Мессі, партнера Ropes & Grey LLP, який відбудеться на Keynote Stage у середу, 5 червня, з 11.50 до 12.15.

У своїй доповіді під назвою «Оновлення законодавства про кібербезпеку – що буде далі і як це вплине на вас» Мессі обговорить, як передбачити майбутні нормативні зміни та їхній вплив на бізнес. До них належать норми NIS2, які набудуть чинності з жовтня 2024 року, і те, що ще, ймовірно, стане законом.

Крім того, він дослідить, чим відрізняються стратегії відповідності між галузевими секторами та як підприємства можуть керувати різними рівнями складності.

Мессі прокоментував: «Навігація в постійно мінливому ландшафті законодавства про цифрову та кібербезпеку має першочергове значення для компаній, які прагнуть підтримувати відповідність і стійкість. Попередньо дивлячись на Infosecurity Europe 2024, я з нетерпінням хочу обговорити неминучі зміни на горизонті, включаючи впливових нормативних актів NIS2 і заглибитись у їхні наслідки для операційних стратегій.

«Від вивчення глобальних законодавчих тенденцій до розшифровки тонкощів відповідності між галузевими секторами, моя мета полягає в тому, щоб озброїти організації знаннями та ідеями, необхідними для того, щоб залишатися попереду».

Мессі відомий своїм досвідом у законодавстві з кібербезпеки та є довіреним радником багатьох найбільших світових корпорацій і фондів прямих інвестицій, зосереджуючись на складних питаннях захисту даних і кібербезпеки.

Він також консультував у низці провідних випадків управління даними про порушення та допомагав клієнтам успішно отримати схвалення BCR від регуляторних органів ЄС.

Ніколь Міллс, директор заходів Infosecurity Europe, наголосила на нагальній потребі організацій у покращенні своїх стратегій відповідності сьогодні.

«Регулювання продовжує відігравати вирішальну роль у кібербезпеці – сприяючи вдосконаленням, захищаючи конфіденційні дані, сприяючи підзвітності, сприяючи стійкості, стимулюючи інновації, вирішуючи глобальні виклики та зміцнюючи довіру до цифрової економіки», – заявив Міллс.

«Проте наше дослідження виявило, що відповідність нормативним вимогам є перешкодою, яку більшість організацій ще не подолали. Ми з нетерпінням чекаємо виступу Рохана Мессі на Infosecurity Europe 2024. Його висновки, безсумнівно, стануть безцінними вказівками для компаній, які прагнуть посилити свої зусилля з дотримання нормативних вимог і підвищити стійкість своєї кібербезпеки», – додала вона…» ***(James Coker. 44% of Cybersecurity Professionals Struggle with Regulatory***

Compliance // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/cyber-pros-struggle-regulatory/). 14.05.2024).

***

«Згідно з даними Всесвітнього економічного форуму, індустрії кібербезпеки потрібні майже чотири мільйони професіоналів, оскільки глобальна нестача працівників починає вражати цей сектор.

У своїй останній білій книзі WEF стверджує, що до 2030 року глобальний дефіцит талантів досягне понад 85 мільйонів працівників.

«Індустрія кібербезпеки також постраждала від цієї поширеної проблеми», — йдеться у звіті. «У той час як у період з 2022 по 2023 рік чисельність працівників у сфері кібербезпеки зросла на 12,6%, у всьому світі не вистачає майже чотирьох мільйонів спеціалістів із кібербезпеки».

Розподіл дефіциту робочої сили

Згідно зі звітом, брак найбільш очевидний в Азіатсько-Тихоокеанському регіоні, якому потрібно понад 2,5 мільйона працівників кібербезпеки.

У Північній Америці нестача робочої сили становить 522 000 осіб, тоді як в Африці з 1,4 мільярда населення лише близько 20 000 є сертифікованими спеціалістами з безпеки.

Згідно зі звітом, дефіцит талантів найбільше спостерігається в Китаї, Індії, Сполучених Штатах і Бразилії.

Відповідно до звіту, в Індії, яка має найбільше у світі населення молоді, приблизно 40 000 вакансій залишаються незаповненими для фахівців з кібербезпеки.

У США також є приблизно 448 000 вакансій у сфері кібербезпеки в приватному та державному секторах.

Фактори дефіциту робочої сили

Згідно зі звітом, фактори, що сприяють нестачі робочої сили, включають швидку еволюцію ландшафту кібербезпеки.

Це «випереджає розвиток відповідної робочої сили», йдеться у звіті.

Іншим чинником є відсутність різноманітності в робочій силі, де менше професіоналів серед жінок, мігрантів, етнічних меншин і співробітників із нейродиверсифікацією.

Згідно зі звітом, інші фактори, що сприяють дефіциту, включають:

- Нездатність деяких роботодавців конкурувати із зарплатами, які пропонують інші організації
- Неузгодженість освітніх програм
- Змінні потреби галузі кібербезпеки
- Відсутність ясності щодо кар'єрних можливостей у цій галузі
- Усунення дефіциту
- Щоб вирішити проблему дефіциту робочої сили з кібербезпеки, у звіті визначено чотири ключові пріоритетні сфери, зокрема:
- Залучення талантів у кібербезпеку
- Навчання та навчання фахівців з кібербезпеки
- Наймання відповідних спеціалістів із кібербезпеки
- Утримання фахівців з кібербезпеки

«Важливо зазначити, що чотири пріоритетні сфери слід розглядати не ізольовано, а як взаємопов'язані компоненти комплексного підходу до управління талантами в галузі кібербезпеки», – йдеться у звіті.

Серед рекомендацій щодо залучення талантів у кібербезпеку є гнучкість і здатність адаптуватися відповідно до мінливого ландшафту сектора.

Роботодавці також повинні пропонувати конкурентоспроможні зарплати та комплексні пакети пільг, висвітлювати можливості навчання та розвитку кар'єри, зосереджуючи увагу на підвищенні кваліфікації та заохоченні внутрішніх талантів, а також віддавати пріоритет різноманітності та інклюзії». ***(Dexter Tilo. Cybersecurity industry short nearly 4 million professionals // KM Business Information Australia Pty Ltd (https://www.hcamag.com/asia/news/general/cybersecurity-industry-short-nearly-4-million-professionals/489141). 15.05.2024).***

***

«Протягом багатьох років відсоток жінок у сфері кібербезпеки не змінювався на рівні 20-25%, але нещодавнє дослідження показує багатообіцяючу тенденцію: все більше жінок обіймають керівні посади в сфері кібербезпеки, і вони залишаються на цих посадах, сказала Клар Россо, Генеральний директор ISC2.

Россо підкреслила важливість безперервної освіти та сертифікації як інструментів професійного розвитку. «Сертифікації, зокрема, є демонстрацією компетентності та широко поважаються», - сказала вона. Такий підхід не тільки надає жінкам необхідні навички, але й підвищує їхній професійний профіль на конкурентному ринку.

«Сертифікати визнані в усьому світі, і роботодавці прагнуть їх шукати», — сказала Россо. «У нас є дані, які свідчать про те, що понад 80% роботодавців воліли б бачити когось із дипломом, а не з університетським дипломом»…

Россо відповідає за стратегічний напрямок і управління ISC2. Вона має понад два десятиліття досвіду, допомагаючи глобальним професійним асоціаціям і органам сертифікації розвивати та зміцнювати цінність членів». ***(Anna Delaney. Women in Cybersecurity: Light at the End of the Tunnel? // Information Security Media Group, Corp. (https://www.govinfosecurity.com/women-in-cybersecurity-light-at-end-tunnel-a-25083). 13.05.2024).***

***

«У складному ландшафті кібербезпеки випливає суперечлива істина: люди є як найслабшою ланкою, так і найсильнішим активом у захисті систем від кібератак. Ця подвійність виникає через складну взаємодію між людською поведінкою, технологічною вразливістю та тактикою кіберзлочинців, яка постійно змінюється.

З кількох причин людський фактор часто вважається найслабшою ланкою кібербезпеки.

1. Вразливість до соціальної інженерії: кіберзлочинці є експертами в експлуатації людської психології за допомогою методів соціальної інженерії.

Фішингові електронні листи, SMS-шахрайство та цькування – це лише кілька прикладів того, як зловмисники маніпулюють людьми, змушуючи їх розголошувати конфіденційну інформацію, натискати шкідливі посилання чи завантажувати зловмисне програмне забезпечення.

2. Ненавмисні помилки: навіть працівники з добрими намірами можуть ненавмисно порушити безпеку. Прості помилки, як-от потрапити на фішинг, використання ненадійних паролів або неправильне розташування пристроїв, можуть створити точки входу для кібератак. Крім того, співробітники можуть несвідомо встановити неавторизоване програмне забезпечення або обійти протоколи безпеки, поставивши під загрозу всю мережу.

3. Недостатня обізнаність: багато порушень безпеки є результатом недостатньої обізнаності користувачів щодо кібербезпеки. Співробітники можуть не знати про останні загрози, методи безпечного перегляду чи важливість дотримання політики безпеки. Це незнання робить їх сприйнятливими до маніпуляцій і нападів.

4. Внутрішні загрози: у деяких випадках незадоволені співробітники або зловмисні інсайдери можуть навмисно порушити безпеку. Це може включати викрадення даних, саботування систем або надання доступу зовнішнім зловмисникам. Інсайдерські загрози небезпечні, оскільки вони часто мають привілейований доступ і знання про вразливі місця організації.

5. Опір змінам: люди часто опираються змінам у своїх розпорядках, навіть якщо ці зміни підвищують безпеку. Складні процедури безпеки, часті оновлення та обмеження певних дій можуть сприйматися як незручні або руйнівні, що призводить до невідповідності та підвищеного ризику.

Незважаючи на ці вразливості, люди також можуть бути найсильнішою ланкою в кібербезпеці, якщо вони належним чином уповноважені та освічені.

1. Раннє виявлення загроз: співробітники часто першими помічають підозрілу активність, наприклад незвичайні спроби входу, запити на неавторизований доступ або встановлення незнайомого програмного забезпечення. Їхня пильність може

призвести до раннього виявлення та стримування загроз, запобігаючи переростанню незначних інцидентів у серйозні порушення.

2. Реагування на інциденти: коли трапляються інциденти безпеки, співробітники відіграють вирішальну роль у стримуванні збитків. Оперативне повідомлення про підозрілі електронні листи, зламані облікові записи або незвичайну поведінку системи дозволяє командам безпеки швидко й ефективно реагувати.

3. Культура безпеки. Сильна культура безпеки, коли працівники знають свою роль у захисті активів компанії та беруть активну участь у заходах безпеки, може значно покращити загальну кібербезпеку організації. Регулярне навчання, просвітницькі кампанії та відкриті канали спілкування сприяють усвідомленню спільної відповідальності за безпеку.

4. Людський брандмауер: навчаючи співробітників тактиці соціальної інженерії, методам безпечного перегляду та важливості захисту даних, організації можуть створити «людський брандмауер», який доповнює технологічний захист. Добре поінформовані співробітники з меншою ймовірністю попадуться на фішингові шахрайства, натиснуть зловмисні посилання або розкриють конфіденційну інформацію.

5. Постійне вдосконалення. Відгуки та ідеї співробітників можуть бути неоціненними для виявлення слабких місць у політиках і процедурах безпеки. Організації можуть постійно підвищувати рівень кібербезпеки, заохочуючи співробітників повідомляти про потенційні вразливості та пропонувати покращення.

У безперервній боротьбі з кіберзагрозами люди є двосічним мечем. Зловмисники можуть використовувати їх вразливі місця, але їхня пильність, обізнаність і активна участь у заходах безпеки є важливими для побудови надійного захисту.

Для організацій, які підтримуються урядовими ініціативами з кібербезпеки, вкрай важливо інвестувати в комплексні програми навчання, сприяти розвитку культури обізнаності про безпеку та розширювати можливості працівників як

основного засобу захисту від кібератак. Визнаючи подвійний потенціал людей як найслабшої та найсильнішої ланок, ми можемо створити більш стійке та безпечне цифрове майбутнє. Цей підхід узгоджується з більш широкими цілями державної політики щодо підвищення готовності національної кібербезпеки». ***(Art Samaniego. The two faces of cybersecurity: Humans as both risk and asset // Manila Bulletin Publishing Corporation (https://mb.com.ph/2024/5/14/the-two-faces-of-cybersecurity-humans-as-both-risk-and-asset). 13.05.2024).***

***

«У сучасному цифровому середовищі надійні інструменти оцінки ризиків кібербезпеки мають вирішальне значення для ефективного виявлення та пом'якшення кіберзагроз. Ці інструменти служать першою лінією захисту, допомагаючи організаціям визначати пріоритетність ризиків, ефективно розподіляти ресурси та зміцнювати свою цифрову інфраструктуру. Інтегровані в цикл управління кіберризиками, оцінки ризиків забезпечують постійне розуміння мінливих загроз, дозволяючи організаціям завчасно адаптувати свої стратегії безпеки. Проводячи регулярні оцінки кіберризиків, організації можуть випереджати кіберзлочинців, мінімізувати вразливі місця та підтримувати стійку безпеку, захищаючи свої дані та операції від потенційних порушень і збоїв.

Критичні можливості інструментів оцінки ризиків кібербезпеки

Оцінка вразливості: Надійний інструмент оцінки ризиків повинен мати можливість проводити комплексне сканування систем, мереж і програм, виявляючи вразливості та слабкі місця, готові для використання зловмисниками. Цей процес передбачає сканування мережі, тестування на проникнення та перевірку коду для виявлення потенційних точок входу для кібератак.

Кількісна оцінка кіберризиків. Оцінка кібербезпеки повинна кількісно оцінювати ризики за допомогою складних механізмів підрахунку балів, визначаючи їх пріоритетність на основі серйозності, можливості використання та потенційного впливу. CyberStrong, наприклад, використовує такі моделі, як FAIR (факторний аналіз інформаційних ризиків) і NIST 800-30, щоб кількісно оцінити

ризики в термінах «цінності втрат», допомагаючи в прийнятті стратегічних рішень. Призначаючи оцінки ризику виявленим вразливостям, організації можуть ефективно визначати пріоритети своїх зусиль з усунення, зосереджуючись на першочерговому усуненні найбільш критичних ризиків.

Всебічне покриття: Сфера кіберзагроз не має меж, тому потрібні інструменти з повним охопленням усієї IT-інфраструктури, включаючи мережі, кінцеві точки, хмарні середовища та програми. Інструмент ретельної оцінки ризиків повинен бути здатний оцінювати ризики в усіх цих аспектах IT-середовища, надаючи цілісне уявлення про стан безпеки організації.

Моніторинг безперервного контролю: завдяки інтеграції можливостей безперервного моніторингу та перевірки відповідності організації можуть завчасно передбачати нові загрози, забезпечуючи дотримання нормативних вимог через перехід. CyberStrong Система Continuous Compliance Automation (CCA) проводить постійну оцінку кіберризиків, виявляючи прогалини в системі контролю в інфраструктурі безпеки. Цей процес дозволяє групам безпеки пов’язувати засоби контролю з конкретними ризиками, сприяючи обґрунтованому управлінню ризиками та прийняттю рішень щодо пом’якшення. Крім того, CCA автоматизує перевірку відповідності нормам, таким як GDPR, HIPAA та PCI DSS, швидко виявляючи прогалини та області невідповідності для своєчасного усунення. Використовуючи безперервний моніторинг контролю, організації підвищують стійкість своєї кібербезпеки та відповідність нормативним вимогам, мінімізуючи вразливі місця та зміцнюючи загальну безпеку.

Інтеграція з каналами аналізу загроз. Інтеграція з каналами аналізу загроз додатково підвищує точність оцінки ризиків кібербезпеки, надаючи доступ до інформації в реальному часі про нові загрози та відомі вектори атак. Ця інтеграція дозволяє організаціям використовувати колективні знання спільноти з кібербезпеки для покращення своїх можливостей оцінки ризиків. Наприклад, інтеграція CyberStrong Snowflake дозволяє організаціям імпортувати дані аналізу загроз із зовнішніх джерел, збагачуючи свої оцінки ризиків актуальною інформацією про нові загрози.

Гнучкість: гнучкість життєво важлива, оскільки кожна організація має унікальні вимоги та профілі ризику. Параметри налаштування дають можливість організаціям адаптувати процеси оцінювання та звітність відповідно до своїх потреб. Ця гнучкість дозволяє організаціям адаптувати інструмент оцінки ризиків до свого унікального середовища, гарантуючи, що він відповідає їхнім конкретним вимогам і надає практичну інформацію, яка стимулює ефективні стратегії управління ризиками.

Звітування та візуалізація: чіткі та вичерпні можливості звітування є важливими для ефективного інформування зацікавлених сторін про результати оцінки ризиків. Такі функції візуалізації, як діаграми, графіки та інформаційні панелі, допомагають зрозуміти складні дані та тенденції. Керівницька інформаційна панель надає високорівневу інформацію про стан кібербезпеки організації, тоді як інформаційна панель управління пропонує детальну інформацію для команд безпеки. Теплові карти візуально представляють розподіл ризиків, виділяючи проблемні області, а спеціальні шаблони слів дозволяють створювати індивідуальні звіти для різних зацікавлених сторін, забезпечуючи ефективне спілкування та прийняття рішень.

Автоматизовані робочі процеси виправлення. Автоматизовані робочі процеси виправлення оптимізують усунення виявлених вразливостей, скорочуючи час на виправлення та мінімізуючи вплив кіберзагроз. Автоматизуючи процес виправлення, організації можуть прискорити реагування на інциденти безпеки та вразливості, зменшивши загальний ризик і підвищивши рівень кібербезпеки організації. Використовуючи можливості програмного забезпечення CyberStrong Risk Remediation, організації можуть безперебійно організовувати й автоматизувати дії з усунення ризиків, забезпечуючи швидке й ефективне реагування на нові загрози й уразливості, ще більше зміцнюючи свої засоби захисту.

Масштабованість: масштабованість гарантує, що інструмент може відповідати змінним потребам організацій, незалежно від розміру чи складності. Масштабований інструмент оцінки ризиків повинен обробляти великі обсяги даних і підтримувати зростаючих користувачів і активи. Така масштабованість дає змогу

організаціям масштабувати свої зусилля з управління ризиками в міру зростання бізнесу, забезпечуючи ефективне керування кіберризиками в усій організації.

Моделювання загроз і аналіз сценаріїв. Розширені можливості моделювання загроз і аналізу сценаріїв дозволяють організаціям симулювати потенційні загрози та їхні наслідки, створюючи кращі стратегії зменшення ризиків. Моделюючи різні сценарії загроз, організації можуть оцінити потенційний вплив кіберзагроз на свої бізнес-операції та відповідно визначити пріоритети своїх зусиль з управління ризиками. Цей проактивний підхід до управління ризиками дозволяє організаціям виявляти й усувати потенційні вразливості до того, як ними зможуть скористатися зловмисники, зменшуючи загальний ризик і підвищуючи стійкість організації до кіберзагроз.

Враховуючи ці важливі можливості, організації можуть вибрати інструменти оцінки ризиків кібербезпеки, які найкраще відповідають їхнім потребам і ефективно зменшують кіберризики. Це дає їм змогу впевнено та стійко орієнтуватися в ландшафті загроз, що постійно змінюється. Завдяки комплексним інструментам оцінки ризиків, таким як CyberStrong, організації можуть покращити свою кібербезпеку та захистити свої критично важливі активи від зростаючої загрози кібератак». ***(Cameron Delfin. Critical Capabilities of Cyber Security Risk Assessment Tools // CyberSaint Security (https://www.cybersaint.io/blog/cyber-security-risk-assessment-tools). 20.05.2024).***

***

«Ландшафт кіберризиків постійно змінюється. Зовсім недавно деякі з найбільш тривожних змін, які відбулися в ландшафті, зосереджені на сторонніх службах. Незважаючи на те, що сторонні служби є цінними партнерами для бізнесу, вони, природно, діють поза основними операціями та захистом корпоративної мережі, а тому є потенційно слабкою ланкою в захисті кібербезпеки будь-якої організації.

Коли ми запитали нашу групу з понад 400 компаній середнього ринку про їхній досвід кібербезпеки за останній рік, 25% з них стикалися з постачальником

послуг, який постраждав від витоку даних або кібератаки в минулому році, що вплинуло на їхні фінанси та репутацію. або оперативно. Це було лише на 17%, коли ми запитували у 2022 році.

Хоча атака третьої сторони може не бути прямою атакою на організацію, важливо, щоб компанії усвідомлювали, яка відповідальність їм загрожує, якщо сторонній постачальник, якого вони найняли, зазнає успішної кібератаки. Це особливо важливо, оскільки зростає тенденція орієнтації на третіх сторін.

Чому сторонні постачальники є такими привабливими цілями?

З компаній нашої панелі, які зазнали кібератак протягом останнього року, 78% з них зазнали атак в результаті того, що постачальник або третя сторона стали мішенню загрози. І 36% з них стали жертвами викрадення даних через скомпрометацію постачальника. Тож чому треті сторони є такою привабливою ціллю?

Сукупне націлювання

Частину уваги учасників загрози на сторонніх постачальниках можна пояснити дуже привабливою сукупною вигодою в результаті успішного злому. На додачу до потенційної «слабкої нижньої частини», яку представляє сторонній постачальник у ланцюжку кібербезпеки організації, багато з цих постачальників також обробляють або зберігають значну кількість даних клієнтів, таким чином пропонуючи плідну економію масштабу для кіберзлочинців». робочі зусилля.

Наприклад, сторонні постачальники пенсійного сектору зберігають величезну кількість надзвичайно конфіденційних даних клієнтів. Зловмисник, який успішно проникне до такого постачальника, отримає доступ до даних у великому масштабі та спричинить хвильовий ефект збою в роботі всіх організацій, які використовують цього постачальника. Вигоди та збитки від націлювання на такі види бізнесу значні та впливові.

Доступ до систем

Для суб’єктів загрози, які мають на меті розгортання зловмисного програмного забезпечення, успішне проникнення в системи третьої сторони забезпечує аналогічну економію масштабу. Це особливо хвилює постачальників

програмного забезпечення. Здатність проникнути в ці агрегатні середовища в якості «безвізового» забезпечує доступ до багатьох інших систем та інфраструктури.

Якщо загроза може маніпулювати постачальником програмного забезпечення та приховувати шкідливий код в оновленні програмного забезпечення, яке розповсюджується багатьом клієнтам, це шкідливе програмне забезпечення може отримати доступ до інфраструктури клієнта у великих масштабах.

Залишаючись на вершині провини

Хоча атаки третіх сторін не вважаються прямими нападами на підрядну організацію, відповідальність рідко несе лише постачальник. Оскільки організація найняла постачальника для виконання роботи від її імені, успішна кібератака несе довгострокову відповідальність і наслідки, зокрема відповідно до GDPR у Великобританії, якщо під час атаки було порушено особисті дані.

Викладення умов договору під час переговорів є першим кроком у встановленні відповідальності. Організації повинні забезпечити наявність надійних процесів належної перевірки як частину адаптації та включити положення про кібербезпеку в умови контракту. Також важливо, щоб угоди окреслювали, як буде повідомлятися про кіберподії між обома сторонами. Багато організацій не мають посібника з реагування на інциденти, який містить інформацію про третіх сторін і те, як вони будуть реагувати, однак це має бути ключовим фактором, оскільки сторонні постачальники відіграють ключову роль у забезпеченні ефективності реагування або розслідування після нападу.

Зростаюча актуальність сертифікатів

Сертифікати, такі як Cyber Essentials та ISO 27001, можуть запропонувати певну ефективність під час належної перевірки під час встановлення нових відносин із постачальником.

Процес належної перевірки залучення нових третіх сторін може бути тривалим. Обсяг інформації, необхідний для встановлення того, що постачальник має ефективні засоби контролю та процеси для захисту надання послуг, може бути значним. Від постачальників зазвичай очікують відповіді на велику кількість

запитань, що, як правило, впливає на їхні ресурси, а це означає, що процес укладання контрактів може бути тривалим і важким.

Отримання незалежно перевіреної акредитації з кібербезпеки може допомогти зменшити тягар. Він повідомляє потенційним клієнтам і замовникам, що мінімальні стандарти, які вимагаються цими сертифікатами, були виконані, пропонуючи гарантію та ефективність у тендерному процесі. 80% учасників нашої комісії сказали, що отримання акредитації безпеки у 2024 році є ключовою проблемою для їхнього бізнесу, щоб продемонструвати, що вони забезпечують належний рівень безпеки для захисту довіреної їм інформації.

Ці сертифікати допомагають встановити мінімальні стандарти, особливо в галузях, які менш регульовані. Для багатьох організацій треті сторони, які мають кібер-акредитацію, вважаються перевагою в процесі прийняття тендерних рішень.

Висновок

У міру того як технологічний ландшафт розвивається, багато компаній прийняли модель аутсорсингу, що включає положення IT та кібербезпеки. Ця зміна поведінки не залишається непоміченою суб'єктами загрози, які бачать третіх сторін як привабливу ціль і слабку ланку в ланцюжку безпеки. Хоча аутсорсинг приносить із собою цінність і задовольняє потреби бізнесу, він також збільшує ризик проблем із безпекою даних і порушення нормативних вимог.

Кількість кібератак на сторонніх постачальників зростає, і ми очікуємо, що з розширеним використанням штучного інтелекту в кібератаках це буде зростати з виконанням у промислових масштабах із використанням ретельно скоординованих, складних і далекосяжних методів, які стають легшими для суб'єктів загрози. Щоб протистояти цьому, життєво важливо, щоб організації мали довіру не лише до своїх власних систем, а й до систем своїх сторонніх постачальників». ***(Sheila Pancholi. Managing third-party risk with cyber security // RSM UK Group LLP (https://www.rsmuk.com/insights/real-economy/cybersecurity/managing-third-party-risk-with-cyber-security). 21.05.2024).***

***

«Кібербезпека стала однією з головних проблем для урядів у всьому світі, оскільки вона може поставити під загрозу національну безпеку та промисловість, що створює системний ризик для стабільності. У відповідь на цю ескалацію загрози регулятори борються з проблемою розробки ефективного законодавства з кібербезпеки для захисту критичної інфраструктури та промисловості. Однак навігація в складному законодавчому ландшафті є серйозною проблемою для бізнесу, оскільки вимоги дотримання різняться в різних галузях, розмірах організацій і географічних регіонах.

Важливо йти в ногу зі змінами, оскільки чинне законодавство визначає найнижчі стандарти кіберконтролю та встановлює базовий рівень очікувань. З огляду на занепокоєння щодо того, як штучний інтелект (ШІ) вплине на ландшафт кіберризиків, законодавство буде лише суворішим.

Потреби промисловості

Існуюча законодавча база характеризується індустріальними ініціативами. Наприклад, водна промисловість встановлює власні очікування щодо кібербезпеки. Незважаючи на те, що стандарт 27001 Міжнародної організації зі стандартизації (ISO) протягом багатьох років був загальноприйнятим галузевим стандартом, організації все частіше застосовують інші структури, такі як Center for Internet Security 18 (CIS 18), NIST і нещодавно NIS2, щоб посилити захист своєї кібербезпеки.

Демонстрація дотримання цих рамок стала стандартною передумовою для роботи в регульованих галузях, що підкреслює важливість бути в курсі законодавчих вимог, що змінюються.

Такі галузі, як фінанси, комунальні послуги та охорона здоров’я, є одними з найбільш регульованих. Фінансові установи, включно з банками, постачальниками платіжних послуг і страховими компаніями, підпадають під дію таких нормативних актів, як Посібник Управління з питань фінансової поведінки (FCA), правила операційної стійкості та Стандарт безпеки даних індустрії платіжних карток (PCI DSS), які передбачають спеціальні засоби контролю кібербезпеки. для захисту фінансової інформації клієнта та запобігання шахрайству. Закон про цифрову

операційну стійкість (DORA) нормативно-правової бази для цифрової операційної стійкості установ, що надають фінансові послуги, також набуває чинності в Європі пізніше цього року.

Законодавство природно розвивалося залежно від галузі, оскільки забезпечити дотримання загального законодавства в багатьох галузях надзвичайно складно. Природно, що тому встановлюються законодавчі вимоги, а сильні галузеві регулятори забезпечують дотримання стандартів кібербезпеки та покращують їх.

Галузі, які перебувають поза чинним законодавством

Певні галузі, як-от роздрібна торгівля та споживчі ринки, працюють у середовищі, яке має обмежене законодавство, яке стосується кібербезпеки. На відміну від більш регульованих секторів, таких як фінансові послуги чи охорона здоров'я, де вимоги дотримання чітко визначені, такі галузі, як роздрібна торгівля, піддаються меншому контролю.

Однією з головних причин відсутності спеціального законодавства з кібербезпеки в цих галузях є відносно нижчий сприйнятий системний ризик порівняно з секторами, пов'язаними з фінансами, конфіденційними даними чи критичною інфраструктурою. Незважаючи на те, що ринки роздрібної торгівлі та споживчі ринки, безумовно, стикаються з кіберзагрозами, такими як шахрайство з платіжними картками та витік даних, регулятивні органи часто зосереджуються на захисті споживачів, а не на кібербезпеці.

Однак відсутність спеціального законодавства про кібербезпеку не означає, що кібербезпека не є пріоритетом для компаній, які працюють у цих галузях. Багато роздрібних торговців усвідомлюють важливість захисту даних клієнтів і збереження довіри до репутації свого бренду.

Хоча регулятивний нагляд може бути меншим, підприємства в цих секторах часто дотримуються таких галузевих стандартів, як PCI DSS і ISO 27001, щоб продемонструвати свою відданість найкращим практикам кібербезпеки.

Прищеплення оперативної стійкості

В основі урядових законодавчих програм лежить мета прищеплення операційної стійкості в організаціях і ширшій економічній інфраструктурі.

Встановлюючи ефективні засоби контролю кібербезпеки, законодавці прагнуть захистити критичну інфраструктуру та галузі, які можуть мати системний вплив у разі атаки.

Однак галузі, на які не поширюється дію чинного законодавства, стикаються з унікальними проблемами в навігації серед кіберризиків. Без чітких нормативних вказівок організації повинні вживати профілактичних заходів для посилення захисту своєї кібербезпеки та пом'якшення нових загроз.

Європейське законодавство стосується британських організацій

Європейський Союз (ЄС) намагається запровадити мінімальний рівень контролю безпеки у своїх державах-членах. Окрім Загального регламенту захисту даних (GDPR), у жовтні 2024 року та січні 2025 року набувають чинності два законодавчі акти, які допомагають встановити цей контроль, Директива 2 про мережеву й інформаційну безпеку (NIS2) і DORA.

Незважаючи на те, що NIS2 безпосередньо не застосовується до підприємств Великобританії, NIS2 вплине на організації в різних галузях, що працюють на міжнародному рівні, причому на фірми, що надають фінансові послуги, постраждають від обох. Організації повинні розглянути, чи підпадають вони під дію директив ЄС і як їхні системи та інфраструктура використовуються для надання послуг клієнтам із ЄС або частинам їхньої організації в ЄС. Організаціям потрібно буде розглянути, як взаємодіють нормативні акти, директиви, акти та законодавство та як вони можуть успішно керувати відповідністю, а це може бути складно визначити…

Глобальний виклик ШІ

Як правило, трансформаційна технологія з'являється та приймається до того, як уряди можуть сформувати відповідні правила. Від широкого використання Інтернету в 1990-х роках до 2023 року прийнято будь-який закон (законопроект про безпеку в Інтернеті), який забезпечує безпеку в Інтернеті. AI не є винятком. Перед самітом безпеки штучного інтелекту у 2023 році британський уряд заявив, що не поспішатиме з регулюванням під час оголошення про створення органу безпеки штучного інтелекту у Великобританії.

Однак, оскільки штучний інтелект продовжує все більше застосовуватися в галузях, занепокоєння щодо його потенціалу зловмисного використання в кібератаках стає все більш поширеним. У той час як уряди повільно регулюють штучний інтелект, нещодавні ініціативи, такі як Закон Європейського Союзу про штучний інтелект, свідчать про зростаюче визнання необхідності регуляторного нагляду. Однак темпи регуляторних заходів можуть не встигати за технологічними інноваціями, що змушує організації самостійно боротися з ризиками, пов'язаними з ШІ.

Небажання деяких урядів поспішати з регулюванням штучного інтелекту, включаючи Великобританію, відображає складні етичні та технічні міркування. Хоча ШІ має величезний потенціал для стимулювання інновацій та ефективності, його неправильне використання створює значні ризики для кібербезпеки. Оскільки політики порівнюють потребу в регулюванні з імперативом сприяння інноваціям, підприємства повинні обережно орієнтуватися в мінливому нормативному ландшафті.

Залишаючись попереду

Перетин кібербезпеки та законодавства представляє складний ландшафт, що розвивається, у якому компанії повинні орієнтуватися. У той час як галузеві ініціативи та урядові мандати забезпечують основу для підвищення стійкості кібербезпеки, швидкий розвиток технологій створює нові виклики. Організації повинні зберігати пильність у моніторингу законодавчих розробок і активно адаптувати свої стратегії кібербезпеки для пом'якшення нових загроз. Залишаючись на випередження, компанії можуть ефективно орієнтуватися в законодавчому ландшафті кіберризиків і захищати свою діяльність у все більш цифровому світі». ***(Sheila Pancholi. How to stay on top of evolving cyber security legislation // RSM UK Group LLP (https://www.rsmuk.com/insights/real-economy/cybersecurity/how-to-stay-on-top-of-evolving-cyber-security-legislation). 21.05.2024).***

***

«Стійкість до кібербезпеки має першочергове значення для будь-якої організації в світі, що стає все більш цифровим, де швидко розвиваються загрози кібербезпеці та зростають вимоги до захисту даних. У цьому мінливому ландшафті ризиків головний спеціаліст з інформаційної безпеки (CISO) відіграє вирішальну роль у зміцненні кібербезпеки організації...

Зрозумійте базову лінію вашої програми кібербезпеки

Перш ніж запроваджувати план дій щодо покращення кібербезпеки організації, CISO повинен мати чітке уявлення про поточні засоби контролю кібербезпеки та їхнє порівняння з аналогами. Такий інструмент, як Marsh Cyber Self-Assessment, може проаналізувати зрілість стану кібербезпеки організації за допомогою багатьох точок даних як на страховому ринку, так і за його межами, і точно визначити області, які потребують вдосконалення. Оцінка також надає огляд погляду страховика на існуючі засоби контролю в організації.

Запатентовані дослідження Marsh визначили 12 ключових засобів контролю, які експерти з кібербезпеки та страхові компанії вважають передовими методами, а саме:

Минулого року страховики зосередилися на управлінні виправленнями, враховуючи, що невиправлені вразливості є основною причиною вторгнень у системи. Страховики також постійно перевіряють управління привілейованими рахунками (PAM). Привілейовані облікові записи є ключами мережі, тому, коли вони скомпрометовані зловмисниками, ймовірність значної шкоди надзвичайно висока. Страховики також очікують, як мінімум, рішень для захисту кінцевих точок

(EPP) і виявлення та реагування на кінцеві точки (EDR) на серверах і ноутбуках організації для виявлення шкідливих програм і стримування їх поширення.

Адаптуйте засоби кіберконтролю до своєї бізнес-моделі

Покращення кібербезпеки, безсумнівно, підвищує здатність організації отримати ефективне кіберстрахування. Однак CISO зазвичай потрібно знайти баланс між посиленням контролю та запровадженням безпеки, яка може уповільнити робочий процес, і провести аналіз витрат і вигод кожного з них.

Наприклад, застосування складних паролів і часті зміни паролів можуть призвести до частих запитів на скидання пароля та затримок у доступі до систем. Забагато сканувань може перервати діяльність користувача, тоді як суворі правила брандмауера та системи запобігання вторгненням можуть блокувати законний мережевий трафік. CISO може забезпечити підтримку заходів безпеки та активізувати бізнес-операції, а не перешкоджати їм, постійно адаптуючи засоби контролю відповідно до бізнес-моделі. Слід регулярно переглядати контракти зі сторонніми постачальниками, які надають засоби контролю, щоб оцінити, чи їхні послуги все ще відповідають потребам організації.

Розставте пріоритети для своїх кіберзагроз

Чітке уявлення про пріоритети кібербезпеки організації дає змогу CISO вирішити, куди розподілити ресурси для усунення ризиків. Існують доступні рішення, які допоможуть CISO сформулювати рентабельність інвестицій від впровадження певного контролю. Наприклад, Марш може співпрацювати з організацією, щоб провести фінансовий стрес-тест. Оцінка може визначити потенційний вплив впровадження рішення PAM, призначеного для захисту та керування привілейованими обліковими записами та доступом в організації. Наявність рішень PAM в організації зазвичай призводить до менших претензій у разі кіберінциденту.

Контекстуалізуйте потенційні кіберінциденти для C-suite

Хоча великі кібератаки отримують широку увагу ЗМІ, існує значна кількість серйозних кібератак, які залишаються закритими. Організації, які зазнають кібератак, часто не бажають публічно розголошувати про інцидент, щоб захистити

свою репутацію та бренд, тоді як керівництво може не мати тонкого розуміння поточних кібертенденцій і ризиків.

Настільні вправи можуть показати, як кіберінцидент може вплинути на діяльність організації та її відносини з зацікавленими сторонами. Сухі тести кібератак досліджують репутаційні, операційні, фінансові та юридичні наслідки, які інциденти можуть мати на організації, а також відповідні стратегії для управління та мінімізації цих наслідків.

Продемонструйте свою надійну культуру кібербезпеки страховикам

Страховики з більшою ймовірністю покриють ризик, якщо організація зможе продемонструвати активну програму кібербезпеки. CISO можуть продемонструвати повне розуміння своїх повноважень і надати гарантії — наприклад, щодо рівня підготовки персоналу з питань кібербезпеки та управління організацією — шляхом проведення зустрічей зі страховиками, чи то в рамках ринкової презентації, чи то під час зустрічі один на один.

Для CISO важливо підтримувати відкриті лінії зв'язку зі страховиками. Під час поновлення, якщо була претензія щодо кіберполісу, CISO, ймовірно, попросять надати деталі про інцидент, включаючи його фінансові витрати та отримані уроки. Чітка та чесна комунікація зі страховиками та завчасне залучення до поновлення є ключовими для забезпечення безперебійного процесу передачі ризиків». ***(Will Vernon. A CISO's guide to cyber risk: How to make cyber risk more insurable // Marsh (https://www.marsh.com/uk/services/cyber-risk/insights/cisos-guide-to-cyber-risk-make-cyber-more-insurable.html). 15.05.2024).***

***

«Сучасні технології кібербезпеки виробляють величезну кількість даних, що вимагає переосмислення того, як зберігати та керувати всіма різними типами інформації, що генерується. Багато платформ кібербезпеки все більше покладаються на одну з двох технологій баз даних — графічні або потокові бази даних — для ефективного представлення та запитів до баз даних індикаторів загроз, інвентаризації активів та іншої важливої інформації про кібербезпеку.

Бази даних Graph дозволяють об’єднувати та шукати властивості та зв’язки різних об’єктів — груп загроз, пристроїв у мережі чи програмних уразливостей. Технологія потокової бази даних дозволяє ефективно обробляти та зберігати дані про загрози та оновлення статусу в реальному часі. Обидві технології допомагають компаніям вийти за межі списків, які використовувалися захисниками в минулому, щоб відстежувати все і робити це в режимі реального часу.

«Усі ми, хто працює в цій сфері, давно скаржимося на труднощі захисту від кіберзловмисників, але не було жодної зміни, лише поступове збільшення складності з часом», — каже Ірен Міхлін, штатний інженер із додатків. Керівник безпеки в Neo4j, постачальнику баз даних графів. «Ми досягли переломного моменту труднощів, коли дані все більше пов’язані між собою зв’язками «багато-до-багатьох».

Змінний характер збору та використання даних у сфері кібербезпеки зумовив необхідність переходу до інших підходів до зберігання та обробки даних. Соціальні мережі суб’єктів загрози, пов’язані активи в мережах захисників і індикатори компрометації – це деякі типи даних, для яких зв’язки між елементами набору даних надзвичайно важливі.

Графові бази даних дозволяють ефективно представляти та запитувати зв’язки між об’єктами даних — це критично важливо для кібербезпеки для виявлення таких шаблонів, як шахрайство або вторгнення в мережу, — каже Веймо Лю, генеральний директор виробника графічних движків PuppyGraph.

«Зловмисники використовують взаємозв’язок мережі, розглядаючи її як графік, щоб ідентифікувати та використовувати вразливі місця», — каже він. «Прийнявши подібну перспективу на основі графіків, захисники можуть значно підвищити рівень безпеки».

Дані про кібербезпеку потребують кращого представлення

Різноманітні графові представлення даних розвивалися разом із мережевими моделями даних у 1970-х роках, об’єктно-орієнтованими базами даних у 1980-х роках і моделями графових баз даних у 1990-х роках, згідно з одним опитуванням

графових моделей баз даних. Сучасні системи керування базами даних графів почалися з Neo4j у 2007 році, який випустив версію 1.0 у 2010 році.

У середині 2010-х років фахівці з кібербезпеки почали розглядати бази даних графів як природне представлення взаємозв'язків між бізнес-активами, властивостями кібербезпеки, такими як уразливості, і ландшафтом загроз. Джон Ламберт, видатний інженер Центру аналізу загроз Microsoft, зауважив це в 2015 році, коли заявив: «Захисники думають списками. Зловмисники думають графіками. Поки це правда, зловмисники виграють».

«Більшість захисників зосереджуються на захисті своїх активів, розставляючи їх за пріоритетами та сортуючи їх за навантаженням і бізнес-функціями», — сказав він. «Захисники завалені списками активів — у службах керування системою, базах даних інвентаризації активів, електронних таблицях BCDR (безперервність бізнесу, аварійне відновлення). У всьому цьому є одна проблема. У захисників немає списку активів — у них є графік».

Обсяг даних, пов'язаних із кібербезпекою, створений бізнес-операціями, величезний. Однією з головних проблем у роботі з цими даними та використанні графіків для кібербезпеки є управління складністю та обсягом даних, каже Лю з PuppyGraph.

«Середовища кібербезпеки генерують величезні обсяги даних з різних джерел, включаючи мережевий трафік, журнали та канали аналізу загроз», — говорить він. «Моделювання цих даних у вигляді графіків може швидко призвести до великих, складних структур, які важко аналізувати та інтерпретувати».

Згідно з опитуванням, проведеним консалтинговою компанією McKinsey, середня компанія відстежує приблизно половину свого загального обсягу журналів і сподівається відстежити до 80% протягом наступних кількох років.

Візуалізація загроз безпеці

Графові бази даних природно дозволяють візуалізувати дані та зв'язки між елементами бази даних. Для кібербезпеки ця візуалізація дозволяє захисникам краще виявляти та пом'якшувати вразливі вузли, каже Лю.

«Забезпечуючи графічне представлення топології мережі, графіки виявляють потенційні вразливості та можливе поширення загроз у мережі, пропонуючи таким чином безцінне розуміння складних мережевих структур», — говорить він.

Потокові бази даних допомагають обробляти інформацію в режимі реального часу та приймати рішення на основі цих даних, як, наприклад, у системах боротьби з шахрайством, які використовуються фінансовими установами, каже Рейес Паша, керівник продукту RisingWave Labs, постачальника потокових баз даних.

«Тепер у вас є передові методи виявлення шахраїв — не лише того, чи є особа тим, ким вона себе видає на основі простого пароля та імені користувача та системи входу в систему», — каже він. «Це також залежить від того, звідки вони входять в систему... в якому місці та в який час доби. Можливо, ви враховуєте багато інших аспектів, і тепер вам потрібна база даних, яка може з'єднати ці точки».

Ключовими є концепції, а не реалізації

Незважаючи на те, що багато графічних і потокових служб бази даних є пропрієтарними, наприклад AWS Kinesis, зусилля з відкритим кодом встановили планку та наздоганяють. Для потокових баз даних Apache Kafka є, мабуть, найвідомішою платформою не лише для зберігання даних, але й для створення цілого конвеєра обробки.

Розробка нових платформ баз даних графів призвела до різноманітних власних способів представлення графів, але реляційні бази даних також наздоганяють. Наприклад, остання версія мови SQL (SQL:2023) представляє абсолютно нову специфікацію для представлення графів властивостей і запитів графів властивостей (PGQ), підмови для взаємодії з новими структурами даних.

Реалізація нової мови як плагіна для реляційної бази даних DuckDB показала «втішну продуктивність і масштабованість», згідно з документом дослідницької групи з Інституту Centrum Wiskunde & Informatica в Нідерландах.

«Ми вважаємо, що все більше проблем з даними потребують графічної бази даних, особливо коли ваші дані сильно зв'язані, і існує потреба проходити через ці численні з'єднання», — говорить Міхлін з Neo4j. «Вони глибоко, легко та швидко

знаходять приховані зв’язки та шаблони в мільярдах з’єднань даних, і вони природно підходять для такого роду даних». ***(Robert Lemos. Picking the Right Database Tech for Cybersecurity Defense // Informa PLC (https://www.darkreading.com/cybersecurity-analytics/picking-right-database-tech-cybersecurity-defense). 21.05.2024).***

***

«Я к свідчать нещодавні повідомлення SEC, правління компаній дедалі частіше покладають на відповідальність за кібербезпеку; тоді як управління ризиками кібербезпеки є відповідальністю генеральних директорів, які зазвичай делегують більшу частину повсякденного управління CISO або тому подібному, нагляд за цим управлінням є відповідальністю директорів.

Проте, незважаючи на те, що, здається, шквал щоденних новин про кібератаки, що сіють хаос, триває десятиліття, коли справа доходить до нагляду за пом’якшенням кіберризику, правління компаній часто не справляються з необхідністю та задумом. Неважко зрозуміти, чому така проблема існує; кібербезпека є відносно новачком у списку основних ризиків, з якими стикається бізнес, і кіберризики розвиваються набагато швидше, ніж інші «класичні» форми ризику, наприклад ті, що пов’язані з бухгалтерським обліком, юридичними чи фізичними небезпеками. Діловий світ має набагато менш відповідний колективний досвід управління кіберризиками, ніж більшість інших форм ризиків, і ми можемо використати ще менше мудрості попередніх поколінь, коли справа доходить до фактичного нагляду за управлінням такими ризиками.

Правління, звісно, не ігнорують кібербезпеку — навпаки, сьогоднішні директори, загалом, добре усвідомлюють важливість кібербезпеки та дуже віддані тому, щоб їхні відповідні команди управління належним чином пом’якшували кіберризики. Правління регулярно не тільки віддають належне кіберризикам, але й підтверджують свої слова, заохочуючи вище керівництво виділяти постійно зростаючі бюджети на захист від них.

Але, як кажуть, «добрими намірами вимощена дорога в пекло»; хоча ради директорів, безумовно, хочуть робити те, що вони повинні робити, щоб контролювати управління кіберризиками, сумна реальність полягає в тому, що ради директорів часто не можуть досягти своєї місії в цьому відношенні, насамперед тому, що багато рад просто не мають членів з достатньою кваліфікацією. достатньо відповідних знань, досвіду та навичок, щоб зрозуміти, як суттєво виконувати роль правління щодо кібербезпеки. Таке явище також створює небезпеку; у деяких випадках непродумані дії правління можуть навіть зашкодити кібербезпеці організації, а не допомогти її покращити.

У деяких випадках ради директорів, у яких недостатньо представлено людей із належним досвідом роботи в галузі кібербезпеки, можуть тривалий час працювати без жодних проблем, пов’язаних із недоліком. Фактично, організації з такими радами можуть навіть похвалитися великими інвестиціями в програми інформаційної безпеки; Однак, зрештою, після того, як стався певний «інцидент» у сфері кібербезпеки, помилкове відчуття безпеки швидко зникає, виявляється, що інвестиції були зроблені далеко не оптимальним способом, і бар’єр для кібератак, який багато хто вважав віртуальним еквівалентом виявлено, що стіни форту за своєю природою ближчі до стін швейцарського сиру.

Іноді дискусії, пов’язані з кібербезпекою в залах засідань, здаються багатообіцяючими, але насправді є непродуктивними сесіями, під час яких директори намагаються виконати частину роботи CISO замість того, щоб зосередитися на своїй відповідальності щодо нагляду за управлінням кіберризиками CISO. Іноді можуть підніматися важливі питання, але, оскільки керівники вважають, що вони розуміють обговорюване питання краще, ніж насправді, вони не усвідомлюють, що важливі питання залишаються невирішеними. В інших випадках у кімнаті недостатньо досвіду, щоб зрозуміти обговорюване питання; Я навіть знаю про засідання правління, на якому директор пожартував, що йому потрібен перекладач, щоб зрозуміти презентацію CISO.

Як фідуціарії, ради директорів доручено переконатися, що їхні відповідні управлінські команди реалізували належні плани, щоб забезпечити належну

стійкість їхніх відповідних компаній у разі кібератак (які з часом стають неминучими) і щоб будь-які залишкові ризики були обмежені відомими, прийнятні та керовані рівні ризику. У результаті ризик кібербезпеки стає основною частиною функцій внутрішнього аудиту. Проте, оскільки кібербезпека є відносно новою дисципліною, багато організацій планують і вимірюють питання, пов’язані з кібербезпекою, використовуючи ключові показники ефективності, які можуть здатися бухгалтерам і юристам так, ніби вони є відповідними та ефективними критеріями для вимірювання успіху, але які насправді вибрані неправильно та серйозно пошкоджений.

Члени правління часто чують і приймають за чисту монету звіти про успіхи в кібербезпеці на основі критеріїв, які не тільки не є значущими, але часто вводять в оману. Скільки разів я чув про організації, які вимірювали кількість зломів за квартал — не знаючи, скільки атак було здійснено, не розуміючи відносної потенційної шкоди від різних компрометацій і ігноруючи той факт, що, безумовно, найшкідливішими порушеннями є ті, про які не було повідомлено, оскільки вони не були виявлені?

У зв’язку з цим важливо розуміти, що на правління покладено завдання нагляду за ризиками, тобто забезпечення того, щоб вище керівництво належним чином реалізувало відповідні плани управління ризиками, а не здійснювати фактичне управління ризиками. Проте, коли йдеться про кіберризики, нерідко можна зустріти директорів, які приділяють значну кількість часу обговоренню питань кібербезпеки, якими повинен займатися CISO, і залишаються поза межами своєї сфери уваги, водночас не обговорюючи ключові елементи того, що їм насправді потрібно охопити.

Я бачив, як засідання правління відволікалися, коли директори без потреби брали участь у детальному обговоренні результатів недавньої симуляції фішингу в масштабах усієї компанії; замість того, щоб зосередити увагу на тому, наскільки добре компанія може протистояти фішинговій атаці — або будь-якій формі кібератаки — люди, відповідальні за нагляд за управлінням кіберризиками, витратили багато часу та енергії на припущення, чому співробітники певних

відділів перевершують своїх колег у порівнянні з -à-vis не стати жертвою підроблених електронних листів. Правління має розуміти, наскільки добре компанія може протистояти збитку від атаки, а не те, чи 27% чи 28% працівників мають пройти навчальний курс.

Коротше кажучи, для правління надзвичайно важливо переконатися, що в них є члени з досвідом кібербезпеки, але потрібно приділити час, щоб переконатися, що це правильний тип досвіду кібербезпеки; просте додавання когось до правління через те, що вони працювали у сфері кібербезпеки, може призвести до проблемних обставин і, зрештою, неприємних сюрпризів». ***(Joseph Steinberg. Oversight of the Management of Cybersecurity Risks: The Skill Most Corporate Boards Need, But Don't Have // NEWSWEEK DIGITAL LLC (oversight-management-cybersecurity-risks-skill-most-corporate-boards-need-dont-have-1903706). 23.05.2024).***

***

«Хоча деякі з найбільших компаній у світі зараз значною мірою покладаються на дані, занепокоєння щодо безпеки досягло найвищого рівня. Згідно з нещодавнім опитуванням Deloitte Center for Controllership Poll, у 2022 і 2023 роках 34,5 відсотка керівників стикалися з кібератаками, спрямованими на бухгалтерські та фінансові дані їхніх компаній. Тим часом 62 відсотки споживачів у Європі, Латинській та Північній Америці вважають, що порушення є неминучою рисою ведення бізнесу в Інтернеті. Через цю постійну небезпеку співробітники та клієнти, зрозуміло, хвилюються про безпеку своїх особистих даних. Це змусило і компанії, і кінцевих користувачів задуматися, чи їхні дані колись повністю захищені.

Такі фактори, як поспішні або некеровані міграції в хмару, різке зростання віддаленої роботи, недостатньо розвинена інфраструктура та загальне зростання цифрового сліду людей призвели до збільшення таких атак через збільшення обсягу даних, створених у цих сценаріях. У результаті кібератаки продовжують зростати, незважаючи на підвищену обізнаність про найкращі практики

кібербезпеки. За даними Forbes, у 2023 році кількість шкідливих програм перевищила один мільярд.

У цьому нестабільному цифровому середовищі необхідно захистити безпеку даних співробітників і споживачів, а також активів та інтелектуальної власності самих компаній.

Резонансні порушення змушують споживачів бути надзвичайно обережними

Дослідження Statista оцінюють загальну вартість транзакцій на світовому ринку цифрових платежів у 9 трильйонів доларів США у 2023 році з очікуваним річним темпом зростання на 11,8 відсотка, що досягне 15 трильйонів доларів США протягом наступних п’яти років.

Оскільки резонансні витоки даних продовжують домінувати в новинах, важливо відновити довіру споживачів до цифрових продуктів і запропонувати ефективні рішення. За минулий рік у Північній Америці кілька відомих організацій зазнали зломів. Наприклад, компанія American Airlines зазнала зламу, розкривши особисту інформацію пілотів, коли їхню централізовану базу даних найму було зламано. Подібним чином UPS Canada мала повідомити своїх клієнтів про те, що особисту інформацію випадково виявив інший користувач, який зловживав інструментом пошуку пакетів.

Відомі компанії, такі як Twitter (тепер відомий як «X»), гігант продуктів харчування та напоїв Mondelez і власник KFC і Pizza Hut, Yum! Бренди також потрапили в заголовки. Гігант соціальних медіа X зіткнувся зі значним зломом: адреси електронної пошти 200 мільйонів користувачів були продані в темній мережі. Цей інцидент стався після початкового витоку, який стався рік тому.

Тим часом у серпні в Європі поліцейська служба Північної Ірландії зазнала «значного витоку даних», спричиненого ручною помилкою у відповідь на запит щодо свободи інформації. Регуляторні зміни у Великій Британії за останні роки призвели до того, що Управління пруденційного регулювання (PRA) і Управління фінансової поведінки (FCA) змінили свої правила для організацій, щоб боротися з таким рівнем кіберзлочинності або ненавмисного витоку даних. Це включає більшу співпрацю та прозорість з регуляторними органами, відповідальність за оновлення

систем і засобів контролю, а також швидше та повніше надання деталей будь-яких інцидентів безпеки. Ці поправки до правил є прямою відповіддю на заклики до певної цифрової трансформації та потенційної заміни існуючих систем, які мають захищати клієнтів, співробітників та їхні дані. Подібні правила кібербезпеки в Європі через NIS2 (Директива про мережеві та інформаційні системи) і DORA (Закон про цифрову операційну стійкість) спрямовані на посилення операційної стійкості та стійкості до кіберзагроз. Пам'ятаючи про це, організації розглядають нові рішення для досягнення підвищеного рівня захисту та контролю в децентралізований спосіб.

Адаптація технологій для покращення безпеки: важливість біометрії

До цього часу реакцією організацій на тиск з боку регуляторів і широкої громадськості було включення кібербезпеки в зусилля з цифрової трансформації. Організації прагнуть розробити архітектуру нульової довіри, яка передбачає, що всі спроби доступу є незаконними, доки не буде автентифіковано. У цьому відношенні двофакторна автентифікація також стала обов'язковою в багатьох країнах, додаючи додатковий рівень захисту для споживачів. Поточні хмарні міграції, хоча й створюють нову потенційну поверхню для атак у майбутньому, також розроблені для кращого захисту даних компанії.

Потенціал біометрії також досліджено як основного способу забезпечення доступу до даних і використання фінансів, пов'язаного більш прямо та однозначно з потрібною людиною. Ринок біометричних датчиків, де доступ або використання доступні за допомогою особистих ідентифікаційних маркерів, таких як відбитки пальців або розпізнавання обличчя, має потроїти свою вартість у 2020 році до 3,3 мільярда доларів США до 2030 року. Ініціативи, які підтримують зростання цього сектора, включають біометричну автентифікацію Mastercard. Сервіс, який спрощує біометричну інтеграцію для бізнесу. Ця ініціатива спрямована на вирішення проблем із паролями та багатофакторною автентифікацією та зосереджена на використанні біометрії для підвищення безпеки, одночасно спрощуючи та прискорюючи цифровий досвід.

Вплив біометрії на споживачів також починає зростати. Цілих 58 відсотків заявили, що біометричні платежі за допомогою біометричних смарт-карт роблять транзакції більш безпечними, порівняно з 48 відсотками роком раніше. Замість використання PIN-коду чи запам'ятовування пароля як режиму доступу для цих платіжних операцій, метод пов'язує картку особи виключно з відбитками пальців, голосом або рисами обличчя людини. Таким чином, він не схильний до неправильного використання, що забезпечує додаткову зручність.

Перетворення системи зберігання даних для підвищення довіри споживачів

Окрім того, що організації запроваджують технологію за закритими дверима для збереження даних у безпеці, інтерес до біометричних смарт-карт показує, що споживачі також хочуть бачити покращений захист у своїх фізичних транзакціях та управлінні фінансами. Ця зміна парадигми відображає не лише прагнення до підвищеного захисту, але й визнання обмежень традиційних методів автентифікації. Приписування доступу до відбитка пальця або розпізнавання обличчя підтверджує цю особу в цей момент, що її облікові дані є унікальними, а отже, що дані всередині безпечні. Шифрування даних відбитків пальців на самій картці додатково забезпечує повну впевненість у рішенні. Шифрування особистих даних лише посилює цей захист, гарантуючи, що конфіденційна інформація залишається недоступною для неавторизованих сторін. Ці смарт-карти ефективно пом'якшують уразливості, пов'язані з централізованими базами даних.

Біометричні смарт-карти також змінюють динаміку зберігання даних. Замість розміщення біометричних облікових даних у централізованих базах даних, де цілі також зібрані в одному місці; смарт-карти уникають цього ризику.

Як рішення для відновлення довіри споживачів, біометричні смарт-карти відповідають усім вимогам: максимальна безпека, поза хмарою, через повне шифрування особистих ідентифікаційних даних, що керує як фізичним, так і логічним доступом і зберігає фінанси, а також особисту безпеку. Позахмарний характер біометричних смарт-карт особливо пропонує переконливу перевагу в епоху, позначену зростаючим занепокоєнням щодо конфіденційності даних і порушень безпеки. На відміну від звичайних хмарних систем зберігання даних, які

чутливі до злому та витоку даних, смарт-карти забезпечують локалізоване, захищене від підробок середовище для зберігання важливих біометричних даних.

Це поєднання передових технологій і надійних заходів безпеки не тільки підвищує довіру споживачів, але й встановлює новий стандарт автентифікації в епоху цифрових технологій. Пропонуючи комплексне рішення як для фізичного, так і для логічного контролю доступу, біометричні смарт-карти дають людям можливість захистити свої фінансові активи та конфіденційність із безпрецедентною ефективністю та спокоєм.

Використання біометрії для створення та підтримки довіри споживачів

Значні досягнення в автентифікації та платежах стали можливими завдяки використанню біометричних смарт-карт. Масштаби міграцій, які відбулися в останні роки, змушують законодавців і великих технологічних новаторів вказувати на хмару як на наступний кордон для кібер-зловмисників. У своєму останньому дослідженні, звіті «Зростаюча загроза споживчим даним у хмарі», Apple визначає біометричну автентифікацію як «неймовірно цінний» метод «входу без пароля», який може захистити клієнтів і персонал навіть у корпоративних хмарах. навколишнє середовище. У рамках безперервного переходу організації підвищуватимуть свій голос у дискусіях, щоб підвищити рівень безпеки. Трансформація, яка зрештою спрямована на відновлення та підбадьорення довіри споживачів». ***(Vince Graziani. Who is looking out for your data? Security in an era of wide-spread breaches // Biometrics Research Group, Inc. (https://www.biometricupdate.com/202405/who-is-looking-out-for-your-data-security-in-an-era-of-wide-spread-breaches). 26.05.2024).***

***

«Технології підвищили продуктивність, ефективність і зв'язок у кожній галузі по всьому світу, і сільське господарство не є винятком. Колись вважалася традиційно низькотехнологічною галуззю, але все більше використання електронної пошти, інструментів онлайн-моніторингу, дистанційного керування та платіжних систем разом з автоматизованим

інтелектуальним сільськогосподарським обладнанням, таким як підключені до Інтернету трактори, означає, що рівень цифрової загрози для фермерів зріс.

Як і в багатьох галузях промисловості по всьому світу, зростаюча залежність від підключених онлайн-технологій означає, що бізнес стає більш уразливим до кібератак. Використання інтелектуальних пристроїв, зокрема датчиків і аналітики, пристроїв Інтернету речей, робототехніки, дронів і точного землеробства, змінило сільськогосподарський ландшафт на краще. Ці інструменти також збирають велику кількість конфіденційної інформації, яка може бути прибутковою для злочинців, які прагнуть отримати фінансову вигоду.

У звіті, опублікованому в 2023 році, Південна Африка посіла п’яте місце в списку країн, які найбільше постраждали від кіберзлочинності. Збої в IT-додатках Transnet після кібератаки призвели до зупинки імпорту та експорту сільськогосподарської продукції в липні минулого року. У світі, який все більше залежить від цифрових технологій, вразливість сільськогосподарського сектора до кібератак не лише загрожує окремим сільськогосподарським підприємствам, але й створює ризик для національної продовольчої безпеки, що робить надійні заходи кібербезпеки надзвичайно важливими.

Загроза, безумовно, не є унікальною для Південної Африки, оскільки звіт Кембриджського університету показує, що технології розумного землеробства, такі як автоматичні обприскувачі сільськогосподарських культур і роботизовані комбайни, можуть бути зламані, і ймовірність того, що це може статися, зростає. Кіберзлочинці визнають глобальну залежність від продовольства та сільського господарства як можливість здійснити кібератаки на галузь, щоб отримати фінансову вигоду за допомогою програм-вимагачів або соціально-економічних зривів.

Атаки програм-вимагачів можуть бути особливо зловмисними, наприклад, видаляючи резервні копії або погрожуючи опублікувати конфіденційну інформацію в Інтернеті як стратегію тиску на організацію, щоб вона сплатила викуп з невеликим ризиком бути спійманою та затриманою.

Сьогодні майже кожен фермер і сільськогосподарське підприємство буде використовувати ті чи інші технології для ведення бізнесу. Для невеликих підприємств важливі прості рішення безпеки, такі як автоматичне оновлення програмного забезпечення, антивірусне програмне забезпечення та багатофакторна автентифікація. Однак для більших і інтенсивних сільськогосподарських операцій з використанням автоматизованих систем землеробства можуть знадобитися більш складні заходи безпеки.

Історично було показано, що сільське господарство загалом має низький рівень кібербезпеки, оскільки атаки не сприймаються як такі поширені, як у фінансовому секторі.

Серед деяких секторів південноафриканського фермерського співтовариства поширений міф про те, що їхній бізнес просто не є привабливою мішенню для кіберзлочинців. Але враховуючи величезні обсяги даних, властиві багатьом сільськогосподарським видам діяльності, а також значні фінансові транзакції, перед обличчям складних кіберзагроз краще використовувати проактивний підхід до цифрової безпеки.

Хоча вирішення проблем кібербезпеки в сільському господарстві може бути складним, вона додає, що є кроки, які сільськогосподарські фірми можуть вжити, щоб зменшити свій ризик, обмежити шкоду від існуючої атаки та поставити своїх працівників як першу лінію захисту.

Необхідним першим кроком у зміцненні захисту є визначення того, де критична інфраструктура вразлива для атак. Це буде різним для кожного бізнесу. Для деяких операцій може знадобитися більше інвестицій у хмарну безпеку або виявлення вразливостей, тоді як компаніям може знадобитися розширити свої зусилля з кібербезпеки, щоб захистити себе від кіберзагроз у формі фішингових електронних листів від компаній, з якими вони співпрацюють і від яких закуповують.

Оскільки майже 88% порушень даних спричинені помилками співробітників, ефективна програма управління людськими ризиками з регулярним навчанням

працівників і обізнаністю про кібербезпеку є ключовим елементом будь-якої стратегії кібербезпеки.

Співробітники можуть бути настільки ж сприйнятливими до кіберзагроз, тому їм слід постійно нагадувати про існуючі ризики та вплив, який вони можуть мати на них і на сільськогосподарський бізнес. Люди схильні до помилок, але цим помилкам, починаючи з невдалого видалення даних із пристроїв і закінчуючи помилками, яким можна запобігти, як-от натисканням посилань у фішингових електронних листах, також можна запобігти.

Сільське господарство є життєво важливим для світової харчової промисловості та потребує максимального захисту від кібератак.

Від основ, таких як впровадження менеджерів паролів і використання багатофакторної автентифікації до використання передових технологій безпеки для протистояння атакам на великі сільськогосподарські компанії, можна зробити набагато більше, щоб гарантувати підтримку фермерам за допомогою найкращих стратегій і рішень кібербезпеки». ***(Why farmers need cybersecurity // World Wide Worx (https://gadget.co.za/farmcybersecurity3/). 27.05.2024).***

***

«Протягом останнього десятиліття спільнота, що займається політикою цифрової торгівлі, була поглинена боротьбою за конфіденційність даних, транскордонні потоки даних та електронні митні збори, щодо яких поки що неможливо досягти міжнародного консенсусу. Проте серед геополітичної штовханини з цих питань є принаймні одна важлива сфера, де ми бачимо стійкий, відчутний прогрес у політиці цифрової торгівлі: кібербезпека.

У сучасній глобальній економіці все більш фрагментований стан глобального кіберрегулювання підриває кібербезпеку та потенціал зростання цифрової торгівлі. Учасники торговельних переговорів повинні використовувати можливість отримати більш амбітні зобов’язання щодо кібербезпеки, просуваючи справедливе, інклюзивне, стійке та безпечне середовище цифрової торгівлі, навіть якщо переговори щодо більш спірних цифрових питань залишаються в глухому куті.

Загальний регламент захисту даних Європейського Союзу (GDPR) і наступні трансатлантичні баталії за безпечні потоки даних стали першим джерелом напруженості в цифровій торгівлі під час останніх переговорів. Вимоги до адекватності GDPR, які встановлюють жорсткі стандарти захисту даних для країн, що не входять до ЄС, блокували попередню співпрацю США та ЄС щодо транскордонних потоків даних, створюючи паніку щодо того, чи зможуть дані продовжувати перетинати Атлантику.

Увага, яку не привернула політика щодо даних, була зосереджена на переговорах щодо цифрових податків і митних зборів в Організації економічного співробітництва та розвитку (ОЕСР) і Світовій організації торгівлі (СОТ), відповідно.

Потім, у жовтні минулого року, торгове представництво США послало грім із ясного неба, перевернувши кілька десятиліть політики цифрової торгівлі США. Рішення припинити підтримку США в питаннях транскордонних потоків даних, локалізації даних і перегляду вихідного коду в переговорах щодо Ініціативи спільної заяви щодо електронної комерції в СОТ стало шоком для багатьох.

Промислові та торгові асоціації США закликали уряд США скасувати своє рішення та підтвердити свою підтримку транскордонних потоків даних. Занепокоєння поширилося на Конгрес, де були проведені слухання, щоб зрозуміти причину такого рішення. Торгові партнери США тим часом відчували себе осторонь, роками виступаючи за такі положення за підтримки США.

Яскраве місце в цифровій політиці

Тим часом політика кібербезпеки виявилася набагато менш суперечливою, сприяючи більшій міжнародній співпраці, і з поважної причини: довіра до цифрової економіки є основою. Оскільки політики продовжують брати активнішу роль у розробці внутрішньої політики кібербезпеки, уряди також повинні забезпечити взаємодію нормативів з нормативними актами своїх колег, щоб уникнути непотрібних нетарифних бар’єрів у торгівлі. Наразі центральні уряди в усьому світі заклали міцну основу, засновану на міжнародному консенсусі, але попереду ще багато роботи, щоб узгодити міжнародні стандарти цифрової безпеки.

Цю основу можна знайти в новому звіті «Захист глобальної торгівлі: як кібербезпека розглядається в міжнародних торгових угодах» Коаліції зі зменшення кіберризику. У звіті оцінюється 11 угод про вільну торгівлю (ЗВТ), які на сьогодні містять положення про кібербезпеку. Він розподіляє ці положення на вісім окремих сфер і аналізує спільні риси та відмінності в тому, як вони розглядаються.

У звіті зазначено, що з 2018 року все більше угод про вільну торгівлю включають положення про кібербезпеку, і ці положення стають все більш комплексними. Розбудова державного потенціалу кібербезпеки, співпраця у вирішенні інцидентів безпеки та використання підходів, що ґрунтуються на управлінні ризиками, і міжнародних стандартів у розробці внутрішньої кіберполітики стають базовими очікуваннями в сучасних торгових угодах. Тим часом більш амбітні угоди, такі як Угода про цифрову економіку Сінгапуру та Великої Британії, дійшли до «встановлення угоди про взаємне визнання базового стандарту безпеки» для пристроїв Інтернету речей.

Незважаючи на те, що торгова політика в цілому продовжує стикатися з проблемами, є можливості для подальшого прогресу. Ініціатива Спільної заяви Світової організації торгівлі щодо електронної комерції — угода 90 країн, що охоплює більшу частину світової економіки — може бути укладена до осені. Майбутні торговельні переговори між США та Тайванем пропонують можливість відповідати амбітним зобов’язанням щодо цифрової торгівлі, які взяли на себе аналогічні країни, такі як Великобританія, Сінгапур та Австралія.

Для США чудовим початком було б прийняття формулювання, що віддзеркалює DEA Сінгапуру та Великобританії щодо взаємного визнання базових показників безпеки IoT. Включення узгоджених вимог щодо розкриття вразливостей для критичної інфраструктури знову виведе США на передовий край цієї теми. Незважаючи на те, що ми постійно стикаємося з труднощами щодо таких положень, як потоки даних і електронні митні збори, подальший прогрес необхідний і досяжний у політиці цифрової торгівлі. Офіс торгового представника Сполучених Штатів повинен скористатися цією можливістю». ***(Alex Botting. Can Cybersecurity Be a Unifying Factor in Digital Trade Negotiations? // Informa PLC***

(https://www.darkreading.com/cybersecurity-operations/can-cybersecurity-be-unifying-factor-in-digital-trade-negotiations-). 21.05.2024).

***

«Зі зростанням важливості супутникового зв'язку зростає також важливість захисту цих супутникових систем із загрозами, які варіюються від хакерів до сонячної погоди, заявили експерти на конференції RSA цього місяця.

Наприклад, сонячна буря минулого уїк-енду була більше, ніж просто гарною світловою демонстрацією – це також було серйозне порушення та нагадування про те, наскільки суспільство залежить від надійних супутникових з'єднань. Сонячний спалах був серйозною проблемою для фермерів, які покладаються на точні дані GPS, щоб керувати своїми тракторами, повідомляє 404 Media. Не маючи змоги довіряти системам, багато хто був змушений припинити посів на ключову частину сезону.

Сонячні спалахи стають «все більш і більш проблематичними», оскільки повсякденне життя все більше покладається на космічні технології, сказав Манан Далал, помічник IT-директора з супутників Національної екологічної супутникової служби, даних та інформації (NESDIS), під час конференції RSA.

Збої в роботі супутників можуть вплинути на все: від телефонних дзвінків у всьому світі до щоденного прогнозування погоди та прогнозування місць, де урагани досягнуть суші, сказала Далал. Сонячний спалах у 2023 році порушив роботу радіо в усьому світі, і одне село в Нью-Йорку вже планує продовжити роботу, якщо майбутня подія, як-от потужний сонячний спалах, спричинить місячне відключення Інтернету.

І космічна погода — не єдина загроза — національні держави все більше зацікавлені в порушенні зв'язку інших країн, націлюючись на їхні космічні системи, що може вплинути на військові операції, — сказала Міке Еоянг, заступник помічника міністра оборони з питань кіберполітики Департаменту США.

Захист, під час тієї ж колегії. Одним із прикладів є злом Росією супутникової мережі Viasat, що обслуговує Україну.

З огляду на ризики, уряди повинні гарантувати, що вони можуть видавати ранні попередження до того, як відбудуться значні сонячні події, сказав Далал, і кілька учасників дискусії сказали, що потрібно зробити більше для зміцнення космічної кібербезпеки.

Захист космічних систем вимагає захисту кожного з трьох технологічних рівнів: технології на землі, обладнання на орбіті та технології, що забезпечує зв'язок між ними.

Наземна сторона включає системи обробки даних і розповсюдження інформації, сказав Далал. Але це також системи, в які хакерам найпростіше проникнути, зазначив Еоян. Тому особливо важливо забезпечити наявність надійних методів автентифікації, захищеність технології та дотримання інших ключових принципів кібербезпеки.

Водночас зв'язок між приладами на орбіті та наземними системами має бути зашифрований і захищений від таких атак, як глушіння або підробка, сказав Еоян.

Обладнання на орбіті також стикається з загрозою зовнішніх умов. Зробити цю технологію безпечнішою може означати встановлення міжнародних норм, які забороняють будь-кому проводити дії, що викликають уламки в космосі, сказав Еоян.

Одна з проблем, однак, полягає в тому, що значні технологічні досягнення, ймовірно, відбудуться протягом 10-15 років, протягом яких супутник може залишатися на орбіті, що робить моральне старіння серйозною проблемою, сказала Далал.

«Як тільки ви запускаєте супутники на орбіту, вони працюють: ми не можемо відправити когось туди, щоб вирішити будь-які проблеми», — сказала Далал. «... Ви повинні створювати системи, де вам потрібно пристосуватися до невеликої частини цих технологічних змін. Один нещодавній приклад, який я можу вам навести: що відбувається, коли ми перебуваємо в постквантовому світі? Ну, [для]

нашого системи шифрування в космосі, я не можу піднятися туди й почати з ними працювати».

Що стосується кібербезпеки в космосі, уряд не може зробити це сам.

Значна частина космічної техніки закуповується у постачальників, тому уряд і промисловість повинні тісно спілкуватися. Компанії повинні ділитися подробицями про загрози, які вони бачать, а уряд має ділитися оперативною розвідкою, сказав Еоян. Центр обміну та аналізу космічної інформації, або Space ISAC, є одним із напрямів діяльності з обміну розвідувальною інформацією про космічні загрози між державним і приватним секторами.

Політики в США ще не встановили узгоджених базових вимог до кібербезпеки, що залишає компаніям можливість робити власні, різні інтерпретації, сказала під час дискусії Тахара Докінз, голова апарату Національної ради з космосу.

Але федеральний міжвідомчий комітет зараз працює над розробкою мінімальних вимог до кібербезпеки для «закуплених федеральними органами цивільних космічних систем національної безпеки», які повинні вийти цього літа, сказав Докінз. Також у роботі: план реалізації, який детально описуватиме конкретні кроки для впровадження принципів кібербезпеки космічної системи, викладених у Директиві щодо космічної політики-5». ***(Jule Pattison-Gordon. Cybersecurity in space: Why hacking has gone off world // Star Media Group Berhad (https://www.thestar.com.my/tech/tech-news/2024/05/23/cybersecurity-in-space-why-hacking-has-gone-off-world). 23.05.2024).***

***

«Майже половина (42%) торгових посередників вважають кібербезпеку головною проблемою, як показало нове дослідження.

Згідно з новим звітом BT Wholesale, управління ризиками є основним завданням, серед яких кібербезпека має бути «абсолютним пріоритетом».

Згідно з даними, торгові посередники значно частіше називають кібербезпеку головним бізнес-пріоритетом, ніж працівники кінцевих клієнтів (25%) або навіть особи, які приймають рішення в сфері IT (27%).

І це незважаючи на те, що понад 13% осіб, які приймають рішення в IT, самі ставали жертвами шахрайства.

Згідно з даними, торговельні посередники каналів також лідирують у питаннях сталого розвитку, оскільки 40% торговельних посередників бачать сталість як «бізнесу пріоритет» в порівнянні з лише третиною респондентів клієнтів (32% співробітників і 33% IT-рішень). виробників), відповідно.

Тим часом BT Wholesale також виявила, що більше половини (59%) співробітників хочуть, щоб їхні організації інвестували в штучний інтелект, при цьому 61% керівників IT очікують інвестувати в штучний інтелект в наступному році.

BT Wholesale Channel Partners Директор Гевін Джонс сказав: «Після року швидких змін ми хотіли, щоб це дослідження дало безцінні уроки для наших партнерів. розвитку бізнесу

«Я зрозуміло, що впровадження 5G, штучного інтелекту та кібербезпеки має першочергове значення, але довіра та простота залишатимуться основою успіху.

«Канал повинен перейти від розмов про технології до розмов, орієнтованих на клієнта, сприяючи міцним стосункам, щоб підтримувати клієнтів, коли вони орієнтуються в технологічному ландшафті, що постійно змінюється».

Він додав: «У всьому цьому ми тут, щоб підтримувати партнерів Partner Plus у адаптації їхніх стратегій до сьогоднішнього та майбутнього ринку. Завдяки нашому асортименту інноваційних рішень, експертним порадам і готовим до використання матеріалам партнери можуть зосередитися на побудові відносин і використанні можливостей». ***(Jasdip Sensi. Data: 42% of channel resellers see cyber-security as a 'top concern' // Mobile Marketing (https://mobilemarketingmagazine.com/data-cyber/). 24.05.2024).***

***

«Частота та серйозність кібератак зростає, але більшість компаній залишаються неготовими, повідомляє VikingCloud. У зв'язку зі зростаючим браком кадрів, втомою та новими витонченими методами атак компанії стають більш вразливими, ніж будь-коли.

Дослідження показує, що 40% кіберкоманд не повідомляли про кіберінциденти через страх втратити роботу. Ця інформація свідчить про серйозне заниження інформації про кіберзломи в усьому світі.

Ця тенденція також загрожує підприємствам невідповідністю новим галузевим нормам, а також уразливості до зростання кількості атак, частота яких, як повідомляється в опитуванні, зросла для 49% компаній і серйозність для 43% за останні 12 місяців.

Компанії впевнені у своїй здатності виявляти кібератаки

Дані, зібрані в результаті кількісного опитування майже 170 фахівців з кібербезпеки на рівні керівників, віце-президентів, директорів і менеджерів у Сполучених Штатах, Великобританії та Ірландії, показують, що 96% компаній впевнені у своїй здатності виявляти та реагувати на кібератаки в реальному часі.

Проте ті самі компанії також визнають, що вони не готові до найактуальніших кіберризиків сучасності, включаючи атаки програм-вимагачів проти критично важливих третіх сторін (48%), фішингових атак (40%), атак DNS (33%) і атак програм-вимагачів проти своїх бізнес (32%).

«Кіберкоманди стикаються з серйозними проблемами, такими як зростаючий дефіцит кадрів, нові методи атак і прогресуюча розвиненість кіберзлочинців», — сказав Кевін Пірс, CPO VikingCloud. «Хоча багато керівників повідомляють про впевненість у своїх оборонних можливостях, очевидно, що це помилкове відчуття безпеки робить багато компаній уразливими. Команди намагаються зробити більше з меншими витратами, тоді як кіберзлочинці продовжують бути на крок попереду. Без розуміння свого фактичного статусу ризику та інвестування в правильні технології, людей і експертних партнерів компанії стануть ще більш сприйнятливими до новітніх методів атак».

Розрив у кваліфікації між кіберкомандами та злочинцями зростає

53% виявили, що нові методи атаки ШІ створюють нові точки атаки, до яких вони не готові. Серед загроз штучного інтелекту, які викликають найбільше занепокоєння, є швидкий злом моделі GenAI (46%), отруєння даних великої мовної моделі (LLM) (38%), програмне забезпечення-вимагач як послуга (37%), атаки на чіп обробки GenAI (26%), інтерфейс програмування додатків (API) порушення (24%) і фішинг GenAI (23%).

55% компаній вважають, що кіберзлочинці є більш просунутими, ніж їх внутрішня команда. 35% повідомили, що технологія, яку використовують кіберзлочинці, є більш складною, ніж технологія, до якої має доступ їхня команда. Незважаючи на це, третина компаній досі не навчили свою команду кіберризикам, пов'язаним з GenAI.

Лише 10% компаній збільшили кібернайм'ання за останні 12 місяців, і майже 20% компаній кажуть, що брак кваліфікованих кадрів є ключовою проблемою для подолання кібератак. 35% компаній не мають достатнього бюджету, щоб інвестувати в нові технології, а 32% не мають достатнього бюджету, щоб найняти більше персоналу.

Втома від кібератак скорочує час реагування на кібератаки

33% компаній запізнилися з реакцією на кібератаки, тому що вони мали справу з хибним спрацьовуванням, а 63% витрачають більше 208 годин на рік на керування хибними спрацьовуваннями.

Загалом, 68% опитаних кіберкоманд наразі не можуть відповідати вимогам Комісії з цінних паперів і бірж щодо розкриття інформації протягом чотирьох днів і контрольним показникам кіберіндустрії на основі середньої кількості часу, який, за їхніми оцінками, знадобиться для відповіді на нову серйозну атаку.

Технологія має потенціал стати вирівнювачем для кіберкоманд. 63% компаній прагнуть запровадити нові технології, які можуть допомогти пом'якшити наслідки дефіциту кіберталантів. 41% стверджують, що GenAI має найбільший потенціал для подолання втоми від кіберсповіщень. Проте лише 5% компаній

виділили додатковий бюджет на свої кіберпрограми в минулому році для вирішення цих поточних проблем.

«Кіберлідери можуть дивитися на такі передові технології, як GenAI, двома способами – як на загрозу чи як на зброю. Реальність полягає в тому, що це і те, і інше, тому компаніям важливо агресивно впроваджувати правильні рішення, щоб озброїти свої команди та перемогти кіберзлочинців у їхній грі», — сказав Пірс». ***(Worried about job security, cyber teams hide security incidents // Help Net Security (https://www.helpnetsecurity.com/2024/05/24/cyber-teams-major-challenges/). 24.05.2024).***

***

«За словами Cado Security, реагування на інциденти сьогодні займає надто багато часу та займає вручну, що робить організації вразливими до збитків через нездатність ефективно розслідувати виявлені загрози та реагувати на них.

Завдання реагування на інциденти ще більше ускладнюється, оскільки підприємства швидко розгортають хмарні та контейнерні технології та приймають багатохмарну стратегію.

Звіт, у якому досліджується критична роль і виклики реагування на інциденти, розкриває широко поширені недоліки, які роблять організації вразливими до затримок у вирішенні інцидентів і нездатності дотримуватись нормативних вимог. Основним фактором, що сприяє цьому, є відсутність видимості та контролю над хмарними середовищами.

«Надійна програма реагування на інциденти, особливо та, яка поширюється на технології наступного покоління, має вирішальне значення для захисту організацій від нових загроз», — сказав Джеймс Кемпбелл, генеральний директор Cado Security. «Проте, як виявилося в нашому останньому звіті, організаціям досі не вистачає спрощених стратегій реагування на інциденти для хмарних середовищ. Отримані дані підтверджують те, що організаціям терміново необхідно прийняти нові підходи до швидкого розслідування та реагування – не лише для кращого

усунення ризиків, але й для дотримання складних і постійно мінливих мандатів щодо звітування про інциденти по всьому світу».

Організації борються з розширенням сфери регулювання

90% організацій зазнають збитків, перш ніж локалізувати та розслідувати інциденти. Організації повідомляють, що 23% хмарних сповіщень залишаються нерозслідуваними через різні проблеми та складності.

Основним фактором, що спричинив затримки розслідувань, був брак видимості та контролю над хмарними середовищами, що викликано такими операційними труднощами: 82% організацій повідомляють про необхідність використання кількох платформ та інструментів для проведення розслідувань у хмарі. Крім того, 34% організацій повідомляють про обмежені навички кібербезпеки, характерні для хмарних технологій.

У міру того, як нормативні вимоги до звітності розвиваються, організації стикаються зі збільшенням масштабів і не відстають від нових правил. 42% організацій повідомляють, що основною проблемою відповідності, окрім впровадження хмарних технологій, є відсутність видимості даних, а 34% респондентів були оштрафовані за недотримання нормативних вимог.

Майбутні стратегії дослідження хмари та реагування

Оскільки організації переходять на хмару, вони повинні застосовувати нові технології, щоб краще захищатися від нових загроз. У звіті виявлено, що організації дещо покращили свою здатність проводити розслідування в хмарі: респонденти повідомили, що 23% сповіщень у хмарі ніколи не досліджуються, порівняно з понад 33% у 2021 році.

Проблеми видимості, пов'язані з розслідуванням і реагуванням у хмарі, змушують організації все частіше звертатися до інструментів криміналістики. З цією метою 83% виділили бюджет на хмарну криміналістику, підкреслюючи зростаючу важливість криміналістичних можливостей в управлінні хмарною безпекою.

Оскільки організації намагаються використовувати існуючі інструменти, такі як платформи SOAR (Security Orchestration, Automation, and Response), щоб

отримати видимість у хмарних загрозах, звіт показує, що автоматизація реагування на інциденти вдвічі ефективніша порівняно з SOAR для хмарних розслідувань. Хоча визначення пріоритетів впровадження автоматизації має важливе значення, ця автоматизація має бути налаштована чітко для реагування на інциденти, а не для застосування загальних рішень автоматизації». ***(34% of organizations lack cloud cybersecurity skills // Help Net Security (https://www.helpnetsecurity.com/2024/05/28/cloud-visibility-challenges/). 28.05.2024).***

***

«Незважаючи на те, що побоювання щодо кібератак продовжують зростати, CISO демонструють зростаючу впевненість у своїй здатності захищатися від цих загроз, що відображає значні зміни в ландшафті кібербезпеки, повідомляє Proofpoint.

Впевненість CISO зростає, незважаючи на побоювання кібератак

70% опитаних CISO відчувають ризик серйозної кібератаки протягом наступних 12 місяців, порівняно з 68% роком раніше та 48% у 2022 році. Сьогодні CISO явно залишаються у стані підвищеної готовності, але впевненість серед них зростає: лише 43% відчувають себе неготовими протистояти цілеспрямованій кібератаці, що демонструє помітне зниження порівняно з минулорічними 61% і 50% у 2022 році.

Людські помилки продовжують сприйматися як ахіллесова п’ята кібербезпеки, причому 74% CISO вважають їх найбільш суттєвою вразливістю. У рік зростаючих інсайдерських загроз і втрат даних, викликаних людьми, більше, ніж будь-коли, CISO (80%) вважають людський ризик, зокрема недбалих працівників, головною проблемою кібербезпеки протягом наступних двох років.

Проте зростає оптимізм щодо ролі рішень на базі штучного інтелекту для пом’якшення людських ризиків, що відображає стратегічний поворот до захисту, керованого технологіями.

«У той час як ландшафт кібербезпеки продовжує розвиватися із зростанням загроз, орієнтованих на людину, у звіті Voice of the CISO за 2024 рік

підкреслюється життєво важливий зрушення до більшої стійкості, готовності та впевненості між глобальними CISO», — сказав Патрік Джойс, міжнародний резидент CISO у Proofpoint. «Цьогорічні результати підкреслюють колективний рух до стратегічних засобів захисту, включаючи покращену освіту, впровадження технологій і адаптивний підхід до нових загроз, таких як генеративний ШІ».

CISO стурбовані загрозами безпеці ШІ

Цього року ми спостерігаємо різке зростання кількості CISO, які вважають людські помилки найбільшою кібервразливістю своєї організації — 74% у цьому році опитування проти 60% у 2023 році. Проте 86% CISO вважають, що співробітники розуміють свою роль у захист організації.

Ця впевненість вища, ніж у попередні роки — 61% у 2023 році та 60% у 2022 році. Це можна пояснити тим, що 87% опитаних CISO прагнуть розгорнути можливості на базі штучного інтелекту для захисту від помилок людини та передових кіберзагроз, орієнтованих на людину.

У 2024 році 70% опитаних CISO відчували ризик зазнати серйозної кібератаки впродовж наступних 12 місяців, порівняно з 68% у 2023 році та 48% у 2022 році. Однак лише 43% вважають, що їхня організація не готова впоратися з цілеспрямованою атакою. кібератак порівняно з 61% у 2023 році та 50% у 2022 році.

54% опитаних CISO вважають, що генеративний ШІ становить загрозу безпеці для їхньої організації. Трьома найбільшими системами, які CISO вважають небезпечними для своїх організацій, є: ChatGPT/інший GenAI (44%), Slack/Teams/Zoom/інші інструменти для співпраці (39%) і Microsoft 365 (38%).

46% керівників служби безпеки повідомили, що їм довелося мати справу з істотною втратою конфіденційних даних за останні 12 місяців, і з них 73% погодилися, що співробітники, які залишили організацію, сприяли втраті. Незважаючи на ці втрати, 81% CISO вважають, що вони мають належний контроль для захисту своїх даних.

51% CISO, опитаних у 2024 році, мають технологію запобігання втраті даних (DLP) порівняно з лише 35% у 2023 році. 53% опитаних CISO інвестували в

навчання співробітників найкращим практикам безпеки даних, що більше у 2024 році порівняно з 2023 (39%).

Програми-вимагачі та зловмисне програмне забезпечення найбільше хвилюють CISO

Найбільшими загрозами кібербезпеці, які вважали CISO у 2024 році, були атаки програм-вимагачів (41%), зловмисне програмне забезпечення (38%) і шахрайство електронною поштою (36%). Ці основні загрози відрізняються від минулорічних; компрометація бізнес-електронної пошти (BEC) опустилася з першого місця, програми-вимагачі піднялися на перше місце, а зловмисне програмне забезпечення — на друге.

У 2024 році не змінився погляд CISO на виплату викупу. 62% CISO вважають, що їхня організація заплатить за відновлення систем і запобігання видачі даних у разі атаки програм-вимагачів протягом наступних 12 місяців. 79% CISO заявили, що покладаються на вимоги кіберстрахування для відшкодування потенційних збитків, порівняно з 61% у 2023 році.

84% CISO погоджуються, що їхні члени правління погоджуються з ними віч-на-віч у питаннях кібербезпеки. Це значний стрибок з 62% у 2023 році та 51% у 2022 році.

У 2024 році 53% CISO визнали вигорання порівняно з 60% минулого року, тоді як 66% вважають, що вони стикаються з надмірними очікуваннями, стабільне зростання порівняно з 61% минулого року та 49% у 2022 році. Стійкість поточних очікувань щодо CISO продовжує зростати. пройти тестування — 66% стурбовані особистою відповідальністю (62% у 2023 р.), а 72% (61% у 2023 р.) не приєдналися б до організації, яка не пропонує страхування директорів і посадових осіб (D&O).

Крім того, 59% CISO погодилися, що поточний економічний спад перешкодив їхній здатності здійснювати критично важливі для бізнесу інвестиції, причому 48% з них попросили скоротити персонал або відкласти заповнення, а також скоротити бюджет безпеки.

«Оскільки ми орієнтуємося в складності сучасного середовища кіберзагроз, приємно бачити, що CISO набувають довіри до своїх стратегій та інструментів», —

прокоментував Райан Калембер, головний стратегічний директор Proofpoint. «Однак постійні проблеми, пов'язані з плинністю кадрів, тиском на ресурси та необхідністю постійної участі правління, нагадують нам, що пильність і адаптація є ключовими для нашої колективної кіберстійкості».

У звіті Voice of the CISO за 2024 рік розглядаються відповіді глобального стороннього опитування від 1600 CISO з організацій із 1000 співробітників або більше в різних галузях». ***(Human error still perceived as the Achilles' heel of cybersecurity // Help Net Security (https://www.helpnetsecurity.com/2024/05/27/cisos-cyber-attacks-defense-confidence/). 27.05.2024).***

***

Сполучені Штати Америки та Канада

«Двопартійний законопроект Сенату, оприлюднений у середу, передбачає посилення заходів безпеки навколо штучного інтелекту, перегляд низки заходів, включаючи відстеження кіберуразливості та публічну базу даних для звітів про інциденти ШІ.

Закон про безпеку штучного інтелекту від 2024 року, представлений сенаторами Марком Ворнером, штат Вірджинія, і Томом Тіллісом, штат Каліфорнія, вимагає від Національного інституту стандартів і технологій оновлювати національну базу даних про вразливості (NVD), а також кібербезпеку та інфраструктуру. Агентство безпеки має оновити програму Common Vulnerabilities and Exposure (CVE) або створити новий процес, згідно з коротким викладом законопроекту.

Крім того, законопроект доручає Агентству національної безпеки створити Центр безпеки штучного інтелекту, який забезпечить випробувальний стенд ШІ для досліджень приватного сектору та академічних дослідників, а також розробить інструкції щодо запобігання або пом'якшення «контртехніки ШІ».

«Захист організацій від ризиків кібербезпеки, пов'язаних зі штучним інтелектом, потребує співпраці та інновацій як з боку приватного, так і державного сектору», — сказав Тілліс у прес-релізі. «Це логічне законодавство створює

добровільну базу даних для звітування про випадки безпеки та безпеки штучного інтелекту та сприяє найкращим практикам для зменшення ризиків штучного інтелекту».

Згідно із законодавством, CISA та NIST матимуть один рік, щоб розробити та запровадити добровільну базу даних для відстеження інцидентів безпеки та безпеки ШІ, яка буде доступна громадськості.

Подібним чином NIST матиме лише 30 днів після набрання чинності цим законодавством, щоб ініціювати «процес за участю багатьох зацікавлених сторін», щоб оцінити, чи узгоджені стандарти звітування про вразливості враховують уразливості безпеки ШІ. Після встановлення цього процесу NIST матиме 180 днів, щоб подати до Конгресу звіт про достатність процесів звітування.

«Забезпечуючи відкритість публічно-приватних комунікацій і інформування про поточні загрози, з якими стикається наша галузь, ми вживаємо необхідних заходів для захисту від цього нового покоління загроз, з якими стикається наша інфраструктура», — сказав Уорнер у прес-релізі». ***(Caroline Nihill. Bipartisan Senate bill on AI security would bolster voluntary cyber reporting processes // FedScoop (https://fedscoop.com/senate-bill-on-ai-security-bolster-voluntary-cyber-reporting/). 02.05.2024).***

***

«30 квітня 2024 року президент Байден підписав Меморандум про національну безпеку (NSM) щодо безпеки та стійкості критичної інфраструктури (NSM-22), оновлюючи політичні цілі та оперативні контури підходу уряду США (USG) до забезпечення безпека критичної інфраструктури. NSM-22 замінює президентську політичну директиву 21 (PPD-21), політичну директиву, видану в 2013 році, яка визначила сектори критичної інфраструктури та створила стратегію уряду США для підвищення їх стійкості. NSM, що готується за пропозицією про правило, що розширює збір даних про кіберінциденти від власників і операторів інфраструктури, додатково вказує на те, що федеральний

уряд планує зайняти набагато більш оперативну позицію у взаємодії з об’єктами критичної інфраструктури.

Через широкий спектр ініціатив, викладених у NSM, власникам і операторам критичної інфраструктури слід розглянути можливість взаємодії з відповідними галузевими координаційними радами та перегляду публічних випусків відповідним регулятором. Суб’єкти в секторах, де є організації, що встановлюють добровільні стандарти, також повинні розглянути можливість активної взаємодії з цими організаціями для підготовки до включення таких добровільних стандартів в обговорення обов’язкових вимог.

Сектори критичної інфраструктури та секторальні агентства з управління ризиками

NSM-22 підтверджує позначення 16 секторів критичної інфраструктури та відповідного федерального департаменту чи агентства, що взаємодіє з кожним сектором. Незважаючи на те, що NSM-22 замінює номенклатуру PPD-21 «Секторальних агентств» на «Секторальні агентства з управління ризиками» («SRMA»), вперше сформульовану в Законі про дозвіл на національну оборону на 21 фінансовий рік, жодних змін не було внесено до відповідних департаментів чи агентств. діючи як федеральний інтерфейс для будь-яких секторів. 16 секторів критичної інфраструктури та їхні SRMA:

Хімічна: Департамент внутрішньої безпеки («DHS»)

Комерційні приміщення: DHS

Зв'язок: DHS

Критичне виробництво: DHS

Дамби: DHS

Оборонно-промислова база: Міністерство оборони

Екстрені служби: DHS

Енергетика: Департамент енергетики

Фінансові послуги: Департамент казначейства

Харчування та сільське господарство: Департамент сільського господарства та Департамент охорони здоров’я та соціальних служб («HHS»)

Державні служби та установи: DHS та Адміністрація загального обслуговування

Охорона здоров'я та громадське здоров'я: HHS

Інформаційні технології: DHS

Ядерні реактори, матеріали та відходи: DHS

Транспортні системи: DHS і Департамент транспорту

Системи водопостачання та водовідведення: Агентство з охорони навколишнього середовища

Мінімальні вимоги до безпеки та стійкості

Хоча принципи політики, викладені в NSM-22, загалом базуються на стратегічних ініціативах із PPD-21, новим пріоритетом є розробка мінімальних вимог безпеки та стійкості для об’єктів критичної інфраструктури. Цей NSM доручає органам регулювання та нагляду встановити та запровадити мінімальні вимоги та механізми підзвітності для безпеки та стійкості критичної інфраструктури.

Це підвищення мінімальних вимог щодо безпеки та стійкості відповідає міркуванням Національної кіберстратегії щодо обмежень добровільних стандартів. У той час як дії, які державні зацікавлені сторони зобов’язані вживати в рамках NSM-22, залежать від урядової інтерпретації його існуючих повноважень, SRMA доручено координувати з відповідними регуляторами прийняття нормативних актів, які сприяють реалізації мінімальних вимог. Оскільки DHS діє як SRMA для 8 секторів, така координація з регуляторними органами необхідна для створення обов’язкових вимог лише за допомогою існуючих повноважень. У секторі інформаційних технологій, наприклад, можливість залучати Міністерство торгівлі та інші створить набагато більшу різноманітність варіантів для розгляду урядом у сприянні безпосереднім цілям NSM. SRMA також доручено розробити пропозиції щодо нових повноважень у Конгресу для сфер, де існуючих повноважень недостатньо.

Крім того, SRMAs і національний координатор з питань безпеки та стійкості критичної інфраструктури («Національний координатор») [1] зобов’язані надати

огляд доступних інструментів і повноважень, щоб вимагати та стимулювати власників і операторів критичної інфраструктури запроваджувати мінімальну безпеку та стійкість. вимоги до 25 січня 2025 р. Цей огляд виявить прогалини в спроможності федерального уряду вимагати та забезпечити дотримання мінімальних вимог до критичної інфраструктури та створить законодавчу пропозицію щодо будь-яких додаткових повноважень або можливостей, необхідних для виконання таких вимог.

Позначення системно важливої сутності

Цей NSM також доручає національному координатору ідентифікувати системно важливі суб'єкти («SIE»), які є «організаціями, які володіють, експлуатують або іншим чином контролюють критичну інфраструктуру, яка має пріоритет на основі потенціалу її порушення або несправності, що спричинить національно значущі та каскадні негативні впливи». Пріоритезація SIE стосуватиметься надання федеральними зацікавленими сторонами інформації щодо зменшення ризиків та інших операційних ресурсів. Список SIE також служить для задоволення вимоги до Міністерства внутрішньої безпеки щодо розробки списку критичної інфраструктури, яка «піддається найбільшому ризику» відповідно до розділу 9 виконавчого наказу 13636. Список ДІП не буде відкритим.

Ключові федеральні департаменти та агентства

Одним із важливих оновлень PPD-21, який було видано до створення CISA, є кодифікація функції CISA в загальному підході уряду до безпеки критичної інфраструктури. Як національний координатор, CISA відіграватиме центральну роль в оцінці прогресу ініціатив, викладених у NSM-22, маючи комплексний погляд на галузеві зусилля.

На міністра внутрішньої безпеки покладається роль координації національних зусиль із забезпечення безпеки критичної інфраструктури.

Міністерство юстиції керуватиме антитерористичною та контррозвідувальною діяльністю щодо критичної інфраструктури, включаючи кримінальні розслідування та оперативне реагування на інциденти, які стосуються критичної інфраструктури.

Міністерство торгівлі очолить розробку стандартів, сприятиме і підтримуватиме керівні принципи, найкращі практики, методології, процедури та процеси для зменшення ризиків кібербезпеки для критичної інфраструктури.

Міністерство енергетики й надалі керуватиме політикою, готовністю, аналізом ризиків, технічною допомогою, дослідженнями та розробками, оперативним співробітництвом і реагуванням на надзвичайні ситуації в енергетичному секторі США». ***(Brock Dahl, Madeline Cimino and Megan M. Kayo. New Federal Policy Creates Path Forward for Mandatory Requirements for Critical Infrastructure Entities // Freshfields Bruckhaus Deringer (https://blog.freshfields.us/post/102j77x/new-federal-policy-creates-path-forward-for-mandatory-requirements-for-critical-i#page=1). 09.05.2024).***

***

«Офіс кіберцаря Білого дому вважає, що стан кібербезпеки США покращився за останній рік, оскільки зацікавлені сторони запровадили широку стратегію, спрямовану на зміцнення цифрового захисту США. Але він підкреслив, що численні загрози зберігаються.

До них належать програмне забезпечення-вимагач і тривалі кібератаки на критично важливу інфраструктуру, пара хакерських дій, які місяцями ставали новинами.

Оновлення Офісу Національного директора з питань кібербезпеки щодо стану кібербезпеки Сполучених Штатів також постачається з продовженням минулорічного Плану впровадження національної кіберстратегії, який розміщує більше директив під раніше встановленими стовпами, зокрема захист критичної інфраструктури та налагодження партнерства за кордоном.

Друга версія рамки впровадження містить заклик до використання «всіх інструментів національної влади», щоб ускладнити хакерам загрозу національній або громадській безпеці, повідомляє ONCD.

«Ми перебуваємо в розпалі фундаментальної трансформації кібербезпеки нашої країни», — сказав у своїй заяві директор National Cyber Гаррі Кокер. «Ми

досягли прогресу в реалізації позитивного бачення безпечного, процвітаючого та справедливого цифрового майбутнього, але загрози, з якими ми стикаємося, залишаються страшними».

Офіс Національного кібердиректора повідомляє, що 33 із 36 ініціатив у рамках першого плану реалізації, який має бути заплановано на другий квартал 2024 року, завершено, а останні три знаходяться на стадії розробки. Ще 33 планується завершити протягом наступних двох років, включаючи зусилля з модернізації федеральних цивільних технологій відділення з багаторічним планом життєвого циклу для усунення застарілих систем.

Новий план впровадження включає 31 нову ініціативу, включаючи зусилля, спрямовані на посилення кібербезпеки в секторах охорони здоров'я, освіти та водопостачання. Нові ініціативи також включають плани щодо просування спільних послуг, орієнтованих на кібербезпеку, у федеральній цивільній виконавчій владі та спільного використання інструментів управління ризиками в ланцюжках кіберпостачання між агентствами.

Зусилля, спрямовані на припинення програм-вимагачів та усунення ризиків безпеці, пов'язаних із програмним забезпеченням з відкритим кодом, також включені до нових ініціатив, як і ініціатива, зосереджена на просуванні досліджень і настанов щодо цифрової ідентичності через Національний інститут стандартів і технологій — тема, яка була пропущена. початкового плану впровадження, на розчарування зацікавлених сторін.

У новому плані реалізації зазначено, що робота з цифрової ідентифікації «може включати» публікацію вказівок щодо цифрової ідентифікації — те, над чим NIST уже працює — міркування щодо технології перевірки атрибутів або оцінки технології розпізнавання обличчя.

Робоча сила з кібербезпеки, яка є предметом власної стратегії Офісу Національного директора з кібербезпеки, також отримує деякі зауваження в оновленому плані реалізації, зокрема акцент на сприянні найму на основі навичок у федеральному уряді та серед його підрядників.

Що стосується решти загроз, з якими ці зусилля спрямовані на боротьбу, у звіті вказується на загрозу експлуатації ланцюга поставок, зростаючий ринок комерційного шпигунського програмного забезпечення та виклики, які створює штучний інтелект для кібербезпеки.

«Постійний прогрес у цифрових комунікаціях, передових обчисленнях, квантовій інформатиці, зберіганні й обробці даних та інших критичних і нових технологіях стрімко ускладнює нашу економіку та суспільство», — йдеться у звіті про кібернетичний ландшафт.

«У міру того як цей ландшафт розвивається, зловмисники як державні, так і недержавні суб'єкти використовують його шви зі зростаючими можливостями та стратегічними цілями, даючи зрозуміти, що кіберпростір тісно пов'язаний з іншими сферами міжнародних конфліктів і конкуренції», – продовжується в документі.

Кіберофіс Білого дому заявляє, що план впровадження буде продовжувати щорічно оновлюватися та координуватиметься з Адміністративно-бюджетним управлінням, щоб узгодити щорічні бюджетні запити з ініціативами в плані впровадження». ***(Natalie Alms and David DiMolfetta. US advances on cyber goals amid rapidly changing threat environment, White House says // Government Media Executive Group LLC (https://www.nextgov.com/cybersecurity/2024/05/us-advances-cyber-goals-amid-rapidly-changing-threat-environment-white-house-says/396370/?oref=ng-next-story). 07.05.2024).***

***

«Серед співробітників США зростає занепокоєння щодо ескалації загроз кібербезпеці на робочому місці: 53% стурбовані тим, що їх організація стане об'єктом кібератак, а третина (34%) стурбована тим, що вони можуть залишити свою організацію вразливою через дій, згідно з новими даними Ernst & Young LLP (EY US).

Примітно, що страх піддати свою організацію кібератаці «особливо високий серед молодих поколінь, оскільки працівники покоління Z і Millennial менш

схильні відчувати себе готовими виявляти кіберзагрози та реагувати на них порівняно зі своїми старшими колегами».

Опитування людських ризиків у кібербезпеці 2024 року – це «дослідження 1000 працюючих американців у державному та приватному секторах, яке слідує за початковим аналізом 2022 року, проведеним EY US, і досліджує поточний стан кібербезпеки та зміни з часом, відкриваючи ключові ідеї для бізнес-лідерів щодо обізнаності з кібербезпекою. і практики».

Цього року EY US розширила дослідження, «щоб проаналізувати сприйняття співробітниками ролі штучного інтелекту (ШІ) у ескалації загроз, виявивши, що 85% працівників вважають, що ШІ зробив атаки на кібербезпеку більш складними, 78% стурбовані використанням ШІ в кібератак, а 39% співробітників не впевнені, що знають, як відповідально використовувати ШІ».

Подібно до висновків 2022 року, останнє дослідження кібербезпеки EY US «підкреслює постійний розрив у підготовленості між поколіннями, коли молоді працівники продовжують не вміти застосовувати безпечні практики кібербезпеки більше, ніж старші покоління».

Насправді покоління Z втрачає впевненість у «своїй здатності розпізнавати спроби фішингу — одну з найпоширеніших і найуспішніших тактик атак соціальної інженерії — і, швидше за все, зізнається у відкритті підозрілого посилання».

А тепер, завдяки потужності фішингових електронних листів, згенерованих штучним інтелектом, «виявляти шкідливі посилання та вміст стає ще важче».

Незважаючи на те, що вони належать до цифрового покоління, лише 31% представників покоління Z дуже впевнено розпізнають спроби фішингу, «що означає зниження на тривожні дев’ять процентних пунктів порівняно з 40% у 2022 році, а 72% сказали, що відкривали незнайоме посилання, яке здавалося підозрілим у роботи, набагато більше, ніж міленіали (51%), покоління X (36%) і бебі-бумери (26%)».

Майже двоє з трьох представників покоління Z і міленіалів «особливо бояться наслідків кібербезпеки, у тому числі 64% представників покоління Z і 58%

міленіалів, які бояться, що втратять роботу, якщо колись залишать свою організацію вразливою для атаки. Молодші покоління також, швидше за все, не повністю розуміють, який процес їхньої організації повідомляє про ймовірні кібератаки, навіть якщо в їхній організації є процес (39% Gen Z і 29% Millennials проти 19% Gen X і 15% бебі-бумерів).»

Однак, це не «все загибель і морок».

Незважаючи на занепокоєння щодо їхньої здатності запобігати атакам, дослідження EY «показує, що працівники покоління Z все більше вважають себе обізнаними з кібербезпеки (86% проти 75% у 2022 році), вказуючи на можливості краще підготувати молодих працівників, щоб перетворити ці знання на впевненість за допомогою інвестування в підвищення кваліфікації та навчання, яке обслуговує їхній унікальний досвід як справжніх цифрових вихідців».

Швидкий розвиток штучного інтелекту змусив організації «регулярно адаптувати навчальні протоколи та залишатися відданими наданню частих, оновлених тренінгів, які стосуються останніх загроз, спричинених штучним інтелектом, і тенденцій кіберзлочинності».

Переважна більшість співробітників (91%) стверджують, що організаціям «слід регулярно оновлювати свою підготовку, щоб йти в ногу з ШІ, особливо враховуючи, що роль ШІ в кіберзагрозах розвивається; але лише 62% кажуть, що їхній роботодавець зробив пріоритетом навчання працівників відповідальному використанню ШІ».

Команда EY Cybersecurity рекомендує керівникам і старшим бізнес-лідерам «включити наступні провідні практики в свою програму кібербезпеки, щоб культивувати сильну та впевнену культуру безпеки» у своїй організації:

Створюйте надійні тренувальні вправи, які закріплюються цілий рік. Дослідження EY у США показує, що працівники, які «не пройшли» навчання з кібербезпеки, найбільше бояться використання технологій на роботі. Навпаки, 94% співробітників, які пройшли навчання протягом останнього року, кажуть, що кібербезпека є для них пріоритетом.

Стимулюйте залучення співробітників за допомогою гейміфікації. Таблиці лідерів і багатокористувацькі функції в гейміфікованих навчальних програмах сприяють здоровій конкуренції серед співробітників, спонукаючи їх працювати краще. Гейміфікація особливо ефективна для антисоціальних інженерних кампаній, якщо вона спрямована на природну людську цікавість, яка часто робить працівників уразливими.

Партнер, не поліція. Організації, які перевіряють своїх співробітників, щоб перевірити, чи вони належним чином реагують на загрози кібербезпеці, можуть ненавмисно перетворити кібернавчання на момент, який «захоплюється». Позиціонуйте протоколи кібербезпеки як роботу в партнерстві зі своїми співробітниками, а не як поліцію, дотримуючись натомість політики «побачте щось, скажіть щось».

Зробіть процес повідомлення про потенційні атаки та вразливості достатньо простим, щоб працівники всіх поколінь могли легко інтегрувати його у своє повсякденне життя.

Включіть практичні протоколи навчання ШІ. Включно з протоколами, які включають практичне навчання з використання штучного інтелекту на робочому місці, надає працівникам доступ до основних можливостей і ризиків. Безпосередній досвід використання нових технологій, таких як генеративний ШІ, відкриває новий рівень розуміння та стимулює оборонне мислення.

Показуйте приклад із відповідальним штучним інтелектом: згідно з дослідженням EY у США, 39 відсотків працівників не впевнені, що знають, як відповідально використовувати штучний інтелект. Як розпорядники своєї організації, керівники та старші керівники повинні дотримуватися прозорості в тому, як розробляється та розгортається штучний інтелект у масштабах підприємства, і самі демонструвати відповідальні практики штучного інтелекту, щоб зменшити ризики.

Методологія

EY US доручила третій стороні «провести дослідження людських ризиків у кібербезпеці 2024».

Онлайн-опитування серед n=1000 штатних і неповних працівників США «віком від 18 років, чия поточна робота вимагає використання робочого ноутбука/комп'ютера (тобто професіонала з технічними підходами)».

Вибірка була збалансована «за віком, статтю, доходом домогосподарства, расовою та етнічною приналежністю та регіоном. Опитування проводилося з 7 по 15 березня 2024 року. Похибка (MOE) для загальної вибірки становить +/- 3 відсоткові пункти». ***(Omar Faridi. Cybersecurity Concerns Reportedly Rise Among US Workers with Most Worried About AI in Online Security // Crowded Media Group (https://www.crowdfundinsider.com/2024/05/224901-cybersecurity-concerns-reportedly-rise-among-us-workers-with-most-worried-about-ai-in-online-security/). 11.05.2024).***

***

«Стратегія корпоративної кібербезпеки уряду Канади – це перспективний план покращення кібербезпеки в урядових департаментах і установах, щоб продовжувати надавати безпечні та надійні цифрові державні послуги. Він служить основою для ще більшого переходу уряду від оборонної позиції до проактивного підходу до кібербезпеки шляхом вдосконалення навчання, додатків, політики та моніторингу.

За останнє десятиліття уряд вжив заходів для покращення стану кібербезпеки шляхом стандартизації IT-інфраструктури та інтеграції послуг кіберзахисту, створення Канадського центру кібербезпеки та впровадження чіткого управління, політики та інструментів для підтримки кібербезпеки. Незважаючи на цей прогрес, прогалини все ще залишаються. Стратегія корпоративної кібербезпеки спрямована на усунення цих прогалин і забезпечення того, щоб уряд мав хороші можливості для боротьби з майбутніми кіберзагрозами.

Стратегія побудована на 4 стратегічних цілях, щоб допомогти федеральним організаціям використовувати ширший підхід для всього підприємства для захисту своїх систем від кіберризиків:

- Реально сформулюйте кіберризик і його вплив на бізнес для ефективного, орієнтованого на дії та підзвітного прийняття рішень
- Ефективніше запобігайте кібератакам і протидійте їм для кращого захисту інформації та активів GC
- Посилення можливостей і стійкості в GC для проактивної підготовки до кіберподій, реагування на них і відновлення після них
- Стимулюйте різноманітну робочу силу GC з відповідними навичками, знаннями та культурою кібербезпеки

Кожна з цілей, перелічених вище, має відповідні ключові дії для забезпечення досягнення мети. Приклади ключових дій:

- забезпечення того, щоб федеральні департаменти та агентства мали щорічні процеси управління ризиками та звітність, що допоможе уряду бути більш ефективним і проактивним у виявленні та управлінні кіберризиками з точки зору всього підприємства
- формування кіберталантів в уряді за допомогою міжфункціональних навчальних програм для використання різноманітних навчальних рішень
- просування культури управління талантами для найму та утримання кандидатів із необхідними кібернавички, а також
- покращення управління ризиками третіх сторін за допомогою таких заходів, як стандартизація положень і умов у контрактах, а також виконання планової перевірки дотримання постачальниками положень

Перший етап впровадження розпочнеться негайно та підтримає:

- Створення централізованої системи оцінювання з незалежними оцінками та ретельними аналізами кібербезпеки відділів для виявлення та визначення пріоритетів ризиків.
- Створення об’єднаної інтегрованої платформи управління ризиками для визначення пріоритетів і звітності на основі даних як ключової частини ширшої системи управління корпоративним портфелем.

• Створення загальнодержавної програми управління вразливістю для скоординованого процесу розкриття вразливостей і зосередження на людях, процесах, політиках і технологіях.

• Створення нової фіолетової команди, яка буде імітувати методи, які використовують зловмисники проти урядових систем, щоб проактивно тестувати та перевіряти будь-які прогалини в безпеці…» ***(Government of Canada's Enterprise Cyber Security Strategy // Government of Canada (https://www.canada.ca/en/treasury-board-secretariat/news/2024/05/government-of-canadas-enterprise-cyber-security-strategy.html). 22.05.2024).***

***

«Національний інститут стандартів і технологій США (NIST) випустив третю редакцію своєї спеціальної публікації (SP) 800-171 «Захист контрольованої несекретної інформації в нефедеральних системах і організаціях». Ця публікація є основою стандартів кібербезпеки, яких підрядники повинні дотримуватися при роботі з контрольованою несекретною інформацією (CUI) для Міністерства оборони США (DOD) і для нового коефіцієнта готовності до кібербезпеки Міністерства внутрішньої безпеки США (DHS). Крім того, майбутня програма сертифікації моделі зрілості кібербезпеки (CMMC) Міністерства оборони використовує NIST SP 800-171 для отримання рівня 2 сертифікації (хоча очікується, що спочатку CMMC використовуватиме попередню версію SP 800-171 у програмі CMMC).

Також випущено другу версію (але також називається Редакція 3) NIST SP 800-171A під назвою «Оцінка вимог безпеки для контрольованої несекретної інформації». Згідно з описом NIST, ця допоміжна публікація надає організаціям «процедури та методології оцінки» під час оцінювання того, чи було виконано контроль NIST SP 800-171. Востаннє цей документ оновлювався у 2018 році.

Ключові зміни

Є деякі важливі зміни між попередньою версією (Редакція 2) і поточною версією (Редакція 3), які підрядники повинні розуміти:

Введення визначених організацією параметрів (ODP). Ці нові параметри нададуть підрядникам можливість адаптувати елементи керування до своїх систем. Наприклад, 03.01.01, Керування обліковими записами, дозволяє власникам систем визначати період часу, коли користувачів припиняється або передається.

У той час як кількість елементів керування зменшилася (зі 110 до 97), багато попередніх елементів керування було складено в інші подібні елементи керування, а фактичні вимоги натомість зросли.

Додатково пов’язуючи відповідність кібербезпеки та відповідність ланцюга постачання, NIST SP 800-171 представив нову сімейство засобів управління ризиками ланцюга постачання (SCRM) (запозичено з NIST SP 800-53). Це сімейство містить три елементи керування, включаючи вимогу щодо плану управління ризиками ланцюга постачання (03.17.01), стратегій, інструментів і методів придбання (03.17.02) і вимог до ланцюга постачання та процесів (03.17.03). У сукупності підрядникам потрібно буде забезпечити безпеку ланцюга постачання в рамках виконання всіх заходів контролю в NIST SP 800-171.

Існує також прямий перехід від NIST SP 800-53, редакція 5 (пов’язана із захистом федеральних інформаційних систем) до NIST SP 800-171, редакція 3 (пов’язана із захистом федеральної інформації в системах підрядників), відома як «Пошиття». Критерії». Кожен елемент керування NIST SP 800-53 відображається на елемент керування NIST SP 800-171. Якщо жодного контролю NIST SP 800-171 не нанесено на карту, NIST зазначає, чи це: 1) не пов’язане із захистом CUI, 2) є відповідальністю федерального уряду, 3) керування достатньо охоплено іншим контролем, або 4) не застосовується.

У попередньому проекті перегляду незалежні оцінки вимагалися як один із засобів контролю. NIST виключив цей контроль у цій останній редакції як «не пов'язаний безпосередньо» із захистом CUI.

Висновки та наступні кроки

Випуск цього нового стандарту вплине на простір державних контрактів на довгі роки. Незважаючи на це, негайних дій не потрібно. Нещодавно Міністерство оборони опублікувало відхилення від класу, що впливає на Розділ 252.204-7012

Федерального нормативного доповнення для оборонних закупівель (DFARS), яке дасть підрядникам злітно-посадкову смугу для прийняття Ревізії 3 (раніше ефект був би негайним). Крім того, проект правила CMMC встановив Редакцію 2 як стандарт. Незважаючи на це, існує правило FAR, яке вимагатиме прийняття NIST SP 800-171 для всього уряду, і незрозуміло, який перегляд буде використано в цьому правилі. І відхилення класу DOD може бути скасовано в будь-який час. Враховуючи це, підрядникам доцільно почати підготовку до впровадження цієї нової версії зараз». ***(Eric S. Crusius. Foundational Cybersecurity Standards for Contractors Updated // Holland & Knight LLP (https://www.hklaw.com/en/insights/publications/2024/05/foundational-cybersecurity-standards-for-contractors-updated). 14.05.2024).***

***

«Визнаючи новітні технології та кіберзагрози переломним моментом для конкуренції США з геополітичними суперниками, Державний департамент США оголосив про стратегію міжнародної кіберпростору та цифрової політики США.

За словами Держсекретаря США Ентоні Блінкена, Сполучені Штати віддані «не «цифровому суверенітету», а «цифровій солідарності».

Це підкреслює партнерство США з зацікавленими сторонами в усьому світі, які поділяють відданість відкритому, безпечному та захищеному технологічному майбутньому, яке сприяє розвитку стійких і демократичних суспільств. У стратегії далі пояснюється, що цифрова солідарність передбачає допомогу жертвам кіберзлочинців; підтримка партнерів у розгортанні безпечних, надійних, стійких і стійких технологій; створення коаліцій для формування цифрової революції на всіх рівнях стека технологій; сприяння управлінню даними та нормам, що поважають права людини.

Державний департамент визначив чотири напрямки, які мають бути пріоритетними протягом наступних трьох-п’яти років для побудови цифрової солідарності.

Відкрита, всеохоплююча, безпечна та стійка цифрова екосистема: у цьому напрямі діяльності наголошується на захищених телекомунікаційних мережах, хмарних службах, центрах обробки даних, підводних кабелях, мережах супутникового зв'язку та відповідних інфраструктурних технологіях.

Підходи до цифрового управління, що поважають права: Державний департамент підтримуватиме міжнародні зусилля з гармонізації механізмів безпечної транскордонної передачі даних, сумісних стандартів, прозорих процесів розробки міжнародних стандартів із різноманітною участю, побудови заснованого на правах бачення цифрового майбутнього та переговори щодо договору про кіберзлочинність, що поважає право.

Відповідальна поведінка держави в кіберпросторі: Сполучені Штати наголошуватимуть на відповідальних нормах кіберпростору в Організації Об'єднаних Націй, підтримуватимуть союзників, які стикаються з кіберзлочинами, очолитимуть зусилля з боротьби з кібератаками на критично важливу інфраструктуру, притягатимуть держави до відповідальності за зловмисну кіберактивність, підтверджуватимуть застосування угод про взаємну оборону в кіберпросторі, а також боротися з злочинними діячами програм-вимагачів і використанням комерційних шпигунських програм.

Цифрова політика та кіберспроможність: щоб розширити цифрову політику, правову та регуляторну спроможність як вдома, так і за кордоном, Державний департамент координуватиме роботу з іншими відомствами та зацікавленими сторонами, збільшуватиме зусилля партнерів із нарощування потенціалу та модернізуватиме нові інструменти для кібердопомоги». ***(Nathan Salminen, Soojin Jeong. Security Snippets: Biden Administration announces global cybersecurity strategy // Hogan Lovells International LLP (https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9VapOkb%2BnlYB6OF7eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF3dzoxprWhI6w%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true). 23.05.2024).***

***

«7 травня 2024 року Офіс Національного кібердиректора Білого дому (ONCD) опублікував кілька звітів про стан кібербезпеки та стратегічний план Сполучених Штатів. Ці документи реалізують Національну стратегію кібербезпеки (NCS) до 2023 року та містять:

(1) Звіт про стан кібербезпеки Сполучених Штатів за 2024 рік (Звіт про стан) та інформаційний бюлетень; і

(2) Версія 2 Плану впровадження національної стратегії кібербезпеки (NCSIP) і інформаційний лист.

За словами директора ONCD Гаррі Кокера-молодшого, режим кібербезпеки Сполучених Штатів перебуває в розпалі «фундаментальної трансформації», переходячи від позиції реагування до проактивної, щоб йти в ногу з ландшафтом кіберзагроз, що швидко розвивається. Ці документи містять оновлену інформацію про перехід США та кроки, необхідні для впровадження NCS.

Ключові висновки

Звіт про позицію в основному ретроспективний і служить покажчиком федеральних кіберініціатив за минулий рік, перераховуючи різноманітні досягнення понад 24 федеральних агентств, які сприяли цій роботі. Навпаки, NCSIP є перспективним і окреслює 100 ініціатив, які федеральний уряд вживатиме для впровадження NCS.

Разом ці звіти аналізують виклики та можливості, які ONCD планує націлити на наступний рік. Еталонні показники вказують на посилення перевірки та опори на приватний сектор для зміни цифрової екосистеми та підвищення стійкості Сполучених Штатів до кіберзагроз. Організації приватного сектору часто мають бачення певних аспектів зловмисної діяльності, чого немає у федерального уряду, і володіють значною частиною повноважень, щоб змінити небезпечні практики шляхом впровадження принципів Secure by Design і виправлення вразливостей безпеки. Іншою тенденцією є посилення уваги до розробок у передових обчислювальних технологіях, таких як квантові обчислення та штучний інтелект, а

також підготовка до цих технологій через навчання кіберперсоналу та міжвідомчу координацію.

Крім того, федеральний уряд дивиться ззовні на ризики, створені Китаєм, Росією, Іраном і Північною Кореєю, а також недержавними злочинними організаціями. Однак у цих звітах наголошується, що багато рішень щодо цих ризиків є також зовнішніми для Сполучених Штатів, заснованими на створенні коаліції та сумісних міжнародних стандартах.

Звіт про стан кібербезпеки за 2024 рік

The Posture Report, виданий ONCD відповідно до 6 USC § 1500(c)(1)(C)(iv), надає першу у своєму роді оновлену інформацію про те, як Сполучені Штати вирішують виклики та можливості, що постають у кіберпросторі., прогрес, досягнутий у реалізації безпечного, процвітаючого та справедливого цифрового майбутнього, а також загрози, які залишаються.

Звіт про поставу аналізує:

(1) Стратегічне середовище, включаючи тенденції, що виникають, можливості та наміри суб'єктів загрози, а також уразливі місця, що розвиваються;

У звіті Posture Report зосереджено п'ять тенденцій, які змінили стратегічне середовище у 2023 році: розвиток ризиків для критичної інфраструктури, програмне забезпечення-вимагач, використання ланцюга поставок, комерційне шпигунське програмне забезпечення та ШІ.

Сполучених Штатів (2) поточні зусилля щодо посилення внутрішньої кібербезпеки;

У звіті про позицію перелічено дії, вжиті 24 державними установами за останній рік для покращення політики кібербезпеки, паралельно з версіями 1 і 2 NCSIP (про які докладніше йдеться нижче). Ці дії зосереджені, серед інших тем, на захисті критичної інфраструктури, посиленні федерального співробітництва та партнерства з приватним сектором і міжнародними партнерами, припиненні ворожої діяльності, зміцненні національної робочої сили в кіберпространстві та інвестуванні в стійкі технології нового покоління.

Ці ініціативи спрямовані на підвищення вимог до кібербезпеки там, де їх бракує, гармонізацію та узгодження нових і існуючих нормативних вимог як у країні, так і за кордоном, допомогу жертвам кібератак і надання інструментів потенційним жертвам.

(3) Погляд на майбутнє.

У звіті про позицію висвітлюються нові технічні та управлінські виклики та можливості, які адміністрація візьме на себе в наступному році, включаючи вирівнювання ресурсів для підтримки зусиль, більш детально викладених у NCSIP.

2024 NCSIP

Версія 2 NCSIP доповнює висновки Звіту про стан справ і описує кроки, необхідні для подальшого покращення стану кібербезпеки США. У версії 1 NCSIP, опублікованій у липні 2023 року, представлено 69 федеральних контрольних показників, призначених для досягнення цілей NCS до 2025 року. Надалі NCSIP оновлюватиметься щорічно у координації з Управлінням управління та бюджету.

Версія 2 забезпечує оновлення статусу та доповнює цілі, викладені у звіті про позицію, додавши 31 новий контрольний показник, довівши загальну кількість до 100. Ці контрольні показники відповідають п’яти стовпам NCS:

(1) Захист критичної інфраструктури.

Еталонні показники в рамках цього стовпа походять від Агентства з кібербезпеки та безпеки інфраструктури (CISA) та інших галузевих агентств з управління ризиками та зосереджуються на забезпеченні та масштабуванні співпраці державно-приватного сектору з власниками та операторами критичної інфраструктури. Серед критично важливих галузей інфраструктури, на які націлена робота, – охорона здоров’я та охорона здоров’я, освіта, енергетика та комунальні послуги, такі як системи водопостачання та водовідведення. Конкретні ініціативи включають розробку таксономії для федеральних центрів кібербезпеки, запровадження центру енергетичних загроз і аналізу (ETAC), активізацію міжвідомчої координації шляхом видання остаточного правила звітування про кіберінциденти CIRCIA, заохочення найкращих практик через впровадження оновленого NIST CSF і розвиток ланцюга поставок правила оцінки ризиків.

(2) Знищення та ліквідація загрозливих суб’єктів.

Ця складова спрямована на зміцнення співпраці між федеральними, державними, місцевими, племінними та територіальними правоохоронними органами, приватним сектором і міжнародними партнерами для запобігання, стримування та припинення кіберзлочинності. Конкретні контрольні показники, запроваджені у версії 2 NCSIP, зосереджені на стримуванні кіберзлочинності неповнолітніх, знищенні безпечних гаваней для злочинів із програмами-вимагачами та розробці політики, яка підтримує співпрацю з приватним сектором.

(3) Сформуйте ринкові сили для забезпечення безпеки та стійкості.

Еталонні показники в рамках цього стовпа зосереджуються на покладанні відповідальності за кібербезпеку на організації, які мають найкращі можливості для зниження ризиків і створення більш стійкої цифрової екосистеми. Вони включають оновлення національної стратегії дослідження конфіденційності, розробку добровільної програми маркування для інтелектуальних пристроїв Інтернету речей (IoT) (US Cyber Trust Mark) та оцінку ризику безпеки програмного забезпечення з відкритим кодом.

(4) Інвестуйте в стійке майбутнє.

На підтримку цього стовпа NCSIP зосереджується на прискоренні розробки та впровадження безпечних інтернет-стандартів і технологій, збільшенні федерального залучення до досліджень і розробки методів кібербезпеки, поєднанні декарбонізації та кібербезпеки для операторів розподілу електроенергії з більш широкими цілями адміністрації в галузі кібербезпеки, підготовці до зростання квантових обчислень і розширення доступу до кіберосвіти та навчання для підтримки національної кіберробочої сили.

(5) Налагодити міжнародне партнерство для досягнення спільних цілей.

Цей стовп підкреслює важливість побудови коаліцій для розробки відкритих і сумісних мереж на основі стандартів, надання допомоги союзникам у реагуванні на інциденти, покращення стійкості ланцюга постачання, реалізації Міжнародної стратегії кіберпростору та цифрової політики, розробки вказівок щодо безпечної

розробки та виробництва напівпровідників., а також підтримка розвитку відкритих і сумісних бездротових мереж.

Висновок

Обсяг програм, представлених у Звіті про положення та версії 2 NCSIP, є широким і вказує на реальну прихильність федерального уряду оцінці та покращенню стійкості кібербезпеки США. Ці ініціативи продовжують тенденцію до глибшої опори на приватний сектор і бажану координацію між федеральними агентствами в уже переповненому просторі». ***(Shoba Pillay, Zoë Higgins Reinstein. Client Alert: White House Releases Report on US Cybersecurity Posture // Jenner & Block LLP (https://www.jenner.com/en/news-insights/publications/client-alert-white-house-releases-report-on-us-cybersecurity-posture). 14.05.2024).***

***

«У середу Канада оприлюднила свою першу в історії стратегію кібербезпеки для федеральних державних департаментів і агенцій, спрямовану на вирішення проблем, пов'язаних із віддаленою роботою, хмарними обчисленнями, старінням інфраструктури та наймом персоналу.

У стратегії, оприлюдненій президентом Міністерства фінансів Анітою Ананд, зроблено висновок, що державним департаментам і агенціям загалом не вистачає «повторюваних» процесів для виявлення та реагування на нові та нові кіберзагрози станом на фінансовий рік, що закінчується у 2023 році.

До 2024 року Центр аналізу фінансових операцій і звітів Канади, Королівська канадська кінна поліція та Міністерство глобальних справ Канади усі мали справу з кіберінцидентами.

«Не тільки інші уряди в нашій країні та приватні підприємства повинні забезпечити надійний захист від кіберзагроз і кібератак, але й сам уряд Канади повинен забезпечити захист наших систем», — сказав Ананд в інтерв'ю Bloomberg.

«Отже, інформація окремих громадян захищена, і тому ми можемо краще забезпечити надання послуг».

Вартість стратегії становить 11 мільйонів канадських доларів (8 мільйонів доларів) протягом п’яти років.

Під час пандемії багато державних службовців перейшли на віддалену роботу, використовуючи свої домашні мережі, а не виключно державні системи. Тепер, оскільки багато з цих працівників залишаються гібридними, стратегія спрямована на те, щоб зробити роботу вдома більш безпечною за рахунок розширення багатофакторної автентифікації та запровадження постійного захисту від шкідливих програм і вірусів.

Уряд також використовує більше мобільних пристроїв, хмарних служб і програмного забезпечення сторонніх розробників. Деякі з цих систем працюють на рівні департаменту чи агентства, що може призвести до неузгодженості.

«Швидкість технологічних змін означає, що заходи безпеки, які колись були ефективними, можуть швидко застаріти, що підкреслює необхідність проактивного та адаптивного підходу до кібербезпеки», — йдеться в стратегії.

Уряд планує створити центр безпеки, який контролюватиме локальні, хмарні та інші підключені до мережі пристрої в департаментах і установах. Деякі також матимуть спеціалізовані операційні центри. Відповідно до стратегії також буде створено фіолетову команду, до складу якої ввійдуть команди, які моделюватимуть кібератаки та оцінюватимуть захист, щоб виявити прогалини в державній кібербезпеці.

Старіння інфраструктури також є причиною вразливості. «Слабка практика управління інформацією є неприйнятною, а застарілі IT-інструменти, які неналежним чином захищають інформацію, є неприйнятними для того, щоб гарантувати мінімізацію інцидентів кібербезпеки та порушень конфіденційності», — сказав Ананд.

Кіберзагрози викликають дедалі більше занепокоєння та можуть надходити від державних чи недержавних суб’єктів незалежно від географічних кордонів. Деякі дати також особливо ризиковані для кіберінцидентів, як-от 24 лютого, день, коли Росія вторглася в Україну в 2022 році, сказав Ананд.

Крім того, уряд намагається найняти фахівців з кібербезпеки. У новій стратегії планується створити партнерські відносини з коледжами та університетами, прискорити наймання за рахунок автоматизації та навчити працівників інших відділів працювати на місцях.

Стратегія встановлює часові рамки для досягнення результатів протягом двох-п’яти років. Уряд очікує, що деякі інциденти з кібербезпекою будуть, але він зможе швидко реагувати на них і мінімізувати наслідки». ***(Monique Mulima. Remote Work, Aging Tech Targeted by Canada Cybersecurity Plan // Bloomberg LP (https://www.bloomberg.com/news/articles/2024-05-22/remote-work-aging-tech-targeted-by-canada-cybersecurity-plan). 22.05.2024).***

***

«Споживчі етикетки, покликані допомогти американцям вибрати розумні пристрої, менш вразливі до злому, можуть почати з'являтися на товарах перед сезоном святкових покупок, заявили в середу федеральні чиновники.

Згідно з новою ініціативою США «Знак довіри до кібербезпеки» (Cyber Trust Mark Initiative), виробники можуть наносити цей знак на свою продукцію, якщо вона відповідає федеральним стандартам кібербезпеки. Типи пристроїв, які можуть бути марковані, включають радіоняні, камери домашньої безпеки, фітнес-трекери, холодильники та іншу техніку, підключену до Інтернету.

Білий дім вперше оголосив про мітки «Cyber Trust» минулого року, а Федеральна комісія зі зв’язку завершила деталі в березні, розчистивши шлях для того, щоб мітки почали з’являтися через кілька місяців.

«Сподіваюся, що до святкового сезону ви почнете бачити пристрої з цим знаком довіри», — сказав Ніколас Лейзерсон, помічник національного кібердиректора з кіберполітики та програм. Лейзерсон зробив свої коментарі в середу під час дискусії з кібербезпеки в Інституті Маккрері Обернського університету у Вашингтоні.

Етикетки також включатимуть QR-коди, які споживачі зможуть сканувати для отримання інформації про безпеку своїх пристроїв.

Офіційні особи порівняли етикетки з програмою Energy Star, яка оцінює енергоефективність приладів, і кажуть, що ідея полягає в тому, щоб розширити можливості споживачів, а також заохотити виробників підвищити свою кібербезпеку.

Amazon, Best Buy, Google, LG Electronics USA, Logitech і Samsung є серед учасників галузі.

Поширення так званих розумних пристроїв збіглося зі зростанням кіберзлочинності, коли один незахищений пристрій часто може дати кіберзловмисникам небезпечну точку опори в домашній мережі». ***(Cybersecurity labeling for smart devices aims to help people choose items less likely to be hacked // National Post (https://nationalpost.com/pmn/news-pmn/cybersecurity-labeling-for-smart-devices-aims-to-help-people-choose-items-less-likely-to-be-hacked). 22.05.2024).***

***

Країни ЄС та Великобританія

«Запропонований проект Кодексу практики кіберуправління (проект кодексу) є частиною плану уряду щодо підвищення кіберстійкості, як зазначено в Національній кіберстратегії на 2022 рік, у якій зазначено, що 2,6 мільярда фунтів стерлінгів буде інвестовано в кібернетичні та застарілі IT. Стратегія встановлює підхід уряду для забезпечення того, щоб «Велика Британія залишалася впевненою, спроможною та стійкою в цьому швидкозмінному цифровому світі», а також для захисту та просування інтересів Великобританії в кіберпросторі. Ці зміни пов’язані з визнанням урядом того факту, що, хоча Велика Британія має скористатися можливостями, які надає зростаючий кібер- і технологічний ландшафт (оскільки це є фундаментальним для ведення бізнесу), ризиками, пов’язаними з їх впровадженням і використанням, потрібно керувати пропорційно.

Проект кодексу, який спільно розробили Департамент науки, інновацій і технологій, лідери галузі та Національний центр кібербезпеки (NCSC),

спрямований на реагування на зростаючі ризики кібербезпеки, наприклад, збільшення можливостей «для зловмисників використовувати вразливості в IT-системах і порушувати безперервність бізнесу. Як зазначає уряд, цифри показують, що «майже кожна третя (32%) фірма зазнала кіберзлому або атаки протягом минулого року, причому зросла кількість згубних атак програм-вимагачів і зловмисники, які створюють значні загрози, коли вони намагаються впоратися перевага вразливостей кібербезпеки».

Оскільки ці ризики продовжують матеріалізуватися, уряд вважає, що ризики кібербезпеки повинні мати таку ж «видимість, як фінансові чи юридичні ризики», і що процеси управління кіберризиками повинні бути інтегровані «з існуючою практикою стійкості бізнесу та управління ризиками».

Тому ради та директори організацій будь-якого розміру вимагатимуть «охоплення, взаємодії та розуміння кібербезпеки у своїх організаціях». «Нехтування кібербезпекою та відсутність розуміння кібернетики в ширшому контексті безперервності бізнесу наразі передає ідею про те, що «багато вищих керівників не вживають відповідальних дій для пом'якшення загроз бізнес-операціям».

Однак, проводячи консультації щодо цього проекту кодексу, уряд сподівається забезпечити краще управління, яке має ключове значення для покращення кіберстійкості, використовуючи підхід зверху вниз, за якого вищі керівники організацій можуть взяти на себе відповідальність за питання кібербезпеки.

Сфера застосування та цілі проекту Кодексу

Представленням проекту кодексу уряд сподівається формалізувати очікування директорів щодо управління кіберризиками. Це відповідає результатам Огляду стимулів і регулювання кібербезпеки 2020 року, який показав, що організації знайшли кібернетичний ландшафт складним і складним для навігації, при цьому 83% респондентів вимагали «додаткових рішень, щоб проілюструвати, «як виглядає добре.»

Щоб досягти цього, проект кодексу окреслює сферу застосування рекомендацій через запропоновані «дії» відповідно до п’яти ключових принципів:

Управління ризиками: Пропозиція окреслює п’ять дій щодо управління ризиками, які спрямовані на забезпечення того, щоб ризики кібербезпеки належним чином враховувалися як частина ширшої діяльності організації з управління ризиками підприємства та внутрішнього контролю».

Кіберстратегія: Проект кодексу спрямований на те, щоб підприємства регулярно відстежували та переглядали стратегії кіберстійкості. Крім того, ці дії будуть спрямовані на те, щоб «відповідні ресурси та інвестиції розподілялися та ефективно використовувалися для розвитку можливостей, які керують загрозами кібербезпеці та пов’язаними з ними бізнес-ризиками».

Люди: як частина забезпечення кібервідмовостійкості, проект Кодексу окреслює дії щодо заохочення позитивної культури кібербезпеки в організаціях, як-от забезпечення наявності чіткої політики кібербезпеки, підвищення кіберграмотності шляхом проведення навчання та встановлення показників для виміряти ефективність цих програм.

Планування і реагування на інциденти. Основна мета проекту Кодексу полягає в тому, щоб організації мали докладні плани реагування на потенційні кіберінциденти та відновлення після них. Щоб вирішити цю проблему, проект кодексу вимагає регулярного (принаймні щорічного) тестування планів, щоб переконатися, що вони є надійними, з формальною системою звітності про інциденти та процесом перегляду після інцидентів для врахування отриманих уроків. Ці дії також заохочують озброїти працівників відповідними навичками та обізнаністю з кіберпроблемами, щоб вони могли впевнено працювати з новими технологіями.

Гарантія та нагляд: Останні дії, описані в проекті кодексу, встановлюють заходи для посилення кіберстійкості через управління та визначення ролей і обов’язків. Управління кіберризиками, як зазначено в проекті Кодексу, буде ключовим фактором для того, щоб організації могли використовувати «в повній

мірі переваги цифрових технологій, які стимулюють інновації та стимулюють їх конкурентоспроможність».

Значення відповідності

Хоча проект кодексу буде запущено як добровільний інструмент без законодавчої основи, уряд тісно співпрацюватиме з регуляторними органами, такими як Офіс комісара з питань інформації (ICO), щоб зрозуміти, як проект кодексу можна використовувати для забезпечення дотримання іншого законодавства, наприклад Загальний регламент захисту даних (GDPR) і Регламент мереж і інформаційних систем (NIS). Враховуючи «матеріальний ризик», який становить кібербезпека для бізнесу, сприйняття проекту кодексу буде заохочуватись, щоб переконатися, що організації випереджають ці проблеми та забезпечити цілісність економіки Великобританії.

Хоча залишається незрозумілим, чи намагатиметься уряд запровадити схему гарантій у зв'язку із запропонованим режимом, він визнає, що це може сприяти реалізації та відповідності. Як зазначалося в нашій попередній статті, у першій схемі сертифікації для постачальників юридичних послуг, яка буде затверджена ICO, можуть бути значні переваги гарантії:

Подібно до схеми сертифікації, дотримання Проекту кодексу та гарантування проти нього можуть зменшити ризик кіберінцидентів шляхом розробки та моніторингу надійної стратегії кібербезпеки.

Крім того, впевненість дозволить численним зацікавленим сторонам, таким як акціонери, клієнти, страховики та ділові партнери, «заробити довіру до організації, яка має зовнішню гарантію свого управління кіберризиками». Таким чином, гарантія забезпечить прямий спосіб продемонструвати ключовим сторонам, що кіберстійкість інтегрована в плани управління бізнесом.

Як ще одне важливе міркування, ICO може розглядати сертифікацію як пом'якшувальний фактор під час розгляду примусових дій у разі даних/кіберінциденту. Як зазначено в нещодавніх Посібниках ICO щодо штрафів із захисту даних, опублікованих 18 березня 2024 року, «Уповноважений враховуватиме дотримання затверджених кодексів поведінки відповідно до статті

40 GDPR UK або затверджених механізмів сертифікації відповідно до статті 42 GDPR UK. Отже, запевнення щодо проекту кодексу та вжиття всіх необхідних заходів щодо даних та інфраструктури кібербезпеки може зменшити схильність до примусових дій у разі порушення.

Порушення даних також мають законодавчі вимоги щодо сповіщення відповідно до розділу 67 Закону про захист даних 2018 року та статті 33 GDPR Великобританії. Таким чином, наявність ретельного планування реагування на інциденти, включаючи звітність, як того вимагає проект Кодексу, сприятиме спроможності організацій дотримуватися нормативних вимог.

Наступні кроки

19 березня 2024 року завершилися консультації та запит на отримання доказів, тому ще належить побачити, як розвиватиметься розвиток і дизайн проекту кодексу відповідно до будь-яких отриманих відгуків. Поточні ознаки того, що уряд дасть відповідь цього літа». ***(Rosehana Amin and Georgia Schulberg. UK Cyber Governance Code of Practice: what it could mean for you // Clyde & Co LLP (https://www.clydeco.com/en/insights/2024/04/uk-cyber-governance-code-of-practice-what-it-could). 08.05.2024).***

***

«Директива NIS2 була прийнята Європейським парламентом у грудні 2022 року, і очікується, що шведський закон, який імплементує цю директиву, набуде чинності 1 січня 2025 року. Директива NIS2 є загальною структурою, і було важко передбачити більш детальне застосування - дотепер. Законопроект нового Закону про кібербезпеку був представлений у березні цього року. Нижче наведено огляд нового запиту NIS2, його зміст і те, як ви можете підготувати свій бізнес до нового регулювання. Якщо вам потрібна додаткова інформація чи допомога, не соромтеся звертатися до нас. Ліндаль має значний досвід у таких галузях права, як дотримання нормативних вимог, інформаційна безпека, IT/технології та захист даних.

Директива NIS2 має суворіші вимоги до операторів і містить положення щодо більш далекосяжної співпраці в межах ЄС порівняно з її попередницею, NIS1. Загальна мета нових правил — досягти вищого рівня кібербезпеки для розширеної кількості секторів, визначених законодавством.

5 березня 2024 року «Запит про імплементацію директив NIS2 і CER» подав проміжний звіт «Нові правила кібербезпеки» (SOU 2024:18) разом із пропозицією щодо нового Закону про кібербезпеку.

З 1 січня 2025 року пропонується набути чинності Закон про кібербезпеку, який замінить чинний закон про NIS, і передбачає низку важливих змін у сфері інформаційної безпеки та кібербезпеки.

По суті, між чинним законодавством і новою пропозицією є дві важливі відмінності:

Розширене застосування та розширена кількість секторів: пропонується, щоб Закон про кібербезпеку поширювався на більше учасників, а кількість секторів було збільшено з 7 до 18. Прикладами нових секторів, які тепер будуть включені, є: стічні води, адміністрування послуг ІКТ (між підприємствами), державне управління (це означає, що охоплено майже весь державний сектор, включаючи муніципалітети та регіони), космос, поштові та кур'єрські послуги, управління відходами, виробництво, виробництво та розподіл хімічних речовин і харчових продуктів, виробництво, цифрові постачальники та дослідження.

Включається вся операція: пропозиція означає, що вимоги стосуватимуться всієї операції, а не лише тих частин, які вважаються критично важливими для суспільства, або які пропонують цифрові послуги. Він також запроваджує вимоги щодо розміру приватних організацій, згідно з якими підприємство повинно мати щонайменше 50 працівників або мати річний обіг понад 10 мільйонів євро, щоб відповідати вимогам Закону. Однак менші, але особливо важливі операції також можуть бути визначені Агентством з питань цивільного захисту (MSB), яке також має відповідати вимогам Закону.

Окрім двох вищезазначених нових елементів, ми хотіли б коротко висвітлити ряд інших частин нової пропозиції.

Нова класифікація: пропонується, щоб як державні, так і приватні оператори підпадали під дію нового Закону про кібербезпеку. Однак включені операції повинні бути класифіковані як важливі або важливі на основі значущості та розміру. В принципі, правила однакові незалежно від категорії, однак, залежно від класифікації, вони відрізняються щодо нагляду та санкцій.

Відповідальність вищого керівництва за порушення оператора: Директива посилює вимоги до участі керівництва в роботі організації з кібербезпеки. У запиті пропонується запровадити можливість звернення контролюючого органу до суду щодо заборони керівній особі основного оператора виконувати функції управління. Це стосується, наприклад, членів правління та головних виконавчих директорів. Інші санкції спрямовані на оператора у формі юридичної особи. Натомість ця санкція спрямована на фізичних осіб і повинна розглядатися як крайній засіб для досягнення певної дії.

Чіткі вимоги до заходів безпеки: оператори повинні запровадити відповідні заходи з управління ризиками та проводити оцінку ризиків, щоб захистити свої мережі та інформаційні системи від інцидентів. Заходи повинні бути оцінені та базуватися на оцінці ризику, а також бути пропорційними по відношенню до ризику. Крім того, це вимагає, щоб оператори зареєструвалися в наглядовому органі. Для забезпечення однакового застосування та моніторингу цих вимог пропонуються органи нагляду для кожного сектору, причому певні органи мають розширені сфери відповідальності та нові органи нагляду, створені для управління розширеними вимогами. Вимоги, ймовірно, не будуть визначені в повному обсязі, поки ці наглядові органи не видадуть детальні положення, як це було, коли директива NIS1 була імплементована в шведське законодавство.

Крім того, оператор зобов’язаний проводити систематичну, засновану на оцінці ризиків роботу щодо інформаційної безпеки, при цьому керівництво підприємства має пройти навчальні курси, а працівникам також пропонується необхідне навчання.

Вимоги до безпеки в ланцюгах постачальників: Вимога операцій щодо введення заходів також включає ланцюг постачання. Проте кожен оператор несе

відповідальність лише за одну ланку в ланцюзі постачання, тобто потребує впровадження заходів з управління ризиками по відношенню до своїх постачальників, а не до субпостачальників. Будуть введені вимоги щодо регулювання кібербезпеки в угодах з постачальниками, що означатиме, що існуючі та нові угоди необхідно буде переглянути, щоб адаптувати їх відповідно до цих вимог.

Розширені вимоги до звітування про інциденти: звітування про інциденти буде обов'язковим, і це також стосується ланцюжка поставок. Відповідно, оператор зобов'язаний повідомляти MSB про значні інциденти протягом певних встановлених часових рамок. Попередження має бути подано протягом 24 годин після того, як оператору стало відомо про значний інцидент. Згодом звіт про інцидент подається протягом 72 годин, а остаточний звіт – протягом одного місяця.

Запровадження санкцій: Директива NIS2 містить детальні правила щодо втручання наглядових органів та їх можливості накладати штрафні санкції.

Найнижчий рівень штрафу пропонується становити 5000 шведських крон (як і раніше). З точки зору максимального рівня штрафів, директива NIS2 встановлює дві різні підстави для розрахунку та суми залежно від того, чи є оператор важливим чи важливим.

Для основних операторів максимальні штрафні санкції становлять 10 000 000 євро або 2 відсотки загального річного обороту за попередній фінансовий рік. Для важливих операторів відповідні суми мають становити не більше 7 000 000 євро або 1,4 відсотка від загального глобального річного обороту протягом попереднього фінансового року.

Паралельно з директивою NIS2, директива CER, яка стосується посилення стійкості критичних операцій, буде включена в Швецію. Розслідування подасть пропозиції щодо такого включення в остаточний звіт у вересні 2024 року. Директива CER містить деякі вимоги, подібні до директиви NIS2, однак вона стосується не лише кібербезпеки, а й інших загроз, таких як стихійні лиха, тероризм тощо.

Відповідно до директиви CER, держави-члени повинні визначити суб'єктів, які надають критично важливі державні послуги у вибраних секторах (енергетика, транспорт, банківська справа, інфраструктура фінансового ринку, охорона здоров'я та медичне обслуговування, питна вода, стічні води, цифрова інфраструктура, державне управління, космос, а також виробництво, переробка та розподіл харчових продуктів). Крім того, директива містить зобов'язання для таких учасників вживати заходів для посилення своєї стійкості та повідомляти про інциденти. Директива також містить положення щодо нагляду та санкцій. Іншими словами, директива CER містить подібні вимоги до директиви NIS2, але застосування скоординовано, і якщо є збіги, директива NIS2 має застосовуватися до тих пір, поки директива CER не встановлює більш далекосяжні вимоги.

Нарешті, можна також згадати, що багато організацій підпадають як під дію Закону про захист безпеки (2018:585), так і Закону про кібербезпеку. У цьому випадку відправною точкою є те, що лише обмежена кількість положень Закону про кібербезпеку застосовується до частин операції, на які поширюється Закон про захист безпеки, тобто тих, що стосуються зобов'язань щодо сповіщення та звітності.

Ми рекомендуємо всім організаціям негайно розпочати роботу над дотриманням директиви NIS2 та нового Закону про кібербезпеку. Ті організації, які не впевнені, чи на їхню діяльність поширюється дія Закону, повинні провести аналіз, у тому числі оцінити, на які частини діяльності (якщо такі є) впливає Закон про захисну безпеку. Ті організації, які вже провели цей аналіз, повинні розпочати оцінку ризиків, щоб визначити, які IT-послуги є критичними для роботи.

Насамкінець слід зазначити, що наведене вище є лише загальним підсумком певних питань, пов'язаних із директивою NIS2 та пропозицією щодо нового Закону про кібербезпеку. Отже, ця стаття не є юридичною консультацією в окремому випадку». ***(Isabelle Selemba, Hanna Lundqvist and Pontus Etéus. Proposal for new Cybersecurity Act - implementation of the NIS2 directive in Swedish law // Advokatfirman Lindahl (https://www.lindahl.se/en/latest-***

news/knowledge/2024/proposal-for-new-cybersecurity-act-implementation-of-the-nis2-directive-in-swedish-law/). 05.2024).

***

«Як ідеться в розслідуванні видання Die Zeit, дані про тисячі конференцій та нарад Бундесверу фактично були доступні для всіх охочих. Журналістам вдалося виявити дані про 6000 конференцій, проте насправді ця цифра може бути значно більшою.

Причиною витоку стали безпекові проблеми відеоплатформи Webex, що належить американській компанії Cisco. Цікаво, що Федеральне управління з інформаційної безпеки схвалило для використання Webex лише у 2019 році, до того ж платформа дійсно вважається достатньо безпечною.

Згідно з матеріалом Die Zeit, у мережі можна було доволі просто знайти дані про розклад конференцій, їхню тривалість, теми нарад та навіть ім'я організатора. Втім, варто розуміти, що запис самих розмов не був доступний. Водночас такий витік усе одно можна вважати надзвичайно серйозним, оскільки частина зустрічей була секретною.

Журналістам Die Zeit вдалося додатися до особистих кабінетів для відеоконференцій співробітників Бундесверу. Зокрема голови ВПС Німеччини генерал-лейтенанта Інґо Ґергарца. За даними видання, ці кабінети навіть не були захищені паролями.

Бундесвер поки що офіційно не коментував витік даних. Проте після отримання журналістського запиту від користування Webex тимчасово відмовилися». ***(Олена Дячук. У Бундесвері стався витік даних про таємні відеонаради — ЗМІ // RFR (https://www.rfi.fr/uk/%D1%94%D0%B2%D1%80%D0%BE%D0%BF%D0%B0/20240505-%D1%83-%D0%B1%D1%83%D0%BD%D0%B4%D0%B5%D1%81%D0%B2%D0%B5%D1%80%D1%96-%D1%81%D1%82%D0%B0%D0%B2%D1%81%D1%8F-%D0%B2%D0%B8%D1%82%D1%96%D0%BA-***

%D0%B4%D0%B0%D0%BD%D0%B8%D1%85-%D0%BF%D1%80%D0%BE-%D1%82%D0%B0%D1%94%D0%BC%D0%BD%D1%96-%D0%B2%D1%96%D0%B4%D0%B5%D0%BE%D0%BD%D0%B0%D1%80%D0%B0%D0%B4%D0%B8-%D0%B7%D0%BC%D1%96). 05.05.2024).

***

«У середу, 16 травня, уряд опублікував Галузевий аналіз кібербезпеки за 2024 рік, в якому міститься інформація про розмір і масштаб галузі кібербезпеки Великобританії. Аналіз базується на звіті за 2023 рік, який був опублікований у квітні минулого року.

Департамент науки, інновацій і технологій (DSIT) доручив Ipsos і Perspectives Economics за підтримки glass.ai і Центру безпечних інформаційних технологій (CSIT) при Королівському університеті Белфаста провести перевірку.

У цьому звіті застосовано методологічний підхід для аналізу ефективності сектору з використанням різних джерел даних, у тому числі Cyber Exchange – спільного підприємства DSIT і techUK, яке дозволяє постачальникам кібербезпеки демонструвати на ринку продукти та послуги, які вони надають.

Висновки показують, що у Великобританії існує 2091 активна практика кібербезпеки. Переважна більшість із них є малими (24% або мікро-підприємствами (55%), що відображає ширший склад підприємств Великобританії. Більше половини цих компаній (56%) є постачальниками послуг, 27% зосереджені на продуктах і 16% є постачальниками керованих послуг (MSP), лише 1% яких зосереджено на перепродажу.

З точки зору економічного внеску, річний дохід сектору кібербезпеки Великобританії оцінюється в 11 859 мільйонів фунтів стерлінгів, що відображає збільшення на 13% порівняно з минулорічним дослідженням. З цієї суми 75% припадає на великі компанії, які становлять лише 8% загального ринку. Навпаки, невеликі фірми спостерігали зниження доходу з £893 млн до £862 млн.

У звіті визнаються рекордні рівні інвестицій у кіберкомпанії з 2019 по 2021 рік. Однак ці рівні під впливом ширших макроекономічних умов у 2023 році

знизилися, і організації в усіх секторах зіткнулися з проблемами залучення інвестицій. У сфері кібербезпеки спостерігалося зниження на 10% порівняно з показниками 2022 року. Ці інвестиції також були значною мірою зосереджені в Лондоні, з часткою 54%, тоді як інші регіони, такі як Південний Схід, Північний Захід, Східна Англія, Йоркшир і Хамбер і Північна Ірландія, мали більш рівномірний розподіл інвестицій.

У заключному розділі звіту розглядаються останні державні інвестиції та ініціативи підтримки в кіберсекторі. У ньому висвітлюється робота таких програм, як Cyber Exchange, UK Cyber Cluster Collaboration (UKC3), NCSC for Start-ups і Cyber Runway, які підтримують стартапи у зборі коштів і підвищенні їхнього профілю в секторі.

У цьому розділі також розглядаються бар'єри, з якими стикаються компанії з кібербезпеки при пошуку талантів. Три найпоширеніші перешкоди:

- Конкурс для кандидатів у кіберсекторі
- Вимоги до зарплати не по кишені
- Кандидати, які не мають технічних навичок

Хоча у звіті зроблено кілька подібних висновків до попередніх ітерацій, він показує, що продовжує існувати значна кількість проблем, які впливають на кіберкомпанії, від великих транснаціональних до малих і середніх підприємств і стартапів». ***(Cyber Security Sectoral Analysis 2024 // techUK (https://www.techuk.org/resource/cyber-security-sectoral-analysis-2024.html). 20.05.2024).***

***

«Офіс уповноваженого з питань інформації Великобританії («ICO») випустив заяву, в якій закликав організації докласти більше зусиль для боротьби зі зростаючою загрозою кібератак. Це сталося після того, як ICO відреагувала на повідомлення про кіберзлам у Міністерстві оборони, а його власне дослідження показало, що більше організацій, ніж будь-коли, стикаються з порушеннями кібербезпеки.

Заява супроводжувалася новим звітом «Вчимося на помилках інших», який містить практичні поради організаціям, щоб «розуміти загальні збої в безпеці та вжити простих кроків для покращення власної безпеки, запобігаючи майбутнім витокам даних, перш ніж це станеться».

Звіт зосереджений на п'яти основних причинах порушень безпеки: (1) фішинг; (2) атаки грубою силою; (3) відмова в обслуговуванні; (4) помилки; та (5) атаки на ланцюги поставок. У звіті, що супроводжується корисними тематичними дослідженнями, підсумовано, що це за атаки, як вони відбуваються, основні принципи, які слід враховувати, щоб пом'якшити або зменшити рівень шкоди від порушення безпеки, а також деякі можливі події, які означають, що ці загрози стають більш складними в майбутнє (наприклад, через використання штучного інтелекту або квантових обчислень). Він також містить деякі вказівки щодо програм-вимагачів і зловмисного програмного забезпечення, хоча ICO містить вказівки на цю тему в інших місцях.

У звіті чітко зазначено, що багатьох витоків даних, пов'язаних з кібернетичною мережею, «цілком можна уникнути», якщо організації впровадять типи фізичних і технічних заходів, згаданих у звіті, і приймуть підхід «конфіденційності та безпеки за проектом і за замовчуванням». Не менш важливим є наявність в організаціях відповідних «організаційних засобів контролю», таких як забезпечення того, щоб ради «використовували більш проактивний підхід до нагляду за кіберризиками в своїх організаціях». Крім того, підкреслюється, що організації не повинні порівнювати себе з іншими організаціями, навіть якщо вони працюють на подібному ринку: «найкращою базою для вимірювання вашої ефективності є ваша власна». Він також нагадує організаціям, що ICO може вжити примусових заходів, якщо заходи є неадекватними, і наводить приклади таких заходів проти організацій, які, наприклад, не змогли захистити зовнішні з'єднання за допомогою багатофакторної автентифікації, використовували неадекватні паролі для внутрішніх облікових записів, або не вдалося пом'якшити відомі вразливості.

Коментуючи публікацію заяви та звіту, заступник комісара ICO (регуляторний нагляд) Стівен Боннер сказав:

«Люди повинні бути впевнені, що організації роблять усе можливе, щоб захистити їх особисту інформацію. Хоча кібератаки стають все більш витонченими, ми бачимо, що багато організацій не реагують належним чином і все ще нехтують самими основами кібербезпеки.

Як регулюючий орган із захисту даних ми хочемо підтримувати та надавати організаціям можливості для досягнення цього права. Хоча немає єдиного рішення для запобігання кібератакам, немає жодного виправдання відсутності базових засобів контролю. Це важливо для захисту особистої інформації людей, і ми вживемо заходів, зокрема штрафів, проти організацій, які все ще не вживають простих кроків для захисту своїх систем.

Якщо ви зазнаєте кібератаки, ми завжди заохочуємо до прозорості, оскільки ваші помилки можуть допомогти іншій організації уникнути подібного порушення». ***(Patrick Rennie. Cyber Security: Information Commissioner issues statement calling for organisation to do more // Wiggin LLP (/insight/cyber-security-information-commissioner-issues-statement-calling-for-organisation-to-do-more/). 20.05.2024).***

***

«Якщо ваш бізнес виробляє, імпортує або розповсюджує споживчі «розумні» продукти у Великій Британії, режим кібербезпеки вашого продукту має бути переглянуто у світлі нового вдосконаленого законодавства Великої Британії, що набуло чинності з 29 квітня 2024 року. Компанії в ланцюжку постачання Інтернету речей (пристрої IoT) мають відповідати оновленим стандартам безпеки продуктів Великобританії. Розробка продукту, виробництво та процеси документування повинні бути оцінені на відповідність.

Недотримання вимог може призвести до значних штрафів, у тому числі до 10 мільйонів фунтів стерлінгів або 4% світового доходу.

Які нові правила?

Правила 2023 року щодо безпеки продукції та телекомунікаційної інфраструктури (Вимоги безпеки для відповідних підключених продуктів) (PSTI) є

частиною ширшого Закону Великобританії про безпеку продукції та телекомунікаційну інфраструктуру 2022 року. Цей закон встановлює нові вимоги безпеки для виробників, імпортерів і розповсюджувачів Інтернет- підключаються та підключаються до мережі продукти.

Норми, які набувають чинності з 29 квітня 2024 року, спрямовані на посилення кібербезпеки підключених споживачів, тобто «розумних» продуктів.

Законодавство запроваджує зобов’язання уряду Великої Британії покращити стійкість Великої Британії до кібератак і покращити зв’язок для окремих осіб і компаній у всій Великобританії...

Наш «розумний» продукт у масштабі?

Правила спрямовані на споживчі продукти, які можуть підключатися до Інтернету чи інших мереж і передавати або отримувати цифрові дані. Це включає різні інтелектуальні пристрої, наприклад пристрої Інтернету речей.

Однак деякі продукти виключені з правил, наприклад:

- Продукція, призначена для постачання в Північну Ірландію.
- Пункти зарядки електромобілів.
- Медичні прилади.
- Розумні лічильники.
- Комп’ютери без підключення до стільникової мережі, якщо вони не призначені для дітей віком до 14 років.

Які підприємства підпадають під дію?

Посилені зобов'язання застосовуються до всіх ролей у ланцюжку постачання.

Виробники: будь-яка організація, яка розробляє, виробляє або продає підключаються продукти під своїм ім’ям або торговою маркою. Сюди входять компанії, які розробляють або виробляють продукти від свого імені.

Імпортери: будь-яка організація, яка імпортує підключаються продукти до Великобританії з інших країн. Імпортери повинні переконатися, що продукти, які вони постачають на британський ринок, відповідають нормам.

Дистриб’ютори: організації, які випускають підключні продукти для продажу у Великобританії. Дистриб'ютори повинні переконатися, що продукція, яку вони

постачають, відповідає нормативним вимогам і містить необхідну документацію щодо відповідності.

А якщо ми виробляємо за кордоном?

Якщо ви виробляєте продукти, що підключаються, за кордоном і постачаєте їх на ринок Великої Британії, правила все одно застосовуються до ваших продуктів.

Що необхідно зробити?

Виробники повинні відповідати основним вимогам безпеки, вести записи про відповідність, досліджувати та виправляти будь-які порушення відповідності.

Імпортери та дистриб'ютори повинні переконатися, що продукти мають заяву про відповідність і припинити постачання, якщо продукт не відповідає стандартам безпеки.

Що станеться, якщо наші «розумні» продукти не будуть відповідати нормам?

Управління з безпеки продукції та стандартів (OPSS) має повноваження накладати максимальний штраф у розмірі 10 мільйонів фунтів стерлінгів або 4% світового доходу, залежно від того, що більше. Примусові заходи у менш серйозних випадках невідповідності можуть призвести до офіційного повідомлення, яке вимагає привести продукт у відповідність, або до того, щоб учасник ланцюга постачання вжив заходів для виконання своїх зобов'язань. Можливо, вимагатиметься зняття продукту з ринку.

Деякі порушення Закону про PTSI (зокрема невиконання попередження) є кримінальними злочинами. Окрім корпоративної відповідальності, потенційно можуть бути визнані відповідальними відповідальні посадові особи корпорації.

Ті, хто експортує пристрої IoT, також повинні стежити за Законом ЄС про кібернетостійкість, який ще не набрав чинності, але наближається до остаточного прийняття. Він представляє подібні зусилля для підвищення стійкості кібербезпеки пристроїв IoT, доступних на ринку ЄС». ***(Amber Strickland, Patrick Arben, Louise Macdonald. Are you meeting new, enhanced UK cyber security requirements for consumer "smart" products? // Gowling WLG (https://gowlingwlg.com/en/insights-***

resources/articles/2024/new-cyber-security-requirements-for-smart-products/). 23.05.2024).

***

«Європейська рада з виробництва сонячних батарей (ESMC) закликала докладати більше зусиль для посилення кібербезпеки інверторів і даних.

Виробнича асоціація опублікувала рекомендаційний документ щодо імплементації Закону Європейського Союзу про нульову чисту промисловість (Net Zero Industries Act, NZIA). «Ми передбачаємо, що необхідно ще більше працювати над питанням кібербезпеки та безпеки даних», підкреслюючи важливість інвертори в управлінні всією фотоелектричною системою.

Оскільки приблизно 80% інверторів, встановлених у Європі, надходять із Китаю, ESMC стверджує, що в найгіршому випадку конфлікт із Китаєм може призвести до нападу на інвертори та спричинити відключення електроенергії. Щоб зменшити цю ймовірність, він пропонує закуповувати інвертори європейських компаній, а не китайських.

Так само ESMC пропонує, щоб зменшити залежність Європи від третьої країни для більш ніж половини певної технології, вона також повинна включати потужності, вироблені за її межами. Компанії, потужності яких виробляються за межами національних кордонів, але все ще контролюються цією компанією, повинні враховуватися в загальній кількості країни походження.

Хоча це прямо не згадується у звіті, це може вплинути на китайські компанії, які побудували виробничі підприємства в Південно-Східній Азії.

Ще одна рекомендація зі звіту стосується важливості відстеження та доступу до надійних і перевірених даних, щоб уникнути будь-якого зеленого та білого кольору продуктів.

Впровадження NZIA на початку 2025 року

Поточний термін, протягом якого кожна держава-член адаптує свої схеми підтримки відповідно до NZIA, встановлює це не пізніше жовтня 2025 року. ESMC закликає прийняти впровадження NZIA набагато раніше, ніж це дозволено,

заявляючи вже у 2025 році для найамбітніших держав-членів. Це дозволяє збільшити можливості для бізнесу та покращити передбачуваність.

ESMC додає, що відповідно до угоди в Європейській сонячній хартії регулярні діалоги між політиками, виробниками та державами-членами гарантуватимуть, що регулювання та інвестиції йдуть рука об руку. «Критерії прийнятності/попередньої кваліфікації та винагороди або бонусів, представлені в цьому документі, повинні бути впроваджені державою-членом після обговорення з національними виробниками ЄС, щоб відповідати виробничим потужностям».

«З адекватними критеріями стійкості, стійкості та прав працівників аукціони мають потенціал для того, щоб стати ключовим інструментом для відновлення сонячного виробництва в Європі», — сказав Вінсент Делпорт, керівник відділу зв'язків із громадськістю Holosolis і відповідальний за критерії NZIA в ESMC. робоча група з питань стійкості.

Це важливий аспект, який слід враховувати, враховуючи, що за оцінками Міжнародного енергетичного агентства, публічні аукціони забезпечуватимуть 70% зростання відновлюваної потужності Європи в період між 2023 і 2028 роками. У звіті підкреслюється, що: «Використання аукціонів сонячної фотоелектричної продукції з критеріями, які явно приносять користь. Європейська сонячна фотоелектрична система матиме важливе значення для відновлення цієї екосистеми».

Критерії мають бути незалежними від технології

Крім того, ESMC рекомендує, щоб технологічні критерії були агностичними і не зосереджувалися виключно на сонячних модулях на основі кремнію, а також включали інші маршрути, такі як тонкоплівкова фотоелектрична мережа.

Щодо критеріїв, пов'язаних із країною походження, ESMC закликає Європейську комісію надати «чітке визначення країни походження, щоб уникнути обходу».

За словами ESMC, через ризики кібербезпеки та безпеки даних слід віддавати перевагу закупівлі інверторів європейського виробництва перед інверторами китайського виробництва.

У ньому також пропонується включити вуглецевий слід як критерій нагороди або прийнятності, поряд з іншими критеріями, щоб допомогти досягти 40% цілі внутрішнього вироблення PV потужності до 2030 року. Пропонується включення обов'язкових інформаційних точок для розміщення магнію кремнію (Mg-Si) і виробництво полікремнію». ***(Jonathan Touriño Jacobo. 'More work needed on cyber- and data security,' says ESMC // Solar Media Limited (https://www.pv-tech.org/more-work-needed-on-cyber-and-data-security-says-esmc/). 22.05.2024).***

***

Китай та країни східної Азії

«Змінений Закон Китаю про охорону державної таємниці («SSL») набув чинності 1 травня 2024 року. Ця поправка є частиною ширшого законодавчого поштовху для посилення національної безпеки та захисту даних, узгоджуючи його з іншими останніми законами, такими як Закон про безпеку даних («DSL»), Закон про контршпигунство та змінений Закон про національну безпеку.

Поправки до SSL в першу чергу стосуються державних установ КНР, а також підприємств, які мають доступ до державної таємниці (разом «Регульовані організації»). Однак транснаціональні компанії («МНК»), які можуть зіткнутися з державною таємницею чи іншою конфіденційною інформацією під час взаємодії з регульованими організаціями, також повинні подумати про вимоги SSL, DSL та іншого законодавства під час обробки даних у Китаї, як у рутинних операцій і під час проведення належної обачності та внутрішніх розслідувань.

Це сповіщення клієнта містить огляд ключових змін, внесених зміненим SSL, і окреслює найкращі практики для MNC, що працюють у Китаї.

Ключові оновлення

Розширення захищеної інформації. Сфера застосування SSL тепер охоплює не лише державну таємницю, але й «робочу таємницю», категорію, яка охоплює ширший спектр конфіденційної інформації, створеної регульованими організаціями, де її розголошення може мати негативні наслідки. Інші існуючі правила вже захищають робочі секрети, тому ця концепція не є новою, але

включення робочих секретів у сферу дії SSL додатково кодифікує та посилює їх захист.

Класифікація та розсекречення. Змінений SSL містить більш чіткі вказівки та процедури для класифікації та розсекречення державної таємниці, а також маркування документів для підкреслення конфіденційності інформації.

Цифрова інформація та кібербезпека. Поправки модернізують SSL, включивши електронні файли до видів носіїв, які можуть містити державну таємницю. Вони також накладають спеціальні обов'язки на інтернет-компанії керувати інформацією, створеною користувачами, і видаляти інформацію у випадках підозрілих порушень.

Інституційні зміни. Від регульованих організацій тепер вимагається створювати спеціальні органи або призначати спеціального персоналу, відповідального за роботу в режимі секретності. SSL також тепер вимагає від місцевих органів влади та регульованих установ виділяти кошти на захист державної таємниці у своїх бюджетах.

Децентралізація повноважень щодо визначення державної таємниці. Центральні органи влади можуть делегувати органам нижчого рівня повноваження визначати, що є державною таємницею за обмежених обставин, наприклад, коли цього вимагає терміновість ситуації.

Контроль експорту. Поправка передбачає новий механізм нагляду за вивезенням державної таємниці за кордон. Згодом можна очікувати імплементаційні нормативні акти, потенційно затвердивши структуру, яка вже регулює експорт даних, що регулюється DSL.

Регулювання агрегації даних. Нове положення вимагає від регульованих установ вживати заходів безпеки під час обробки даних, які можуть становити державну таємницю, якщо вони зведені або пов'язані з іншими даними.

Найкращі практики комплаєнсу для ТНК

Для ТНК, які працюють у Китаї, поправка до SSL ще більше підкреслює зростаючу потребу мати надійну політику та методи обробки даних для пом'якшення регуляторного ризику. Дані, згенеровані чи отримані під час ділових

операцій або використані в рамках належної перевірки та внутрішніх розслідувань, можуть належати до сфери державної таємниці чи робочої таємниці відповідно до SSL або до так званих «важливих даних» відповідно до DSL. Ризики цього вищі з даними, пов'язаними з державними установами, державними підприємствами та чутливими секторами.

Політику та практику обробки даних ТНК можна адаптувати з урахуванням характеру їхнього бізнесу в Китаї. Ті, хто взаємодіє з регульованими організаціями або з інших причин, мають більшу ймовірність отримати конфіденційну інформацію через свої бізнес-операції; можуть бути прийняті такі стратегії:

Безпека та обробка даних. Впровадити офіційну програму захисту даних як частину повсякденної діяльності MNC, яка може:

Класифікувати дані, отримані від урядових установ, державних підприємств та інших відповідних зовнішніх джерел, на основі рівня чутливості та застосовувати відповідні рівні контролю на основі такої класифікації.

Прагніть, де це можливо, зберігати та обробляти дані, зібрані або створені в Китаї.

Забезпечте регулярне навчання працівників програмі захисту даних, SSL, DSL та іншим відповідним законодавством, щоб підвищити їхню обізнаність щодо відповідності.

Due Diligence або внутрішні розслідування. Розробіть стратегію з адвокатом та іншими консультантами щодо процесів збору та перевірки даних, щоб обмежити доступ до державної таємниці та іншої конфіденційної інформації та уникнути випадкового обміну або експорту інформації.

Забезпечте дотримання нормативних вимог Китаю під час надання інформації іноземним регуляторам.

Наскільки це можливо, локалізуйте належну обачність і внутрішні розслідування діяльності в Китаї.

Уважно оцінюйте зовнішні джерела даних і обмежте залежність від зовнішніх джерел даних, наскільки це можливо.

Застосовуйте надійні протоколи безпеки даних під час збору даних від зовнішніх сторін, звертаючись за допомогою зовнішніх консультантів щодо ідентифікації та редагування конфіденційної інформації, якщо це необхідно». ***(B. Chen Zhu, Paul D. McKenzie, Yuting Xie and Derik Rao. China Strengthens Protection of State Secrets as Revised Law Takes Effect // Morrison & Foerster LLP (https://www.mofo.com/resources/insights/240524-china-strengthens-protection-of-state-secrets?utm_source=publication&utm_medium=email). 24.05.2024).***

***

«Законопроект про кібербезпеку (поправка) був ухвалений парламентом Сінгапуру 7 травня 2024 року. Прийняття такого законопроекту є життєво важливим для ландшафту кібербезпеки Сінгапуру та його подальшого розвитку як цифрово розвиненої нації. У цій короткій статті ми коротко виклали основні пункти законопроекту про кібербезпеку (з поправками).

1. Кого стосується Закон про кібербезпеку?

Наразі Закон про кібербезпеку поширюється на критичну інформаційну інфраструктуру («CII»), яка повністю або частково розташована в Сінгапурі.

У майбутньому, коли поправки до законопроекту про кібербезпеку (з поправками) набудуть чинності, Закон про кібербезпеку застосовуватиметься до ICI, власників систем тимчасової кібербезпеки («STCC»), організацій, що становлять особливий інтерес у кібербезпеці («ESCI») та засновників Постачальники послуг цифрової інфраструктури («FDI»).

2. Як зміни впливають на ICI?

CII – це критично важливі комп’ютерні системи, необхідні для безперервного надання основних послуг у Сінгапурі; втрата або компрометація таких комп’ютерних систем матиме виснажливий вплив на доступність відповідних основних послуг у Сінгапурі. Приклади ICI включають основні послуги, такі як комунальні послуги та банківські послуги. Перелік власників ICI публічно не оприлюднюється.

Зміни, що стосуються ІСІ, такі:

a. Захищає як фізичні, так і віртуальні системи CII

Зараз Закон про кібербезпеку захищає лише фізичні системи CII. У майбутньому це поширюватиметься на віртуальні системи CII, які включають системи хмарних обчислень.

b. Посилене регулювання відповідальності постачальників основних послуг, які використовують ІСІ, що належать третім особам

Поправки гарантуватимуть, що постачальники основних послуг відповідатимуть за відповідність ІСІ, що належать третім особам, необхідним стандартам і вимогам кібербезпеки.

в. Поширюється на ІСІ, які повністю розташовані за кордоном

Зараз Закон про кібербезпеку поширюється лише на ІСІ, якщо вони повністю або частково розташовані в Сінгапурі. У майбутньому це також поширюватиметься на ІСІ, розташовані повністю за межами Сінгапуру.

d. Розширення списку інцидентів кібербезпеки, про які потрібно повідомляти

Наразі власник ІСІ зобов'язаний лише повідомляти про інциденти кібербезпеки, пов'язані з ІСІ або комп'ютерами чи комп'ютерними системами, які взаємопов'язані з ІСІ або спілкуються з ним. Поправка вимагатиме від власників ІСІ повідомляти про додаткові інциденти, які впливають на: (i) інші комп'ютери під контролем власника та (ii) комп'ютери під контролем постачальника, які взаємопов'язані з ІСІ або спілкуються з ним.

3. Як поправки впливають на STCC?

STCC – це комп'ютерні системи, які повністю або частково розташовані в Сінгапурі та є критично важливими для Сінгапуру протягом обмеженого періоду, які піддаються високому ризику атак на кібербезпеку, і втрата або компрометація таких систем матиме шкідливий вплив на національну безпеку, оборону, іноземні відносин, економіки, громадського здоров'я, громадської безпеки чи громадського порядку Сінгапуру.

Поправки, що стосуються STCC, є такими:

a. Регулювання НТРК

Поправки дозволять відповідному регулятору (Агентству кібербезпеки Сінгапуру) регулювати STCC та кібербезпеку STCC. Це включає надання Агентству кібербезпеки Сінгапуру повноважень видавати письмові вказівки STCC, а також повноваження надавати та скасовувати призначення STCC.

b. Обов'язок повідомляти про інциденти кібербезпеки

STCC зобов'язані повідомляти про певні встановлені інциденти кібербезпеки в Агентство кібербезпеки Сінгапуру.

в. Вимоги до встановлення механізмів і процесів

Власники STCC зобов'язані встановити механізми та процеси для виявлення загроз та інцидентів кібербезпеці.

4. Як поправки впливають на ESCI?

ESCI — це суб'єкти, які зберігають конфіденційну інформацію в комп'ютерній системі під контролем суб'єкта або суб'єкти, які використовують комп'ютерну систему під їхнім контролем для виконання функцій, які в разі порушення можуть мати значний шкідливий вплив на оборону, зовнішні відносини, економіку, охорону здоров'я, громадської безпеки або громадського порядку Сінгапуру.

Поправки, що стосуються ESCI, є такими:

а. Регулювання ESCI

Поправки дозволять Агентству кібербезпеки Сінгапуру регулювати ESCI. Це включає надання Агентству кібербезпеки Сінгапуру повноважень видавати письмові вказівки ESCI, а також повноваження надавати та скасовувати призначення ESCI.

b. Обов'язок повідомляти про інциденти кібербезпеки

ESCI зобов'язані повідомляти про певні встановлені інциденти кібербезпеки до Агентства кібербезпеки Сінгапуру, якщо інцидент призводить до порушення доступності, конфіденційності чи цілісності даних суб'єкта або має значний вплив на бізнес-операції суб'єкта.

в. Вимоги до встановлення механізмів і процесів

ESCI зобов’язані встановити механізми та процеси для виявлення загроз кібербезпеці та інцидентів щодо системи, що представляє особливий інтерес з точки зору кібербезпеки, як зазначено в будь-якому застосовному кодексі практики.

5. Як поправки впливають на FDI?

FDI – це комп’ютерні системи, необхідні для безперервного надання послуг базової цифрової інфраструктури, що надаються з Сінгапуру або за його межами (повністю або частково) особам у Сінгапурі, і втрата або погіршення надання таких послуг може призвести до або спричинити порушення або погіршення роботи великої кількості підприємств або організацій у Сінгапурі, які покладаються на такі FDI. Прикладами FDI можуть бути постачальники хмарних послуг і оператори центрів обробки даних.

Поправки, що стосуються FDI, є такими:

a. Регулювання FDI

Поправки дозволять Агентству кібербезпеки Сінгапуру регулювати постачальників послуг FDI. Це включає надання Агентству кібербезпеки Сінгапуру повноважень видавати письмові вказівки постачальникам послуг FDI, а також повноваження надавати та скасовувати призначення постачальників послуг FDI.

b. Обов’язок повідомляти про інциденти кібербезпеки

Постачальники послуг FDI зобов’язані повідомляти про певні встановлені інциденти кібербезпеки до Агентства кібербезпеки Сінгапуру, включно з інцидентами, які призводять до зриву або погіршення безперервної доставки FDI в Сінгапурі, для яких постачальник призначений і якщо інцидент має значний вплив на бізнес-операції постачальника послуг FDI в Сінгапурі.

в. Вимоги до встановлення механізмів і процесів

Постачальники послуг FDI зобов’язані встановити механізми та процеси для виявлення загроз кібербезпеці та інцидентів щодо FDI, як зазначено в будь-якому застосовному кодексі практики.

6. Заключні слова

Оскільки цифрові технології є невід'ємною частиною розвитку бізнесу та нашого повсякденного життя, безперечно, загрози кібербезпеці продовжують зростати не лише в Сінгапурі, а й у всьому світі. Оскільки Сінгапур продовжує прогресувати як цифрово безпечна та технологічно підкована нація, законопроект про кібербезпеку (з поправками) дає Сінгапуру значну перевагу, не лише зміцнюючи наш існуючий ландшафт кібербезпеки, але й підвищуючи довіру користувачів до використання онлайн-сервісів у Сінгапурі.

Надалі ICI, STCC, ESCI та FDI повинні переглянути свої процеси та політики, щоб переконатися, що вони юридично відповідають Закону про кібербезпеку, щойно поправки до Закону про кібербезпеку (з поправками) набудуть чинності». ***(Thomas Choo, Zhen Guang Lam, Heather Lim. Singapore's Cybersecurity Landscape: Further Protection Through The Enhancement Of The Cybersecurity Act // Clyde & Co LLP (https://www.clydeco.com/en/insights/2024/05/singapore-s-cybersecurity-landscape-further-protec). 16.05.2024).***

***

«Президентський указ № 47 від 2023 року про національну стратегію кібербезпеки та управління кіберкризами Індонезії («PR 47/2023») був прийнятий 20 липня 2023 року. Ця постанова містить стратегічні вказівки для державних установ та зацікавлених сторін щодо посилення (i) національної кібербезпеки та (ii) управління кіберкризами.

Центральне місце в цих зусиллях займає Національне агентство з питань кібербезпеки та криптографії (Badan Siber dan Sandi Negara або "BSSN"), яке було призначено головним координатором з управління кіберкризами, що включає в себе співпрацю з постачальниками електронних систем («ESP»).

На виконання PR 47/2023 BSSN видала ключові правила щодо (i) створення груп реагування на кіберінциденти (Tim Tanggap Insiden Siber) ("CIRTs") та (ii) рамок для управління кіберкризами. Ці правила такі:

- Регламент BSSN № 1 від 10 січня 2024 року щодо управління кіберінцидентами («Регламент BSSN 1/2024»); та - Регламент BSSN № 2 від 10 січня 2024 року щодо управління кіберкризами («BSSN Reg. 2/2024»).

Правила стосуються, зокрема, постачальників життєво важливої інформаційної інфраструктури («VII-провайдери»), до яких належать державні установи, суб'єкти господарювання та організації, які володіють або керують життєво важливою інформаційною інфраструктурою («VII»). Хоча основним напрямком цих правил є захист VII, деякі вимоги також застосовуються до ESP, які не кваліфікуються як постачальники VII.

Визначення та визначення VII

Указ Президента № 82 від 24 травня 2022 року щодо захисту життєво важливої інформаційної інфраструктури визначає VII як електронні системи, що використовують інформаційні технології та/або оперативні технології незалежно чи взаємозалежно з іншими електронними системами для підтримки стратегічних секторів, які, якщо перерваний, пошкоджений та/або знищений матиме серйозний вплив на суспільні інтереси, державні служби, оборону та безпеку або національну економіку.

VII сектори включають:

- державне управління;
- енергетичні та мінеральні ресурси;
- транспортування;
- фінанси;
- здоров'я;
- інформаційно-комунікаційні технології;
- харчування;
- захист; і
- інші галузі, визначені президентом.

ESP повинні принаймні раз на рік проходити самооцінку та повідомляти про результати відповідним органам влади, щоб визначити, чи відповідають вони кваліфікації провайдера VII. Оцінка включатиме наступне:

- інвестиційна вартість встановленої електронної системи;
- загальний річний операційний бюджет, виділений на управління електронною системою;
- зобов'язання дотримуватися певних правил або стандартів;
- використання спеціальних криптографічних методів захисту інформації в електронній системі;
- кількість користувачів електронної системи;
- персональні дані, якими керує електронна система;
- класифікація/рівень критичності даних в електронній системі щодо загрози спроб атак або порушень інформаційної безпеки;
- рівень критичності обробки в електронних системах щодо загрози спроб атак або порушень інформаційної безпеки;
- географічний вплив відмови електронної системи; і
- потенційні втрати або негативний вплив від випадків порушення інформаційної безпеки в електронній системі.

BSSN Рег. 1/2024: Управління кіберінцидентами

Виданий 10 січня 2024 року Регламент BSSN № 1 від 2024 року визначає CIRT та їхні обов’язки. CIRT організовано на трьох рівнях:

- Національна група реагування на кіберінциденти («Національна CIRT»);
- Секторальна група реагування на кіберінциденти («Секторальна CIRT»);
- Організаційна група реагування на кіберінциденти («Організаційна CIRT»).

Стаття 8 регламенту зобов’язує всі ESP, у тому числі не-VII ESP, створювати CIRT, хоча регламент не визначає покарань за невиконання. Ці команди повинні зареєструватися в Національній CIRT, причому реєстрація в Організаційній CIRT дійсна протягом трьох років.

Ключові моменти цього положення включають наступне:

- Обов'язки CIRT
- BSSN Рег. 1/2024 визначає обов’язки CIRT, які включають:
- Стримування та відновлення після кіберінцидентів;
- Повідомлення про кіберінциденти відповідним сторонам; і

- Поширення інформації для запобігання або пом’якшення майбутніх інцидентів.
- Протоколи звітності для VII ESP і не-VII ESP

BSSN Peг. 1/2024 вимагає, щоб у разі виникнення кіберінциденту організаційна CIRT повідомляла CIRT наступного рівня. Кіберінцидент визначається як одна або серія подій, які порушують або загрожують роботі електронної системи. У разі кіберінциденту обов’язки VII ESP і не-VII ESP є такими:

VII ESP: Звітування вимагається про кіберінциденти, які порушують безперервність роботи електронних систем і послуг. Організаційна CIRT має повідомити про кожний кіберінцидент до секторальної CIRT, а копію – до Національної CIRT. Про кіберінциденти, пов’язані з VII, необхідно повідомити протягом 24 годин до секторального CIRT і надіслати копію до національного CIRT. Якщо галузевий CIRT ще не створено, звіт слід направити до відповідного міністерства чи відомства для цього сектора, а копію надіслати до національного CIRT.

Не-VII ESP: Звітування вимагається для кіберінцидентів, які впливають на безперервність власних електронних системних послуг не-VII ESP, хоча в регламенті не вказано кінцевий термін для таких звітів. Реагуванням на кіберінциденти з боку ESP, що не належать до VII, може керувати секторальна або національна CIRT. Секторальний CIRT розглядає інциденти, що впливають на безперервність обслуговування принаймні двох організацій до половини організацій у секторі.

Національна CIRT керує інцидентами, що впливають на:

- щонайменше два сектори, з мінімум двома постраждалими організаціями в кожному секторі; або
- більше половини організацій в одному секторі.
- Кожне повідомлення про кіберінцидент має містити як мінімум:
- контактна інформація особи, яка звітує;
- опис події;

- хронологія подій; і
- вплив інциденту.

BSSN Рег. 2/2024: Управління кіберкризою

Видано 10 січня 2024 р., BSSN Reg. 2/2024 охоплює (i) підготовку управління кіберкризою та (ii) впровадження управління кіберкризою.

Підготовка до управління кіберкризою

Цей етап передбачає розробку Планів дій у разі кіберкризи, стратегічних документів, сформульованих керівником BSSN за участю відповідних міністерств, відомств, CIRT та інших зацікавлених сторін. Ці плани мають важливе значення для підвищення готовності до пом’якшення наслідків кіберкриз і повинні бути розроблені протягом 12 місяців після оприлюднення BSSN Reg. 2/2024, тобто до 10 січня 2025 року.

Плани дій у надзвичайних ситуаціях складаються з урахуванням:

- національні оцінки ризиків кібербезпеки;
- національні пріоритети порядку денного; і
- ландшафт кібербезпеки.
- Плани дій у надзвичайних ситуаціях також повинні включати:
- сценарії загроз;
- характеристики та історія кіберзагроз;
- ролі, обов'язки та моделі спілкування;
- процеси стримування;
- процеси відновлення;
- механізми фінансування; і
- процедури звітності.

BSSN Рег. 2/2024 також вимагає, щоб ці Плани дій у надзвичайних ситуаціях проходили моделювання для перевірки їх практичності, обґрунтованості та якості. BSSN повинен проводити ці симуляції принаймні один раз на два роки, включаючи технічні тренування та моделювання прийняття управлінських рішень.

Крім того, BSSN та інші відповідні міністерства чи відомства зобов'язані щорічно або за потреби періодично оцінювати Плани дій у надзвичайних ситуаціях, результати яких можуть призвести до внесення необхідних змін.

Впровадження управління кіберкризою

BSSN Рег. 2/2024 розподіляє управління кіберкризою на три етапи:

1. Докризовий період:

Реагування на кіберінциденти: дії щодо вирішення ескалації кіберінцидентів, які можуть призвести до кіберкризи.

Раннє попередження: національна CIRT попереджає ESP про потенційну ескалацію кризових ситуацій через кіберінциденти, інформацію передають організаційні, галузеві та національні CIRT.

Визначення кризового статусу: Президент за рекомендацією голови BSSN оголошує кіберкризу.

2. Під час кризи:

Стримування кризи та відновлення: заходи з управління та відновлення після кризи.

Звітування про кризове управління: Документування та звітування про дії з кризового менеджменту.

Припинення кризового статусу: процес офіційного завершення кризи.

3. Посткризовий період:

Оцінка впливу та збитків: BSSN у співпраці з відповідними ESP розраховує збитки, економічні збитки та погіршення репутації, а також оцінює зусилля з пом'якшення.

Оцінка витрат на відновлення: розрахунок витрат, необхідних для відновлення електронної системи до її докризового стану.

Оцінка поранених: підрахунок загальної кількості загиблих та ідентифікація зниклих безвісти та поранених.

Висновок

Правила, видані BSSN, є критично важливими кроками в реалізації національної стратегії кібербезпеки та управління кризовими ситуаціями,

викладеної в PR 47/2023. Встановлюючи вичерпні вказівки щодо ідентифікації VII, формування та роботи CIRT, а також управління кіберкризами, ці правила спрямовані на посилення стану кібербезпеки Індонезії та забезпечення скоординованої реакції на кіберзагрози та інциденти.

Основні терміни, на які варто звернути увагу, включають:

18 липня 2024 року: Кінцевий термін створення та реєстрації галузевих та організаційних CIRT постачальниками VII.

10 січня 2025 року: Кінцевий термін розробки Планів дій у надзвичайних ситуаціях у кіберкризі.

Ці терміни підкреслюють нагальну потребу у відповідності для забезпечення досягнення стратегічних цілей національної кібербезпеки та ефективного врегулювання криз». ***(Winnie Yamashita Rolindrawan, Agung K. Sihombing. Fortifying Indonesia's Cyber Defenses: New Regulations for National Security and Crisis Management - SSEK Law Firm // SSEK Law Firm (https://ssek.com/blog/fortifying-indonesias-cyber-defenses-new-regulations-for-national-security-and-crisis-management/). 20.05.2024).***

***

«1 травня 2024 року Національний комітет з кібербезпеки Таїланду (NCSC) опублікував проект повідомлення NCSC Re: Cloud Cybersecurity Standards для публічного слухання, яке було відкрито до 14 травня 2024 року. перша політика з метою мінімізації ризиків від кіберзагроз для хмарних сервісів, які використовуються урядовими установами, наглядовими або регулюючими організаціями та організаціями критичної інформаційної інфраструктури (CII).

Ключові моменти проекту Стандартів хмарної кібербезпеки наведені нижче.

Область застосування

Стандарти застосовуються до державних установ, наглядових або регулюючих організацій та організацій CII відповідно до Закону про кібербезпеку BE 2562 (2019), а також до постачальників хмарних послуг (визначено нижче).

Стандарти передбачають заходи кібербезпеки хмарних систем для клієнтів хмарних послуг (визначених нижче) і постачальників лише в тій мірі, в якій послуга надається організаціям, що входять до сфери дії, описаної вище.

визначення

Клієнти хмарних послуг (CSC): організації, що входять до сфери дії, які мають офіційну договірну угоду про використання хмарних послуг, що надаються постачальником хмарних послуг.

Постачальники хмарних послуг (CSP): особи, які забезпечують використання хмарних послуг клієнтом хмарних послуг, відповідальні за підтримку інфраструктури, платформ і програмного забезпечення, які забезпечують надання хмарних послуг, і за керування цими ресурсами для забезпечення їх доступності, безпеки та масштабованість для своїх клієнтів хмарних послуг.

застосування

Організації, що розглядаються, які використовуватимуть або використовували хмарні служби, повинні відповідати стандартам хмарної кібербезпеки, беручи до уваги рівень впливу своїх даних або технологічних інформаційних систем, як зазначено в попередньо виданому Повідомленні NCSC Re: Standards for Defining Категорія безпеки для даних та інформаційних систем BE 2566 (2023).

Рівень впливу, пов’язаний з персональними даними, має бути оцінений як щонайменше середній, і необхідно прийняти мінімальні стандарти для цього рівня, визначені в проекті Стандартів хмарної кібербезпеки.

Організації, які входять до сфери дослідження, повинні повідомити про впровадження Стандартів хмарної кібербезпеки Національному агентству з кібербезпеки (NCSA) протягом 30 днів після завершення впровадження.

Проект стандартів хмарної кібербезпеки набуде чинності через рік після їх публікації в Урядовому віснику.

Структура

Вимоги стандартів хмарної кібербезпеки поділяються на дві сфери: (1) управління безпекою в хмарі та (2) хмарна інфраструктура та операції:

Сфера вимог 1: Управління безпекою в хмарі

Політики інформаційної безпеки

Організація інформаційної безпеки

Відносини із зовнішніми постачальниками

Відповідність

Сфера вимог 2: Безпека та експлуатація хмарної інфраструктури

Безпека людських ресурсів

Управління активами

Управління доступом

Криптографія

Фізична та екологічна безпека

Оперативна безпека

Безпека зв'язку

Придбання, розробка та обслуговування системи

Відносини із зовнішніми постачальниками

Управління інцидентами інформаційної безпеки…» ***(Thailand Issues Draft Cybersecurity Standards For Cloud Services // Conventus Law (https://conventuslaw.com/report/thailand-issues-draft-cybersecurity-standards-for-cloud-services/). 27.05.2024).***

***

«2 травня 2024 року Міністерство юстиції В’єтнаму опублікувало на своїй онлайн-платформі останню версію проекту указу про адміністративні санкції за порушення у сфері кібербезпеки («Проект указу про санкції»), щоб зібрати відгуки та внески від спільноти та зацікавлених сторін. Отримавши оцінку Міністерства юстиції, Міністерство громадської безпеки (MPS), відповідальне за розробку проекту Указу про санкції, може внести додаткові зміни перед тим, як подати його уряду для розгляду та прийняття остаточного рішення щодо введення в дію. Очікується, що указ набере чинності з 1 червня 2024 року.

Суворі покарання за порушення, пов’язані з персональними даними попередньої редакції проекту санкцій, залишаються в цьому проекті Указу про санкції, що свідчить про проактивну позицію MPS у виконанні Указу про захист персональних даних («PDPD»).

Дата набрання чинності та перехідні положення

Важливо зазначити, що проект постанови про санкції не покладає жодних нових зобов’язань на організації чи фізичних осіб, а лише встановлює адміністративні санкції, які можуть бути накладені на порушників уже з 1 червня 2024 року, що зазначено як дату набрання чинності у ст. Стаття 49. Це сигналізує про прагнення МПС почати вживати примусових заходів проти непокірних організацій та осіб, які не дотримуються різноманітних зобов’язань, покладених на них відповідно до Закону «Про безпеку мережевої інформації» (введеного в дію у 2015 році), Закону «Про кібербезпеку» (введеного в дію у 2018 році).) і його керівний указ (указ 53 – прийнятий у 2022 році), а також останній PDPD (введений в дію у 2023 році).

Стаття 50.1 Проекту постанови про застосування санкцій містить перехідні положення щодо адміністративних правопорушень у сфері кібербезпеки. У ньому уточнюється, що постанова не має зворотної дії в часі, зазначаючи, що порушення, які сталися до дати її набрання чинності, але виявлені або розглядаються після такої дати набрання чинності, підпадають під дію положень про адміністративні санкції, що діяли на момент вчинення порушення. Крім того, у випадках, коли в проекті указу про санкції або відсутні санкції, або вводяться більш м’які санкції за минулі дії, ці більш м’які положення матимуть переважну силу при розгляді порушень.

Коригування штрафів і пені

Було дещо скориговано санкції згідно з проектом наказу про санкції, що застосовуються до порушень, зі змінами розміру грошових штрафів та кількості застосованих додаткових штрафів та/або заходів усунення. Бізнес із задоволенням зауважить, що багато штрафів у розділі, пов’язаних із порушенням PDPD, зменшено порівняно з попереднім проектом. Однак максимальний фіксований

грошовий штраф, накладений проектом указу про санкції, все ще становить 1 мільярд в'єтнамських донгів (приблизно 40 000 доларів США), як це було запропоновано в попередньому проекті, а також штраф у розмірі до 5% від обороту підприємства-порушника безпосередньо за попередній фінансовий рік. на в'єтнамському ринку також все ще стосується певних екстремальних порушень, зокрема:

Повторне та наступне порушення правил захисту персональних даних у маркетинговій та рекламній діяльності;

Повторне та наступне порушення правил незаконного збору, передачі, купівлі та продажу персональних даних; і

Розголошення або неправильне розміщення персональних даних 5 мільйонів або більше суб'єктів даних, які є громадянами В'єтнаму.

У разі транскордонного розкриття, неправильного розміщення чи транскордонної передачі персональних даних понад 5 мільйонів суб'єктів даних, які є громадянами В'єтнаму, штраф може становити від 3% до 5% від обороту підприємства за попередній фінансовий рік на ринку В'єтнаму.

За певні порушення також можуть бути застосовані додаткові покарання, включаючи, серед іншого, анулювання ліцензій на види діяльності, які потребують збору персональних даних, а також конфіскацію речових доказів і засобів, які використовувалися для вчинення порушень. Також можуть бути застосовані заходи правового захисту, включаючи, серед іншого, призупинення обробки персональних даних на 1-3 місяці; примусове знищення або невідновне видалення персональних даних; та примусове повернення неправомірної вигоди, отриманої від порушень; публічне вибачення. Проект постанови про санкції змінив ці додаткові покарання та заходи захисту за деякі порушення.

Інші зміни до проекту

Цікаво, що проект Указу про санкції містить нову формулювання, яке виключатиме вихідні та національні свята з 72-годинного графіка для розгляду запитів, пов'язаних із правами суб'єктів даних, і для повідомлення MPS про порушення PDPD, якщо законом не передбачено інше. Це може бути ознакою того,

що MPS змінює свою початкову позицію і що 72-годинна шкала часу стосується 72 годин робочих днів (тобто 3 робочих днів). MPS також не змінив деякі посилання на 48-годинний графік, який був введений у попередньому проекті, але вважався опечаткою або помилкою.

Нарешті, проект постанови про санкції більше не включає статтю 50.2 попереднього проекту, яка мала на меті скасувати різні покарання за адміністративні порушення у сферах пошти, телекомунікацій, радіочастот, інформаційних технологій та електронних транзакцій відповідно до постанови № 15/2020. /ND-CP, зі змінами («Постанова 15»). Таким чином, очікується, що ці санкції продовжуватимуть застосовуватися навіть після оприлюднення проекту Указу про санкції. Однак, згідно з принципом розгляду адміністративних правопорушень у В'єтнамі, компанія не може бути оштрафована двічі за одне й те саме порушення. Таким чином, органу влади може знадобитися вибрати, чи він бажає застосувати санкцію згідно з проектом указу про санкції чи указу 15.

Outlook

Оскільки цей проект указу про санкції просувається на останніх стадіях ухвалення, зацікавленим сторонам пропонується бути в курсі та негайно виконувати вимоги законодавства, що застосовуються до них, особливо їхні зобов’язання згідно з PDPD, до того, як проект указу про санкції набере чинності (очікується в червні). 1, 2024)». ***(Decree on Sanctions For Cybersecurity Violations In Vietnam Nearing Enactment // Conventus Law (https://conventuslaw.com/report/decree-on-sanctions-for-cybersecurity-violations-in-vietnam-nearing-enactment/). 27.05.2024).***

***

«Оскільки цифровий ландшафт на Філіппінах продовжує розвиватися швидкими темпами, важливість жорстких заходів кібербезпеки була такою важливою, як ніколи.

Нещодавно оприлюднений Національний план кібербезпеки на 2023-2028 роки (NCSP) показує, що країна вживає додаткових заходів для захисту філіппінців від кіберзлочинів.

NCSP прагне побудувати стійку та безпечну цифрову екосистему на Філіппінах шляхом співпраці, нарощування потенціалу та стратегічних ініціатив, спрямованих на боротьбу з кіберзагрозами.

У світлі його випуску лідери галузі та зацікавлені сторони, включаючи експертів з кібербезпеки, таких як Касперський, пропонують цінну інформацію про наслідки NCSP та його потенційний вплив на майбутнє кібербезпеки на Філіппінах.

Джіні Сугене Ган, директор відділу зв'язків з урядом і державної політики в Азіатсько-Тихоокеанському регіоні, Японії, Близькому Сході, Туреччині та Африці Kaspersky, підкреслив, що випуск NCSP є важливим кроком уряду Філіппін у захисті філіппінців від кіберзлочинів. Крім того, він має на меті забезпечити національні державні установи та органи місцевого самоврядування необхідними інструментами для ефективного захисту своєї юрисдикції.

«Просуваючись вперед, кіберзлочини, безсумнівно, ставатимуть все більш витонченими, і кіберзлочинці невпинно полюватимуть на нових жертв. Вкрай важливо, щоб нація та її громадяни були готові протистояти цим викликам, забезпечуючи їхню безпеку в цифровому світі», – сказав Ган.

Ган підкреслив, що враховуючи те, що кібератаки не тільки завдають економічної шкоди, але й мають глибокі емоційні наслідки для суспільства, вкрай важливо, щоб напрям політики та оперативні вказівки в рамках NCSP були реалізовані.

«NCSP забезпечує стратегічну основу для комплексної боротьби з кіберзагрозами та забезпечення стійкості нашої цифрової інфраструктури, і ми оптимістично налаштовані щодо її ефективного впровадження», — додала вона.

Касперський був на передньому краї підвищення обізнаності про кіберзлочини та розширення можливостей окремих осіб і організацій для захисту себе. Окрім використання потужних інструментів кібербезпеки, ще один хороший спосіб залишатися в безпеці в Інтернеті – зробити кілька речей самостійно. Це

включає регулярну зміну паролів і постійне оновлення останніх новин кібербезпеки. Роблячи ці дії, ви можете ускладнити кіберзлочинцям націлювання на вас і знизити ймовірність атаки в Інтернеті.

Протягом багатьох років Kaspersky також встановив успішні партнерські стосунки з державними та правоохоронними органами по всьому світу, включаючи Інтерпол.

З вересня по грудень 2023 року Kaspersky провів серію тренінгів Kaspersky Expert для співробітників правоохоронних органів Інтерполу, розкриваючи нові передові стратегії виявлення загроз і пом'якшення їх для дослідників кібербезпеки. Глобальна дослідницько-аналітична група Касперського (GReAT) і експерти CERT провели для співробітників агентства тренінги з зворотного проектування та реагування на інциденти.

Останнім прикладом взаємної співпраці Kaspersky з урядовими установами в Південно-Східній Азії є меморандум про угоду, підписаний між Kaspersky та Національним агентством кібербезпеки Таїланду (NCSA) у квітні минулого року. Ця співпраця спрямована на підвищення можливостей Таїланду в галузі кібербезпеки.

Kaspersky також проводить онлайн- програму розвитку кіберпотенціалу, яка навчає компанії, державні та наукові кола покращувати безпеку своєї ІКТ-інфраструктури». ***(Exploring the future of PHL cybersecurity: Kaspersky shares insights on NCSP // BusinessMirror (https://businessmirror.com.ph/2024/05/24/exploring-the-future-of-phl-cybersecurity-kaspersky-shares-insights-on-ncsp/). 24.05.2024).***

***

«За словами представників галузі, факультативів з КІБЕРБЕЗПЕКИ, які пропонуються в університетах і коледжах, недостатньо, щоб заповнити брак експертів у цій галузі на Філіппінах.

«Ми не змогли виробляти багато [нашої] робочої сили, тому що наша академія не надає ступенів з кібербезпеки. Натомість вони пропонують це як

факультатив», – сказав у повідомленні Viber Аллан С. Кабанлонг, регіональний директор у Південно-Східній Азії Global Forum on Cyber Expertise.

За його словами, такі органи сертифікації, як Агентство кібербезпеки та безпеки інфраструктури, Сертифікація сертифікованих етичних хакерів, Інститут комп'ютерної криміналістичної експертизи та безпеки тощо, збільшили кількість професіоналів галузі.

Проте сертифікація, яку можна отримати за кілька тижнів, не гарантує, що студент володітиме знаннями з операцій, додав він.

Попит на фахівців з кібербезпеки досяг рекордного рівня на тлі зростання кількості онлайн-атак, а нещодавні схеми націлені навіть на державні установи.

За даними Національної асоціації спеціалістів із захисту даних Філіппін, країні потрібно близько 180 000 фахівців.

«У Сінгапурі працює близько 2000 фахівців з кібербезпеки, а на Філіппінах — близько 200. І з цих 200 80 відсотків працюють за кордоном», — сказав раніше секретар Департаменту інформаційних і комунікаційних технологій (DICT) Іван Джон Уй.

Пан Кабанлонг сказав, що ідеальним варіантом для філіппінських шкіл, які пропонують програми з кібербезпеки, є партнерство з іноземними академічними закладами та приватними фірмами для навчання без відриву від роботи,

«Якщо хтось хоче запропонувати кібербезпеку — будь то розслідування кіберзлочинів, мережеву безпеку, кіберзахист чи кібердипломатію — основи або просунуту частину або курси для керівників, у них уже повинні бути інструкції», — сказав він.

Пан Кабанлонг був колишнім помічником секретаря DICT. Під час його роботи агентство уклало партнерство з Університетом AMA в 2018 році, щоб запропонувати ступінь бакалавра наук з кібербезпеки.

Серед інших навчальних закладів пропонують факультатив бакалавра комп'ютерних наук із кібербезпеки в Університеті Атенео Давао, Університеті Святого Павла, Мапуа, а також ступінь магістра з кібербезпеки в Університеті Святих Ангелів.

Університет Сходу (UE) Caloocan нещодавно оголосив, що запропонує чотирирічну програму бакалавра кримінології зі спеціалізованими курсами з кібербезпеки.

Мішель Консепсьйон, декан Коледжу мистецтв і наук UE (CAS), сказала, що в університеті є група експертів з інформаційних технологій (IT) і кримінології, які зможуть викладати курси з кібербезпеки та кримінології для програми.

«Університет має вісім аудиторій IT-лабораторії, обладнаних комп'ютерами та програмним забезпеченням для курсів спеціалізації з кібербезпеки, таких як кіберпростір і кібербезпека, забезпечення інформації та безпека, протоколи мережі та передачі даних, цифрова криміналістика, машинне навчання в безпеці, тестування на проникнення в безпеку та аудит», - повідомила пані Консепсьон у повідомленні Viber.

За її словами, UE планує отримати від 100 до 200 абітурієнтів на пілотний навчальний рік.

UE CAS Caloocan прагне підготувати випускників, які є компетентними та будуть підтримувати суворі етичні стандарти в наданні послуг, включаючи запобігання злочинам, виявлення, розслідування, правоохоронні органи, громадську безпеку, опіку, реабілітацію правопорушників та кримінологічні дослідження, додала вона.

Рональд Б. Густіло, представник національної кампанії Digital Pinoys, однак зазначив, що ці спеціалізовані курси здебільшого проводяться в приватних навчальних закладах і мають відносно високу плату за навчання.

«Уряд повинен виділити кошти державним коледжам і університетам (SUC), щоб вони могли пропонувати курси з кібербезпеки та інформаційних технологій. Держава має покращити матеріально-технічну базу ДУЦ і найняти фахівців, які будуть навчати студентів», – сказав він.

ІКТ АКАДЕМІЯ

Згідно з Національним планом кібербезпеки, створення Академії ІКТ і Центру передового досвіду з кібербезпеки є однією зі стратегій для підготовки більшої кількості експертів з кібербезпеки.

До 2028 року DICT планує підготувати 300 000 фахівців з кібербезпеки.

Заступник секретаря DICT з управління інформаційними структурами, кібербезпеки та підвищення кваліфікації Джеффрі Ян Дай сказав, що ці об'єкти планується неофіційно створити протягом року.

«Однак інституціоналізація академії потребує відповідного закону. Ми будемо виступати за його створення в рамках законопроектів про кібербезпеку, які знаходяться на розгляді в Конгресі», — сказав він у повідомленні Viber.

Агентство надає часткові стипендії та пропонує студентам онлайн-навчання та навчання на комп'ютері. Нещодавно компанія видала 500 сертифікатів кібербезпеки Google, наданих через систему управління навчанням агентства, сказав пан Дай.

«З Microsoft у нас є угода про обмін розвідданими та навчання персоналу нашого Центру національної безпеки», — додав він». ***(Aubrey Rose A. Inosante. Academic programs seen to help address workforce gap in cybersecurity sector // BusinessWorld Publishing (https://www.bworldonline.com/technology/2024/05/23/596761/academic-programs-seen-to-help-address-workforce-gap-in-cybersecurity-sector/). 23.05.2024).***

***

«У перші кілька місяців 2024 року низка кібератак на системи VNDirect і PVOIL надіслала попереджувальний знак про зростання загрози хакерських атак у В'єтнамі. Інциденти спонукають компанії задуматися про свої інвестиції в систему безпеки.

Нго Туан Ань, віце-президент В'єтнамської асоціації інформаційної безпеки (VNISA), зазначив, що витрати великої суми грошей недостатні для забезпечення безпеки та безпеки системи.

Необхідно враховувати три чинники, включно з хорошою технологією, хорошим персоналом для реалізації та моніторингу загроз, а також ефективним робочим процесом для забезпечення безпеки та уникнення людських помилок.

«Більшість кібератак спричинені прогалинами в роботі та людях. Зловмисники часто користуються слабкими ланками, щоб скомпрометувати систему», — сказав він, додавши, що дефіцит навичок кібербезпеки залишається проблемою, з якою стикається галузь.

За даними Міністерства інформації та зв'язку, станом на 2023 рік у секторі кібербезпеки працювало 3866 співробітників, що на 13 відсотків більше, ніж у 2022 році. Однак ця цифра надто мала, щоб впоратися з величезним навантаженням, спричиненим зростаючою тенденцією кібератак на окремі особи, підприємства та організації.

Фам Трунг Дук, менеджер з обслуговування VNPT Cyber Immunity, сказав: «Кількість фахівців з кібербезпеки у В'єтнамі – як крапля в морі. З іншого боку, за оцінками, у Сінгапурі працює понад 77 400 співробітників з кібербезпеки, що значно менше, ніж у В'єтнамі за площею та чисельністю населення, але Сінгапур повідомляє про брак понад 6000 працівників у цій галузі».

У тому ж дусі Ха Фуонг, генеральний директор CMC Cyber Security, сказав: «В'єтнам стикається з нестачею талантів у сфері кібербезпеки як кількісно, так і якісно. Більшості аспірантів у цій галузі бракує навичок для реалізації реальних проектів. Тим часом університети Щоб вирішити цю проблему, багато компаній з кібербезпеки змушені брати студентів з інших галузей і перенавчати їх для роботи в цій галузі».

Через дефіцит талантів фахівці з кібербезпеки стикаються з більшим виснаженням.

Відповідно до звіту «Майбутнє кібербезпеки в Азіатсько-Тихоокеанському регіоні та Японії», проведеного Sophos у співпраці з Tech Research Asia (TRA), 90 відсотків респондентів, які працюють на посадах у сфері кібербезпеки та IT, страждають від виснаження та втоми.

Дослідження показало, що виснаження відчувається майже в усіх аспектах діяльності з кібербезпеки, причому 30 відсотків респондентів сказали, що відчуття вигорання «значно» зросло за останні 12 місяців, а 41 відсоток сказав, що це вигорання робить їх «менш старанними» 17 відсотків респондентів вказали, що

виснаження чи втома в кібербезпеці сприяли або були безпосередньо відповідальними за порушення кібербезпеки, а 17 відсотків компаній мали час реагування на інциденти кібербезпеки менший за середній.

Існує п’ять основних причин кібервигоряння та втоми, включаючи брак ресурсів для підтримки діяльності з кібербезпеки та рутинні аспекти ролі, які створюють відчуття монотонності.

Іншою причиною є підвищений рівень тиску з боку правління та/або виконавчого керівництва. У той же час постійне перевантаження попередженнями від інструментів і систем також сприяє кібервигоранню та втомі. Нарешті, спостерігається збільшення активності загроз і впровадження нових технологій, які сприяють створенню складнішого, «постійно активного» середовища.

«У той час, коли організації борються з дефіцитом навичок кібербезпеки та дедалі складнішим середовищем кібератак, стабільність і продуктивність співробітників є критично важливими для забезпечення надійного захисту бізнесу. Вигорання та втома підривають ці сфери, і організаціям необхідно активізуватися, щоб надати належну підтримку співробітникам, особливо коли, згідно з нашим дослідженням, 17 відсотків респондентів вказали, що виснаження або втома з питань кібербезпеки сприяли чи були безпосередньо відповідальними за порушення кібербезпеки», – сказав Аарон Бугал, технічний директор Sophos.

«Хоча це непросте рішення, коригування ставлення значною мірою допоможе визначити правильні очікування щодо того, що означає еволюція до кіберстійкого бізнесу. Правління та виконавчі комітети повинні стимулювати зміни та вимагати відповідальності від своїх заступників, По суті, для кращого управління навколо кіберпідходів, однак вони повинні чітко сформулювати свою відповідальність у розробці та підтримці плану, тому що кібербезпека зараз є постійно інтерактивним видом спорту – і потрібна команда, яка забезпечує адекватне покриття цілодобово», – сказав він». ***(Cybersecurity professionals key to filling gaps in cyberattack environment // Vietnam Investment Review (https://vir.com.vn/cybersecurity-professionals-key-to-filling-gaps-in-cyberattack-environment-111088.html). 14.05.2024).***

***

«Дані — це цар, як кажуть, і кожен усвідомив важливість і використання даних у всіх сферах життя. Дані допомагають організаціям приймати обґрунтовані рішення щодо свого бізнесу, профілювати клієнтів і замовників, виявляти проблеми та пропонувати рішення, вимірювати ефективність різних стратегій, які вони використовують, аналізувати ефективність і визначати заходи для покращення тощо. Через важливість даних, доступ до них надзвичайно цінний для одержувача, і тому зростає кількість кібератак для використання даних у часто злочинних цілях. Таким чином, збирачі даних, такі як уряди, організації та окремі особи, повинні запровадити відповідну нормативну базу та вжити заходів, щоб бути на крок попереду цієї злочинної діяльності.

У Нігерії доступ до Інтернету, гнучка робота, соціальні мережі, зростання електронної комерції тощо збільшили обробку даних організаціями та окремими особами. Станом на 2019 рік у Комісії з корпоративних справ Нігерії було зареєстровано понад 3,1 мільйона компаній. Це означає, що існують мільйони співробітників, дані яких обробляються щодня. Таким чином, конфіденційність даних, яка стосується того, як дані збираються, обробляються та зберігаються, має стати ключовим напрямком для роботодавців у Нігерії.

Багато організацій, розробляючи свою систему кібербезпеки та конфіденційності даних, зазвичай зосереджуються на захисті особистих даних, які вони збирають ззовні, тобто від клієнтів/споживачів, постачальників, підрядників, сторонніх постачальників послуг тощо, нехтуючи даними, що обробляються всередині. Реальність така, що працівники також користуються правами, наданими суб’єктам даних відповідно до чинного законодавства про захист даних. Насправді приватне життя є основним правом людини згідно з конституцією Нігерії.

Злочинці можуть використовувати особисті дані працівників для шахрайства, переслідування або навіть продажу третім особам, що може призвести до

відстеження та моніторингу діяльності таких працівників, порушуючи таким чином їхнє право на конфіденційність і, у більшості випадків, фінансові збитки.

Чому конфіденційність даних важлива і як роботодавці можуть захистити персональні дані своїх працівників? Це деякі з питань, які будуть розглянуті в цій статті.

Що таке персональні дані співробітника?

Персональні дані працівника включають будь-яку інформацію, яка може бути використана для ідентифікації працівника, наприклад ім'я, адреса, фотографія, адреса електронної пошти, банківські реквізити, публікації на веб-сайтах соціальних мереж, медична інформація та інші унікальні ідентифікатори.

Що таке конфіденційність даних і чому це важливо?

Конфіденційність даних означає захист персональних даних від несанкціонованого доступу, використання та розголошення, гарантуючи, що вони обробляються, зберігаються та обробляються у спосіб, який поважає їхні права та очікування щодо конфіденційності. Конфіденційність даних важлива, оскільки, серед іншого, вона забезпечує захист інформації організацій та їхніх працівників, клієнтів, клієнтів тощо від шахрайських дій, які можуть призвести до жахливих наслідків, таких як недовіра та втрата доходу. Крім того, дотримання суворих стандартів конфіденційності даних може підвищити репутацію компанії та імідж бренду, сприяючи підвищенню лояльності клієнтів і позитивному сприйняттю громадськості.

Які закони регулюють конфіденційність даних у Нігерії?

Конституція Федеративної Республіки Нігерія.

NDPA.

NDPR 2019.

Концепція реалізації NDPR.

У певних випадках можуть застосовуватися інші галузеві закони.

Як роботодавці можуть захистити персональні дані своїх працівників?

Мінімізація даних: роботодавці повинні збирати та зберігати лише ті особисті дані, які необхідні для законних цілей організації. Вони повинні уникати збору

надмірної або нерелевантної інформації, яка може створити непотрібний ризик для конфіденційності співробітників.

DPIA: роботодавці повинні проводити DPIA, щоб виявити й оцінити потенційні ризики конфіденційності, пов'язані з обробкою персональних даних працівників. Висновки слід використовувати для впровадження відповідних заходів для зменшення ризиків і забезпечення дотримання законів про захист даних.

Повідомлення про конфіденційність співробітників: роботодавці можуть відобразити просту та зрозумілу політику конфіденційності, яка описує, як організація збирає, використовує, зберігає та захищає персональні дані своїх співробітників. Він слугує комунікаційним інструментом для інформування працівників про їхні права на конфіденційність і методи захисту даних в організації. Політика конфіденційності повинна передбачати опис персональної інформації, яка збирається, мету збору та технічні методи, що використовуються для збору та зберігання особистої інформації серед іншого.

Захист персональних даних: роботодавці повинні розробити заходи безпеки для захисту персональних даних, які вони збирають від своїх працівників. Такі заходи включають, але не обмежуються захистом систем від хакерів, встановленням брандмауерів, безпечним зберіганням даних із доступом до певних уповноважених осіб, використанням технологій шифрування даних, розробкою організаційної політики щодо обробки персональних даних, захистом систем електронної пошти та постійним підвищенням кваліфікації персоналу.

Аудит: проведення регулярних перевірок систем роботодавця, щоб переконатися, що вони функціонують належним чином, і всі встановлені заходи безпеки працюють правильно.

Навчання: регулярне навчання співробітників важливості їхніх особистих даних, їх ролі в захисті та тому, чому заходи, які вводить роботодавець, повинні виконуватися та виконуватися.

Крім того, підписання договорів про захист даних і включення положень про захист даних у трудові договори є заходами, які роботодавці також можуть прийняти для захисту персональних даних своїх працівників. Ці заходи є

важливими для виконання їхніх зобов'язань щодо захисту даних перед працівниками, оскільки їх можна використовувати для інформування працівників про конкретні причини обробки їхніх даних до отримання згоди.

Яке використання даних працівників дозволено законодавством Нігерії?

Дозволене використання особистих даних працівників зазвичай залежить від внутрішньої політики організації та законних бізнес-інтересів, як це визначено чинним законодавством. Деякі поширені дозволені види використання персональних даних працівників можуть включати:

Роботодавці можуть збирати, обробляти та використовувати персональні дані співробітників для законних цілей, пов'язаних із працевлаштуванням, таких як підбір персоналу, прийом на роботу, оцінка ефективності, просування по службі, винагорода, управління пільгами та звільнення.

Роботодавці можуть використовувати особисті дані співробітників для керування обробкою заробітної плати, включаючи виплати зарплати, податкові відрахування, зарахування пільг і пенсійні внески. Це може передбачати передачу персональних даних стороннім постачальникам заробітної плати, фінансовим установам і адміністраторам пільг.

Роботодавцям дозволяється використовувати персональні дані працівників для дотримання законодавчих і нормативних вимог, таких як податкова звітність, трудове законодавство, правила безпеки на робочому місці, імміграційне законодавство та антидискримінаційне законодавство. Це може включати передачу персональних даних відповідним державним установам, регуляторним органам і правоохоронним органам, як того вимагає закон.

Роботодавці можуть використовувати персональні дані співробітників, щоб спілкуватися з ними щодо питань, пов'язаних з роботою, зокрема про призначення роботи, можливості навчання, політику компанії та організаційні зміни. Це може включати збір і використання особистих даних для спілкування електронною поштою, внутрішніх платформ обміну повідомленнями та опитувань співробітників.

Роботодавці можуть збирати та обробляти особисті дані працівників для цілей управління продуктивністю, наприклад, для проведення оцінювання ефективності, встановлення цілей, надання зворотного зв'язку та визначення потреб у навчанні чи розвитку.

Особисті дані працівників можуть використовуватися роботодавцями для забезпечення їхнього здоров'я та безпеки на робочому місці, наприклад для моніторингу відвідуваності, відстеження лікарняних, проведення перевірок стану здоров'я та впровадження адаптацій на робочому місці для людей з обмеженими можливостями. Роботодавці повинні з особливою обережністю поводитися з даними, пов'язаними зі здоров'ям, і в цьому відношенні дотримуватися NDPA.

Які наслідки порушення конфіденційності даних співробітника?

Наслідки порушення конфіденційності даних співробітника дуже різноманітні та можуть мати далекосяжні наслідки для постраждалих осіб і організації. Можливі наслідки включають санкції проти роботодавця з боку Комісії із захисту даних, судовий позов працівника проти роботодавця за порушення конфіденційності даних, фінансові втрати, репутаційні збитки, збої в роботі, втрату конкурентної переваги тощо». ***(Olufunmilola Oyinkansola Binuyo, Samuel Salako and Adewunmi Salami. Protecting employee data - requirements and best practices // DLA Piper (https://knowledge.dlapiper.com/dlapiperknowledge/globalemploymentlatestdevelopments/2024/protecting-employee-data-requirements-and-best-practices#page=1). 21.05.2024).***

***

«Нещодавнє скасування директиви щодо збору з кібербезпеки Центральним банком Нігерії (CBN) є значним подією. Ця директива, яка зобов'язувала банки та інші фінансові установи стягувати збір за кібербезпеку з електронних транзакцій, була потенційним джерелом доходу для плану боротьби з кіберзлочинністю Управління радника з національної безпеки. Його відміна позбавила громадян додаткового фінансового тягаря.

Очікувалося, що збори з кібербезпеки, які є незначними витратами на всі банківські операції, створять значний потік доходів для підтримки плану Управління радника з національної безпеки щодо боротьби з кіберзлочинністю. Однак директива викликала загальнонаціональний резонанс з боку незадоволених громадян, які скаржилися на те, що банківські операції стають все дорожчими та збільшують їх фінансовий тягар і труднощі через ці зміни.

Сенатор Шеху Умар Буба, голова Комітету Сенату з національної безпеки та розвідки, відіграв вирішальну роль у роз'ясненні мети збору з кібербезпеки. В інтерв'ю виданню Economic Confidential він пояснив, що податок спрямований не на фізичних осіб, а на фінансові установи та телекомунікаційні компанії. Його роз'яснення допомогло розвіяти будь-які помилкові уявлення про мету збору та його вплив на ці сектори.

Він підкреслив важливість безпечного та надійного середовища електронних транзакцій для сприяння економічному зростанню та доступності цифрових фінансів. Він сказав, що це також посилить національну безпеку, зміцнить кібербезпеку, захистить критичну інфраструктуру та конфіденційну інформацію, а також вирівняє Нігерію з найкращими міжнародними практиками.

Будучи одним із активних законодавців у верхній палаті, сенатор Буба раніше виступав із обґрунтованими справами щодо питань національного значення після надзвичайної ситуації нинішніх федеральних законодавців. Наприклад, відразу після інавгурації Національної асамблеї минулого року він стояв за одностайно підтриманим Сенатом проханням використати вже виділені N14,2 мільярда в бюджеті на 2023 рік для будівництва Нігерійської митної академії та навчальної школи в Баучі.

Подібним чином на початку року, висловлюючи занепокоєння щодо передбачуваного залишення нафтової свердловини Колмані на кордоні штатів Баучі-Гомбе, сенатор запевнив, що діяльність на ділянках відновиться всерйоз, підкресливши складність проекту розвідки нафти. Це сталося після того, як він ініціював обговорення проекту з ключовими зацікавленими сторонами, включаючи

керуючого директора групи NNPC Меле К'ярі та радника з національної безпеки Малама Нуху Рібаду.

Незважаючи на роз'яснення сенатора Буби та інших, серед громадськості залишається тривога. Багато хто побоюється, що скасування податку на кібербезпеку може призвести до непрямих наслідків, таких як збільшення податків на банківські операції та тарифів телекомунікаційними компаніями. Ці проблеми необхідно вирішити, щоб забезпечити всебічне розуміння проблеми.

Необхідно зазначити, що заходи кібербезпеки є важливими для припинення ексцесів онлайн-шахраїв. Широко повідомляється, що кіберзлочинці нишпорять, намагаючись отримати несанкціонований доступ до банківських рахунків за допомогою шахрайства, атак зловмисного програмного забезпечення та злому. Заходи кібербезпеки, такі як брандмауери, системи виявлення вторгнень і контроль доступу, допомагають запобігти несанкціонованому доступу та захистити конфіденційну інформацію.

Надійна кібербезпека є важливою у все більш цифровому світі. Його переваги включають запобігання несанкціонованому доступу до банківських рахунків, захист від шахрайства та крадіжки особистих даних, а також захист даних клієнтів.

Враховуючи його негативний вплив на домогосподарства з низькими доходами, занепокоєння пересічних громадян щодо податку може бути виправданим. Однією з головних проблем є потенційний вплив на домогосподарства з низькими доходами. Багато нігерійців вважають, що плата несправедливо завдасть шкоди малозабезпеченим особам і сім'ям, які використовують часті транзакції для задоволення своїх основних потреб.

За їх словами, податок додасться до інших зборів, які накладає на них CBN, таких як комісія за обслуговування карток банкоматів, гербовий збір, збір за обслуговування рахунку, податок на додану вартість на перекази, комісія за міжбанківські перекази, збір за переказ електронних грошей, тощо; все це може стати важким тягарем для звичайного нігерійця, що може перешкодити людям використовувати електронний банкінг. Професор економіки Ндубісі Нвокома заявив, що новий збір і нещодавно відновлені збори за обробку великих депозитів є

поганим вітром. За його словами: «Люди страждають, шукають, що їсти, а ви додаєте тягарів. Я розумію, що вони намагаються зібрати гроші, але люди, від яких ви збираєте гроші, не мають жодного реального доходу, щоб їх підтримувати. Людей виганяють з банківської системи». Крім того, він заявив, що ускладнюючи роботу для громадян, вони будуть змушені повернутися до готівкових операцій, оскільки створена проблема набагато більше, ніж гроші, які збираються.

Власники малого бізнесу висловили занепокоєння щодо того, як плата може вплинути на їх повсякденну діяльність. Електронні платежі є поширеним способом для малих підприємств обробляти споживчі транзакції та контролювати свій грошовий потік. Плата може збільшити операційні витрати, і мало хто планує відмовитися від електронного банкінгу. Продавець хліба Абубакар Шека сказав, що він уже вирішив уникати електронних банківських транзакцій до того часу, коли податок повинен був початися 20 травня.

«Я ні в якому разі не погоджуся, щоб мені давали 0,5 відсотка на мої трансфери, коли я заробляю дуже мало. Зараз багато хто не купує хліб, а бізнес крихкий. Чому цей уряд далі змушуватиме нас плакати цим, незважаючи на те, через що ми вже проходимо з високою вартістю продуктів харчування та палива?»

Експерти, як-от професор Нвокома, стверджують, що збір та інші недавні комісії можуть вивести людей з банківської системи та повернутися до готівкових операцій. Запропонований збір за кібербезпеку може здатися несправедливим, але кібербезпека має вирішальне значення в банківській сфері, телекомунікаційному та інших секторах для запобігання атакам і захисту конфіденційної інформації. Уряд, особливо законодавці, мають переглянути податок на кібербезпеку та переконатися, що він відповідає реальним обставинам, оподатковуючи не бідні, а багаті установи.

Хоча очікується, що уряд знову запровадить податок на кібербезпеку, враховуючи його переваги у зміцненні системи безпеки фінансових операцій у країні, він повинен робити це з людським обличчям та відповідною інформаційною кампанією щодо національних інтересів і потенціалу безпеки». ***(WINNIE CHIDIEBUBE. Still on cybersecurity and national interest // Vanguard Media Limited***

(https://www.vanguardngr.com/2024/05/still-on-cybersecurity-and-national-interest/). 27.05.2024).

***

«Запровадження Регламенту 2024 року про зловживання комп'ютером і кіберзлочинність (критична інформаційна інфраструктура та управління кіберзлочинністю) (далі – Регламент) знаменує собою важливу віху у формуванні ландшафту кібербезпеки Кенії.

Правила, опубліковані як юридичне повідомлення № 44 від 2024 року, пройшли всебічну перевірку та набули офіційної чинності. Цей акт узгоджується з Конституцією, Законом про нормативні документи 2023 року та розділом 70 Закону про комп'ютерні зловживання та кіберзлочини 2018 року (Закон). Ці Регламенти не тільки служать для введення в дію існуючих положень Закону, але й підвищують роль Національного координаційного комітету з комп'ютерних і кіберзлочинів як основного органу, який контролює питання кібербезпеки в країні. Розвиваючи співпрацю з Оперативними центрами кібербезпеки, ці Правила спрямовані на зміцнення захисту кібербезпеки та забезпечення безпечнішого цифрового середовища для всіх зацікавлених сторін.

Ці Регламенти підпадають під дію різних секторів і організацій, що потребуватиме проактивних заходів для пом'якшення кіберзагроз і захисту критичної інфраструктури. Правила мають широкі наслідки, зокрема впливають на широку громадськість, яка виграє від більш чітких вказівок щодо обов'язків і прав у сфері кібербезпеки. По-друге, це вплине на власників критичної інформаційної інфраструктури, які контролюють критичну інформаційну інфраструктуру, оскільки їм буде доручено дотримуватись суворих заходів безпеки та вимог до звітності, викладених у Регламенті. По-третє, постачальники інтернет-послуг і постачальники послуг кібербезпеки повинні узгодити свою діяльність з Правилами, щоб забезпечити дотримання вимог і підвищити загальну безпеку країни.

Покращення операцій з кібербезпеки

Регламент засновує Операційні центри кібербезпеки (COC), включаючи Національний операційний центр кібербезпеки (NCOC), Секторальні операційні центри кібербезпеки (SCOC) і Операційний центр кібербезпеки критичної інформаційної інфраструктури (CIICOC). Ці центри відіграватимуть ключову роль у моніторингу, виявленні та розслідуванні загроз кібербезпеці, надаючи інформацію в режимі реального часу та забезпечуючи оперативне реагування на кіберінциденти.

COC також матиме завдання подавати щомісячні звіти та щорічні звіти про відповідність комітету для оцінки дотримання. Ці короткі описи детально описуватимуть кіберризики, загрози та інциденти. NCOC слугуватиме основним пунктом для національного моніторингу та розслідування кібербезпеки. SCOC зосереджуватиметься на галузевих загрозах і звітності до національного центру, а CIICOC відповідатиме за моніторинг у режимі реального часу, виявлення та розслідування загроз для критичної інфраструктури, повідомляючи як національному, так і галузевим центрам.

Критична інформаційна інфраструктура

Визначена відповідно до розділу 9 Закону, критична інформаційна інфраструктура (CII) охоплює системи або дані, які вважаються важливими для національної безпеки та суспільного добробуту. Система класифікується як ICI, якщо її збій призведе до переривання таких життєзабезпечувальних послуг, як водопостачання, медичні послуги та енергетика, що негативно вплине на економіку Республіки, спричинить масові жертви чи смертельні випадки, суттєво порушить грошовий ринок і серйозно вплине на національну безпеку, включаючи розвідку та військові операції.

Регламент зобов’язує критично важливі інформаційні сектори проводити щорічну оцінку кіберризиків і аналіз впливу на бізнес для всіх видів діяльності, продуктів, послуг, бізнес-функцій і процесів. Крім того, кожен власник ICI повинен завершити оцінку ризиків протягом дванадцяти (12) місяців з моменту набрання

чинності Правил, щоб визначити та визначити пріоритети потенційних внутрішніх і зовнішніх загроз.

Після визначення системи як ІСІ директор комітету повинен повідомити власника або оператора системи протягом семи днів із зазначенням причин призначення. Розпорядження директора можуть вимагати від власника:

- Проводити щорічну оцінку ризиків;
- Розробка планів реагування на інциденти;
- Застосуйте відповідні заходи безпеки; і
- Переконайтеся, що персонал належним чином навчений передовим методам безпеки.

Власник може оскаржити будь-які рішення до Високого суду відповідно до розділу 10 Закону, якщо він не задоволений директивами комітету. Власник може подати письмову заявку на те, щоб система була оголошена ІСІ, і директор повинен відповісти протягом семи днів. Про будь-які значні зміни ІСІ необхідно повідомляти Директора заздалегідь.

Власники ІСІ повинні переконатися, що критична інформація про інфраструктуру знаходиться в Кенії. Будь-які плани щодо розміщення критично важливої інформації за межами Кенії потребують схвалення комітету, що забезпечує дотримання стандартів безпеки. Необхідно проводити періодичні перевірки програм інформування про кібербезпеку, щоб переконатися в їх адекватності та актуальності. Власник повинен призначити головного спеціаліста з інформаційної безпеки (CISO) для нагляду за питаннями кібербезпеки.

Інтеграція з іншими інфраструктурами дозволена лише за умови дотримання стандартів безпеки. Положення передбачають, що ІСІ завжди мають бути захищені, а доступ має бути обмежений уповноваженим персоналом. Необхідно підтримувати систему резервного копіювання для забезпечення відновлення інформації у разі втрати.

Обов'язкові вимоги

По-перше, власники ІСІ повинні щорічно проводити всебічну оцінку кіберризиків і аналіз впливу на бізнес, прискіпливо вивчаючи всі аспекти своїх ІСІ,

щоб виявити потенційні вразливості та визначити пріоритетність стратегій зменшення ризиків. Вони будуть зобов'язані впроваджувати надійні заходи безпеки, спрямовані на захист своїх ІСІ, включаючи розробку та реалізацію планів реагування на інциденти, а також забезпечення відповідного навчання персоналу щодо дотримання встановлених протоколів безпеки.

Вони повинні щорічно формулювати, переглядати та оновлювати організаційну політику, процедури та кодекси практики для захисту ІСІ. Це включає визначення процедур зберігання та архівування та обмін даними всередині організації. Ліцензовані оператори міжнародних або національних інтернет-шлюзів повинні відповідати стандартам кібербезпеки та надавати звіти про дотримання вимог безпеки на запит. Вони повинні повідомляти комітету про будь-які затори на дорогах або підозрілі дії, докладно вказуючи причини та способи вирішення. Своєчасне звітування про інциденти кібербезпеки має важливе значення, а власники критичної інформаційної інфраструктури зобов'язані повідомляти відповідні органи влади протягом двадцяти чотирьох (24) годин після виявлення. Посилені покарання за кіберзлочини підкреслюють серйозність, з якою розглядаються такі злочини. Невідповідність може призвести до того, що комітет рекомендує обмеження, призупинення або анулювання ліцензії оператора після консультації з регулюючим органом галузі. Щоб забезпечити відповідність, організації повинні регулярно формулювати, переглядати та оновлювати організаційні політики та процедури. Ліцензовані оператори інтернет-шлюзів зобов'язані дотримуватися стандартів кібербезпеки та повідомляти про відповідність регуляторним органам із застосуванням штрафів за недотримання.

Крім того, у Регламенті наголошується на імплементації Закону про захист даних 2019 року під час обробки персональних даних відповідно до Закону. Недотримання Закону про захист даних 2019 року в Кенії може призвести до штрафів у розмірі до п'яти (5) мільйонів KES або одного (1%) відсотка річного обороту організації, а відповідальні особи можуть бути позбавлені волі на строк до двох років. Крім того, Уповноважений із захисту даних може накладати

адміністративні санкції, включаючи повідомлення про примусове виконання та призупинення діяльності з обробки даних.

Правила знаменують нову еру в боротьбі з загрозами кібербезпеці в Кенії. Запроваджуючи надійну нормативну базу та сприяючи співпраці між зацікавленими сторонами, ці Регламенти спрямовані на посилення захисту кібербезпеки, зменшення кіберінцидентів та захист критичної інформаційної інфраструктури. Як ваші надійні юридичні консультанти, ми прагнемо допомогти вам зорієнтуватися в цих нормативних змінах, забезпечуючи відповідність і використовуючи кібербезпеку як конкурентну перевагу в сучасному цифровому середовищі». ***(Jared Kangwana, Nelly Tuitoek and Milton Kimotho. Unlocking the Potential of Cybersecurity: Navigating the Computer Misuse and Cyber Crime Regulations 2024 // Clyde & Co LLP (https://www.clydeco.com/en/insights/2024/05/unlocking-the-potential-of-cybersecurity-navigatin). 27.05.2024).***

***

Інші країни

«…Експерти з кібербезпеки підкреслюють, що злом паролів і їх використання є одними з найпоширеніших уразливостей для кінцевих користувачів. Ігнорування запобіжних заходів щодо захисту конфіденційних даних і конфіденційності в Інтернеті може призвести до значних фінансових втрат і серйозних цифрових порушень.

Під час нещодавньої інформаційної кампанії під керівництвом Ради з кібербезпеки ОАЕ було виявлено п’ять поширених помилок у паролях. Кампанія, націлена на державні та приватні установи, а також на широку громадськість, була спрямована на підвищення обізнаності щодо безпеки паролів під темою «Національна кампанія з кібербезпеки: рік цифрової обізнаності та освіти».

Рада підкреслила, що помилки в управлінні паролями широко поширені, але становлять реальну небезпеку для облікових записів користувачів, піддаючи їх злому та експлуатації.

П’ять поширених помилок у паролі, які піддають ризику облікові записи користувачів, включають:

- Використання одного пароля для кількох облікових записів
- Не змінювати паролі регулярно
- Включаючи в паролі інформацію, яку легко вгадати (наприклад, дати народження чи імена).
- Обмін паролями з іншими
- Ненадійне зберігання паролів

Кампанія також підкреслила важливість обережності, щоб уникнути фішингу та електронного шахрайства, коли зловмисники обманюють користувачів, щоб отримати їх особисті дані.

Kaspersky, компанія з кібербезпеки, підкреслила, що паролі залишаються основною мішенню для складних атак. Слабкі та прості паролі приваблюють шахраїв, оскільки їх злом може надати доступ до різних типів даних, включаючи особисті, фінансові та медичні записи.

Касперський зазначив, що у 2023 році було здійснено понад 32 мільйони спроб викрасти паролі, що підкреслює потребу в надійних, унікальних і різноманітних паролях для різних облікових записів.

Цифровий уряд ОАЕ наголосив на перевагах використання рішень цифрової ідентифікації, таких як програма UAE Pass, доступна в iTunes і Google Play.

Ця програма забезпечує безпечний спосіб доступу до служб без необхідності вводити кілька паролів, дозволяючи цифровий підпис документів і перевірку без відвідування сервісних центрів.

Попередження поліції

Поліція Абу-Дабі також застерегла від розголошення конфіденційної інформації, такої як паролі онлайн-банкінгу, PIN-коди банкоматів, номери CCV або одноразові паролі (OTP).

Вони підкреслили, що шахраї часто використовують назви національних установ, щоб ввести в оману жертв за допомогою шахрайських повідомлень або шахрайства в соціальних мережах…» ***(Ali Al Hammadi. Cybersecurity Council cites 5***

common password mistakes // GN Media (https://gulfnews.com/uae/cybersecurity-council-cites-5-common-password-mistakes-1.102607896). 14.05.2024).

***

«Національне агентство кібербезпеки Катару (NCSA) готується ліцензувати постачальників послуг кібербезпеки, щоб забезпечити найкращу якість у секторі, сказав високопоставлений чиновник.

«NCSA провела кілька зустрічей з відповідними органами влади, включаючи Міністерство торгівлі та промисловості та Академію фінансів і бізнесу Катару», — сказав директор департаменту кіберзабезпечення NCSA Енг Джассім Аль Муфтах.

Нещодавно виступаючи на Qatar TV, він сказав: «Під час зустрічей було зрозуміло та погоджено, що NCSA досягне мети високого рівня послуг шляхом ліцензування компаній, які надають послуги кібербезпеки, і ми працюємо над цим».

Він зазначив, що Агентство прагне зробити обов'язковим акредитацію для приватних компаній, оскільки його програма акредитації забезпечує високу якість, точність і надійність послуг, що надаються.

«Це відбувається згідно з Указом Еміра № 1 від 2021 року, який передбачає встановлення стандартів і заходів контролю для ліцензій, що надаються постачальникам послуг кібербезпеки», — сказав Аль Муфтах.

Він сказав, що NCSA нещодавно провела зустріч з керівниками компаній з кібербезпеки, щоб поінформувати їх про бачення агентства та дорожню карту щодо управління ланцюгом поставок у сфері кібербезпеки та послуг, що надаються в цьому аспекті. «Агентство прагне зв'язати акредитовані установи та компанії, щоб вони надавали найкращі послуги з кібербезпеки», — сказав Аль Муфтах.

Говорячи про процес акредитації, він сказав, що всі стандарти щодо акредитації доступні на офіційному веб-сайті NCSA в рамках акредитації та сертифікації National Information Security Compliance Framework (NISCF).

На запитання про переваги акредитації Аль Муфтах сказав: «Агентство прагне забезпечити, щоб послуги, що надаються у сфері кібербезпеки, відповідали найвищим міжнародно визнаним стандартам».

Він зазначив, що з новими технологіями агентство постійно працює над оновленням існуючих стандартів.

«Тому цього року ми оновили стандарти акредитації. ми запустили нову послугу акредитації, яка є акредитацією тестування на проникнення, і тому ми постійно розвиваємо ці стандарти та програми в Національному агентстві кібербезпеки», — сказав Аль Муфтах.

Національне агентство кібербезпеки прийшло, щоб об'єднати зусилля державних суб'єктів у сфері підтримки кібербезпеки в країні під однією парасолькою та посилити свої можливості для захисту держави та підтримки її стійкості перед обличчям зростаючих кіберзагроз.

Відтоді агентство взяло на себе завдання протистояти серйозним викликам, підтримуючи та запроваджуючи ініціативи з кібербезпеки, посилюючи співпрацю з установами в уряді та приватному секторах країни для подолання всіх потенційних кіберзагроз, які можуть вплинути на інформаційну інфраструктуру, яка стала життєво важливою артерією економіки країни». ***(Sanaullah Ataullah. NCSA to license cyber security service providers to ensure quality // The Peninsula (https://thepeninsulaqatar.com/article/14/05/2024/ncsa-to-license-cyber-security-service-providers-to-ensure-quality). 14.05.2024).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Масштабна китайська кібератака була спрямована на Великої Британії Міністерство оборони та розкрила інформацію про персонал збройних сил.

Атака, яка, як вважається, була здійснена два або три рази, була спрямована на систему оплати праці третьої сторони, включаючи відомості про десятки тисяч британських збройних сил і ветеранів.

Міністерство оборони працювало протягом останніх трьох днів, щоб зрозуміти масштаби злому після того, як його нещодавно виявили, повідомляє Sky News. За коментарями звернулися до Міністерства оборони.

Вважається, що жодних даних не було зібрано, і МО закликало військовослужбовців не турбуватися про свою безпеку. Депутатам розкажуть про напад у вівторок.

Це сталося після того, як уряд звинуватив китайських «державних акторів» у двох «зловмисних» кампаніях кібератак у Великобританії між 2021 і 2022 роками.

У березні віце-прем'єр-міністр Олівер Доуден повідомив Палаті громад двох осіб і компанію, пов'язану з китайською державою, під санкції за напади на виборчу комісію.

Ця ж компанія також проводила «розвідку» щодо рахунків парламенту Великобританії в окремій кампанії в 2021 році, сказав пан Доуден.

Пан Доуден повідомив депутатам, що Велика Британія накладає санкції на двох осіб і компанію, пов'язану з кібергрупою APT31, яка пов'язана з Міністерством державної безпеки Китаю.

У той час речник посольства Китаю в Лондоні заявив: «Так звані кібератаки Китаю проти Великобританії є повністю сфабрикованими та зловмисним наклепом».

У понеділок президент Китаю Сі Цзіньпін розпочав турне Європою, хоча він не мав наміру відвідати Великобританію. Він провів день у Парижі, де зустрівся з президентом Франції Еммануелем Макроном.

Після його прибуття група із семи французьких законодавців, які стали мішенню для кібератак, приписуваних китайським хакерам, закликала владу розпочати судове розслідування.

Вони хочуть, щоб Франція офіційно приписала атаку APT31 – тій самій компанії, на яку Великобританія наклала санкції в березні.

На відміну від США, Великої Британії та Нової Зеландії, які офіційно звинуватили Китай у кількох кібератаках, влада Франції ухилилася від звинувачень Пекіну…». ***(Alexander Butler. China suspected of massive cyberattack on database of***

UK armed forces personnel // Independent (https://www.independent.co.uk/news/uk/home-news/china-mod-uk-hack-data-breach-b2540489.html?utm_source=flipboard&utm_content=user%2FIndependent). 07.05.2024).

***

«Група із семи французьких законодавців, які стали мішенню для кібератак китайських хакерів, закликали владу розпочати судове розслідування.

Цей крок, оголошений у той день, коли Сі Цзіньпін розпочав дводенний державний візит до Франції, стався після того, як у березні Міністерство юстиції США висунуло обвинувальний акт, у якому говориться, що китайські хакери, пов'язані з його національним шпигунським агентством, Міністерством державної безпеки, в 2021 рік націлений на «кожного члена Європейського Союзу» Міжпарламентського альянсу з питань Китаю (IPAC), коаліції законодавців, які критикують Пекін.

На відміну від США, Великої Британії та Нової Зеландії, які офіційно звинуватили Китай, французька влада ухилилася від того, щоб вказувати пальцем на Пекін.

«Ми не можемо допустити, щоб така кампанія кібератак проти обраних представників французького народу залишилася без відповіді», — сказав французький сенатор Олів'є Кадік на прес-брифінгу в понеділок.

Законодавці, усі нинішні чи колишні члени IPAC, включають Констанс Ле Грип (Відродження), Ізабель Флоренн (Модем) і колишнього міністра Андре Валліні.

Вони хочуть змусити французький уряд офіційно приписати атаку APT31 — хакерській команді, пов'язаній з китайською державою. Французькі служби безпеки традиційно утримуються від приписування кібератак.

«Існує термінова потреба підвищити обізнаність і захистити членів парламенту від ризиків кібератак», - сказав Ле Грип.

Група також закликала розпочати судове розслідування щодо іноземного втручання, а також накласти санкції на членів APT31.

У 2021 році хакери надіслали «понад 1000 електронних листів більш ніж 400 унікальним обліковим записам осіб, пов'язаних з IPAC», щоб спробувати зібрати дані про інтернет-діяльність членів і цифрові пристрої, йдеться в обвинуваченні США.

Деякі з підтверджених цілей атаки включали колишнього прем'єр-міністра Бельгії Гі Верхофстадта, британського міністра у справах Європи Нусрата Гані та чеського міністра закордонних справ Яна Ліпавського». ***(Paul de Villepin. French lawmakers targeted by Chinese cyberattack demand sanctions, amid Xi visit // POLITICO (https://www.politico.eu/article/chinese-cyberattack-apt31-france-xi-jinping-interparliamentary-alliance-on-china/?utm_source=flipboard&utm_content=NewsisContext%2Fmagazine%2FChinese+World+Engagement). 06.05.2024).***

***

«Міністерство оборони Великої Британії постраждало від імовірної китайської кібератаки, в результаті якої особисті дані десятків тисяч військових були розкриті.

Ціллю злому була керована підрядником система розрахунку заробітної плати Міністерства оборони, яка включає імена та банківські реквізити нинішніх і колишніх членів збройних сил.

Постраждали всі війська, окрім сил спеціального призначення Великої Британії, приблизно 270 000 осіб. Порушення також стосується кількох тисяч домашніх адрес.

Оновлюючи Палату громад у вівторок вдень, міністр оборони Грант Шаппс не звинуватив прямо Китай у нападі. Пекін гнівно заперечує свою причетність.

Але Sky News, яка першою оприлюднила цю історію, повідомила, що в кадрі дійсно є Пекін. Попередні публічні вказівки на Китай відбулися після місяців роботи британських служб безпеки. Офіційні особи повідомили інформаційному

бюлетеню POLITICO London Playbook, що їх робота не подолала високу планку для публічного присвоєння авторства.

Шаппс розділив розбіжності у вівторок, сказавши депутатам, що хакерство було «імовірно роботою зловмисника, і ми не можемо виключити причетність держави». Але він сказав, що наразі неможливо «оприлюднити додаткові подробиці».

Він сказав, що є «докази потенційних збоїв» у керованому підрядником програмному забезпеченні для нарахування заробітної плати, що могло полегшити доступ зловмисникам.

Виступаючи в Палаті громад, тіньовий міністр оборони Джон Хілі назвав IT-гіганта Sopra Steria материнською компанією зламаного програмного забезпечення.

Її дочірня компанія SSCL стверджує, що забезпечує основне обслуговування заробітної плати, кадрів і пенсій для 230 000 військовослужбовців і резервістів і 2 мільйонів ветеранів. Під час допиту Шаппс підтвердив, що йдеться про компанію SSCL.

Консервативні яструби прицілюються

Консервативні депутати-яструби швидко вказали пальцем.

Алісія Кернс, член парламенту від Консервативної партії та голова комітету у закордонних справах, сказала в Палаті громад, що очевидно, що Китай є «ворогом» Великобританії, і вона підштовхнула Шеппса сказати, чи причетний Пекін до цього.

Вона зазначила: «За останні шість тижнів Комуністичну партію Китаю було визнано відповідальною за хакерські атаки на наші збройні сили, кібератаку на виборчу комісію, кібератаки на британських і французьких депутатів, німецького помічника було заарештовано за звинуваченням у шпигунстві. а двох британців було звинувачено в отриманні інформації, корисної для ворога».

Другий яструб Торі в Китаї Ієн Дункан Сміт попередив: «Китай має настільки великий потенціал кібершпигунства, що він затьмарює всіх інших».

Посольство Китаю в Лондоні відповіло у вівторок, назвавши заяви «повністю сфабрикованими та злісними наклепами». Він закликав припинити

«антикитайський політичний фарс» у Великобританії». ***(Noah Keate and Stefan Boscia. Thousands of UK troops hit in suspected Chinese hack on defense ministry // POLITICO (https://www.politico.eu/article/suspected-china-hack-hits-uks-defense-ministry/). 07.05.2024).***

***

«Польща заявила, що вона також була «серед цілей» підконтрольної Росії хакерської групи, яка атакувала Німеччину та Чехію.

«Польща солідарна з Німеччиною та Чехією після зловмисної кіберкампанії проти їхніх політичних партій та демократичних інститутів», - йдеться в заяві МЗС Польщі в п'ятницю.

Уряд Німеччини заявив у п'ятницю, що облікові записи електронної пошти, які належать чиновникам з партії канцлера Німеччини Олафа Шольца, були зламані після атаки, здійсненої хакерською групою APT28 або Fancy Bear. Група входить до складу військової розвідки ГРУ Росії.

Уряд Чехії також опублікував заяву, підтверджуючи претензії Німеччини, заявивши, що його розвідувальна служба виявила вторгнення Fancy Bear в чеські установи приблизно в той же час.

«Польща, яка також є однією з цілей APT 28, рішуче засуджує повторювані та неприйнятні зловмисні кіберкампанії, які проводяться російськими акторами», — йдеться у заяві. Міністерство закордонних справ не надає жодних подробиць щодо нападу». ***(Carlo Boffa. Poland says it too was targeted by Russian hackers // POLITICO (https://www.politico.eu/article/poland-targeted-russia-hackers-germany-czechia-malicious-cyber-campaign/). 04.05.2024).***

***

«Ескалація інцидентів збоїв GPS у регіоні Балтійського моря, пов'язаних в основному з перешкодами та підробкою, що походять з російських територій, викликає серйозне занепокоєння не лише для глобальної навігації та безпеки, але й для сфер кібербезпеки, управління інформацією та

eDiscovery. Ці збої створюють багатогранні виклики, які виходять за рамки безпосередніх ризиків для авіації та морських операцій, торкаючись ширших питань, які є критичними для професіоналів у цих секторах.

Наслідки для кібербезпеки

Перешкоди та підробка GPS свідчать про вразливість, притаманну нашій залежності від цифрових систем зв'язку. Для фахівців з кібербезпеки ці інциденти підкреслюють необхідність надійних протоколів безпеки та розробки стійких систем, здатних протистояти складним формам кібервійни. Здатність захистити навігаційні та комунікаційні технології від перешкод має вирішальне значення для запобігання потенційним каскадним ефектам, які можуть поставити під загрозу критичну інфраструктуру та цілісність даних.

Актуальність управління інформацією

З точки зору управління інформацією, цілісність даних стає сумнівною, коли маніпулюють сигналами GPS. Точність даних про місцезнаходження має першорядне значення в різних секторах, зокрема в юридичному, транспортному та логістичному. Забезпечення автентичності та надійності цих даних має важливе значення для дотримання нормативних вимог і підтримки достовірності цифрових записів. Ці інциденти підкреслюють необхідність посилених заходів для перевірки та підтвердження даних, особливо в середовищах, сприйнятливих до таких збоїв.

Міркування щодо eDiscovery

Для професіоналів eDiscovery маніпулювання даними GPS може мати серйозні наслідки. Дані про місцезнаходження часто відіграють вирішальну роль у судових розглядах, будь то реконструкція подій, встановлення часових рамок або надання доказів у суперечках. Надійність цих даних має вирішальне значення, а підробка GPS ставить під сумнів фундаментальні аспекти збору та представлення цифрових доказів. Професіонали повинні знати про ці потенційні вразливості та враховувати їх під час оцінки достовірності даних, що використовуються в правовому контексті.

Постійні збої в роботі GPS у регіоні Балтійського моря викликають не лише навігаційну проблему, але й серйозну проблему для кібербезпеки, управління

інформацією та eDiscovery. Ці інциденти служать яскравим нагадуванням про взаємопов'язаність сучасних цифрових систем і широкі наслідки їхньої вразливості. Таким чином, вони вимагають скоординованої відповіді від професіоналів у цих дисциплінах для вирішення поставлених проблем і зміцнення систем проти майбутніх загроз». ***(Cyber warfare: GPS disruptions in the Baltic challenge global security // Emerging Europe (https://emerging-europe.com/partner-content/cyber-warfare-gps-disruptions-in-the-baltic-challenge-global-security/). 06.05.2024).***

***

«Компанії повинні переглянути свою стійкість, постачальників, постачальників і плани щодо партнерства з ФБР у разі кіберподії, каже ФБР.

За словами директора ФБР Крістофера Рея, Китайська Народна Республіка (КНР) позиціонує себе для того, щоб «фізично знищити нашу критично важливу інфраструктуру у зручний для неї час».

Рей попередив, що кожен сектор знаходиться під загрозою, оскільки КНР планує порушити критичну інфраструктуру, щоб «викликати паніку та зламати волю Америки до опору». Підкреслюючи масштаби кіберактивності Китаю, Рей зазначив, що масштабна хакерська програма Китаю перевищує програми будь-якої іншої великої країни разом узяті.

Навіть у 2011 році китайські державні хакери атакували операторів нафти та природного газу. Зіткнувшись із приманкою документів-приманок, хакери викрали конфіденційну організаційну інформацію та дані, пов'язані з диспетчерського контролю та збору даних (SCADA мережами). Хакери залишили фінансову та ділову інформацію, що змусило CISA та ФБР зробити висновок, що ці стратегічні вторгнення були частиною плану Китайської Народної Республіки, щоб підготуватися до майбутніх операцій з фізичного пошкодження або іншого зриву трубопроводів.

Рей підкреслив, що кібератаки КНР на критично важливу інфраструктуру США є «широкими та безжальними».

Раніше цього року спонсоровані Китаєм хакери, відомі як Volt Typhoon, атакували критичну інфраструктуру в секторах зв'язку, енергетики, транспорту та водопостачання. Ці зловмисники керували бот-мережею, щоб приховати свою діяльність, оскільки вони використовували методи «життя поза землею», щоб використовувати інструменти в мережах жертв і підтримувати стійкість. ФБР, АНБ і CISA повідомили, що шляхом проникнення в критичну інфраструктуру Народна Республіка Китай міг би використовувати цей доступ до мережі, щоб зруйнувати цілі галузі в рамках своєї стратегії щодо геополітичної напруженості чи військових конфліктів.

Компанії можуть відігравати центральну роль у захисті критичної інфраструктури. ФБР рекомендує такі заходи для співпраці з ФБР і зміцнення захисту США від кібератак КНР:

Планування стійкості: розробіть, перевірте та відпрацюйте план реагування на інциденти, який має включати ідентифікацію коштовностей, наявність плану відновлення та звернення до ФБР за допомогою.

Прозорість апаратного забезпечення та ланцюга постачання: перевіряйте постачальників, їхні практики безпеки та знайте, хто створює апаратне та програмне забезпечення, яке матиме доступ до мережі.

Координація ФБР: зверніться до місцевого офісу ФБР по допомогу, ще до появи ознак проблеми, щоб сприяти готовності компанії». ***(Nathan Salminen and Soojin Jeong. Security Snippets: Critical infrastructure is a key target of China-sponsored hackers // Hogan Lovells (https://www.engage.hoganlovells.com/knowledgeservices/news/security-snippets-critical-infrastructure-is-a-key-target-of-china-sponsored-hackers). 01.05.2024).***

***

«Сполучені Штати засудили зловмисну кібердіяльність Росії, спрямовану проти їхніх європейських союзників, та пообіцяли допомогти з притягненням її до відповідальності.

Джерело: речник Державного департаменту США Метью Міллер заявив у Twitter (X), повідомляє «Європейська правда».

Деталі: Представник Держдепу вказав, що США засуджують «зловмисну кіберактивність, яку здійснює російська військова розвідка проти Німеччини, Чехії, Литви, Польщі, Словаччини та Швеції».

«Ми приєднуємося до зусиль НАТО і ЄС з протидії такій діяльності і притягнення винних до відповідальності», – додав Міллер.

Раніше у п’ятницю ЄС виступив із засудженням зловмисної кіберкампанії Росії проти Німеччини та Чехії.

У НАТО також висловили солідарність з Німеччиною та Чехією у зв’язку з кібератаками, здійсненими російською групою хакерів, та готові розглянути скоординовану відповідь на загрозу.

Міністерство закордонних справ Німеччини 3 травня викликало тимчасового повіреного у справах посольства Росії у відповідь на російську кібератаку на керівну Соціал-демократичну партію, що сталась минулого року». ***(Олег Павлюк, Тетяна Олійник. США допоможуть НАТО і ЄС покарати Росію за кібератаки проти європейських країн // Українська правда (https://www.pravda.com.ua/news/2024/05/3/7454155/). 03.05.2024).***

***

«У вівторок офіційні особи США та Британії попередили про зростаючу кіберзагрозу з боку Китаю, причому кібердиректор Білого дому заявив, що Пекін здатний спричинити хаос у кіберпросторі, а керівник британського шпигунського агентства попередив про «епохальний» виклик.

У Сполучених Штатах і Європі зростає занепокоєння щодо передбачуваної кіберактивності Китаю та шпигунства, але Пекін заперечує ці звинувачення.

«Китай створює справжню та зростаючу кібернебезпеку для Великобританії», — заявила Енн Кіст-Батлер, директор штаб-квартири британського урядового зв’язку (GCHQ) з прослуховування, на конференції з безпеки в центральному англійському місті Бірмінгем.

Вона сказала, що відповідь на дії Пекіна є головним пріоритетом GCHQ, і що примусові та дестабілізуючі дії Китаю загрожують міжнародним нормам.

Прем'єр-міністр Ріші Сунак заявив у понеділок, що Британія зіткнулася з загрозою з боку «осі авторитарних держав, таких як Росія, Іран, Північна Корея та Китай», і британські прокурори висунули звинувачення трьом чоловікам у допомозі службі зовнішньої розвідки Гонконгу у Великій Британії. Китай відкинув цю справу як вигадку.

Британія заявила у вівторок, що викликала посла Китаю, щоб сказати, що кібератаки та повідомлення про зв’язки зі шпигунством є неприйнятними.

Кіст-Батлер, який був призначений головою GCHQ минулого року, повторив Сунака, сказавши, що наступні кілька років будуть небезпечними та трансформаційними.

«Росія та Іран становлять безпосередню загрозу, але Китай є «визначальним для епохи» викликом», – сказала вона.

'СІЯТИ ХАОС'

Національний кібердиректор США Гаррі Кокер заявив на конференції, що китайські військові хакери обходять захист США в кіберпросторі та націлюються на інтереси США в «безпрецедентному масштабі».

«У сценарії кризи чи конфлікту Китай міг би використати свої заздалегідь створені кіберпотенціали, щоб сіяти хаос у цивільній інфраструктурі та стримувати військові дії США», — сказав він.

Минулого місяця офіційні особи США повідомили Пекіну про широкомасштабну кампанію кібершпигунства під назвою «Volt Typhoon», під час якої китайські хакери зламали десятки американських організацій критичної інфраструктури, використовуючи величезну глобальну мережу скомпрометованих персональних комп’ютерів і серверів.

Директор ФБР Крістофер Рей припустив, що це було пов'язано з більш широким наміром Китаю стримати США від захисту Тайваню. Представник міністерства закордонних справ Китаю заявив, що Volt Typhoon не має відношення до уряду Китаю.

Арешт передбачуваних китайських шпигунів і звинувачення в тому, що підтримувані державою Китаю хакери викрали дані британської служби контролю за виборами та провели операції спостереження, посилили напругу у відносинах між Британією та Китаєм.

Минулого місяця Сунак заявив, що китайські державні суб'єкти провели «зловмисні кіберкампанії» проти британських законодавців і британські ЗМІ, посилаючись на урядові джерела, заявив, що Китай стоїть за хакерською атакою платіжної системи британських збройних сил. У Пекіні назвали звинувачення абсурдними.

Речник міністерства закордонних справ Китаю Ван Веньбінь заявив на прес-конференції у вівторок, що Великобританія неодноразово поширювала звинувачення щодо китайських шпигунів і кібератак». ***(Michael Holden, James Pearson. Britain and US sound alarm over growing Chinese cyber threat // Reuters (https://www.reuters.com/world/uk/china-poses-genuine-increasing-cyber-risk-uk-spy-agency-head-says-2024-05-14/). 14.05.2024).***

***

«У Латвії сталася кібератака на телеканали, що транслюються оператором Balticom. Унаслідок цього там показували прокремлівську пропаганду.

Про це повідомляє мовник LSM з посиланням на главу Національної ради з електронних ЗМІ (NEPLP) Івара Аболіньша, передає Укрінформ.

Під час атаки замість телевізійних програм, що ретранслюються компанією, в ефірі йшов пропагандистський контент Кремля — військовий парад у Москві.

Через атаку компанія втратила контроль над телевізійними ретрансляціями. Наразі сервіс iTV відключено, встановлюються обставини того, що трапилося, повідомив Аболіньш.

Це вже другий випадок, коли в результаті кібератаки латвійським глядачам транслювалася прокремлівська пропаганда. На платформі оператора Tet 17 квітня під час 20-хвилинної прямої трансляції українського телеканалу Freedom

транслювалися пісні та пропагандистські кліпи російських виконавців. У Tet тоді пояснили, що такий сигнал каналу Freeedom було отримано із супутника». ***(У Латвії хакери зламали оператора Balticom - по всіх каналах транслювався парад з Москви // Укрінформ (https://www.ukrinform.ua/rubric-world/3861824-u-latvii-hakeri-zlamali-operatora-balticom-po-vsih-kanalah-transluvavsa-parad-z-moskvi.html). 09.05.2024).***

***

«Державні установи Польщі за останній тиждень зазнали кібератак з боку хакерської групи APT28, яку пов'язують із російськими спецслужбами.

Зазначається, що група APT28 пов'язана з Головним розвідувальним управлінням Генштабу Збройних сил РФ (ГРУ).

Кібератаки здійснені шляхом розповсюдження шкідливого програмного забезпечення.

Додамо, що раніше Польща висловила солідарність з Німеччиною та Чехією у зв'язку з кібератаками на їхні демократичні інститути та політичні партії, йдеться в заяві Міністерства закордонних справ Польщі.

«Польща, яка також є однією з цілей атак APT 28, рішуче засуджує неодноразові, неприйнятні та шкідливі дії, що здійснюються в кіберпросторі російськими організаціями», – зазначено в заяві.

В МЗС Польщі не надали подробиць щодо російських кібератак на країну.

«Зіткнувшись із постійним зростанням загроз у кіберпросторі, Польща активно працює над захистом критичної інфраструктури, підвищення стійкості та зміцнення кіберзахист», – повідомили в міністерстві…». ***(Держустанови Польщі атакувала хакерська група, пов'язана з ГРУ Росії // ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "МЕДІАКОМУНІКАЦІЇ" (https://bukvy.org/derzhustanovy-polshhi-atakuvala-hakerska-grupa-povyazana-z-gru-rosiyi/). 08.05.2024).***

***

«…Ще напередодні широкомасштабного нападу експерти з кібербезпеки попереджали західні уряди про те, що Росія використовує Україну як полігон для відпрацювання своїх майбутніх нападів на західні країни.

Відбувалися напади на інформаційну базу аеропортів, банків, енергетичних компаній. Також, як розповів Голосу Америки чеський експерт з кіберзахисту Томаш Флідр, особисті дані українських військових Росія зі самого початку війни у 2014 році використовувала для психологічного впливу на них.

«Ми з групою чеських волонтерів з команди Team4Ukraine їздили на схід України від самого початку російського нападу, коли кібервійна тільки починалася. Тоді Україна зазнала не лише збройного нападу, а і кібернападів. Одночасно відбувалася інформаційна війна та психологічні операції проти військових на фронті», – розповідає чеський експерт.

Тоді на телефонні номери українських військових приходили СМС-повідомлення зі закликами здаватися, не служити "корумпованому режиму", також приходили повідомлення з погрозами за підписом "ДНР". Через три роки, як повідомляв часопис The Wall Street Journal, під час навчань НАТО на півночі Європи Росія почала застосовувати подібну тактику і щодо них.

«В Україні найактивніші російські кібернапади тривали протягом 2014-2015 років, після цього українці вдосконалили свої системи захисту, навчилися жити в умовах кібервійни», – каже Флідр.

За його словами, очікувалося, що з початком повномасштабного нападу Росія посилить і кібернапади, але цього не сталося.

«За ці трохи понад два роки було лише два великих удари – у перший день, 24-го лютого 2022 року, коли росіянам вдалося вивести з ладу супутникову комунікаційну мережу Viasat. Її використовували українські військові, але також і багато інших суб’єктів по цілій Європі. А другий випадок був наприкінці минулого року, коли напали на телефонний оператор Kyivstar», – нагадує експерт.

За його даними, у перебігу війни були ще інші дрібніші напади, але те, що вони не стали катастрофічними для України, означає, що українці, по-перше,

навчилися захищатися за ці роки, а по-друге, що росіяни виявилися непідготовленими до того, щоб використовувати кібернапади як ефективну зброю.

«Це так само як «Київ за три дні». У кібернетичній сфері вони не були готові до війни так само як і у всіх інших», – каже Флідр.

У деяких випадках доходило до комічних історій.

«Вони не могли взятися за серйозні цілі, тому нападали на кого могли – могли напасти на якусь українську піцерію і вивісити на її сторінці гасло «Смерть укро-фашистам!» Складалося враження, що в них «поштучна оплата» – за кількість нападів, все одно на кого», – каже експерт.

Як він пояснює, підготовка до успішного кібернападу триває багато часу.

«Це не виглядає, як у фільмі – десь натиснуть на якусь кнопку і все відразу відключиться, чи запалають лампочки. Підготовка – проникнення в систему, вивчення її, визначення її слабкостей – на це потрібні місяці. Якщо це все не підготувати заздалегідь, то від того, що хтось скомандує «Вперед!» нічого не станеться», – каже фахівець.

Серед нових тенденцій у світі кіберзлочинності він зауважує, що стає дедалі важче визначити відповідальних за напади, бо в авторитарних країнах стирається грань між злочинними групами і державою.

Томаш Флідр каже, що, наприклад, відповідальність за деякі напади взяли на себе різні російські «хактивісти», або, зауважує він, російські спецслужби, які видають себе за «хактивістів». Він пояснює, що на відміну від демократичних країн, де спецслужби працюють під контролем держави, в таких країнах, як Росія чи Китай, кіберзлочинці можуть працювати під захистом держави, на замовлення держави, або ж спецслужби можуть видавати себе за кіберактивістів.

«На прикладі Китаю ми бачимо сильну комерціалізацію сфери розвідки. У Росії розвідка від самого початку була пов’язана з кіберкримінальними групами. Дуже часто було важко розрізнити, де закінчується ФСБ, а починається якась кримінальна банда. А тепер з’явилися комерційні компанії, які часто також мають кримінальне минуле, але тепер вони стали легальними компаніями, які надають послуги з кібербезпеки. А їхніми клієнтами є ФСБ, ГРУ, СВР, чи якісь інші

російські служби розвідки. Тому дуже важко сказати, хто є відповідальний за кібернапади, бо вони сьогодні працюють на ФСБ, а завтра СВР, вчора він був злочинцем, а сьогодні – респектабельний підприємець у сфері ІТ», – пояснює експерт.

Вивчення українського досвіду, яке відбувалося в багатьох західних країнах призвело до того, що і в них почали приділяти більше уваги кіберзахисту, каже Флідр. Бо, як каже чеський експерт, там довго не усвідомлювали, що авторитарні держави ведуть проти них неоголошену війну, а на Україні лише тренуються.

Томаш Флідр вважає, що кроки в напрямку обмеження китайських технологій та соцмереж, які робляться останнім часом, є свідченням про визнання загрози та необхідності протиставити їй системні згуртовані дії». ***(Наталія Чурікова. Україна зазнає менше успішних кібератак росіян, бо навчилася з ними боротися – чеський ІТ-експерт Томаш Флідр // Голос Америки (https://www.holosameryky.com/a/creaky-it-expert-pro-kiberataky/7604614.html). 09.05.2024).***

***

«Виступаючи перед спеціалістами ІТ-індустрії, Блінкен підкреслив, що досвід захисту українських мереж США хотіли б масштабувати по всьому світу.

США та партнери посилили захист українських цифрових мереж на тлі масованих кібератак з боку Росії. Про це заявив Держсекретар США Ентоні Блінкен, виступаючи на конференції RSA у Сан-Франциско, присвяченій кібербезпеці.

«Коли Росія розпочала загарбницьку війну, вона піддала інфраструктуру країни натиску кібератак…. Ми допомогли їм посилити їхні мережі, перенести важливі державні дані в хмару, підвищити стійкість національних комунікацій та іншої критичної інфраструктури», – заявив Блінкен.

Виступаючи перед спеціалістами ІТ-індустрії, Блінкен підкреслив, що досвід захисту українських мереж США хотіли б масштабувати по всьому світу.

Так держсекретар США оголосив про Національну стратегію кібербезпеки, яка передбачає спільну боротьбу із союзниками проти кіберзагроз.

«Ваша (кіберспільноти – ред.) роль як партнерів у цьому – різниця між перемогою та поразкою в технічному змаганні. І це важливо для сприяння становленню більш демократичного світу, де дотримується верховенство права, де диктатори та агресори несуть відповідальність», – підкреслив державний секретар США.

У документі про стратегію кібербезпеки різко критикуються Росія, Китай, Іран і Північна Корея. Ці країни, на думку авторів документу, сприяють безперервним хакерським та шпигунським кампаніям». ***(Держсекретар США: Україні надано підтримку у захисті від кіберзагроз РФ // БлогПост (https://1bpost.com/derzhsekretar-ssha-ukrayini-nadano-pidtrymku-u-zahysti-vid-kiberzagroz-rf/). 12.05.2024).***

***

«Політикам, представникам виборчих органів та іншим особам із високим ризиком у Британії буде запропоновано підтримку, щоб допомогти захистити їх від хакерських атак з боку іноземних шпигунів напередодні виборів, які заплановані наприкінці цього року, повідомили в середу кіберексперти країни.

Британський уряд заявив про зростаючу загрозу демократії з боку людей, які поширюють дезінформацію та підроблений контент, створений штучним інтелектом, іншим державам, які намагаються втрутитися в політичний процес.

Прем'єр-міністр Ріші Сунак і британські керівники служби безпеки попередили, що російська розвідка та групи, пов'язані з китайською державою, намагалися атакувати британські установи та осіб, включаючи законодавців.

У грудні міністерство закордонних справ наклало санкції на двох російських хакерів, які, за його словами, працювали від імені Федеральної служби безпеки Росії (ФСБ), щоб націлити на політиків, журналістів та інші групи, атакуючи їхні особисті скриньки електронної пошти.

Москва заявила, що немає жодних доказів звинувачень у цифровій шпигунській кампанії. У Китаї заявили, що Великобританія неодноразово поширювала звинувачення в китайських шпигунах і кібератаках.

Національний центр кібербезпеки, який є частиною британського шпигунського агентства GCHQ, заявив, що за його оцінками облікові записи кандидатів на виборах і офіційних осіб «майже напевно є привабливими цілями для кіберактрів, які прагнуть здійснювати шпигунські операції».

«Особи, які відіграють важливу роль у нашій демократії, є привабливою мішенню для кіберактрів, які прагнуть порушити чи іншим чином підірвати наше відкрите та вільне суспільство», — сказав Джонатон Еллісон, директор NCSC із національної стійкості та технологій майбутнього.

«Саме тому NCSC посилив нашу підтримку людей, які мають підвищений ризик стати мішенями онлайн, щоб переконатися, що вони можуть краще захистити свої облікові записи та пристрої від атак».

Ті, хто вважається групою ризику, зможуть отримати додатковий рівень безпеки на своїх особистих пристроях, щоб захистити їх від зловмисного програмного забезпечення, фішингу — надсилання електронних листів нібито від надійного відправника, щоб спонукати людей розкрити конфіденційну інформацію — та інших загроз». ***(Politicians and election officials offered cyber protection ahead of UK election // Reuters (https://www.reuters.com/world/uk/politicians-election-officials-offered-cyber-protection-ahead-uk-election-2024-05-15/). 15.05.2024).***

***

«Південна Корея пообіцяла розглянути та підвищити обізнаність про кіберзлочинну діяльність Північної Кореї в Раді Безпеки ООН (РБ ООН), щоб поінформувати інші країни-члени ООН про руйнівний вплив на їхні економіки, а також на міжнародну безпеку.

Це правильний хід правильного гравця.

Кібератаки та їхні шкідливі наслідки – це проблеми, які необхідно швидко та належним чином вирішувати такими країнами, як Південна Корея. Південна Корея

є однією з країн, які постраждали від найбільшої кількості кібератак у світі, тому краще за інших знає, наскільки руйнівними можуть бути наслідки кібератак і чому кібербезпека є важливою.

Хван Чжун Кук, постійний представник Південної Кореї в ООН, заявив, що кібератаки є транснаціональною проблемою, яка потребує глобальних дебатів. «Руйнування основної інфраструктури, викрадення приватної інформації та пограбування віртуальних активів за допомогою кібератак є транскордонними проблемами та становлять серйозну загрозу безпеці для всіх країн», — сказав він під час прес-конференції, що відбулася в його офісі в Нью-Йорку в п’ятницю.

Він оприлюднив план Південної Кореї розпочати просвітницьку кампанію щодо боротьби з кібератаками на порядку денному РБ ООН, оскільки наступного місяця країна збирається взяти на себе ротаційне головування в РБ ООН. Кожна держава-член головує в РБ ООН по черзі протягом одного місяця відповідно до алфавітного порядку їх назв.

Технічно кажучи, Південна Корея мало що може зробити проти кібератак Північної Кореї з її одномісячним головуванням у РБ ООН. Місяць занадто короткий, щоб заручитися підтримкою інших держав-членів ООН для об’єднання зусиль для розробки конкретних заходів для боротьби з незаконною кібердіяльністю.

Однак, незважаючи на обмеження часу, обіцянка Південної Кореї підвищити обізнаність про кібератаки в Радбезі ООН має значення, оскільки деякі країни, включаючи Північну Корею, використовують кібератаки як зброю, щоб порушити роботу своїх ворогів і головної інфраструктури. Як видно з війни в Україні та кількох інших конфліктів, які мали місце в інших частинах світу за останні десятиліття, кібервійна є важливою частиною військових операцій.

У Південній Кореї кібератаки стали частиною повсякденного життя навіть у мирний час. Найгірше те, що багато організацій, як у державному, так і в приватному секторах, навіть не знають, що їх зламали, навіть після того, як їхні системи проникли. Винуватцем у більшості випадків є Північна Корея. Китай і Росія також несуть відповідальність за зловмисні кібероперації в Південній Кореї.

Хакери, пов’язані з російськими військовими, здійснили кібератаки під час церемонії відкриття зимових Олімпійських ігор у Пхенчхані 2018 року. Тим часом китайські хакери створили та керували десятками фейкових новинних сайтів перед виборами до Національної асамблеї 10 квітня для поширення дезінформації.

У п’ятницю SBS повідомила, що північнокорейські хакери здійснили кібератаку на неназване соціологічне агентство на півдні країни в лютому, за кілька тижнів до виборів до Національної асамблеї. Використовуючи вкрадений ідентифікатор адміністратора, вони проникли в систему агентства та марно намагалися викрасти конфіденційну інформацію. Звіт надійшов через кілька днів після повідомлень ЗМІ про зламані електронні листи військового командування. Кібератаки Північної Кореї є поширеними, виходячи далеко за межі крадіжки конфіденційної інформації та збоїв у роботі основних об’єктів.

З 2010-х років Північна Корея віддає перевагу кібератакам, щоб заробити гроші шляхом крадіжок віртуальних активів. Північ, яка перебуває під багатошаровими санкціями, використовує гроші, щоб спонсорувати свої ядерні та ракетні програми. Кібератаки допомагають Північній Кореї продовжувати розробляти та модернізувати свою зброю масового знищення, загрожуючи міжнародній безпеці.

Цей фінансовий стимул спонукав північнокорейських хакерів продовжувати розширювати свої «бізнес-зони» на багато інших країн, допомогвши Північній Кореї заробити приблизно 630 мільйонів доларів у 2022 році.

Незважаючи на те, що кібератаки Північної Кореї стали глобальною загрозою, міжнародне співтовариство реагує на запобігання її зловмисним кібероперація повільно, якщо не взагалі не існує. Південна Корея може зіграти певну роль, щоб спонукати бездіяльну міжнародну спільноту почати притягувати Північну Корею до відповідальності за її зловмисну діяльність у кіберпросторі.

Протягом місячного періоду головування в РБ ООН Південна Корея може поділитися своїм досвідом з іншими державами-членами ООН, щоб поінформувати їх про значні наслідки кібератак Північної Кореї, через які пройшла країна, і залучити їхню підтримку, щоб закласти основу для глобальний режим

кібербезпеки, щоб краще захистити їх від зловмисної кіберактивності». ***(Global cybersecurity regime needed // The Korea Times (https://www.koreatimes.co.kr/www/opinion/2024/05/202_375356.html). 26.05.2024).***

***

«Колишній виконавчий директор Британського національного центру кібербезпеки Кіаран Мартін різко попередив про зростаючі кіберзагрози з боку Китаю, підкресливши, що Сполучене Королівство ігнорує значні зміни в тактиці кібершпигунства Пекіна.

Зауваження Мартіна прозвучали після попередження США на початку цього року, яке виявило, що китайські державні хакери атакують критичні сектори, що стало ключовим моментом у стратегії кібервійни Китаю.

В інтерв'ю The Guardian під час конференції DTX на Manchester Tech Week Мартін наголосив на необхідності підвищеної пильності як у державному, так і в приватному секторах, а також у громадянському суспільстві. Він закликав уряд Сполученого Королівства недвозначно донести до Китаю, що будь-які спроби порушити роботу основної інфраструктури будуть неприпустимими.

За словами Мартіна, вкрай важливо встановити чіткі межі та позначити порушення цивільної інфраструктури червоною лінією.

Підкреслюючи серйозність ситуації, Мартін провів паралелі між кібертактикою Китаю, що розвивається, і тактикою, яку використовує Росія, вказуючи на зсув до стратегій у московському стилі.

Він посилався на квітневе попередження директора ФБР Крістофера Рея, в якому детально описано, як китайські хакери проникли в ключову інфраструктуру США, включаючи телекомунікаційний та енергетичний сектори, з наміром завдати широкомасштабної шкоди.

Мартін зазначив, що хоча такі атаки можуть і не призвести до прямих жертв, вони можуть завдати значної шкоди. Він навів приклад атаки програми-вимагача на Британську бібліотеку, підкресливши потенційні наслідки, якщо подібні атаки відбудуться одночасно на кілька критично важливих установ.

Говорячи про реакцію Великої Британії на кіберзагрози, Мартін привітав розгляд урядом питання про обов'язкове звітування про атаки програм-вимагачів і правила щодо виплати викупу. Він висловив вдячність за серйозність розгляду цих заходів, підкресливши важливість рішучих дій у захисті національних інтересів.

Актуальність попереджень Мартіна підкреслюється нещодавніми інцидентами, включаючи кібератаки, спрямовані на британську організацію, яка спостерігає за виборами, та операції зі спостереження за британськими політиками, які приписують хакерам, яких підтримує Пекін.

У світлі цих подій віце-прем'єр-міністр Олівер Дауден підтвердив зобов'язання уряду вживати рішучих заходів проти будь-яких загроз з боку китайського уряду.

Як професор Школи державного управління Блаватника Оксфордського університету, ідеї Мартіна мають значну вагу в сфері кібербезпеки. Його заклики до посилення готовності та проактивних заходів проти кіберзагроз служать закликом до колективних дій для захисту цифрової інфраструктури Великобританії та національної безпеки». ***(Mehul Reuben Das. UK not heeding how dangerous China's cyber-espionage capabilities are, claims ex-cybersecurity chief // Firstpost (https://www.firstpost.com/tech/uk-not-heeding-how-dangerous-chinas-cyber-espionage-capabilities-are-claims-ex-cybersecurity-chief-13774437.html). 24.05.2024).***

***

«Виступаючи в четвер, Кшиштоф Гавковський сказав, що ці атаки, ймовірно, спрямовані на поширення дезінформації та спрямовані на критичну інфраструктуру.

Він підкреслив постійне зростання кіберзагроз з боку російських і білоруських організацій.

У відповідь на це Польща посилила свої заходи з кібербезпеки, включаючи посилену координацію та спільний центр операцій з кібербезпеки для різних служб безпеки, сказав він.

Це попередження спрямоване проти зростання кіберзагроз для Польщі та інших європейських країн.

Гавковскі, який також є урядовим уповноваженим з кібербезпеки, повідомив про 100-відсоткове зростання хакерських атак у порівнянні з минулим роком, підкреслюючи масштаб і серйозність загрози.

Його коментарі після зустрічі міністрів цифрових технологій ЄС у Брюсселі, де потенційні атаки були ключовою темою обговорення, були зроблені під час інтерв'ю приватному польському мовнику Radio Zet.

За словами Гавковського, очікуваний пік кіберактивності, спрямованої на Польщу та Європу з боку Росії, буде найзначнішим за останні п'ять років.

«У наступні два тижні буде найвищий рівень активності, пов'язаний з різними видами кібератак проти Польщі та Європи, спрямованих з Росії, і найбільший за п'ять років», - попередив він.

Росія має на меті дестабілізувати ситуацію напередодні виборів до ЄС у державах-членах, вважають чиновники по всій Європі.

«Польща, безсумнівно, знаходиться на передовій цього кіберфронту», — сказав Гавковський, перерахувавши «дві ключові сфери: дезінформація та атаки, спрямовані на критичну інфраструктуру».

Незважаючи на те, що Польща розробила надійний захист кібербезпеки, Гавковський наголосив на важливості пильності громадян, застерігши, що державний захист є надійним, але не безпомилковим.

«Держава вас захищає, але ви також повинні бути обережними», - порадив він, підкресливши спільну відповідальність у протистоянні цим загрозам...» ***(Polish gov't minister warns of heightened cybersecurity risks ahead of EU elections // Polskie Radio S.A. (https://www.polskieradio.pl/395/7784/Artykul/3382465,polish-govt-minister-warns-of-heightened-cybersecurity-risks-ahead-of-eu-elections). 123.05.2024).***

***

«У Молдові з 14 травня та протягом наступних днів хакери атакували сайти суспільного телебачення, уряду та міністерств.

Про це повідомляє місцеве видання NewsMaker з посиланням на речника уряду Даніела Воде.

За його словами, співробітники установ встановили програмне забезпечення, розроблене командою Служби інформаційних технологій та кібербезпеки.

Воно перевіряє, хто намагається зайти на сайт: звичайний користувач чи бот, який робить багаторазові спроби входу.

«Якщо спроби входу повторюються, програмне забезпечення блокує робота», — сказав Воде.

Він не уточнив, хто стоїть за кібератаками.

Втім, раніше міністр закордонних справ Міхай Попшой заявив, що російські хакери неодноразово зламували або намагалися зламати сайти держустанов Молдови». ***(Мар'яна Зінченко. У Молдові хакери атакували вебсторінки уряду та суспільного телебачення // «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/34959/2024-05-17-u-moldovi-khakery-atakuvaly-vebstorinky-uryadu-ta-suspilnogo-telebachennya/). 17.05.2024).***

***

«Російські кіберзлочинці майже недоторканні. Протягом багатьох років хакери, що базуються в країні, запускали руйнівні атаки програм-вимагачів проти лікарень, критичної інфраструктури та підприємств, завдаючи мільярдних збитків. Але вони поза досяжністю західних правоохоронних органів і здебільшого ігноруються російською владою. Коли поліція вимикає сервери та веб-сайти злочинців у автономному режимі, вони часто повертаються до злому протягом кількох тижнів.

Тепер дослідники все частіше додають новий вимір до своєї методики підриву: втручаючись у свідомість кіберзлочинців. Відверто кажучи, вони тролять хакерів.

Останніми місяцями західні правоохоронні органи звернулися до психологічних заходів як додаткового способу уповільнити російських хакерів і врізатися в серцевину екосистеми кіберзлочинності. Ці зароджуються психіки

включають спроби підірвати обмежену довіру злочинців один до одного, вбивання тонких клинів між крихким хакерським его і надсилання порушникам персоналізованих повідомлень, що показують, що за ними стежать.

«Ми ніколи не зможемо дістатися до ядра цих організованих злочинних угруповань, але якщо ми зможемо мінімізувати їхній вплив, зменшивши їх здатність до масштабування, тоді це добре», — каже Дон Сміт, віце-президент із дослідження загроз у охоронна фірма Secureworks. «Усі ці дрібниці, які самі по собі можуть не бути вбивчим ударом, усі вони додають тертя», — каже він. «Ви можете шукати тріщини, посилювати їх і створювати подальші розбрат і недовіру, щоб це сповільнило те, що роблять погані хлопці».

Візьміть операцію Кронос. У лютому глобальна операція правоохоронних органів під керівництвом Національного агентства зі злочинності Великої Британії (NCA) проникла в групу програм-вимагачів LockBit, яка, за словами влади, виманила понад 500 мільйонів доларів у жертв, і вимкнула її системи. Слідчі з NCA переробили веб-сайт LockBit про витоки, де він публікував викрадені дані своїх жертв, і використали сайт для публікації LockBit. внутрішньої роботи

Демонструючи контроль і дані, які вони мали, правоохоронні органи опублікували зображення системи адміністрування LockBit і внутрішніх розмов. Слідчі також опублікували імена користувачів і дані для входу 194 «афілійованих» членів LockBit. У травні це було розширено, щоб включити прізвища учасників.

Поліцейська операція також дражнила розкриття «LockBitSupp», головного ідейного органу групи, і заявила, що вони «взаємодіяли» з правоохоронними органами. Громадянину Росії Дмитру Юрійовичу Хорошеву було пред’явлено звинувачення в управлінні LockBit у травні після того, як на вилученому веб-сайті LockBit був опублікований багатоденний годинник зворотного відліку та жирна графіка, в якій він названий організатором групи.

«LockBit пишався своїм брендом і анонімністю, цінуючи ці речі понад усе», — каже Пол Фостер, директор із управління загрозами NCA. «Наша операція зруйнувала цю анонімність і повністю підірвала бренд, відштовхнувши кіберзлочинців від використання їхніх послуг.» NCA стверджує, що ретельно

розглянуло цю операцію, а його зусилля з перебудови сайту LockBit призвели до того, що група стала масово глузувати в Інтернеті, а її бренд став «токсичним» для кіберзлочинців, які працювали з нею.

«Ми визнали, що ізольований технічний збій не обов'язково знищить LockBit, тому наше додаткове проникнення та контроль, а також арешти та санкції в партнерстві з нашими міжнародними партнерами, посилили наш вплив на LockBit і створили платформу для більшої активності правоохоронних органів у майбутнє», — каже Фостер.

Коли учасники LockBit увійшли в системи адміністрування групи, вони отримали персоналізоване повідомлення про те, що органи влади зібрали їх ім'я користувача, деталі гаманця криптовалюти, внутрішні чати та чати з жертвами та IP-адреси. Як зазначили дослідники з фірми з кібербезпеки Analyst1, ці «психологічні тактики» були спрямовані на дві сфери: «репутацію бренду та міжособистісні стосунки між акторами».

Зусилля виходять за рамки видалення LockBit. У квітні столична поліція Лондона порушила роботу LabHost, служби, яка дозволяла шахраям створювати фішингові веб-сайти, щоб обманом змусити людей надати їхні електронні листи та паролі. Близько 800 кримінальним користувачам LabHost поліція надіслала персоналізовані відеоповідомлення з детальним описом «всіх даних, які ми маємо про вас». Були включені країни, де вони націлювалися на жертв, а також IP-адреси, які вони використовували. «Ми спостерігали за вами кожного разу, коли ви були у нас», — говорить голос за кадром у відео.

«Ці повідомлення призначені не лише для існуючих учасників кримінальної екосистеми», — каже Сміт із Secureworks. «Це повідомлення для людей, які, можливо, на межі рішення взяти участь». У розгалуженій екосистемі кіберзлочинності немає великої довіри між злодіями, які можуть виманити один одного на мільйони доларів, але зміцнення та посилення розбіжностей потенційно ускладнює організацію ефективних злочинних компаній.

Важко зрозуміти, який вплив мають психологічні операції, але дослідники кажуть, що злочинці завжди спостерігають. Зі 194 афілійованих осіб LockBit лише

69 повернулися на платформу після дій правоохоронних органів у лютому, повідомляє NCA. За словами дослідників, хакери читали новини та дослідження з кібербезпеки, обговорюючи їх на російськомовних форумах про кіберзлочинність. На форумі XSS є одна тема під назвою «Соковиті арешти», яка нараховує понад 1000 дописів з 2017 року, каже Вікторія Ківілевич, директор із дослідження загроз охоронної фірми KELA, яка стежить за кіберзлочинцями.

За словами Ківілевича, думки користувачів XSS щодо видалення LockBit розділилися. В одному з лютневих повідомлень, каже Ківілевич, кіберзлочинець поставив запитання, чому на той момент не було названо ім’я лідера групи та не застосовано санкції. «У них стільки інформації, вони повинні мати хоча б щось про нього», — йдеться в перекладі допису. «А може, він працює з ними». Інший закликав людей не створювати меми та не жартувати над ситуацією. «Ви розумієте, що в якийсь момент це може торкнутися і вас», — написали вони.

Ківілевич вказує на інші випадки, коли кіберзлочинці на форумах розчаровувалися або були незадоволені тим, що правоохоронні органи атакували деяких учасників. членів груп програм-вимагачів Conti та Trickbot було Коли в лютому 2023 року на застосовано санкції, LockBitSupp запитав, де санкції щодо лідера Trickbot « Стерна » та іншого високопоставленого актора «Baddie». ще 11 членів Conti та Trickbot були Оскільки у вересні 2023 року застосовані до санкцій, через кілька днів після того, як WIRED назвав ім’я одного з учасників, кіберзлочинець поскаржився, що деякі з тих, хто потрапив під санкції, «ніколи не мали високого профілю». Далі вони сказали, що є відчуття «несправедливості»: «Який був сенс додавати довбаних менеджерів, які мало що вирішували в бізнесі».

Андреанн Бержерон, директор відділу досліджень охоронної фірми GoSecure, яка спеціалізується на злочинній поведінці та втручанні поліції, каже, що називати імена одних злочинців може мати два наслідки, а інших — ні. Ті, кого називають, можуть «вважати несправедливим бути покараними, поки інші залишаються на волі», і в результаті можуть співпрацювати з правоохоронними органами або працювати з ними.

Бержерон також каже, що зловмисники часто «жадають визнання» своїх дій. «Коли їхні колеги отримують всю «заслугу», навіть якщо це включає санкції, ці неназвані особи можуть відчувати себе змушеними розкритися, щоб отримати визнання», — каже Бержерон. «Це прагнення до визнання може спонукати їх до ризикованої поведінки, потенційно піддаючи себе владі в їх гонитві за підтвердженням».

Хоча правоохоронні органи можуть використовувати деякі психологічні тактики поряд із більш традиційними технічними видаленнями та санкціями, існують також наукові дослідження, які вивчають способи, якими кіберпсихологія може заважати злочинним хакерам. Дослідницьке агентство розвідувального співтовариства США, Intelligence Advanced Research Projects Activity (Iarpa), розпочало роботу над проектом зі створення нових засобів захисту кібербезпеки, використовуючи людські слабкості зловмисників.

Психологію можна використовувати як спосіб «розуміти, передбачити та впливати» на поведінку кібератак, каже Кімберлі Фергюсон-Волтер, керівник програми Iarpa, яка керує проектом. Дослідження, яке перебуває на початковій стадії, спрямоване на створення інструментів і методів, щоб використати людські слабкості кіберзлочинців на основі встановлених принципів психології. Наприклад, якщо можна змусити зловмисника відчути, що він у безпеці, коли він компрометує систему, він може вдатися до більш ризикованої поведінки та викрити себе.

«Якщо ви можете стримати когось від атаки на вашу мережу, це майже так само добре», — каже Фергюсон-Волтер. «Я думаю, що чим більше вони налякані або невпевнені в тому, як працює захист, тим кращі ваші шанси це зробити». ***(Matt Burgess. Cops Are Just Trolling Cybercriminals Now // Condé Nast (https://www.wired.com/story/cop-cybercriminal-hacker-psyops/?utm_source=flipboard&utm_content=WIRED%2Fmagazine%2FSecurity+News). 28.05.2024).***

***

«У сучасному взаємопов'язаному світі космічна технологія є основою наших глобальних систем зв'язку, навігації та безпеки. Супутники, що обертаються навколо Землі, є ключовими для всього, від GPS-навігації до міжнародних банківських операцій, що робить їх незамінними активами в нашому повсякденному житті та глобальній інфраструктурі.

Однак із зростанням нашої залежності від цих небесних охоронців зростає й їхня привабливість для ворогів, які можуть намагатися скомпрометувати їхню функціональність за допомогою кіберзасобів. Обслуговування супутника може бути перервано, або в гіршому випадку космічний корабель може бути вимкнено. Експансія цифрової сфери в космос відкрила нові кордони для кіберзагроз, створюючи безпрецедентні виклики.

Це поле битви, що розвивається, підкреслює нагальну потребу в надійних заходах кібербезпеки для захисту наших космічних активів від складних атак, які загрожують глобальній стабільності та безпеці.

Недавні кіберінциденти, такі як атака на мережу KA-SAT у 2022 році, підкреслюють безпосередню вразливість супутників. Мережа, що належить глобальному комунікаційному гіганту Viasat, зіткнулася зі складною кібератакою, яка порушила її послуги по всій Європі. Хоча злочинці офіційно не підтверджені, багато хто підозрює причетність Росії.

Оскільки ми є свідками зростання атак, спонсорованих державою, і комерціалізації хакерських інструментів, ставки для захисту космічних активів виходять за межі технічних проблем і охоплюють потенційні порушення світової економіки та дипломатичних відносин між країнами, які керують супутниковими мережами. Нещодавно увагу до космічної безпеки привернуло твердження, що Росія розробляє протисупутникову зброю космічного базування – можливо, ядерну.

Еволюція загроз

Перехід від аналогового до цифрового змінив вразливі місця космічних технологій, наражаючи їх на спектр кіберзагроз. Спочатку, з кінця 1950-х років,

занепокоєння зосереджувалося на фізичному втручанні та шпигунстві, але з розвитком технологій цифрові вразливості стали авангардом проблем безпеки.

Оскільки противники зараз використовують штучний інтелект (ШІ) і машинне навчання для пошуку нових вразливостей, складність атак виходить далеко за рамки традиційних стратегій захисту супутників.

Ранні порушення, такі як злом американо-німецьких супутників у 1998 році, були попередниками складного ландшафту кібербезпеки, який ми маємо сьогодні. Сучасні зловмисники використовують складні методи, щоб використовувати слабкі місця в супутниковому зв'язку та передачі даних, щоб порушити, перехопити або пошкодити безцінні дані, які вони несуть.

Ця еволюція означає кардинальний зсув у тому, як ми повинні підходити до безпеки космічних технологій, підкреслюючи важливість передбачення та пом'якшення цифрових загроз. Це включає наскрізне шифрування, щоб передачу даних було складніше зламати або порушити, а також краще виявлення підозрілої активності до атаки. Однак впровадження цих заходів безпеки вимагає певних витрат, наприклад, обмеження обчислювальної потужності комп'ютера та пропускної здатності.

Вразливі місця в порожнечі

Ізоляція супутників на орбіті та їхня залежність від бездротового зв'язку наражає їх на певні загрози, такі як глушіння сигналу, спуфінг – маскування зв'язку з підозрілого джерела під зв'язок із відомого, надійного джерела – та перехоплення даних.

Крім того, обмеження обчислювальної потужності та пропускної здатності в просторі загострюють проблему впровадження регулярних оновлень програмного забезпечення та виправлень, роблячи системи вразливими для експлуатації.

Уразливості програмного забезпечення в супутникових системах можна використовувати на великих відстанях, дозволяючи зловмисникам потенційно отримати контроль над ними. Ця вразливість ускладнюється постійно зростаючою складністю супутників та їх програмного забезпечення.

Космічна порожнеча не захищає ці активи від кіберсупротивників; натомість це область, повна унікальних проблем. Ці виклики вимагають інноваційних рішень.

У відповідь на ці ескалації кіберзагроз сформувався єдиний фронт серед космічних агентств, технологічних компаній і експертів з безпеки. Ці зусилля спрямовані на розробку надійних захисних механізмів для захисту супутників та інших космічних технологій.

Ключові ініціативи включають створення безпечних протоколів зв'язку, впровадження наскрізного шифрування для передачі даних і розгортання систем виявлення аномалій на основі ШІ для виявлення підозрілої діяльності в супутникових мережах. Окрім ініціатив NASA та Європейського космічного агентства (ESA), інші міжнародні колаборації, що відображають широку прихильність космічній кібербезпеці. набули форми й

Угоди між країнами в розвідувальному альянсі «П'ять очей» (до складу якого входять США, Велика Британія, Канада, Австралія та Нова Зеландія) і партнерство з лідерами приватного сектора в галузі космічних технологій підкреслюють глобальне визнання важливості безпеки космічних активів. Ці спільні зусилля мають вирішальне значення не лише для захисту інтересів національної безпеки, але й для забезпечення безперебійної роботи безлічі послуг, які спираються на космічні технології.

Кіберзахист у космосі

Розробка керованих ШІ протоколів безпеки та квантового шифрування готова зробити революцію в захисті космічних ресурсів.

Безпека, керована штучним інтелектом, пропонує потенціал для прогнозування та протидії кіберзагрозам у режимі реального часу, постійно адаптуючись до нових викликів. Однак ця технологія все ще знаходиться на стадії розробки та стикається зі значними труднощами, включаючи наявність обмежених наборів даних для навчання в унікальному контексті космосу.

Подібним чином квантове шифрування в теорії забезпечує непроникну безпеку, використовуючи галузь фізики, відому як квантова механіка. Але це все ще знаходиться на стадії досліджень і розробок космічних застосувань – практичне

розгортання таких технологій у космосі вимагатиме набагато більше інновацій і випробувань.

Глобальні наслідки

Кібербезпека в космосі виходить далеко за межі технічної сфери, впливаючи на міжнародні відносини, співпрацю та конкуренцію. Існує прагнення до більшого захисту космічної інфраструктури. Міжнародна співпраця була б ідеальною для досягнення цього, але така мета стикається з проблемами через конкуруючі інтереси та різні рівні довіри між націями.

Економічні наслідки кібератак на космічну інфраструктуру є глибокими. Значний кіберінцидент може коштувати мільярдні збитки, порушити глобальні послуги та вимагати значних ресурсів для пом'якшення та відновлення.

Складний взаємозв'язок між необхідністю заходів колективної безпеки, перешкодами на шляху досягнення глобальної співпраці та потенціалом катастрофічних економічних наслідків підкреслює складні взаємозв'язки між кібербезпекою в космосі, міжнародними відносинами та економічною стабільністю.

Прогрес у заходах кібербезпеки в космосі є не просто технічною необхідністю, а й глобальним імперативом для захисту майбутнього дослідження космосу та цілісності критичної космічної інфраструктури. Подолання мінливого ландшафту кіберзагроз вимагає постійної пильності, інновацій та єдиного підходу серед усіх, хто бере участь у космічних польотах». ***(Sylvester Kaczmarek. Cybersecurity for satellites is a growing challenge, as threats to space-based infrastructure grow // GlobalSpec (https://electronics360.globalspec.com/article/21047/cybersecurity-for-satellites-is-a-growing-challenge-as-threats-to-space-based-infrastructure-grow). 12.05.2024).***

***

«Кібератаки на підприємства водопостачання по всій країні стають все більш частими та більш серйозними, попередило Управління з охорони навколишнього середовища в понеділок, коли воно випустило правоохоронне

попередження, закликаючи системи водопостачання вжити негайних заходів для захисту питної води в країні.

Близько 70% комунальних підприємств, перевірених федеральними чиновниками за останній рік, порушили стандарти, призначені для запобігання порушенням або іншим вторгненням, повідомляє агентство. Чиновники закликали навіть невеликі системи водопостачання покращити захист від хакерських атак. Недавні кібератаки груп, пов'язаних з Росією та Іраном, були спрямовані на менші громади.

У попередженні сказано, що деякі системи водопостачання несправні в основних аспектах, включаючи нездатність змінити паролі за замовчуванням або відключити доступ до системи для колишніх співробітників. Оскільки підприємства водопостачання часто покладаються на комп'ютерне програмне забезпечення для роботи очисних споруд і систем розподілу, захист інформаційних технологій і засобів контролю процесів має вирішальне значення, повідомляє EPA. Можливі наслідки кібератак включають перебої в обробці та зберіганні води; пошкодження насосів і клапанів; і зміна хімічних рівнів до небезпечних кількостей, повідомляє агентство.

«У багатьох випадках системи не роблять того, що вони повинні робити, тобто завершити оцінку ризиків своїх вразливостей, що включає кібербезпеку, і переконатися, що цей план доступний і інформує спосіб ведення бізнесу», — заявили в EPA. Заступник адміністратора Джанет Маккейб.

Спроби приватних груп або окремих осіб проникнути в мережу постачальника води та знищити веб-сайти не є чимось новим. Однак нещодавно зловмисники не просто переслідували веб-сайти, вони натомість націлилися на діяльність комунальних служб.

Останні атаки здійснюються не лише приватними особами. Деякі нещодавні хакерські атаки водопровідних служб пов'язані з геополітичними конкурентами та можуть призвести до перебоїв у постачанні безпечної води в будинки та підприємства.

EPA не повідомляє, скільки кіберінцидентів сталося за останні роки, і кількість успішних атак поки що незначна.

Маккейб назвав Китай, Росію та Іран країнами, які «активно шукають можливість вивести з ладу критично важливу інфраструктуру США, включаючи водопостачання та каналізацію».

Наприкінці минулого року пов'язана з Іраном група під назвою «Cyber Av3ngers» націлилася на кілька організацій, у тому числі на постачальника води в невеликому містечку Пенсільванії, змусивши його перейти від віддаленого насоса до ручного керування. Вони шукали пристрій ізраїльського виробництва, який використовувався комунальним підприємством після війни Ізраїлю проти ХАМАС.

Раніше цього року «хактивіст», пов'язаний з Росією, намагався зірвати роботу кількох комунальних підприємств Техасу.

Пов'язана з Китаєм кібергрупа, відома як Volt Typhoon, зламала інформаційну технологію багатьох систем критичної інфраструктури, включаючи питну воду, у Сполучених Штатах і на їхніх територіях, заявили американські чиновники. Експерти з кібербезпеки вважають, що об'єднане з Китаєм угруповання готове до потенційних кібератак у разі збройного конфлікту або зростання геополітичної напруженості.

«Працюючи за лаштунками з цими хактивістськими групами, тепер ці (національні держави) мають правдоподібне заперечення, і вони можуть дозволити цим групам здійснювати деструктивні атаки. І для мене це кардинально змінило правила гри», – сказала Доун Каппеллі, експерт з кібербезпеки компанії Dragos Inc., що займається промисловою кібербезпекою.

Вважається, що світові кібердержави протягом багатьох років проникали в критично важливу інфраструктуру конкурентів, запроваджуючи зловмисне програмне забезпечення, яке могло призвести до порушення основних служб.

Це сповіщення має на меті підкреслити серйозність кіберзагроз і повідомити комунальним службам, що EPA продовжить свої перевірки та притягне цивільні або кримінальні покарання, якщо вони виявлять серйозні проблеми.

«Ми хочемо бути впевненими, що ми розповімо людям: «Гей, ми знаходимо тут багато проблем», — сказав Маккейб.

Запобігання атакам на постачальників води є частиною ширших зусиль адміністрації Байдена щодо боротьби із загрозами для критичної інфраструктури. У лютому президент Джо Байден підписав указ про захист портів США. Системи охорони здоров'я були атаковані. Білий дім підштовхнув електричні підприємства також посилити захист. Адміністратор EPA Майкл Ріган і радник Білого дому з національної безпеки Джейк Салліван попросили штати розробити план боротьби з кібератаками на системи питної води.

«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», — написали Ріган і Салліван у листі всім 50 губернаторам США від 18 березня.

Деякі з виправлень є простими, сказав Маккейб. Постачальники води, наприклад, не повинні використовувати паролі за умовчанням. Їм потрібно розробити план оцінки ризиків, який стосується кібербезпеки, і налаштувати системи резервного копіювання. EPA каже, що вони безкоштовно навчать водопровідні служби, які потребують допомоги. Більші комунальні підприємства зазвичай мають більше ресурсів і досвіду для захисту від атак.

«В ідеальному світі... ми хотіли б, щоб кожен мав базовий рівень кібербезпеки і міг підтвердити, що він є», — сказав Алан Роберсон, виконавчий директор Асоціації державних адміністраторів питної води. «Але це ще далеко».

Деякі бар'єри є фундаментальними. Водний сектор дуже фрагментований. Існує приблизно 50 000 громадських постачальників води, більшість з яких обслуговують невеликі міста. Скромний персонал і анемічні бюджети в багатьох місцях ускладнюють підтримку базового — забезпечення чистою водою та дотримання останніх правил.

«Звичайно, кібербезпека є частиною цього, але це ніколи не було їхнім основним досвідом. Отже, тепер ви просите водопровідне підприємство розробити

цілий новий тип відділу для боротьби з кіберзагрозами, – сказала Емі Хардбергер, експерт з води Техаського технічного університету.

EPA зіткнулася з невдачами. Штати періодично переглядають роботу постачальників води. У березні 2023 року EPA наказав штатам додати оцінки кібербезпеки до цих оглядів. Якщо виявляли проблеми, держава мала змусити покращити.

Але Міссурі, Арканзас і Айова, разом із Американською асоціацією водопровідних заводів та іншою групою водопровідної промисловості, оскаржили інструкції в суді на тій підставі, що EPA не має повноважень відповідно до Закону про безпечну питну воду. Після невдачі в суді EPA відкликало свої вимоги, але закликало штати все одно вжити добровільних заходів.

Закон про безпечну питну воду вимагає від певних постачальників води розробити плани щодо деяких загроз і підтвердити їх виконання. Але його сила обмежена.

«У законі просто немає повноважень щодо (кібербезпеки)», — сказав Роберсон.

Кевін Морлі, менеджер із федеральних зв’язків з Американською асоціацією водопостачання, сказав, що деякі водопровідні підприємства мають компоненти, підключені до Інтернету, що є загальною, але значною вразливістю. Капітальний ремонт цих систем може бути значною та дорогою роботою. І без значного федерального фінансування системи водопостачання намагаються знайти ресурси.

Промислова група опублікувала вказівки для комунальних підприємств і виступає за створення нової організації експертів з кібербезпеки та води, яка б розробила нову політику та забезпечувала її дотримання у партнерстві з EPA.

«Давайте об’єднаємо всіх у розумний спосіб», – сказав Морлі, додавши, що малі та великі комунальні підприємства мають різні потреби та ресурси». ***(Michael Phillis, Matthew Daly. Chinese, Iranian, and Russian gangs are attacking U.S. drinking water and officials are alarmed // Fortune Media IP Limited (https://fortune.com/2024/05/20/chinese-iranian-and-russian-gangs-are-attacking-u-s-drinking-water-and-officials-are-***

alarmed/?utm_source=flipboard&utm_content=geowarner%2Fmagazine%2FDigital+Transformation+AI+ML+Cloud+ChatGPT). 21.05.2024).

***

Кіберзахист закладів охорони здоров'я

«Більш ніж через два місяці після кібер-атаки Change Healthcare у лютому 2024 року галузь охорони здоров'я продовжує боротися з наслідками, створеними значними проблемами, збоями та збоями в роботі лікарень, лікарів, фармацевтів та інших постачальників медичних послуг по всьому світу. І відомий вплив продовжує поширюватися, оскільки нещодавно компанія Change Healthcare, що належить UnitedHealth Group (UHG), підтвердила компрометацію особистої інформації, включаючи захищену інформацію про здоров'я деяких зі своїх 152 мільйонів пацієнтів. Під час нещодавнього звіту про прибутки за перший квартал UHG повідомила, що виплатила понад 6,5 мільярдів доларів тисячам постраждалих провайдерів через програму безвідсоткових позик, а також заявила, що кібератака може коштувати компанії до 1,6 мільярда доларів цього року.

У світлі «безпрецедентного масштабу» кібератаки з метою отримання викупу, Департамент охорони здоров'я та соціальних служб (HHS) публічно оголосив, що проводить розслідування щодо Change Healthcare та UHG, що є прикладом важливості внутрішньої відповідності та заходів безпеки в галузі охорони здоров'я. На додаток до розслідування, яке триває, 1 травня генеральний директор UHG Ендрю Вітті зіткнувся з обома палатами Конгресу, де Change Healthcare критикували за відсутність елементарного контролю безпеки, щоб запобігти початковому злому, а сенатор Рон Вайден (D-OR) заявив, що такий контроль були еквівалентом «Кібербезпека 101» — і де Вітті просили надати конкретні часові рамки, коли пацієнти та постачальники послуг будуть «зроблені цілими», а також коли сторони, які постраждали, будуть ідентифіковані та повідомлені.

Фон

Change Healthcare, постачальник платіжної підтримки для постачальників, аптек і страховиків, має справу з широкою серією атак програм-вимагачів з лютого 2024 року, які призвели до перебоїв у роботі постачальників і аптек у США та призвели до відставання в доставці ліків, що відпускаються за рецептом. Перша атака була пов'язана з операцією ALPHV Blackcat, яка заявила, що вкрала 6 ТБ даних і вимагала викуп у розмірі 22 мільйонів доларів. Change Healthcare нещодавно підтвердила, що заплатила викуп у рамках свого зобов'язання захистити дані пацієнтів від розголошення. Тепер друга група, RansomHub, отримала викрадені дані Change Healthcare, які, як стверджує група, включають «конфіденційні» медичні записи, лікарняні рахунки, платіжну інформацію, номери соціального страхування пацієнтів і контракти компанії з діловими партнерами. Станом на 16 квітня 2024 року зловмисники почали оприлюднювати деякі вкрадені дані та вимагали оплату, щоб запобігти оприлюдненню подальшої інформації.

Чому медичні дані вразливі до атак програм-вимагачів

З 2016 по 2021 рік щорічна кількість атак програм-вимагачів на організації, що надають медичну допомогу, зросла більш ніж удвічі, причому поширеними збоями були простої електронної системи, скасування запланованого лікування та перенаправлення карет швидкої допомоги. Лікарні та інші організації, що мають медичні дані, дуже вразливі до кібератак через колекцію конфіденційної інформації про пацієнтів, а також тому, що системам охорони здоров'я необхідно якомога швидше відновити роботу. Щоб захистити конфіденційну інформацію пацієнтів і відновити надання медичної допомоги, системи охорони здоров'я часто мають більший стимул платити викуп. Звинувачення, висунуті Міністерством юстиції США у 2023 році проти мережі кіберзлочинців, яка ймовірно пов'язана з російською розвідкою, вказують на те, що того року лікарні США заплатили понад 100 мільйонів доларів лише одній організації. Крім того, невеликі лікарні та медичні заклади піддаються особливому ризику, оскільки фінансові та людські ресурси можуть бути недостатньо виділені для захисту інформації про пацієнтів.

Реальні наслідки

У той час як наслідки атаки Change Healthcare продовжують розкриватися, погляд на нещодавні кібератаки на постачальників медичних послуг показує, що наслідки, про які зазвичай повідомляють, тісно пов'язані між собою, а саме, збої в роботі технологій, через які постачальники медичних послуг не можуть переглядати та записувати записи про лікування, подавати замовлення на лікування та рецепти в електронному вигляді., призначати зустрічі та процедури, обробляти претензії, отримувати та передавати платежі та надавати оцінку витрат, що призводить до фінансової нестабільності та операційного блоку в системі охорони здоров'я.

Ця та багато попередніх кібератак підкреслюють необхідність того, щоб сектор охорони здоров'я, особливо ті організації, які обробляють або сприяють транзакціям, ретельно переглядали та діяли відповідно до рекомендацій щодо кібербезпеки від HHS, Американської асоціації лікарень (AHA) та Агентства з кібербезпеки та безпеки інфраструктури. (CISA). Ці агентства ретельно перевіряють поточні вразливості, що впливають на постачальників медичних послуг, і пропонують протоколи захисту від уразливостей, спрямованих на паралізацію платіжних систем, засобів контролю інформаційної безпеки та здатності постачальників медичних послуг надавати допомогу пацієнтам. Узгодження з рекомендаціями агентства не тільки запобіжить або стримає майбутні атаки, але, ймовірно, пом'якшить суворість примусових дій, застосованих такими агентствами після атаки.

Як посилити засоби контролю конфіденційності та безпеки, щоб запобігти зловмисникам

Дотримання як обов'язкових нормативних актів, так і добровільних рекомендацій має вирішальне значення для організацій і постачальників у галузі охорони здоров'я — як для підтримки цілісності, конфіденційності та доступності даних, так і для захисту від серйозних примусових дій у разі успішної атаки. З огляду на те, що на сьогоднішній день було отримано з порушення в системі Change Healthcare, запропоновані засоби контролю включають:

Виявлення перевіреної резервної клірингової палати (тобто посередника) та навіть укладання контракту з нею для участі у випадку, якщо первинна клірингова палата зламана або не працює;

Регулярний перегляд та, у відповідних випадках, впровадження авторитетних галузевих рекомендацій, таких як ті, що опубліковані HHS, AHA та CISA;

Використання створених агентством ресурсів, таких як Інструмент оцінки ризиків безпеки HHS або Набір правил безпеки NIST HIPAA, для забезпечення дотримання Правил безпеки HIPAA;

HHS, що стосуються охорони здоров'я, Впровадження добровільних цілей ефективності кібербезпеки у внутрішніх політиках і практиках кібербезпеки;

Регулярна оцінка практики кібербезпеки постачальників і партнерів, особливо тих, хто обробляє конфіденційні дані про здоров'я, щоб переконатися, що вони відповідають необхідним стандартам безпеки та поточним найкращим практикам;

Оновлення та тестування планів аварійного відновлення та забезпечення безперервності бізнесу для посилення політик і процедур для ключових IT-систем, у тому числі внутрішнього Active Directory, і третіх сторін у разі кібератаки; і

Будьте в курсі тактики, яку використовують певні групи загроз, націлені на сектор охорони здоров'я, наприклад група програм-вимагачів ALPHV Blackcat.

Рекомендації щодо відповідності HIPAA

Відповідність вимогам HIPAA вимагає дотримання численних правил, у тому числі правила безпеки HIPAA, яке встановлює стандарти для захисту електронної особистої інформації про здоров'я (PHI), створеної, отриманої, використаної або збереженої організацією та її діловими партнерами. Правило безпеки вимагає проведення певної оцінки ризиків, щоб підтвердити, що доступ до PHI належним чином обмежено та запобігає несанкціонованому розголошенню, зміні та знищенню.

Крім того, Правило безпеки вимагає від охоплених організацій та їхніх ділових партнерів «[і]запроваджувати політики та процедури для запобігання, виявлення, стримування та усунення порушень безпеки» (45 CFR § 164.308(a)(1)).

Серед інших конкретних вимог цей обов'язковий процес управління ризиками безпеки вимагає аналізу ризиків та огляду діяльності інформаційної системи, що включає оцінку розумно очікуваних ризиків і вразливостей щодо конфіденційності, цілісності та доступності PHI, що зберігається організацією. В рамках своїх свідчень у Конгресі 1 травня Вітті визнав, що хакери отримали доступ до мережі Change Healthcare через скомпрометовані облікові дані, які використовувалися для доступу до сервера компанії, на якому була відсутня багатофакторна автентифікація - відсутність контролю, яку проігнорували аудитори безпеки компанії.

Оскільки вразливі місця в безпеці розвиваються разом із покращенням навичок і можливостей зловмисників, щоб залишатися сумісними та належним чином захищати e-PHI, організації, які охоплюються HIPAA, та їхні ділові партнери повинні переконатися, що їхні існуючі процедури управління ризиками безпеки вимагають регулярних оцінок ефективності та охоплення засобів контролю безпеки, які впроваджуються як охоплена особа, так і її ділові партнери». ***(Jennifer Yoo, Sari Heller Ratican, Ana Razmazma, Blair Mills and Samuel Dodson. Cyber Resilience After the Change Healthcare Breach // Fenwick & West LLP (https://www.fenwick.com/insights/publications/cyber-resilience-after-the-change-healthcare-breach). 03.05.2024).***

***

«Звіт «Аналіз розміру, частки та тенденцій ринку кібербезпеки в охороні здоров'я за видами, типами загроз, кінцевим використанням, регіонами та прогнозами сегментів, 2024 - 2030 рр.» додано до пропозиції ResearchAndMarkets.com.

Очікується, що розмір глобального ринку кібербезпеки охорони здоров'я досягне 56,3 мільярдів доларів США до 2030 року та зросте на 18,5% за прогнозований період. Інтеграція охорони здоров'я та інформаційних технологій призвела до значного прогресу в догляді за пацієнтами, управлінні даними та ефективності роботи. Однак це також піддало галузь зростаючим кіберзагрозам,

зокрема атакам програм-вимагачів і витоку даних, які порушують конфіденційність пацієнтів і порушують роботу медичних послуг.

Згідно зі статтею Health News Florida за лютий 2024 року, аналітики Emsisoft відзначили сплеск кількості кібератак на лікарні: у 2023 році було зареєстровано 46 інцидентів порівняно з 25 у 2022 році. Тим часом злочинні прибутки значно зросли, а середні виплати зросли з дол. 5000 у 2018 році до тривожних 1,5 мільйона доларів США у 2023 році.

Зростання ринку зумовлене регулятивними повноваженнями, зростанням кількості кібератак і поширенням взаємопов'язаних медичних пристроїв і систем. Ринок пропонує різноманітні рішення та послуги, такі як виявлення загроз, шифрування даних, контроль доступу та керування відповідністю, розроблені для захисту конфіденційної інформації та інфраструктури охорони здоров'я. Швидка цифровізація та високий рівень проникнення Інтернету підвищують шанси вразливості галузі охорони здоров'я до кібератак через цінні дані. Сектор став свідком численних кібератак. Наприклад, згідно з оновленням TechTarget, Inc. за січень 2024 року, понад 112 мільйонів людей постраждали від витоку даних у сфері охорони здоров'я, про які у 2023 році повідомили понад 540 організацій до Міністерства охорони здоров'я та соціальних служб США (HHS).

Крім того, нещодавно відбулися кібератаки на Департамент охорони здоров'я Ірландії та Виконавчу службу охорони здоров'я (HSE), включно з керованою людиною атакою програм-вимагачів Conti, яка серйозно вивела з ладу системи HSE, що призвело до завершення роботи більшості інших систем. Федеральне бюро розслідувань (ФБР) і Агентство з кібербезпеки та безпеки інфраструктури (CISA) випустили попередження щодо ескалації атак, відзначивши понад 400 кібератак програм-вимагачів Conti у США та по всьому світу. Крім того, очікується, що технологічний прогрес у розробці продуктів для боротьби з кібератаками та захисту даних сприятиме зростанню ринку. Наприклад, у листопаді 2023 року CyberCatch, Inc. запустила рішення Healthcare Compliance Manager, яке допомагає організаціям охорони здоров'я дотримуватися найновіших практик кібербезпеки галузі охорони здоров'я від Міністерства охорони здоров'я та

соціальних служб США. Це рішення націлено на зростаючу загрозу кібератак на сектор охорони здоров'я, яка вражає понад 26 000 організацій.

Основні моменти звіту про ринок кібербезпеки охорони здоров'я

Залежно від типу рішення, сегмент антивірусного та шкідливого програмного забезпечення домінував на ринку та мав частку доходу понад 25,8% у 2023 році завдяки зростанню впровадження таких рішень у закладах охорони здоров'я. Це пов'язано зі збільшенням кількості атак зловмисного програмного забезпечення в галузі охорони здоров'я, які можуть призвести до зупинки лікарняних мереж, що вплине на лікування пацієнтів.

Виходячи з типу загрози, сегмент зловмисного програмного забезпечення домінував на ринку та приніс найбільшу частку доходу – близько 25,7% у 2023 році. Атака програм-вимагачів є широко використовуваним типом зловмисного програмного забезпечення через обізнаність і переваги хакерів щодо програм-вимагачів.

Очікується, що в Азіатсько-Тихоокеанському регіоні ринок буде свідком прибуткового зростання протягом прогнозованого періоду через збільшення впровадження та проникнення Інтернету в індустрію охорони здоров'я

Виходячи з кінцевого використання, сегмент лікарень мав найбільшу частку доходу — близько 62,6% у 2023 році. Лікарні надзвичайно вразливі до кібератак, оскільки вони зберігають неймовірну кількість даних пацієнтів. Крім того, ці атаки зросли під час пандемії, загрожуючи особистим даним і догляду за пацієнтами

У 2023 році Північна Америка домінувала на ринку та отримала найбільшу частку доходу понад 30,0% завдяки наявності ключових гравців і розширенню сфери застосування кібербезпеки в організаціях охорони здоров'я…» ***(Healthcare Cyber Security Market Analysis 2024 // GlobeNewswire (https://www.globenewswire.com/news-release/2024/05/16/2883552/0/en/Healthcare-Cyber-Security-Market-Analysis-2024.html). 16.05.2024).***

***

«Дослідницький проект вартістю 50 мільйонів доларів має на меті спростити оновлення різноманітних комп'ютерних систем, що використовуються в лікарнях, підвищивши їхній захист від програм-вимагачів та інших ризиків безпеки.

Агентство перспективних дослідницьких проектів США з питань охорони здоров'я (ARPA-H) запустило проект, який воно назвало програмою Universal PatchinG and Remediation for Autonomous DEfense (що скорочується до Upgrade).

Він спрямований на фінансування створення інструментів, які полегшать оновлення та захист IT-систем у лікарнях, які часто важко підтримувати в актуальному стані, що дає можливість зловмисникам проникнути.

«Особливо складно змоделювати всю складність програмного забезпечення, що використовується в даному закладі охорони здоров'я, і це обмеження може зробити лікарні та клініки винятково відкритими для атак програм-вимагачів», — сказав керівник програми Upgrade Ендрю Карні.

Незважаючи на розмір індустрії кібербезпеки, проблеми в секторі охорони здоров'я залишаються «недорозв'язаними», навіть якщо до мережі під'єднано більше обладнання, ніж будь-коли раніше, повідомляє ARPA-H, відносно нова агенція США, яка прагне фінансувати інновації в охороні здоров'я.

Програма спрямована на створення автономної системи для надання «проактивних, масштабованих і синхронізованих оновлень безпеки». Ця програмна платформа запропонує змодельовану оцінку впливу потенційної вразливості та адаптується до будь-якого лікарняного середовища на широкому спектрі звичайних пристроїв, повідомляє агентство.

«Програма спрямована на зменшення невизначеності та ручних зусиль, необхідних для забезпечення безпеки лікарень, гарантуючи, що вразливе обладнання буде відремонтовано, і дозволяючи персоналу зосередитися на догляді за пацієнтами», — йдеться в повідомленні». ***(Steve Ranger. Healthcare cyber attacks have surged in 2024 — this new program aims to improve security // Future US, Inc. (https://www.itpro.com/security/healthcare-cyber-attacks-have-surged-in-2024-this-new-program-aims-to-improve-security). 23.05.2024).***

***

«Управління охорони здоров'я перших націй Британської Колумбії проводить розслідування після атаки на систему кібербезпеки.

Орган охорони здоров’я, який називає себе першим і єдиним провінційним органом у своєму роді в Канаді, каже, що 13 травня йому стало відомо про «незвичайну діяльність» у його корпоративній мережі.

У ньому сказано, що «неавторизовану особу» було перехоплено після отримання доступу до мережі.

Орган охорони здоров’я каже, що є докази того, що це вплинуло на певну інформацію про працівників і обмежену особисту інформацію інших.

Проте в ньому сказано, що немає доказів того, що атака вплинула на будь-які клінічні інформаційні системи, які він використовує.

Ця кібератака є останньою в серії недавніх інцидентів у Британській Колумбії, хоча органи охорони здоров’я кажуть, що жодних ознак зв’язку немає.

У ньому йдеться, що про це повідомили правоохоронні органи та Управління комісара з питань інформації та конфіденційності Британської Колумбії.

Раніше в цьому місяці прем'єр-міністр Девід Ебі заявив, що провінція виявила «складні інциденти кібербезпеки» за участю державних мереж.

В інших нещодавніх випадках хакери, націлені на бібліотеки Британської Колумбії, намагалися отримати інформацію користувачів для отримання викупу, тоді як роздрібний продавець London Drugs закрив усі свої магазини в Західній Канаді більше ніж на тиждень, щоб усунути порушення кібербезпеки.

Цей звіт The Canadian Press було вперше опубліковано 22 травня 2024 року». ***(First Nations Health Authority in B.C. investigating cybersecurity incident // yahoo! news (https://ca.news.yahoo.com/first-nations-health-authority-b-014719079.html). 23.05.2024).***

***

«Зараз у нас є обліковий запис майже для будь-чого. Від одноразового замовлення продукту до наших щоденних акаунтів у соціальних мережах.

Це просто означає, що ще важливіше стежити за своєю кібербезпекою та переконатися, що будь-кому, хто намагається отримати доступ, буде якомога складніше.

«Будь-хто, хто має обліковий запис у соціальних мережах або електронній пошті, може стати мішенню для шахраїв або кібератак», — попередила Полін Сміт, керівник відділу Action Fraud.

«Захистіть свою інформацію, переконавшись, що ваші паролі електронної пошти та соціальних мереж безпечні та відрізняються від усіх ваших інших паролів».

Останнім людям, яких закликають вжити заходів, є користувачі Google Gmail, а також інші власники облікових записів електронної пошти, яких закликають змінити свої паролі. Відповідно до нещодавнього звіту Red9, багато хто з нас все ще використовує слабкі паролі, такі як «пароль», «qwerty» і «123456».

Настав час відмовитися від слабких паролів і покращити свою кібербезпеку. Зрештою, ваша електронна пошта є шлюзом до ваших інших облікових записів у соціальних мережах, а також містить конфіденційну інформацію.

Action Fraud зазначає на своїй сторінці безпеки: «Паролі вашої електронної пошти та соціальних мереж мають бути надійними та відрізнятися від усіх ваших інших паролів.

«Поєднання трьох випадкових слів, кожне з яких щось для вас означає, — чудовий спосіб створити пароль, який легко запам’ятати, але важко зламати».

З’ясувати, де зберігати всі різні паролі, може бути трохи головним болем, але, на щастя, такі компанії, як Apple, пропонують програмне забезпечення, яке зберігає всі паролі в одному безпечному місці.

За даними Центру звітності про кіберзлочинності Великобританії, щоб додати додатковий рівень безпеки та захистити свої облікові записи, доцільно додати 2-етапну перевірку (2SV) до всіх ваших облікових записів в Інтернеті.

Ваш пароль має бути вашою першою лінією захисту, а не єдиною.

Action Fraud пояснює: «Ви також можете налаштувати двоетапну перевірку для додаткового рівня безпеки.

«2SV працює, запитуючи додаткову інформацію, щоб підтвердити вашу особу.

«Наприклад, отримання коду, надісланого на ваш телефон, коли ви входите за допомогою нового пристрою або змінюєте налаштування, наприклад пароль. Вас не запитуватимуть про це кожного разу, коли ви перевірятимете свою електронну пошту чи соціальні мережі.

Застереження щодо 2SV полягає в тому, що ви не повинні нікому ділитися кодом, оскільки це перешкоджає його призначенню.

Хакери були зафіксовані за допомогою тактики, яка називається ланцюговим зломом на платформі. Кіберзлочинці отримують контроль над обліковими записами людей після того, як обманом змушують їх надіслати свої коди автентифікації.

«Це коли шахрай отримує контроль над обліковим записом і починає видавати себе за законного власника», — йдеться в повідомленні Action Fraud.

«Мета полягає в тому, щоб переконати людей розкривати коди автентифікації, які надсилаються їм через текстове повідомлення. Багато жертв цього типу злому вважають, що це друг надсилає їм повідомлення, однак спільний код був пов’язаний з їхнім власним обліковим записом, і тепер імітатор може використовувати його для доступу до свого облікового запису». ***(Rebekah Jordan. Millions of Gmail users to take action today or risk a very costly error // UNILAD (https://www.uniladtech.com/news/millions-of-gmail-users-take-action-today-avoid-error-539929-20240401?utm_source=flipboard&utm_content=user%2FUNILADTech). 01.05.2024).***

***

«Проти JP Morgan Chase & Co. подано колективний позов, стверджуючи, що фінансовий гігант не вжив адекватних заходів безпеки, що призвело до розкриття конфіденційних особистих даних його клієнтів.

Бенджамін Валентайн, колишній співробітник залізниці Лонг-Айленду, подав скаргу, стверджуючи, що його особисту інформацію було отримано неналежним чином під час нещодавнього витоку даних JP Morgan, який скомпрометував облікові записи тисяч користувачів.

Витік даних JP Morgan скомпрометував тисячі користувачів

Згідно з документами, поданими до окружного суду США Південного округу Нью-Йорка 3 травня, справа Валентина детально описана в груповій скарзі (справа 1:24-cv-03438-JLR). У позові стверджується, що JP Morgan, значний гравець у фінансовій індустрії, який пропонує широкий спектр послуг мільйонам клієнтів, не зміг належним чином захистити особисту інформацію співробітників своїх клієнтів, що призвело до істотної шкоди.

У скарзі Валентина описано, як JP Morgan збирала та зберігала конфіденційну особисту інформацію (PII) співробітників своїх клієнтів, включаючи імена, адреси, платіжні дані та номери соціального страхування. Ця інформація, яка має вирішальне значення для фінансових операцій і безпеки, була скомпрометована в результаті витоку даних JP Morgan і потрапила в руки кіберзлочинців.

У позові стверджується, що внаслідок порушення Валентайн і приблизно 451 000 інших постраждалих осіб зазнали відчутної шкоди, включаючи вторгнення в приватне життя, крадіжку особистих даних, а також втрату довіри та цінності їх особистої інформації. Більше того, порушення наразило їх на постійні ризики шахрайства та подальшого зловживання їхніми даними.

Судовий позов проти JP Morgan

У судовому позові також стверджується, що неспроможність JP Morgan запровадити адекватні заходи кібербезпеки та її необачне поводження з конфіденційними даними безпосередньо сприяли порушенню. Незважаючи на заяви JP Morgan про те, що злом не був результатом кібератаки, у позові

стверджується, що недбалість компанії зробила її мішенню для таких зловмисних дій.

Скарга Валентина підкреслює нібито відсутність прозорості та своєчасного сповіщення JP Morgan про порушення, через що постраждалі особи не були поінформовані про першопричину та вжиті заходи для виправлення. в позові Це, як стверджується, посилює емоційні та фінансові труднощі, які зазнають жертви.

Cyber Express звернувся до організації, щоб дізнатися більше про цей витік даних JP Morgan. Однак JP Morgan не надав офіційної заяви щодо кіберінциденту. Після інциденту нормативна заявка показала, що порушення сталося через проблему програмного забезпечення, яку компанія вирішила негайно після виявлення.

Валентин шукає різні форми правового захисту через позов, включаючи компенсацію збитків, судову заборону та відшкодування судових витрат. Його інтереси представляє юридична фірма Milberg Coleman Bryson Phillips Grossman LLC, розташована в Гарден-Сіті, Нью-Йорк.

У міру розгортання судового процесу The Cyber Express уважно стежитиме за ситуацією, і ми оновимо цю публікацію, коли отримаємо більше інформації про витік даних або будь-які нові оновлення щодо судового процесу». ***(Ashish Khaitan. Data Breach Victim Initiates Class Action Lawsuit Against J.P. Morgan for Security Lapses // The Cyber Express (https://thecyberexpress.com/j-p-morgan-data-breach/?utm_source=flipboard&utm_content=TheCyberExpress%2Fmagazine%2FThe+Cyber+Express+by+Cyble). 08.05.2024).***

***

«Більше організацій, ніж будь-коли, стикаються з порушеннями кібербезпеки, які ставлять під загрозу особисту інформацію людей, причому освіта є одним із найбільш постраждалих секторів згідно з тенденціями Офісу комісара з інформації (ICO).

У 2023 році в ICO було повідомлено про понад 3000 кіберзломів, причому найбільше інцидентів повідомили про освіту (11 відсотків), фінанси (22 відсотки), роздрібну торгівлю (18 відсотків) і сектори.

У звіті ICO проаналізовано звіти про порушення даних, отримані ним, і поділилися уроками, які можна винести з типових помилок безпеки.

Юрист Хейс Коннор проаналізував дані ICO та виявив, що минулого року більш ніж одне з трьох порушень у сфері освіти та догляду за дітьми стосувалися даних дітей.

Дослідження показало, що основні персональні дані були найпоширенішим типом даних, які порушуються в галузі освіти та догляду за дітьми (85 відсотків), за якими йдуть дані про здоров'я (29 відсотків).

Аналіз показав, що двома головними причинами витоку даних у секторі були дані, надіслані електронною поштою неправильному одержувачу, і несанкціонований доступ до даних.

Стівен Боннер, заступник комісара з регуляторного нагляду в ICO, сказав: «Люди повинні бути впевнені, що організації роблять усе можливе, щоб захистити їх особисту інформацію. У той час як кібератаки стають все більш витонченими, ми виявляємо, що багато організацій не реагують належним чином і все ще нехтують самими основами кібербезпеки».

Він сказав, що немає «єдиного рішення» для запобігання кібератакам, але немає жодного виправдання відсутності базових засобів контролю». ***(Education one of worst affected sectors by cyber security breaches // PSi (https://educationbusinessuk.net/news/10052024/education-one-worst-affected-sectors-cyber-security-breaches). 10.05.2024).***

***

«Європейська рада із захисту даних («EDPB» — орган ЄС, якому доручено сприяти послідовності та співпраці у забезпеченні виконання GDPR), окреслила свою стратегію на 2024-2027 роки.

Стратегія побудована на чотирьох основних стовпах: (i) посилення гармонізації та сприяння відповідності; (ii) зміцнення спільної культури правозастосування та ефективної співпраці; (iii) забезпечення захисту даних у цифровому та кросрегуляторному ландшафті, що розвивається; та (iv) внесок у глобальний діалог щодо захисту даних.

EDPB має намір зосередитися на зміцненні співпраці правоохоронних органів та ініціації скоординованих дій правозастосування. Він також спрямований на інтеграцію прав захисту даних у ширшу нормативну базу за допомогою вказівок щодо перетину захисту даних і набору нових цифрових правил, які є частиною стратегії ЄС «Цифрове десятиліття» (таких як Закон про штучний інтелект, Закон про цифрові ринки та Закон про цифрові послуги).

Висновок: Стратегія EDPB на наступні три роки відображає зміну нормативно-правового ландшафту в ЄС. На початку дії GDPR пріоритетом EDPB було надання вказівок щодо GDPR. У своїй останній стратегії EDPB визнає свою зростаючу роль «посередника» між національними регуляторами даних і потребу в тому, щоб вона розвивала свої вказівки, щоб враховувати перетину нових нормативних актів ЄС, що регулюють цифровий простір.

FTC шукає повноважень для подання власних позовів споживачів, отримання грошових винагород за рішенням суду

Федеральна торгова комісія Сполучених Штатів (далі — «FTC» або «Комісія») нещодавно опублікувала звіт для Конгресу відповідно до Закону FTC про співпрацю від 2021 року, у якому детально описано її співпрацю з правоохоронними органами штату та рекомендовано законодавчі ініціативи для посилення подальшої співпраці. Звіт FTC містить три розділи, із розділом «Законодавчі рекомендації щодо посилення зусиль співпраці», який є найбільш помітним, оскільки він просить Конгрес розширити повноваження FTC щодо справ про цивільне покарання та справедливу грошову допомогу.

По-перше, FTC закликала Конгрес відновити повноваження FTC відповідно до розділу 13(b) Закону про FTC безпосередньо отримувати за рішенням суду справедливу грошову компенсацію, таку як реституція або звільнення від суб’єктів

її розслідування. Верховний суд Сполучених Штатів скасував ці повноваження у своєму рішенні у справі AMG Capital Management проти Федеральної торгової комісії від 2021 року, вважаючи, що розділ 13(b), який дозволяє FTC звертатися до суду, щоб отримати «тимчасовий заборонний наказ або попередню судову заборону», не дозволив самій Комісії отримати грошову компенсацію за рішенням суду. У своїй заяві щодо звіту голова FTC Ліна Хан охарактеризувала цю зміну як «важливу» для забезпечення того, щоб «порушники закону не отримували прибутку від порушення закону та щоб жертви незаконної поведінки були зцілені».

По-друге, Федеральна торгова комісія звернулася до Конгресу з проханням скасувати існуючу вимогу щодо передачі цивільних покарань до Міністерства юстиції США (DOJ). Ця зміна дозволить FTC подавати власні позови з вимогами цивільних санкцій без попередньої консультації з Міністерством юстиції. У звіті стверджується, що незалежний орган, який вимагатиме цивільних санкцій, оптимізує правозастосовні можливості FTC і покращить здатність Комісії захищати споживачів від несправедливих або оманливих дій чи практик.

Висновок: останніми роками FTC прийняла більш агресивний підхід до правозастосування, і це лише посилить ці зусилля. Багато хто в індустрії вже вважає, що FTC значно перевищує свої примусові заходи. Якби Конгрес задовольнив прохання FTC і відновив свої повноваження щодо отримання справедливої грошової компенсації за рішенням суду та порушував справи, пов’язані з цивільними покараннями, без необхідності передавати ці справи до Міністерства юстиції, FTC мала б значно більше повноважень і можливостей видавати грошові штрафів, ніж зараз.

Точність даних у контексті GenAI - Регулятор даних Великобританії шукає коментарі щодо проекту вказівок

Управління комісара з питань інформації Великої Британії («ICO») розпочало новий етап у своїй поточній серії консультацій щодо питань захисту даних, пов’язаних із генеративним ШІ. Цей третій етап зосереджується на принципі, що персональні дані мають бути точними – «принцип точності». ICO раніше консультувався щодо навчання генеративного штучного інтелекту на даних,

зібраних з Інтернету, і визначення цілей, для яких персональні дані можуть використовуватися в контексті генеративного штучного інтелекту.

ICO наголошує, що мета, з якою використовується генеративна модель ШІ, є критичною для цілей принципу точності, і закликає розробників вживати заходів, щоб запобігти використанню їхніх генеративних систем ШІ для цілей, несумісних із рівнем точності. виходів ШІ. Наприклад, система штучного інтелекту, призначена для використання виключно в творчих цілях, може не мати рівня точності, необхідного для того, щоб використовувати цю систему для прийняття рішень щодо окремих осіб або для отримання інформації про людей. ICO також вважає, що компанії, які розгортають генеративний штучний інтелект сторонніх розробників, несуть відповідальність за те, щоб генеративний штучний інтелект не використовувався у спосіб, який суперечить принципу точності.

Висновок: наразі у Великій Британії немає еквівалента Закону ЄС про штучний інтелект, закон про захист даних забезпечує ключову основу для регулювання ШІ. Серія консультацій і рекомендації ICO на сьогоднішній день також демонструють, що ICO вважає ШІ пріоритетом. Точність особистих даних у результатах штучного інтелекту є важливою проблемою для розробників штучного інтелекту, розробників і користувачів. Компанії, які використовують генеративний штучний інтелект, захочуть зрозуміти обмеження на використання, накладені їхніми постачальниками, а також заходи, які гарантують, що кінцеві користувачі використовують штучний інтелект лише для цілей, які відповідають рівню точності залучених персональних даних. Поточні консультації ICO відкриті для відповідей до 10 травня 2024 року.

Регулятор даних Великобританії публікує рекомендації щодо прозорості в охороні здоров'я та соціальному забезпеченні

Офіс уповноваженого з питань інформації Великобританії («ICO») видав інструкції для організацій, які займаються наданням медичної та соціальної допомоги у Великобританії. Наголошуючи на чутливості персональних даних, що обробляються в контексті охорони здоров'я та соціального забезпечення, керівництво надає поради для окремих секторів щодо дотримання вимог захисту

даних щодо прозорості та зміцнення довіри до систем охорони здоров'я та соціального забезпечення.

Керівництво приймає пропорційний підхід, визнаючи, що в медичному закладі можуть виникнути обставини, коли надання конфіденційної інформації може не бути пріоритетом (наприклад, у разі невідкладної допомоги). Керівництво також пояснює, що, хоча деякі способи використання персональних даних можуть бути очевидними для пацієнтів, для інших видів використання можуть знадобитися додаткові кроки для надання інформації про конфіденційність, наприклад, використання персональних даних для вторинних цілей (наприклад, медичні дослідження).

Висновок: Керівництво ICO надає практичні та детальні пояснення його очікувань щодо прозорості для організацій, які беруть участь у наданні послуг охорони здоров'я чи соціальної допомоги або обробці даних охорони здоров'я та соціальної допомоги. ICO підкреслює, що дотримання принципу прозорості відповідно до GDPR Великобританії не обмежується наданням конкретної інформації про конфіденційність, яка перерахована в GDPR Великобританії. Відповідно до ICO, прозорість, зокрема у сфері охорони здоров'я та соціального забезпечення, передбачає більш комплексний підхід, який виходить за рамки публікації повідомлення про конфіденційність на веб-сайті організації. Це залежатиме від контексту, але може включати такі дії, як публікація політичної документації, надання якої не вимагається відповідно до GDPR Великобританії.

Білий дім/HHS опублікували правила конфіденційності HIPAA для підтримки конфіденційності охорони репродуктивного здоров'я

22 квітня 2024 року Білий дім і Управління з прав людини Департаменту охорони здоров'я та соціальних служб США («HHS») оголосили Правило щодо конфіденційності HIPAA для підтримки конфіденційності охорони репродуктивного здоров'я («Правило»). Правило посилює існуюче правило конфіденційності в Законі про перенесення медичного страхування 1996 року («HIPAA»), яке забороняє певне розголошення захищеної інформації про здоров'я окремих осіб, пов'язаної із законним обслуговуванням репродуктивного здоров'я.

За словами секретаря HHS Ксав'єра Бесерри, Правило захищає осіб, «які шукають законної медичної допомоги з питань репродуктивного здоров'я, незалежно від того, чи надається ця допомога в їхньому рідному штаті, чи вони повинні перетнути межі штату, щоб отримати її». Згідно з Правилом, Управління громадянських прав HHS керуватиме та забезпечуватиме захист, який забороняє постачальникам медичних послуг, планам медичного обслуговування, кліринговим центрам охорони здоров'я та їхнім діловим партнерам використовувати або розголошувати захищену інформацію про здоров'я пацієнта для: (1) «здійснення кримінальної, цивільної, або адміністративне розслідування чи накладення кримінальної, цивільної чи адміністративної відповідальності на будь-яку особу за просте звернення, отримання, надання або сприяння медичній допомозі щодо репродуктивного здоров'я, якщо така медична допомога є законною за обставин, за яких вона надається;» або (2) для ідентифікації «будь-якої особи з метою проведення такого розслідування або покладення такої відповідальності».

Висновок: Правило є реакцією на зростання занепокоєння з приводу обміну інформацією про охорону репродуктивного здоров'я та потенційного негативного впливу, який такий обмін може мати на рішення людей щодо охорони здоров'я. Оскільки суди та державні органи на всіх рівнях продовжують боротися з проблемою охорони репродуктивного здоров'я, особливо у світі після Доббса, компанії, які обробляють інформацію про здоров'я, повинні бути надто пильними у дотриманні чинних законів і правил, а також у моніторингу можливих законодавчих і нормативних змін». ***(Brenda R. Sharton, Timothy C. Blank, Kevin F. Cahill, Olaf Fasshauer, Vernon L. Francis, Paul Kavanagh, Laura Rossi and Benjamin Sadun. Key Developments in Privacy & Cybersecurity // Dechert LLP (https://info.dechert.com/27/18775/may-2024/dechert-cyber-bits---issue-54(1).asp?sid=20169a8d-6746-4997-8e21-5509cf4bb2e5). 02.05.2024).***

***

«З-поміж популярних месенджерів найбільші ризики для конфіденційності користувачів існують у Телеграмі, тому розробляється спеціальний сервіс для мінімізації небезпеки.

Про це розповів аналітик ГО «Аналітичний центр Інформаційних ресурсів» Богдан Соломикін під час презентації в Укрінформі «Захист кіберпростору: які рішення та розробки вже працюють в Україні. Яких заходів ще потрібно вжити, аби протидіяти Росії?».

За словами експерта, все, що потрапляє в інтернет, може з'явитись у відкритому доступі, і найбільш уразливим у цьому сенсі є Телеграм.

«Саме в Телеграмі ми вбачаємо найбільшу небезпеку серед популярних месенджерів. Ми бачимо там багато вразливостей, і багато з них ніколи не зникнуть, бо вони є частиною екосистеми. Тобто, вони використовуються для цілком легального функціонала, але його можна використати не тільки у звичайних цілях. І наш ворог цим теж дуже добре користується», - зазначив Соломикін.

Тож Аналітичний центр інформаційних ресурсів розробляє сервіс, який мінімізує ризики користування Телеграмом.

«Сервіс дозволяє перевірити налаштування приватності свого Телеграму, дає рекомендації, як налаштувати Телеграм, щоб мінімізувати ризик втратити свої дані. У цьому застосунку на цей час можна пройти один етап, а їх там буде декілька. Перший етап стосується перевірки налаштувань приватності. Тобто будь-яка інформація, можливість відправити вам повідомлення з незнайомого номера, можливості додати вас в групу або отримати ваш телефон — може бути використано проти вас», - розповів Соломикін.

Він додав, що буде доступний і другий етап цієї перевірки, який стосуватиметься не тільки Телеграму, а витоку персональних даних узагалі.

За його словами, частково цю розробку вже використовують українські військові.

«Частину цього сервісу вже використовують наші Сили оборони, але ми хочемо відкрити його для цивільних, щоб показати, як можна цілком легально у відкритому доступі отримати інформацію - імена, адреси, пошта, історію ваших

замовлень, банківські дані, кредитну історію. Все це може бути доступно в інтернеті, й насправді там цього дуже багато. Люди не розуміють, наскільки все погано з цим. Найближчим часом ми презентуємо такий сервіс і пропагуватимемо його для використання», - сказав Соломикін.

ГО «Аналітичний центр інформаційних ресурсів» має низку розробок, які вже застосовуються для захисту кіберпростору України. Зокрема, програмне забезпечення, яке дозволяє військовим отримувати дані з російських гаджетів. Представники ГО позиціонують свою організацію як своєрідний RND-центр для аналітики та кібероперацій і організацію безпекових рішень для користувачів». ***(В Україні фахівці розробляють сервіс мінімізації ризиків користування Телеграмом // Укрінформ (https://www.ukrinform.ua/rubric-society/3862309-v-ukraini-fahivci-rozroblaut-servis-minimizacii-rizikiv-koristuvanna-telegramom.html). 10.05.2024).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Google продовжує боротися з кіберзлочинністю і залучає до цього ШІ. У компанії розповіли про новий інструмент Google Threat Intelligence, який використовує Gemini AI, щоби прогнозувати та запобігати майбутнім кібератакам. Інструмент використовує потужності штучного інтелекту, щоб розшифровувати небезпечні шкідливі програми. Окрім цього він пропонує спосіб розв’язання проблем, пов’язаних з хакерською атакою чи ураженням комп’ютерними вірусами.

Використовуючи для роботи інструменту версію Gemini Pro 1.5, компанія сканує велику кількість даних про кіберзагрози. Модель ШІ здатна швидко аналізувати код шкідливого програмного забезпечення та надавати інформацію щодо рішення проблеми.

Представники компанії Google запевняють, що Gemini Pro може повністю декомпілювати код такого комп'ютерного вірусу, як WannCry за 34 секунди. Окрім цього штучний інтелект здатен повністю зупинити його поширення.

Окрім штучного інтелекту, Google також використовує досвід Mandiant для розробки подібних інструментів. У компанії сподіваються, що Google Threat Intelligence допоможе мільйонам користувачів уникнути кіберзагроз». ***(Букач Ірина. Google використовує Gemini AI для виявлення шкідливих програм // techinfo.com.ua (https://techinfo.com.ua/1807-google-vykorystovuie-gemini-ai-dlia-vyiavlennia-shkidlyvykh-prohram/). 08.05.20.24).***

***

«Уряд Великобританії опублікував добровільні рекомендації, спрямовані на те, щоб допомогти розробникам і постачальникам штучного інтелекту захистити моделі від злому та потенційного саботажу.

Опублікований у середу кодекс практики ШІ британського уряду містить такі рекомендації, як моніторинг поведінки системи ШІ та виконання тестування моделі.

«Організації у Великій Британії стикаються зі складним ландшафтом кібербезпеки, і ми хочемо переконатися, що вони мають впевненість у застосуванні штучного інтелекту у своїй інфраструктурі», — сказав міністр ШІ та інтелектуальної власності Джонатан Кемроуз.

Уряд Великої Британії заявив, що компаніям слід посилити безпеку ланцюга поставок штучного інтелекту та зменшити потенційні ризики від вразливих систем штучного інтелекту, таких як втрата даних. Керівництво рекомендує такі заходи, як придбання безпечних компонентів програмного забезпечення, включаючи моделі, фреймворки або зовнішні API, лише від перевірених сторонніх розробників і забезпечення цілісності навчальних даних, отриманих із загальнодоступних джерел.

«Особливу увагу слід приділяти використанню моделей з відкритим вихідним кодом, де відповідальність за підтримку та безпеку моделі стає складною», — йдеться в інструкції.

Інші заходи включають навчання розробників штучного інтелекту безпечному кодуванню, наявність захисних огорож для різних моделей штучного інтелекту та можливість інтерпретувати та пояснювати моделі штучного інтелекту.

Уряд Великобританії має намір перетворити керівництво на глобальний стандарт для сприяння безпеці за проектом у системах ШІ. У рамках плану уряд відкрив консультацію, запрошуючи відповіді до 10 липня.

Під час листопадового саміту консервативний уряд пообіцяв наполягати на спільному глобальному підході до безпеки штучного інтелекту.

Рекомендації з'явилися лише через кілька днів після того, як Інститут безпеки штучного інтелекту Великобританії випустив платформу оцінки моделей штучного інтелекту під назвою Inspect, яка дозволяє стартапам, академічним колам і розробникам штучного інтелекту оцінювати конкретні можливості окремих моделей і виставляти оцінку на основі їх результатів...» ***(Akshaya Asokan. UK Government Publishes AI Cybersecurity Guidance // Information Security Media Group, Corp. (https://www.databreachtoday.com/uk-government-publishes-ai-cybersecurity-guidance-a-25255?utm_source=flipboard&utm_content=rhudaur%2Fmagazine%2FCybersecurity+Today). 16.05.2024).***

***

«Вплив генеративного штучного інтелекту охопив найрізноманітніші сектори, і серед них не можна не згадати кібербезпеку, сферу, де штучний інтелект, навіть генеративний, може дуже допомогти. Насправді IT-команди та експерти з безпеки вже деякий час намагаються не відставати від зростаючої складності IT-інфраструктури та рішень безпеки. Вони ефективні, але не схожі на звичайні антивіруси, які просто працюють у фоновому режимі. Платформи безпеки генерують десятки тисяч подій на день, блокуючи навіть підозрілі дії та віддаючи

пріоритет найбільш критичним попередженням, але потім люди повинні проаналізувати вказані події (а їх досить багато) і зрозуміти, які з них справжні.погрози і які з них є помилковими тривогами.

З цієї причини компанії, що спеціалізуються на безпеці, роками інвестували в рішення, здатні автоматизувати ці процеси, щоб зняти більшу частину роботи та дозволити експертам зосередити свою увагу на фактично актуальних подіях. Складна робота, ідеальна для систем штучного інтелекту, які, крім того, що вони набагато швидші за людину, мають ще одну перевагу: вони здатні виявляти ті кореляції, які часто вислизають від людей. Корпорація Майкрософт, яка інвестує значні кошти в штучний інтелект (зокрема, OpenAI), нещодавно надала в Італії свій другий пілот Microsoft Copilot for Security для підтримки команд безпеки...

Microsoft Copilot for Security — це генеративне рішення ШІ, яке використовує модель GPT-4 OpenAI у поєднанні з моделлю безпеки, розробленою самою Microsoft. Дані, які його живлять, - це саме ті 78 трильйонів сигналів, які щодня отримують зонди компанії. Як згадувалося, це допомагає швидше й ефективніше виявляти спроби атак і реагувати на них. Але також для розуміння вразливостей, які можуть бути присутніми в інфраструктурі, або для аналізу потенційно шкідливих сценаріїв і автоматизації звітів. Перш за все, це вирішує одну з головних проблем галузі: труднощі з пошуком компетентного персоналу, таким чином зменшуючи дефіцит навичок і брак талантів.

На сьогоднішній день Copilot for Security в Італії вже застосовано такими великими компаніями, як Intesa Sanpaolo, Fincantieri, RINA, De Nora, які мали можливість випробувати його в попередній версії та виявили збільшення продуктивності. Зокрема, ці клієнти «знайшли здатність швидше виявляти загрози, мати кращий огляд поверхні атаки» та опитувати системи більш простим та інтуїтивно зрозумілим способом, ставлячи запитання природною мовою. І саме ця остання можливість є значним плюсом, враховуючи те, що можливість «діалогувати» з системами дозволяє швидше набувати навичок безпеки, «підвищувати рівень».

Microsoft Copilot for Security можна використовувати в автономному режимі, схожому на ChatGPT, щоб надати практичний приклад, або інтегрувати в самі програми, як-от Defender XDR, схоже на те, що вже траплялося з іншими копілотами, наприклад, інтегрованими в Microsoft 365. Дозволяючи IT-командам працювати дедалі швидше та точніше, завдяки новим даним, якими живиться цей ШІ». ***(A tu per tu con Microsoft: Copilot for Security, l'intelligenza artificiale generativa a supporto della cyber sicurezza // Hardware Upgrade (https://edge9.hwupgrade.it/news/security/a-tu-per-tu-con-microsoft-copilot-for-security-l-intelligenza-artificiale-generativa-a-supporto-della-cyber-sicurezza_126799.html). 14.05.2024).***

***

«У нинішню епоху цифровізації кібербезпека стала головним пріоритетом для компаній, незалежно від їх розміру та природи. Зі зростанням залежності від цифрової інфраструктури та даних захист від кіберзагроз став вирішальним для забезпечення безперебійної роботи бізнесу. Однак мінлива природа кібератак створює значні проблеми для традиційних заходів безпеки.

Саме тут штучний інтелект (ШІ) стає кардинальним фактором, пропонуючи значні переваги та невід'ємні ризики для кібербезпеки.

Бізнес-цінність ШІ в кібербезпеці

Штучний інтелект зробив революцію в кібербезпеці, доповнивши традиційні заходи безпеки розширеними можливостями для виявлення, запобігання та реагування на кіберзагрози. Давайте заглибимося в важливі бізнес-цінності, які штучний інтелект привносить у кібербезпеку:

1. Покращене виявлення та запобігання загрозам:

Рішення безпеки на основі штучного інтелекту (ШІ) змінили те, як компанії справляються із загрозами безпеці. Ці рішення ефективно аналізують значний мережевий трафік, журнали активності користувачів і дані подій безпеки в реальному часі. На відміну від традиційних систем, заснованих на правилах, штучний інтелект може ідентифікувати тонкі шаблони та кореляції, що вказують на

потенційні загрози, включаючи атаки розподіленої відмови в обслуговуванні (DDoS) або внутрішні загрози.

Рішення безпеки на основі штучного інтелекту використовують складні алгоритми для обробки та аналізу величезних обсягів даних, таким чином виявляючи та прогнозуючи потенційні кіберзагрози в режимі реального часу. Завдяки активному пошуку вразливостей і прогнозуванню векторів атак штучний інтелект дозволяє компаніям бути на крок попереду кіберзлочинців. ШІ також може допомогти компаніям визначити та визначити пріоритетність ризиків безпеки, дозволяючи їм ефективно розподіляти ресурси для їх пом'якшення.

2. Покращена операційна ефективність:

Оскільки обсяг і складність кіберзагроз постійно зростають, організації звертаються до автоматизації на основі штучного інтелекту, щоб допомогти своїм командам безпеки йти в ногу з цифровою трансформацією. Автоматизуючи звичайні завдання безпеки, автоматизація на основі штучного інтелекту дає змогу спеціалістам із безпеки людей зосередитися на більш стратегічних ініціативах, таких як виявлення нових загроз і розробка нових протоколів безпеки, щоб залишатися попереду.

Однією з найбільших переваг автоматизації на основі штучного інтелекту є її здатність оптимізувати процедури реагування на інциденти. Коли відбувається кібератака, кожна секунда на рахунку, і чим швидше організація зможе відреагувати, тим менше часу простою та фінансових наслідків вона матиме. Завдяки автоматизації процедур реагування на інциденти організації можуть мінімізувати час, необхідний для виявлення та реагування на кібератаку, зменшуючи ризик втрати даних та інших негативних наслідків.

Окрім скорочення часу реагування на інциденти, автоматизація на основі штучного інтелекту оптимізує операції безпеки, виявляючи шаблони та аномалії в мережевому трафіку та виявляючи потенційні загрози до того, як вони стануть повномасштабними атаками. Це допомагає організаціям ефективніше розподіляти ресурси безпеки, максимізуючи віддачу від інвестицій у команди безпеки.

Автоматизація на основі штучного інтелекту має вирішальне значення для організацій, які прагнуть залишатися конкурентоспроможними та безпечними в сучасному динамічному цифровому середовищі. Використовуючи штучний інтелект, організації можуть залишатися на випередженні, зменшити ризик кібератак і захистити свої цінні дані та активи від потенційних загроз.

3. Проактивне реагування на інциденти та відновлення:

У нещасливому випадку кібератаки важливо швидко й ефективно реагувати, щоб мінімізувати збитки. На щастя, технологія ШІ може значно прискорити процес реагування на інциденти. Аналізуючи дані зі зламаних систем, ШІ може швидко визначити ступінь атаки та допомогти її стримати. Крім того, штучний інтелект може допомогти з судово-медичною експертизою та аналізом першопричин, дозволяючи компаніям отримати уявлення про те, як стався злом, і вжити превентивних заходів, щоб уникнути майбутніх атак. ШІ в кібербезпеці може допомогти підприємствам уникнути потенційних загроз і захистити свої цінні активи.

Ризики ШІ в кібербезпеці

Оскільки штучний інтелект все більше інтегрується в кібербезпеку, організації повинні усвідомлювати його потенційні ризики. Хоча штучний інтелект може революціонізувати кібербезпеку, виявляючи та пом’якшуючи загрози ефективніше, ніж будь-коли, він також може створювати нові вразливості, якщо його не впровадити належним чином. Організації повинні усунути ці ризики та вжити відповідних заходів, щоб забезпечити безпечне та ефективне використання ШІ в їхніх стратегіях кібербезпеки.

1. Уразливості в системах ШІ:

За останні роки технологія штучного інтелекту (AI) досягла значного прогресу, але створює потенційні ризики для безпеки. Кіберзлочинці можуть використовувати слабкі місця в алгоритмах штучного інтелекту або навчальних даних, щоб маніпулювати засобами захисту та здійснювати складні кібератаки. Як наслідок, організації повинні надавати пріоритет безпеці моделей ШІ. Цього можна досягти шляхом впровадження безпечних практик кодування та надійного

контролю доступу, щоб зменшити ризик використання зловмисниками. Підприємства можуть захистити свої системи від кіберзагроз і витоків даних, вживаючи профілактичних заходів для захисту моделей ШІ.

2. Упередженість і дискримінація:

Важливо зазначити, що алгоритми штучного інтелекту іноді можуть виявляти упередження в даних, які використовуються для їх навчання. Це може призвести до дискримінаційних результатів у рішеннях щодо безпеки, що призведе до несправедливого профілювання або помилкового визнання законної діяльності як зловмисної. Організації повинні використовувати різноманітні та неупереджені навчальні набори даних, щоб мінімізувати такі упередження. Крім того, їм рекомендується впроваджувати процеси для виявлення та пом'якшення потенційних упереджень у рішеннях безпеки на основі ШІ. Таким чином вони можуть переконатися, що їхні системи безпеки є чесними та вільними від будь-яких ненавмисних упереджень.

3. Відсутність прозорості:

Використання штучного інтелекту в кібербезпеці було благом для організацій, але потреба в більшій прозорості в процесі прийняття рішень щодо штучного інтелекту викликала занепокоєння щодо довіри та підзвітності. Часто користувачам потрібно зрозуміти причини сповіщень безпеки, згенерованих ШІ, що викликає скептицизм і сумніви. Для вирішення цієї проблеми було розроблено Explainable AI (XAI), щоб підвищити прозорість у процесі прийняття рішень AI. Однак організаціям необхідно надати пріоритет розробці інтерпретованих моделей штучного інтелекту для додатків безпеки, що дозволить користувачам зрозуміти обґрунтування сповіщень безпеки, створених штучним інтелектом, і надати механізми оскарження рішень.

Збалансування цінності бізнесу та ризику

Важливо збалансувати бізнес-цінність ШІ та пов'язані з ним ризики. Рекомендується, щоб організації застосували збалансований підхід, щоб гарантувати отримання максимальної вигоди від ШІ при мінімізації потенційних ризиків. Цей підхід повинен враховувати різні фактори, такі як тип і обсяг даних,

що обробляються, рівень автоматизації на місці та потенційний вплив штучного інтелекту на загальну безпеку організації. Застосовуючи збалансований підхід, організації можуть ефективно використовувати штучний інтелект для посилення захисту своєї кібербезпеки, одночасно зменшуючи ризики витоку даних, порушення конфіденційності та інші проблеми безпеки.

1. Встановіть комплексну політику та рамки:

Розробка комплексної політики та інфраструктури кібербезпеки має важливе значення для ефективного та відповідального впровадження рішень безпеки на основі ШІ. Ці політики мають стосуватися безпеки даних, керування моделлю та відповідального розвитку штучного інтелекту, щоб забезпечити відповідність цілям організації та нормативним вимогам. Політика безпеки даних повинна включати шифрування, контроль доступу та моніторинг. Типова політика управління має забезпечувати неупереджені дані та уникати збереження упереджень або дискримінації. Відповідальна політика розвитку штучного інтелекту має забезпечувати етичний і прозорий розвиток і відповідальність за дії.

2. Постійний моніторинг і аудит моделей ШІ:

Щоб забезпечити надійність моделей штучного інтелекту, важливо постійно їх контролювати та перевіряти. Цього можна досягти, проводячи регулярні оцінки вразливості та тестування на проникнення для виявлення будь-яких потенційних слабких місць безпеки. Крім того, рекомендується впроваджувати перевірки справедливості, щоб пом’якшити упередженості в рішеннях щодо безпеки на основі ШІ. Дотримуючись цих кроків, організації можуть переконатися, що їхні моделі штучного інтелекту функціонують ефективно та приймають чесні та неупереджені рішення.

3. Інвестуйте в досвід кібербезпеки:

Кібербезпека стала ключовим аспектом бізнес-операцій, оскільки технологічний прогрес продовжує змінювати світ. Штучний інтелект (ШІ) може революціонізувати те, як організації захищають свої цифрові активи. Однак важливо зазначити, що штучний інтелект сам по собі не може гарантувати повну безпеку. Щоб ефективно використовувати інформацію про безпеку, згенеровану

штучним інтелектом, важливо інвестувати в досвід кібербезпеки. Незважаючи на те, що штучний інтелект може надати цінну інформацію, людське судження та нагляд залишаються вирішальними для інтерпретації сповіщень системи безпеки та прийняття обґрунтованих рішень на основі інформації ШІ. Застосовуючи ці стратегії, підприємства можуть покращити свою кібербезпеку, одночасно зменшуючи пов'язані з цим ризики. Загалом, штучний інтелект і людський досвід доповнюють один одного і необхідні для ефективної кібербезпеки.

Висновок

Штучний інтелект надає величезні можливості для підвищення кібербезпеки, дозволяючи організаціям швидше виявляти загрози, автоматизувати завдання та покращувати реагування на інциденти. Однак важливо визнати ризики, пов'язані зі штучним інтелектом, включаючи вразливі місця, упередженість і відсутність прозорості, і розглянути їх. Застосувавши відповідні заходи безпеки та збалансований підхід, компанії можуть використовувати весь потенціал штучного інтелекту для захисту своїх цінних активів у сучасному середовищі цифрових загроз. У міру розвитку технології штучного інтелекту вона, безсумнівно, відіграватиме ключову роль у поточній боротьбі з кіберзлочинністю, роблячи її незамінним інструментом для компаній у всьому світі». ***(Chirag Shah. Cyber security and artificial intelligence -- business value and risk // BetaNews, Inc. (https://betanews.com/2024/05/18/cyber-security-and-artificial-intelligence-business-value-and-risk/). 18.05.2024).***

***

Кіберзлочинність та кібертероризм

«Федеральне бюро розслідувань, Агентство національної безпеки та Державний департамент США опублікували спільне попередження щодо кібербезпеки щодо хакерських атак на електронну пошту, що фінансуються державою, які обходять заходи безпеки автентифікації.

Зловмисників ідентифікували як хакерську групу APT43, пов'язану з військовою розвідкою Північної Кореї. APT43, також відомий як Kimsuky, використовує обхід автентифікації електронної пошти як засіб видавання себе за журналістів, дослідників та інших науковців у рамках скоординованих фішингових кампаній, спрямованих на «надання вкрадених даних і цінної геополітичної інформації режиму Північної Кореї шляхом компрометації політики аналітиків та інших експертів». Спільна порада щодо безпеки рекомендує всім особам, відповідальним за свій домен електронної пошти, звідки надходить електронна пошта, будь то в особистій чи організаційній якості, негайно зробити одне: оновити свою автентифікацію повідомлень на основі домену, звітність і захист відповідності. політики.

Спільне консультування з кібербезпеки розкриває подробиці хакерської кампанії Північної Кореї

У Спільній консультації з кібербезпеки JCSA-20240502-001 агентства національної безпеки та розвідки попереджають не лише тих, хто може стати потенційною мішенню, але й усіх користувачів електронної пошти про небезпеку північнокорейської зловмисної хакерської групи Kimsuky, яка спонсорується державою. Кімсукі, як частина кіберпрограми військової розвідки Північної Кореї, має завдання допомагати підтримувати «постійний доступ до поточних розвідувальних даних про Сполучені Штати, Південну Корею та інші країни, що представляють інтерес, щоб перешкоджати будь-якій політичній, військовій чи економічній загрозі для безпеку та стабільність режиму», – вважають автори JCSA.

Зокрема, групою APT43/Kimsuky керує, так би мовити, 63-й науково-дослідний центр військової розвідки Північної Кореї, який відомий розвідувальним службам США з 2012 року. Основна місія Kimsuky, здається, полягає в тому, щоб скомпрометувати такі експертні цілі, як як політичні аналітики, щоб отримати дані, що пропонують цінну геополітичну інформацію. У такому випадку ви можете подумати, чому це попередження ФБР має хвилювати когось іншого? Простіше кажучи, кожна успішна атака, навіть найпростіша з фішингових кампаній, може допомогти створювати кращі атаки, які ще не відбудуться. Зокрема, створення

найбільш достовірних електронних листів під час фішингових атак, які зосереджуються на цінних цілях, які зберігають найбільш конфіденційні дані. Чому це має вас турбувати, окрім очевидних міркувань національної безпеки, це метод, який використовують зловмисники, який може використовувати ваші неправильно налаштовані параметри автентифікації електронної пошти.

Неправильно налаштовані записи DMARC дозволяють зловмисним спуферам електронної пошти Free Reign

Автентифікація повідомлень на основі домену, звітування та відповідність — одна з тих речей, про які більшість користувачів електронної пошти ніколи не чули, але кожен із власним сервером електронної пошти справді повинен це зробити. Існує причина того, що Google нещодавно запровадив нові правила автентифікації електронної пошти, згідно з якими неавтентифіковані повідомлення від масових відправників на адреси Gmail повертатимуться невідкритими. Ця причина полягає в тому, щоб зменшити кількість спаму та, у свою чергу, зменшити ймовірність того, що цей спам передаватиме шкідливий вміст користувачам Gmail. Хоча кампанії підманного фішингу не запускають обмеження щодо відправників Gmail, зловмисники Kimsuky обходять ту саму технологію автентифікації. То як вони це роблять?

Що таке DMARC?

По-перше, вам потрібно розуміти, що DMARC — це протокол безпеки, який дає змогу серверу електронної пошти, що отримує, знати, чи надійшла електронна пошта з місця, на яке вона претендує. Іншими словами, DMARC засвідчує, що повідомлення не було підроблено, але надійшло від особи або, принаймні, домену електронної пошти організації, як він стверджує. Насправді це дуже добре робити, за винятком випадків, коли це не так. Політика DMARC вказує серверу електронної пошти, що отримує, що робити з цим повідомленням після першої перевірки, що пов’язана структура політики відправника та записи автентифікації DomainKeys Identified Mail збігаються. Саму політику DMARC можна налаштувати так, щоб надсилати електронний лист до папки "Вхідні" одержувача, позначати його як спам або повністю відхиляти.

Використання політики безпеки DMARC Anatia

Тут на допомогу приходить Кімсукі. Вони використовують той факт, що багато політик DMARC залишили порожніми або позначили як такі, що не потрібно виконувати жодних дій, якщо електронний лист не проходить тести, оскільки існує модифікатор ap=none, який показує відсутність політики. Сам JSAC містить низку реальних прикладів електронних листів, надісланих Kimsuky. Після попередження про те, що кампанії Kimsuky розпочнуться з широкого етапу розвідки, у повідомленні зазначається, що «вміст електронних листів із раніше зламаних облікових записів електронної пошти» також використовується для підвищення автентичності спілкування. Kimsuky створюватиме підроблені імена користувачів, але використовуватиме законні доменні імена, щоб підробити людей із таких організацій, як аналітичні центри та вищі навчальні заклади. Ці електронні листи надходять не з справжнього домену організації, а з електронної адреси та домену, контрольованих хакерами. А все через відсутність політики DMARC.

Зробіть це 1 річ зараз, щоб зменшити загрозу атаки на Кімсукі, закликає ФБР

Консультація ФБР і АНБ закликає всіх користувачів електронної пошти дотримуватися однієї поради щодо пом’якшення наслідків, яка може допомогти запобігти успіху таких атак. Ця порада є продовженням нещодавніх кроків Google щодо захисту користувачів служби Gmail від спамерів, вимагаючи, щоб масові електронні листи використовували захист автентифікації домену.

Нові правила Gmail заслуговують на схвалення, але ФБР і АНБ порадили всім користувачам електронної пошти негайно вжити одну дію: оновити політику безпеки DMARC для себе або вашої організації.

Для цього вам слід переконатися, що ваша політика DMARC, яку можна редагувати в налаштуваннях DNS вашого домену електронної пошти, є однією з двох конфігурацій: “v=DMARC1; p=quarantine», яка вказує серверу електронної пошти відправляти в карантин електронні листи, які не пройшли перевірку DMARC, як спам або «v=DMARC1; p=reject», який повідомляє серверу відхилити або заблокувати електронний лист. Якщо ви користуєтеся лише веб-службою,

такою як Gmail, і не адмініструєте власний домен організації, то вам не варто турбуватися. Однак усім іншим слід звернутися до своєї команди IT або веб-хостингу та переконатися, що політику DMARC налаштовано належним чином.

«Спеарфішинг продовжує залишатися основою кіберпрограми КНДР, — сказав директор відділу кібербезпеки АНБ Дейв Любер, — і цей CSA надає нові відомості та засоби пом'якшення, щоб протистояти їхній торгівлі».

Нові правила Gmail заслуговують на схвалення, але ФБР і АНБ порадили всім користувачам електронної пошти негайно вжити одну дію: оновити політику безпеки DMARC для себе або вашої організації.

Для цього вам слід переконатися, що ваша політика DMARC, яку можна редагувати в налаштуваннях DNS вашого домену електронної пошти, є однією з двох конфігурацій: «v=DMARC1; p=quarantine», яка вказує серверу електронної пошти відправляти в карантин електронні листи, які не пройшли перевірку DMARC, як спам або «v=DMARC1; p=reject», який повідомляє серверу відхилити або заблокувати електронний лист. Якщо ви користуєтеся лише веб-службою, такою як Gmail, і не адмініструєте власний домен організації, то вам не варто турбуватися. Однак усім іншим слід звернутися до своєї команди IT або веб-хостингу та переконатися, що політику DMARC налаштовано належним чином.

«Спеарфішинг продовжує залишатися основою кіберпрограми КНДР, — сказав директор відділу кібербезпеки АНБ Дейв Любер, — і цей CSA надає нові відомості та засоби пом'якшення, щоб протистояти їхній торгівлі». ***(Davey Winder. New FBI Warning As Hackers Strike: Email Senders Must Do This 1 Thing // Forbes (https://www.forbes.com/sites/daveywinder/2024/05/08/new-fbi-warning-as-hackers-strike-email-users-must-do-this-1-thing/?sh=465e08db3d65). 08.05.2024).***

***

«У звіті Mandiant Consulting, що входить до Google Cloud, організаціям потрібно менше часу, щоб виявити зловмисників у своєму середовищі. Це означає, що компанії зміцнюють свою безпеку.

У звіті M-Trends 2024 також підкреслюється, що головними цільовими галузями 2023 року були фінансові послуги, ділові та професійні послуги, технології, роздрібна торгівля та готельний бізнес, охорона здоров'я та уряд. Це узгоджується з тим фактом, що 52% зловмисників головним чином мотивувалися фінансовою вигодою, оскільки ці сектори часто володіють великою кількістю конфіденційної — і, отже, цінної — інформації.

Фінансово мотивована діяльність зросла на 8% з 2022 року, що частково пояснюється паралельним зростанням випадків програм-вимагачів і здирництва. Найпоширеніші способи, якими зловмисники отримували доступ до цільової мережі, були через експлойти, фішинг, попередній злом і викрадення облікових даних.

Доктор Джеймі Коллієр, провідний радник Mandiant Threat Intelligence Advisor для Європи, повідомив TechRepublic в електронному листі: «Незважаючи на зосередженість на програмах-вимагачах і здирницьких операціях у спільноті безпеки, ці атаки залишаються ефективними в низці секторів і регіонів. Тому кампанії здирництва залишаються дуже прибутковими для кіберзлочинців.

«Як наслідок, за останні п'ять років багато фінансово вмотивованих груп, які здійснюють інші форми кіберзлочинності, перейшли до операцій здирництва».

TechRepublic глибше розглядає п'ять найкращих тенденцій кібербезпеки 2023 року та рекомендації експертів, висвітлені в 15-му щорічному звіті M-Trends:

- Глобальні організації вдосконалюють свій кіберзахист.
- Кіберзлочинці більше зосереджуються на ухиленні.
- Хмарні середовища стають націленими все частіше.
- Кіберзлочинці змінюють тактику, щоб обійти МЗС.
- Червоні команди використовують ШІ та великі мовні моделі.

1. Глобальні організації вдосконалюють свій кіберзахист

Згідно зі звітом M-Trends, середній час перебування глобальних організацій скоротився з 16 днів у 2022 році до 10 днів у 2023 році і зараз знаходиться на найнижчому рівні за понад десять років. Час перебування — це час, протягом якого зловмисники залишаються непоміченими в цільовому середовищі, і вказує на

міцність кіберпозиції бізнесу. Ця цифра свідчить про те, що компанії вносять значні покращення у свою кібербезпеку.

Однак може бути ще один сприяючий фактор; середня частка атак за допомогою програм-вимагачів зросла до 23% у 2023 році порівняно з 18% у 2022 році.

Доктор Коллієр пояснив TechRepublic: «Вплив операцій здирництва відразу очевидний. У разі розгортання програми-вимагача системи жертви будуть зашифровані та стануть непридатними для використання. Крім того, якщо дані викрадено, кіберзлочинець швидко зв'яжеться з жертвою, щоб вимагати вимагання».

Організації в Азіатсько-Тихоокеанському регіоні спостерігали найбільше скорочення медіанного часу перебування, де він скоротився на 24 дні за останній рік. Аналітики Mandiant пов'язують це з тим фактом, що більшість виявлених атак були пов'язані з програмами-вимагачами, і ця більшість була вищою, ніж у будь-якому іншому регіоні. Тим часом компанії в Європі, на Близькому Сході та в Африці спостерігали збільшення середнього часу перебування на два дні. Вважається, що це пов'язано з нормалізацією регіональних даних після узгоджених оборонних зусиль Mandiant в Україні в 2022 році.

Ще одним доказом того, що компанії стають кращими у виявленні кіберзагроз, є те, що Mandiant виявив, що 46% скомпрометованих організацій вперше виявили докази компрометації всередині себе, а не сторонньою організацією, наприклад правоохоронним органом або компанією з кібербезпеки, порівняно з 37% у 2022 році.

2. Кіберзлочинці більше зосереджені на ухиленні

Кіберзлочинці все частіше націлюються на периферійні пристрої, використовуючи методи «живуть за рахунок землі» та розгортають експлойти нульового дня, що свідчить про те, щоб знову зосередитися на підтримці стійкості в мережах якомога довше.

Доктор Кольєр сказав TechRepublic: «Оскільки мережеві захисники все частіше шукають кампанії здирництва, тактика ухилення збільшує шанси на

успішну операцію. Операції з програмами-вимагачами набагато ефективніші, коли кіберзлочинці можуть дістатися до найбільш чутливих і критичних зон мережі цільової цілі, а тактика ухилення допомагає їм досягти цього».

Націлювання на крайні пристрої

Пристроям Edge зазвичай не вистачає можливостей виявлення та реагування на кінцеві точки (EDR), тому вони є надійними мішенями для кіберзлочинців, які хочуть залишитися поза увагою. У 2023 році дослідники Mandiant виявили, що перша і третя найбільш цільові вразливості були пов'язані з периферійними пристроями. Це були:

CVE-2023-34362: уразливість SQL-ін'єкції в програмі передачі файлів MOVEit.

CVE-2023-2868: вразливість до ін'єкції команд у фізичних пристроях Barracuda Email Security Gateway.

Автори звіту пишуть: «Mandiant очікує, що ми й надалі спостерігатимемо націлювання на крайні пристрої та платформи, які традиційно не мають EDR та інших рішень безпеки через проблеми, пов'язані з виявленням і розслідуванням компрометації. Експлуатація цих пристроїв і надалі залишатиметься привабливим початковим вектором доступу для китайських шпигунських груп, щоб залишатися непоміченими та підтримувати стійкість у цільових середовищах».

Інструменти віддаленого адміністрування та методи «живого за рахунок землі».

Близько 20% сімейств зловмисного програмного забезпечення, виявлених Mandiant у 2023 році, не підпадають під типову категорію, що є більшою часткою, ніж у попередні роки. Крім того, 8% атак у цій категорії «інше» передбачали використання інструментів віддаленого адміністрування та інших утиліт. Менш імовірно, що вони будуть позначені за замовчуванням EDR або іншими інструментами безпеки, які можуть утримати зловмисника непоміченим, і часто поєднуються з методами «живого за межами землі».

Життя за рахунок землі – це використання законних, попередньо встановлених інструментів і програмного забезпечення в цільовому середовищі під

час кібератаки, щоб допомогти уникнути виявлення. Це може зменшити загальну складність зловмисного програмного забезпечення, дозволяючи зловмиснику використовувати наявні функції, які вже перевірені організацією на безпеку. Це особливо ефективно для периферійних пристроїв, оскільки вони зазвичай не контролюються захисниками мережі, що дозволяє їм залишатися в мережі довше.

Останнім прикладом, який помітили дослідники Mandiant, є бекдор під назвою THINCRUST, який було додано до файлів веб-фреймворку, які відповідали за надання інтерфейсу API для пристроїв FortiAnalyzer і FortiManager. Зловмисники змогли використати власну реалізацію API для доступу та надсилання команд до THINCRUST, просто взаємодіючи з новою URL-адресою кінцевої точки, яку вони додали.

Подвиги нульового дня

У 2023 році дослідники Mandiant відстежили 97 унікальних уразливостей нульового дня, використовуваних у дикій природі, що свідчить про зростання використання нульового дня більш ніж на 50% у порівнянні з 2022 роком. Нульові дні використовували шпигунські групи та фінансово вмотивовані зловмисники, які прагнули вкрасти цінні речі. даних для отримання прибутку.

Автори звіту передбачають, що кількість виявлених уразливостей нульового дня та експлойтів, спрямованих на них, продовжить зростати в найближчі роки через низку факторів, зокрема:

Поширення використання програм-вимагачів і груп вимагачів даних у режимі нульового дня: у 2023 році експлойти нульового дня в MOVEit, GoAnywhere, Citrix і PaperCut були значною мірою спрямовані завдяки публікаціям із сайтів, що витоку інформації.

Постійні атаки з експлуатації, спонсоровані державою: звіт Microsoft показує, що минулого року зросла кількість випадків кібершпигунства національної держави.

Зростання наборів експлойтів «під ключ». Готові набори експлойтів — це готові інструменти, які можна придбати у комерційних постачальників засобів спостереження. У звіті HP Wolf Security відзначено сплеск файлів Excel із

бібліотеками DLL, зараженими дешевим трояном віддаленого доступу Parallax у 2023 році.

Рекомендації зі звіту M-Trends

Підтримуйте керування виправленнями крайніх пристроїв, щоб запобігти використанню відомих уразливостей.

Використовуйте підхід «поглибленого захисту», щоб допомогти у виявленні доказів використання нульового дня.

Проводьте розслідування та мережевий пошук, якщо є підозра на компрометацію, і, якщо є, намагайтеся виявити, як зловмисники увійшли та зберегли доступ.

Дотримуйтеся вказівок постачальників засобів безпеки щодо посилення архітектури для посилення захисту.

Переконайтеся, що у вас є план реагування на інциденти та проведіть широкий моніторинг навколишнього середовища.

Рівнева сегментація мережі та журналювання за допомогою розширених рішень EDR.

Оцініть методи безпеки постачальників і вимоги до мережі, перш ніж розгортати нове обладнання або програмне забезпечення, щоб створити базову лінію для нормального використання.

3. Хмарні середовища стають націленими частіше

Застосування хмарних технологій постійно зростає — Gartner прогнозує, що понад 50% підприємств використовуватимуть галузеві хмарні платформи до 2028 року — і, отже, все більше зловмисників звертають увагу на ці середовища. За даними CrowdStrike, у 2023 році кількість хмарних вторгнень зросла на 75% порівняно з 2022 роком.

Аналітики Mandiant кажуть, що зловмисники націлені на слабко реалізовані практики керування ідентифікацією та зберігання облікових даних, щоб отримати законні облікові дані та обійти багатофакторну автентифікацію (MFA).

Mandiant спостерігав випадки, коли зловмисники отримували доступ до хмарних середовищ через облікові дані, які не зберігалися надійно. Облікові дані

були виявлені на доступному в Інтернеті сервері з конфігураціями за замовчуванням або були викрадені чи витік під час попереднього порушення даних і з тих пір не змінювалися. Вони також отримали доступ за допомогою різних методів обходу MFA, про які детальніше йдеться в наступному розділі.

Опинившись у хмарному середовищі, автори помітили зловмисників, які використовували низку тактик для зловживання хмарними службами, зокрема:

Використання власних інструментів і служб для підтримки доступу, переміщення вбік або викрадення даних: використання попередньо встановлених інструментів, таких як Azure Data Factory і Microsoft Entra ID, означало, що зловмисники могли зменшити свій робочий профіль і довше уникати виявлення.

Створення віртуальних машин (ВМ) для отримання неконтрольованого доступу до хмари організації: коли зловмисник створює віртуальну машину, яка працює в хмарній інфраструктурі організації, на ній не буде встановлено обов'язкове програмне забезпечення безпеки та журналювання. Це також може дозволити латеральне переміщення до локальної мережі через VPN.

Використання обчислювальної потужності хмари для криптомайнінгу.

Використання наборів інструментів безпеки з відкритим вихідним кодом для дослідження середовища.

Рекомендації зі звіту M-Trends

Оновіть політику автентифікації співробітників.

Використовуйте стійкі до фішингу MFA, такі як автентифікація на основі сертифіката та ключі безпеки FIDO2 через SMS замість телефонних дзвінків і одноразових паролів.

Впровадити елементи керування, які обмежують доступ до хмарних ресурсів лише надійним пристроям.

4. Кіберзлочинці змінюють тактику, щоб обійти МЗС

Тепер, коли багатофакторна автентифікація стала стандартною практикою безпеки в багатьох організаціях, зловмисники досліджують нові креативні тактики, щоб її обійти. За словами Mandiant, кількість компромісів проти хмарних ідентифікацій, налаштованих за допомогою MFA, зростає.

У 2023 році фірма спостерігала збільшення фішингових сторінок супротивника посередині (AiTM), які викрадають маркери сеансу після автентифікації та дозволяють зловмисникам обійти MFA. У кампанії AiTM зловмисники встановлюють проксі-сервер, який фіксує облікові дані користувача, коди MFA та маркери сеансу, видані порталом входу, під час ретрансляції з'єднання з законним сервером.

Більшість випадків компрометації бізнес-електронної пошти, на які Mandiant відповів у 2023 році, стосувалися того, що загроза обходила MFA користувача через AiTM. У минулому відносна складність налаштування фішингової інфраструктури AiTM у порівнянні з традиційними формами збору облікових даних могла підтримувати низьку кількість цих атак. Однак, згідно з Mandiant, зараз у підпіллі кіберзлочинців рекламується ряд наборів AiTM і пропозицій фішингу як послуги. Ці продукти значно знижують бар'єр для проникнення фішингу AiTM, що призводить до зростання.

Інші методи, які дослідники Mandiant спостерігали за використанням зловмисниками для обходу MFA, включають:

Атаки соціальної інженерії: наприклад, розповсюдження фішингових електронних листів, де ціль змушують розкрити свої дані для входу на підроблений сайт. Потім зловмисник використовує їх для входу на законному сайті, який надсилає сповіщення MFA користувачеві, який приймає. Довідкова служба організації також може отримати інструкцію щодо скидання пароля або пристрою MFA.

Заміна SIM-карти: це передбачає перенесення номера телефону цільової особи на SIM-карту, контрольовану зловмисником, щоб вони могли прийняти повідомлення MFA та заволодіти обліковим записом. У 2023 році Mandiant спостерігав збільшення кількості атак із заміною SIM-карти.

Підбір пароля: зловмисники вгадують паролі до неактивних або службових облікових записів, для яких не налаштовано MFA, щоб вони могли зареєструвати власний пристрій.

Рекомендації зі звіту M-Trends

Застосуйте стійкі до AiTM методи MFA та політики доступу, які блокують вхід на основі, наприклад, визначених організацією місць розташування, статусу керування пристроєм або історичних властивостей входу.

Відстежуйте журнали автентифікації для IP-адрес, пов'язаних із фішинговою інфраструктурою, автентифікацію за допомогою вкраденого токена або географічно неможливих входів.

5. Червоні команди використовують ШІ та великі мовні моделі

Червоні команди складаються з аналітиків кібербезпеки, які планують і здійснюють атаки на організації з метою виявлення слабких місць. У 2023 році консультанти Mandiant використовували генеративні інструменти штучного інтелекту, щоб прискорити певні дії під час оцінювання червоної команди, зокрема:

Створення початкових чернеток шкідливих електронних листів і цільових сторінок для фіктивних атак соціальної інженерії.

Розробка спеціальних інструментів для випадків, коли аналітики стикаються з незвичайними або новими програмами та системами.

Дослідження та створення інструментів у випадках, коли середовища не відповідають робочим нормам, які можна використовувати знову і знову.

Доктор Коллієр сказав TechRepublic: «Роль штучного інтелекту в червоній групі дуже ітеративна з великою кількістю взаємодій між великими мовними моделями (LLM) і людиною-експертом. Це підкреслює унікальний внесок обох.

«ШІ часто добре підходить для повторюваних завдань або отримання інформації. Тим не менш, мати червону команду консультантів, які розуміють ремесло торгівлі та володіють навичками застосування контексту, наданого LLM, у практичних ситуаціях є ще важливішим».

Штучний інтелект також використовувався в заходах фіолетової команди Mandiant, де аналітики повинні ознайомитися з середовищем клієнта з точки зору нападника та захисника, щоб сприяти співпраці між червоною та синьою командами. Generative AI використовувався, щоб допомогти їм швидше зрозуміти платформу клієнта та її безпеку.

У звіті автори припускають, як аналітики з кібербезпеки можуть використовувати ШІ в майбутньому. Червоні команди генерують значну кількість даних, які можна використовувати для навчання моделей, налаштованих для захисту середовища клієнтів. Однак розробникам штучного інтелекту також доведеться знайти нові способи, щоб гарантувати, що моделі мають відповідні огорожі, водночас дозволяючи правомірне використання зловмисної діяльності червоними командами.

«Поєднання досвіду червоної команди та потужного керівництва ШІ може призвести до майбутнього, де червоні команди будуть значно ефективнішими, а організації зможуть краще випереджати ризики, створені мотивованими зловмисниками», — пишуть автори.

Методологія

Показники, представлені в M-Trends 2024, базуються на дослідженнях Mandiant Consulting цілеспрямованих атак, проведених у період з 1 січня 2023 року по 31 грудня 2023 року». ***(Fiona Jackson. Top 5 Global Cyber Security Trends of 2023, According to Google Report // TechnologyAdvice (https://www.techrepublic.com/article/cyber-security-trends-google-report/). 03.05.2024).***

***

«…Ринок підробок еволюціонував від простої тактики копіювання до складної, багатошарової галузі, яка вміло використовує технологічні досягнення для виробництва цілого спектру підробок — від явно дешевих підробок до високоякісних «суперпідробок», які майже неможливо виявити. Ця система класифікації обслуговує різні демографічні категорії споживачів, зосереджуючись на категоріях товарів, які є найбільш затребуваними та найбільш сприйнятливими до підробок, як-от шкіряні вироби, взуття та годинники.

Поширення електронної комерції та платформ соціальних медіа ще більше сприяло створенню анонімних, великих ринків та інноваційних рекламних шляхів, значно ускладнюючи зусилля з виявлення. Крім того, передові технології

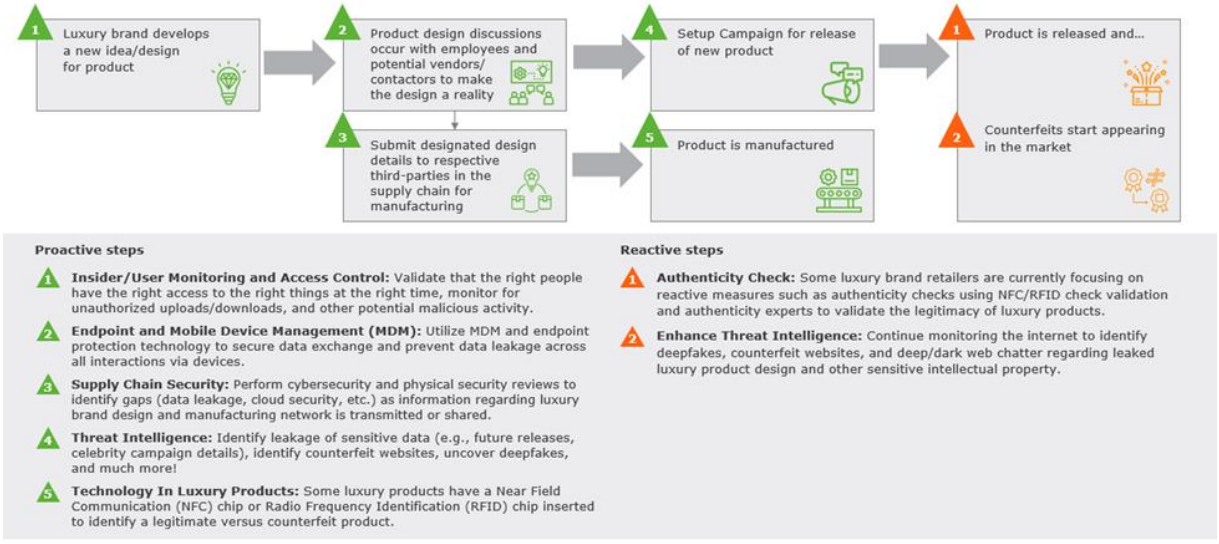
виробництва, такі як 3D-друк і прихована інтеграція в законні ланцюги поставок, зробили деякі підробки практично ідентичними справжнім продуктам.

Ця зростаюча складність вимагає, щоб бренди класу «люкс» постійно вдосконалювали свої заходи боротьби з підробками за допомогою кібербезпеки, правових стратегій і міжнародної співпраці, щоб захистити свою репутацію та споживачів.

У складній боротьбі з підробками ключовим захистом стає надійна кібербезпека

Бренди класу «люкс» традиційно вживають заходів для боротьби з підробками, включаючи вбудовування міток або мікрочіпів у свої продукти. Однак існує значний невикористаний шлях для боротьби з підробками, і саме тут кібербезпека відіграє вирішальну роль. Наразі ринок брендів класу «люкс» реагує на підробки проведенням перевірок автентичності, а не пріоритетом профілактичних заходів, як-от виявлення внутрішніх загроз або запобігання витоку критичних даних із середовища (рис. 1).

Малюнок 1. Типовий робочий процес високого рівня продукту бренду класу люкс із проактивними та реактивними заходами безпеки



У цю еру підробок і штучної реальності репутація та вартість брендів класу «люкс» піддаються більшому ризику, ніж будь-коли раніше. Глибокі підробки передбачають використання штучного інтелекту для створення тексту, відео, зображень і потокової трансляції в реальному часі на схожість персонажа (наприклад, знаменитості чи впливової особи) із загальною метою обману або

поширення дезінформації. Враховуючи природу соціальних медіа, миттєве задоволення та швидке розміщення реклами між коротким вмістом, розповсюдження підробки може бути увічнено через глибокий фейк, схожий на амбасадора бренду.

Створення підробленого продукту включає в себе кілька взаємопов'язаних аспектів, які повинні узгоджуватися для успішного виробництва. Це передбачає потенційне зворотне проектування розкішного продукту, отримання інсайдерської інформації про продукт, аналіз виробничих процесів (включно з комерційною таємницею) і порушення ланцюжка постачання (наприклад, постачання матеріалів).

Чи не було б вигідно боротися з підробками та дипфейками до того, як вони дійшли до споживача? Існує ряд заходів, орієнтованих на кібербезпеку, які бренди класу «люкс» можуть застосувати, щоб швидко пом'якшити ерозію бренду та втрату доходу:

Покращення аналізу загроз: Традиційно аналіз загроз набуває форми компанії, яка проводить постійне сканування свого бренду в Інтернеті. Те, що люди чують, говорять і в що вірять, можна контролювати, розширивши можливості аналізу загроз. Розвідка про загрози зазвичай розширюється через партнерство з організаціями (урядом, захистом споживачів, законодавством) і за допомогою інструментів розвідки загроз. Ідентифікація контенту deepfake, наприклад тексту, зображень, відео та потокового вмісту в реальному часі, може здійснюватися за допомогою аналізу загроз для виявлення підроблених веб-сайтів, що продають підроблені предмети розкоші, тексту дезінформації щодо бренду класу «люкс», помилкових зображень продуктів бренду класу «люкс» і видалення їх з Інтернету. Цього можна досягти шляхом розгортання автоматизованих рішень для аналізу загроз на основі ШІ. Вони використовують алгоритми обробки природної мови для ретельного вивчення візуальних і звукових сигналів, позначаючи сумнівний вміст для глибшого вивчення. Крім того, для дискредитації підробленого вмісту використовуються алгоритми аналізу зображень і відео. Простіше кажучи, компаніям люксових брендів потрібні інструменти кібербезпеки на основі штучного інтелекту, щоб протистояти глибоким фейковим загрозам ШІ.

Перевірка безпеки ланцюга постачання: як правило, у ланцюжку постачання продукту можуть існувати значні вразливості, що може призвести до витоку даних щодо продукту розкоші. З високим попитом і значними ресурсами суб'єкти загрози можуть бути стратегічно розміщені в різних частинах цього ланцюга створення вартості, збираючи необхідну інформацію про проекти, популярні статті, використані матеріали та виробничі процеси. Безпека ланцюга постачання є невід'ємною частиною захисту комерційних таємниць, пов'язаних із проектуванням у штаб-квартирі, обробкою матеріалів, складанням і остаточною доставкою продукту клієнту. Це включає передачу інструкцій зі складання заводам. Бренди класу «люкс» повинні зосередитися на перевірці постачальників, яка включає процес перевірки, що включає анкетування, співбесіди та збір даних, щоб зрозуміти прогалини в кібербезпеці постачальника, пов'язані з цим рівні ризику, а також надійний план дій для захисту секретів протягом усіх відносин. Крім того, команди з кібербезпеки мають виконати етап перевірки, відвідуючи сайти постачальників, щоб перевірити виконання належних процедур безпеки.

Захищені мобільні пристрої та кінцеві точки: дані про організацію слідують за користувачем. Камери можуть сприяти швидшому витоку конфіденційної інформації про майбутні випуски, дорожню карту та проекти. Співробітник може використовувати мобільні пристрої для фотографування конфіденційних даних або знімків екрана конфіденційних електронних листів. Керування мобільними пристроями відбувається саме так, як це звучить, керуючи пристроями, які надаються співробітникам для контролю доступу та витоку даних. Щоб запобігти витоку даних, бренди класу «люкс» повинні обов'язково використовувати на персональних пристроях корпоративні мобільні пристрої або ефективно налаштовані рішення для керування мобільними пристроями (MDM). Ця практика дозволяє брендам класу «люкс» відстежувати дії користувачів, такі як доступ, зміна та передача даних. Керуючи мобільними пристроями та регулюючи типи пристроїв, які користувачі можуть використовувати в бізнес-цілях, організації можуть керувати потоком даних і мінімізувати ризик втрати конфіденційної інтелектуальної власності.

Зверніть увагу на інсайдерів: інсайдери є співробітниками, а також можуть бути партнерами, постачальниками, підрядниками та іншими третіми особами бренду класу люкс, які мають доступ до конфіденційної інформації. Це може включати конфіденційні випуски продуктів із найбільш «затребуваними» знаменитостями або доступ до інтелектуальної власності щодо того, що робить продукти розкоші особливими. Інсайдери можуть ділитися конфіденційною інформацією та комерційними секретами за межами організації через звичайну цікавість або навіть підкуп. Бренди класу «люкс» можуть посилити свої програми безпеки та захисту даних, відображаючи конфіденційні дані в середовищі, вимагаючи маркування та класифікації даних, зосереджуючись на контролі доступу та вдосконалюючи конфігурації інструментів запобігання втраті даних. Крім того, інструменти безпеки можна використовувати для централізації даних і показників про користувачів, призначення рівнів поведінки та, зрештою, додавання показників ризику на основі внутрішньої активності користувачів. З різними назвами посад можуть бути призначені різні рівні ризику та вимагати подальшого перегляду для продовження роботи в організації.

Масштаби підробок і дипфейків швидко розвиваються, чому сприяє повсюдне поширення Інтернету. Тим не менш, триваюча динаміка котів-мишок відкриває можливості для підвищення репутації та вартості бренду, а також потенційного збільшення доходу шляхом простого зміцнення кібербезпеки в міру розвитку ситуації.

Бренди класу «люкс» повинні встановити контроль і жорстко захищати свою ідентичність бренду на тлі ескалації загроз підробок, особливо оскільки прогрес у генеративних моделях штучного інтелекту значно підвищує ставки. У технологічному середовищі, що швидко розвивається, профілактичні заходи для забезпечення наскрізного ланцюжка створення вартості продукту не просто необхідні — вони мають вирішальне значення для виживання, захисту капіталу бренду від розмивання та забезпечення безкомпромісної цілісності бренду». ***(Megha Kalsi, Edward Chua, Catherine Nekavand, Folasade Owoeye and Lindy Firstenberg. Cybersecurity: Empowering luxury brands in the battle against "the***

fakes" // AlixPartners LLP (https://www.alixpartners.com/insights/102j6j1/cybersecurity-empowering-luxury-brands-in-the-battle-against-the-fakes/#page=1). 01.05.2024).

***

«Кіберзлочинність продовжує зростати і не має ознак припинення.

У звіті, опублікованому на Statista, оцінюється, що річні витрати на кіберзлочинність у Великій Британії становили 320 мільйонів доларів США (приблизно 250 мільйонів фунтів стерлінгів) у 2023 році. За прогнозами, до 2028 року ця сума зросте до понад 1,82 трильйона доларів США (приблизно 1,424 трильйона фунтів стерлінгів).

Цифри високі, а вплив широко поширений, оскільки кіберзлочинність впливає на бізнес у різних секторах, включаючи сектор роздрібної торгівлі. Британський роздрібний консорціум (BRC) повідомляє, що 32% організацій роздрібної торгівлі зазнали порушення безпеки у 2022/2023 роках.

Чому це має значення?

Зростання кіберзлочинності може бути спричинене, принаймні частково, зростаючою доступністю та використанням штучного інтелекту (ШІ). Згідно зі звітом NCSC про вплив штучного інтелекту на кіберзагрозу, ми побачимо, що «штучний інтелект насамперед запропонує суб'єктам загрози підвищення можливостей соціальної інженерії». Злам облікових даних облікового запису, часто через фішингові електронні листи, залишається поширеним способом входу. Якщо зловмисники використовують штучний інтелект для створення все більш переконливих фішингових електронних листів, які з більшою ймовірністю будуть взаємодіяти, результатом буде зростаюча здатність отримувати облікові дані облікового запису для отримання доступу до систем організації та, згодом, до її даних.

Масштабні інциденти в ланцюзі поставок 2023 року також сприяли збільшенню кіберзлочинності. До них належать атаки програм-вимагачів, яких зазнали: (i) CTS, постачальник IT-послуг, які вплинули на низку клієнтів його

юридичної фірми; і (ii) MOVEit, компанія з передачі файлів, яка залучила понад 600 організацій у всьому світі до сфери одного інциденту, повідомляє Reuters. Ці інциденти демонструють широке розповсюдження, яке можуть мати інциденти в ланцюзі постачання, і важливість для управління цими ризиками, як було передбачено та обговорено в минулорічному осінньому випуску Retail Compass.

Вплив зростання кіберзлочинності посилюється збільшенням масштабів кібератак. Ми спостерігаємо тенденцію до отримання більшої кількості даних із проникнутих систем, особливо у сценаріях програм-вимагачів. Якщо раніше зловмисники забирали гігабайти даних від організацій, тепер іноді ми спостерігаємо викрадання кількох терабайтів даних. Результатом є більший вплив на жертв, оскільки більший обсяг даних, отриманих із систем, до яких здійснюється доступ, може означати, що існує більша ймовірність отримання даних, які є або (i) особистою інформацією, що стосується суб'єктів даних, або (ii) конфіденційною або конфіденційна інформація про клієнта. Це може становити значний ризик для організацій роздрібної торгівлі, де для аналітики роздрібної торгівлі може збиратися велика кількість даних про споживачів і/або де дані, які розглядаються, можуть включати конфіденційну інформацію, пов'язану з випуском продуктів.

Які дії слід розглянути?

Збільшення кількості випадків і впливу кіберзлочинності підкреслює необхідність впровадження базових протоколів безпеки. Ми бачили, як деякі кіберстраховики відмовлялися задовольняти претензії, коли розслідування інциденту показало, що таких заходів, як багатофакторна автентифікація (яка може значно зменшити вразливість до компрометації облікових даних), не було.

Ми також спостерігаємо зростаючу увагу до планування реагування на інциденти в різних секторах. За даними BRC, лише 48% роздрібних продавців мають офіційний план програм-вимагачів. Планування порушень кібербезпеки до того, як вони відбулися, шляхом створення планів управління кризою та участі в семінарах перед порушенням може допомогти мінімізувати наслідки інциденту». ***(Elizabeth Zang and Richard Breavington. Higher stakes cybercrime - prepare now //***

Reynolds Porter Chamberlain LLP (https://www.rpc.co.uk/perspectives/retail-therapy/higher-stakes-cybercrime-prepare-now/#page=1). 08.05.2024).

***

«Бібліотека Конгресу стала мішенню кібератаки, яка сталася паралельно з резонансним вторгненням у Британську бібліотеку Сполученого Королівства наприкінці жовтня, але хакерам не вдалося отримати доступ до систем бібліотеки США, згідно з внутрішніми документами, отриманими Nextgov/FCW.

Спроба злому сталася приблизно 28 жовтня, того самого дня, коли Національна бібліотека Великобританії почала повідомляти про технічні проблеми на своєму веб-сайті. Кіберзлочинці не досягли успіху, тому що LOC мав багатофакторну автентифікацію — метод цифрової перевірки входу користувача в систему — увімкнений у точці входу хакерів.

IT-персонал бібліотеки також швидко закрив цільові служби, як тільки було виявлено атаку, йдеться в документах. Відтоді LOC виводить із експлуатації застаріле обладнання та інтегрує нові інструменти безпеки у свої мережі.

Відповідальність за жовтневу атаку на Британську бібліотеку взяла група програм-вимагачів Rhysida. Група вкрала дані та тримала їх у заручниках в обмін на викуп у розмірі 20 біткойнів, що на момент погрози становило близько 600 000 фунтів стерлінгів. Але бібліотека відмовилася платити, і хакери опублікували близько 500 000 викрадених файлів, які містили особисту інформацію співробітників.

Колишній керівник Національного центру кібербезпеки Великобританії назвав кібернаступ одним із найгірших в історії Великобританії. Бібліотека все ще стикається з перебоями в роботі.

ФБР і CISA відмовилися від коментарів. LOC не відповів на численні запити про коментарі. Залишається незрозумілим, чи ті ж оперативники, пов'язані з Rhysida, намагалися проникнути в бібліотеку США.

Цілком ймовірно, що початковий брокер доступу — хакер, який спеціалізується на отриманні доступу до систем і продає свої методи входу іншим групам на підпільних дискусійних форумах — перевірив системи LOC і відступив, коли вони не змогли зламати, — сказав Аллан Ліска, аналітик аналізу загроз програм-вимагачів у Recorded Future.

«Ви замикаєте свою машину не тому, що це може зупинити рішучого злодія, а тому, що це змушує випадкового злодія підійти до наступної машини та спробувати влізти», — сказав він. Динаміка подібна до інциденту з Британською бібліотекою, за винятком того, що початковий брокер доступу був успішним і продав свою техніку злому Rhysida, додав він.

Група Rhysida, яка, ймовірно, має зв'язки з Росією, була предметом листопадової консультації CISA та інших, яка попередила, що банда з травня минулого року націлена на державну освіту, охорону здоров'я, IT та виробничий сектор.

За словами Ліски, як найбільшої культурної науково-дослідної установи в Америці, успішне вторгнення в LOC було б руйнівним для внутрішніх досліджень і систем файлів.

Примітно, що Бюро захисту авторських прав США працює в парі з бібліотекою. «Ви не зможете захистити авторське право на жодну роботу протягом цього періоду [відновлення]. Тож додатковий ефект відчують не тільки люди, які користуються бібліотекою», — сказав він.

Хакери використали подібну вразливість під час нещодавнього зламу підрозділу Change Healthcare UnitedHealth. Компанія визнала, що не мала протоколів багатофакторної автентифікації, встановлених на сервері, який окрема група програм-вимагачів зламала за допомогою вкрадених облікових даних». ***(David DiMolfetta. Thwarted cyberattack targeted Library of Congress in tandem with October British Library breach // Government Media Executive Group LLC (https://www.nextgov.com/cybersecurity/2024/05/thwarted-cyberattack-targeted-library-congress-tandem-october-british-library-breach/396399/). 08.05.2024).***

***

«Збої в кібербезпеці, які досягли громадської свідомості, спіткали такі відомі компанії, як Yahoo, Microsoft, Facebook, Target і JPMorgan Chase. Але захист даних є такою ж великою проблемою, якщо не більшою, для малого та середнього бізнесу (SMBs): серйозне порушення може призвести до того, що вони зникнуть.

Згідно з новим звітом про дослідження, проведене компанією з управління паролями LastPass і дослідницькою компанією InnovateMR, останніми роками зросла кількість кібератак, спрямованих на SMB.

З одного боку, йдеться у звіті, чому злочинці визначили малий і середній бізнес як відносно легку мішень через обмеження ресурсів і в деяких випадках слабку політику кібербезпеки. Крім того, зловмисники все частіше атакують малий і середній бізнес, щоб проникнути у великі організації, які знаходяться далі в ланцюжках поставок.

В опитуванні взяли участь 633 керівника американських компаній малого (10-499 співробітників) і середнього (500-2999 співробітників) підприємств. Доповідь також розділила учасників на три групи: керівники, IT-лідери та лідери не-IT-бізнесу.

Значна більшість респондентів сказали, що вони стають більш активними щодо кібербезпеки, наприклад, шляхом підвищення обізнаності та інвестицій у заходи безпеки.

Фактично, 82% опитаних сказали, що цього року бюджети на кібербезпеку збільшуються. Але, незважаючи на те, що ці кількісні інвестиції є багатообіцяючими, «лідерам слід витрачати більше часу на якісні інвестиції для покращення кібербезпеки, включаючи політику, освіту та культуру», — радить звіт.

Проте були докази розриву між групами. Переважна більшість керівників і IT-керівників висловили переконання, що співробітники розуміють очікування безпеки, з відривом у 92% і 93% відповідно. Однак значно менше (78%) лідерів, які

не займаються IT, відчувають те саме. Грунтуючись на цих цифрах, LastPass висловив думку, що «керівники та IT-лідери надто оптимістичні».

У звіті рекомендовано, щоб керівники всієї організації провели спільні консультації, щоб визначити справжній рівень розуміння серед співробітників і найкращий шлях досягнення загальноорганізаційної політики кібербезпеки.

Зазначаючи, що лише троє з 10 лідерів вважають, що їхня компанія стикається з дуже високим ризиком зіткнутися з проблемою кібербезпеки, Алекс Кокс, директор із аналізу загроз для LastPass, наголосив у дописі в блозі, що лідери повинні «розуміти свою корону, яка є насувається на них та їхні найімовірніші загрози».

Тим часом деякі додаткові результати опитування викликали занепокоєння, незважаючи на те, що вони стосувалися меншості респондентів. Наприклад, приблизно кожен п’ятий бізнес-лідер і кожен 10-й керівник сфери IT-безпеки зізналися в обході політики безпеки. Крім того, кожен четвертий молодший працівник, ймовірно, порушує правила, а 36% фахівців покоління Z зізналися, що записували паролі.

Кокс закликав малий і середній бізнес застосувати «збалансований підхід до сильніших стимулів для відповідності та суворіших наслідків за порушення».

Але в той же час, додав Кокс, лідери повинні запровадити спрощені процеси для тимчасових винятків із політики кібербезпеки, які необхідні для завершення важливої роботи. Це може «допомогти працівникам виконувати роботу, не вживаючи нечесних заходів», — написав він». ***(David McCann. 82% of SMB leaders increased cybersecurity budgets YoY: Report // Industry Dive (https://www.cfo.com/news/82-of-smb-leaders-increased-cybersecurity-budgets-yoy-report-risk-compliance/715586/). 13.05.2024).***

***

«ESET повідомляє про виявлення небезпечної активності групи кіберзлочинців Ebury, яка скомпрометувала сотні тисяч серверів принаймні за 15 років. Серед діяльності зловмисників та ботнета Ebury — поширення

спаму, перенаправлення вебтрафіку та викрадення облікових даних. За останні роки також були зафіксовані випадки викрадення даних банківських карток та криптовалюти.

Зокрема Ebury було використано як бекдор для компрометації майже 400 000 серверів Linux, FreeBSD та OpenBSD. Варто зазначити, що станом на кінець 2023 року понад 100 000 все ще були скомпрометовані. У багатьох випадках зловмисники Ebury могли отримати повний доступ до великих серверів Інтернет-провайдерів та відомих хостинг-провайдерів.

Скомпрометовані сервери є майже у всіх країнах світу. Серед жертв цієї групи кіберзлочинців — університети, малі та великі підприємства, Інтернет-провайдери, торговці криптовалютою, вузли виходу Tor, провайдери віртуального хостингу та виділених серверів тощо.

Які шкідливі методи використовували зловмисники?

Ebury, який активний принаймні з 2009 року, є бекдором OpenSSH та інструментом для викрадення облікових даних. Він використовується для розгортання додаткового шкідливого програмного забезпечення з метою монетизації ботнету (наприклад, модулів для перенаправлення вебтрафіку), поширення спаму, виконання атак «людина посередині», а також як хост для шкідливої інфраструктури. У період з лютого 2022 року до травня 2023 року спеціалісти ESET виявили понад 200 цілей у понад 75 мережах у 34 країнах.

«Ми виявили інциденти, коли інфраструктура хостинг-провайдерів була скомпрометована групою Ebury. У цих випадках було зафіксовано розгортання Ebury на серверах, орендованих цими постачальниками. Це призвело до компрометації тисячі серверів ботнетом Ebury одночасно, — коментує Марк-Етьєн М. Левей, дослідник ESET. — Ebury становить серйозну загрозу для безпеки Linux. Хоча простого рішення для знешкодження Ebury не існує, можна мінімізувати його поширення та вплив».

Крім того, зловмисники використовували ботнет Ebury для викрадення криптовалюти, облікових та банківських даних. Хакери Ebury також

використовували «0-денні» уразливості в програмному забезпеченні адміністратора, щоб масово зламати сервери.

Після зламу системи ряд деталей перехоплюється зловмисниками. Використовуючи відомі паролі та ключі, отримані в цій системі, облікові дані повторно використовуються для спроб входу в пов’язані системи…

Що робити

Для зменшення ризиків інфікування подібними загрозами спеціалісти ESET рекомендують дотримуватися основних правил кібербезпеки, зокрема створювати надійні паролі та використовувати багатофакторну автентифікацію, не переходити за невідомими посиланнями в електронних листах та вчасно оновлювати програмне забезпечення, а також встановити рішення для захисту пристроїв корпоративної мережі від сучасних векторів атак…» ***(Герман Богапов. Кіберзлочинці атакували 400 тисяч серверів Linux // HiTech.Expert. Хостинг (https://expert.com.ua/182542-kiberzlochynci-atakuvaly-400-tysyach-serveriv-linux.html). 15.05.2024).***

***

«Бішкек, столиця Киргизстану, наразі переживає жорстоке насильство натовпу та ескалацію кібератак на Киргизстан, знаменуючи бурхливий період для нації.

Нещодавні потрясіння, головним чином спрямовані проти іноземних студентів, привернули значну увагу міжнародної спільноти та дипломатичне занепокоєння, особливо Індії та Пакистану.

Каталізатор хаосу

Заворушення почалися в ніч з 17 на 18 травня після того, як 13 травня в мережі з'явилося відео, на якому нібито зображена бійка між киргизькими та єгипетськими студентами-медиками.

Відео, яке швидко поширилося в соціальних мережах, нібито показало конфлікт киргизьких студентів з єгипетськими студентами. Цей інцидент спровокував широке насильство натовпу, а місцеві жителі спрямували свою агресію на іноземних студентів, що загострило напругу в Бішкеку.

Незважаючи на відсутність підтверджених доказів того, що задіяні особи були киргизькими молодими людьми, відео спричинило значні соціальні хвилювання.

Хаос, що виник, призвів до 28 поранень, у тому числі трьох іноземців, що змусило поліцію втрутитися та огородити райони, де зібралися натовпи. На кадрах, які циркулюють в Інтернеті, видно, як натовпи нападають на іноземних студентів на вулицях і навіть у гуртожитках, створюючи атмосферу страху та ворожості для іноземних студентів.

Кібератаки на Киргизстан посилюють кризу

Серед фізичного насильства цифрова інфраструктура Киргизстану зазнає серйозної атаки з боку різних хактивістських груп. Ці скоординовані кібератаки на Киргизстан були націлені на критично важливі системи урядового та приватного секторів, що погіршило і без того нестабільну ситуацію.

У цих кібернападах беруть участь кілька груп хакерів:

Команда Insane PK нібито атакувала Міністерство сільського господарства, Освітній портал Міністерства надзвичайних ситуацій, Saima Telecom, платформу моніторингу клімату (http://climatehub.kg) і кілька університетів, включаючи Ошський державний університет і Киргизьку державну медичну академію.

Silent Cyber Force, інша пакистанська група, також нібито атакувала Міністерство оборони та Міністерство сільського господарства Киргизстану.

Golden Don’s нібито здійснив кібератаки на Міністерство економіки та торгівлі, веб-сайт Kirgyzstan Visa та Киргизький турецький університет Манас.

Anon Sec BD з Бангладеш нібито напав на MBank і Finca Bank.

Окремий хактивіст, відомий як «раджіб», нібито атакував офіційний портал залізниці Киргизстану.

Стверджується, що Sylhet Gang порушила роботу Міністерства закордонних справ Киргизії та киргизьку телекомунікаційну мережу Nur, спричинивши значні збої.

Крім того, є твердження, що Mysterious Team Bangladesh планує майбутні кібератаки на Киргизстан.

Одна з хактивістських груп, Silent Cyber Force, опублікувала повідомлення під назвою «Вітаю, громадяни світу», засуджуючи насильство проти іноземних студентів і заявляючи про свій намір знищити урядові веб-сайти та великі мережі Киргизстану.

У їхньому повідомленні прямо згадувалося про націлювання на різних міжнародних супротивників, але вказувалося, що наразі увага зосереджена на Киргизстані через передбачувану бездіяльність його уряду щодо захисту іноземних студентів.

Незважаючи на ці загрози, офіційні веб-сайти цільових установ функціонували нормально під час доступу. Це викликає питання щодо реальних можливостей хакерів або можливих тактичних затримок у виконанні їхніх загроз. Повний масштаб і вплив цих кібератак на Киргизстан стануть більш зрозумілими після оприлюднення офіційних заяв.

Наслідки та необхідність пильності

Поєднання фізичного насильства та цифрових атак підкреслює критичну потребу в посилених заходах безпеки як у фізичній, так і в кіберсфері. Ці кіберзагрози не тільки порушують діяльність уряду, але й створюють значні ризики для основних послуг, які впливають як на громадян, так і на іноземців у Киргизстані.

Поточна ситуація в Киргизстані підкреслює вразливість цифрової інфраструктури в періоди соціальних заворушень. Хактивістські групи використовують хаос для досягнення своїх планів, націлюючись на ключові інституції та поширюючи страх і збурення. Триваючі кібератаки на Киргизстан демонструють важливість розвідки про кіберзагрози та необхідність комплексних стратегій кібербезпеки для захисту національної інфраструктури.

У відповідь на ці події Киргизстану вкрай необхідно зміцнити захист кібербезпеки та посилити заходи фізичної безпеки, щоб захистити всіх жителів, включаючи іноземних студентів». ***(Samiksha Jain. Kyrgyzstan Unrest Escalates: Hackers Target Nation Amidst Mob Violenc // The cyber express (https://thecyberexpress.com/cyberattacks-on-kyrgyzstan-admist-***

violence/?utm_source=flipboard&utm_content=FlipboardCanada%2Fmagazine%2FTechnology). 20.05.2024).

***

«Оскільки обробна промисловість все більше покладається на передові технології, такі як промисловий Інтернет речей, автоматизація та великі дані, виробники особливо вразливі до кібератак. Виробничі підприємства будь-якого розміру є бажаною мішенню для загрозливих осіб і злодіїв, які сподіваються отримати доступ до величезних сховищ конфіденційної інформації, інтелектуальної власності та фінансових записів клієнтів.

Зараз багато компаній використовують штучний інтелект («ШІ»), щоб оптимізувати виробництво та уникнути збоїв у ланцюзі поставок. Наприклад, глобальна компанія споживчих товарів Unilever використовує штучний інтелект для пошуку альтернативних інгредієнтів, намагаючись посилити стійкість свого ланцюжка поставок. Крім того, Walmart почав використовувати ШІ для переговорів зі своїми постачальниками. Це програмне забезпечення використовує текстовий інтерфейс користувача для переговорів з потенційними постачальниками.

Відповідно до Індексу розвідки загроз IBM X-Force 2024, обробна промисловість була найбільш цільовою галуззю у 2023 році третій рік поспіль. У звіті зазначається, що зловмисне програмне забезпечення спричинило 45% атак, а програми-вимагачі — 17% атак. Оскільки очікується, що обробна промисловість залишатиметься головною мішенню для викрадачів даних до 2024 року та надалі, компанії повинні наголошувати на відповідальному використанні даних, надійній внутрішній політиці кібербезпеки та заходах безпеки.

Проблеми кібербезпеки та конфіденційності даних

Кібератаки створюють низку різних ризиків і негативних наслідків, серед яких збої в ланцюжку поставок, втрачені прибутки, втрата інтелектуальної власності та репутаційна шкода. Деякі з основних ризиків кібербезпеки, з якими стикаються виробники, включають:

програми-вимагачі

Програми-вимагачі – це тип зловмисного програмного забезпечення, яке блокує доступ власників даних до конфіденційних даних, якщо зловмиснику не буде сплачено значну суму грошей. Під час розгортання програм-вимагачів організації часто змушені видаляти заражені системи зі своєї мережі, що може зайняти багато часу, зашкодити роботі та коштувати.

Фішинг

Фішингові атаки використовують текстові повідомлення, електронні листи та інші форми електронного зв'язку, щоб змусити людей перейти за шкідливими посиланнями або розкрити конфіденційну інформацію. За допомогою цих атак зловмисники можуть отримати облікові дані для входу в облікові записи компанії, які потім використовуються для здійснення шахрайства — часто у формі шахрайських платіжних запитів клієнтам компанії-жертви. Виробники вразливі до фішингових атак через їхні великі списки клієнтів і сильну залежність від сторонніх постачальників.

Атаки на ланцюги поставок

Ланцюг поставок є одним із найбільш вразливих аспектів бізнесу виробника. Ланцюжок постачання дозволяє компаніям створювати та доставляти продукти та матеріали, використовуючи бази даних і автоматизацію для координації з діловими партнерами та постачальниками. Наприклад, виробник може включити продукт іншого виробника у свій кінцевий продукт. Таким чином, атака на одного виробника може мати згубні наслідки і для інших компаній.

Існує три типи порушень ланцюга поставок:

Атаки на ланцюг поставок програмного забезпечення – зловмисники скомпрометують лише одну програму або частину програмного забезпечення, щоб порушити весь ланцюжок поставок. Ці атаки націлені на вихідний код програми та доставляють шкідливий код до довіреної програми чи програмної системи.

Атаки на ланцюг поставок вбудованого програмного забезпечення – зловмисники вставлятимуть зловмисне програмне забезпечення в завантажувальний запис комп'ютера, яке потім можна буде активувати за лічені хвилини. Після завантаження цільового комп'ютера зловмисне програмне

забезпечення запускається, і зловмисник отримує доступ до мережі. Ці атаки швидкі, завдають шкоди та іноді їх неможливо виявити.

Атаки на ланцюг поставок обладнання – ці типи атак залежать від фізичних пристроїв. Зокрема, зловмисники можуть націлитися на пристрої, критичні для виробничого процесу, що призведе до тривалих затримок виробництва та шкоди репутації.

Щоб ефективно зменшити ймовірність витоку даних, виробники повинні запровадити комплексну програму захисту та безпеки даних. Ця програма повинна включати:

Заходи безпеки даних, такі як шифрування, мережеві брандмауери, системні аудити, багатофакторна автентифікація, контроль доступу та звичайні виправлення та оновлення системи;

Навчальні та навчальні програми з кібербезпеки для працівників;

Оцінка ризиків і тестування на проникнення; і

Політики та процедури, такі як політика інформаційної безпеки, політика збереження записів, план реагування на інциденти та план безперервності бізнесу.

Крім того, Національний інститут стандартів і технологій («NIST») опублікував «Практику управління ризиками кібербезпеки в ланцюжку поставок для систем і організацій», в якій виробники містять інструкції щодо виявлення, оцінки та реагування на ризики кібербезпеки в усьому ланцюжку поставок. Відповідно до NIST, багато ризиків ланцюга поставок пов’язані з недостатньою видимістю та розумінням організацій щодо використовуваних технологій і процедур, які використовуються для забезпечення «безпеки, стійкості, надійності, безпеки, цілісності та якості продуктів і послуг». Керівництво NIST закликає виробників враховувати ризики кібербезпеки та керувати ними протягом усього процесу постачання.

Нарешті, виробники, які мають державні контракти, повинні вжити заходів для відповідності програмі сертифікації моделі зрілості кібербезпеки (CMMC) 2.0 Міністерства оборони («DoD»). CMMC розроблено для того, щоб забезпечити застосування надійних методів кібербезпеки для захисту конфіденційної

несекретної інформації та інформації про федеральні контракти, якою Міністерство оборони ділиться зі своїми підрядниками та субпідрядниками…» ***(Jessica L. Copeland, Mario F. Ayoub, Victoria M. Okraszewski. Tackling Cyber Risks in the Manufacturing Industry // Bond, Schoeneck & King PLLC (https://www.bsk.com/news-events-videos/tackling-cyber-risks-in-the-manufacturing-industry). 16.05.2024).***

***

«Індустрія професійного спорту являє собою унікальний перетин численних мотиваційних факторів для кіберзлочинців. Останніми роками хакери-злочинці, які прагнуть отримати фінансову вигоду, атакували великі спортивні команди за допомогою програм-вимагачів. Політично вмотивовані хакери зірвали прямі трансляції спортивних подій і злили особисті дані гравців. Іноземні уряди навіть втручалися в міжнародні спортивні події для досягнення геополітичних цілей.

Професійні спортивні команди спостерігали значне зростання загроз кібербезпеці за останнє десятиліття — часто цитоване опитування Національного центру кібербезпеки Великобританії (NCSC) у 2020 році показало, що 70% спортивних організацій зазнають принаймні однієї кібератаки на рік. Так само спортивні вболівальники все частіше стають мішенями кіберзлочинців, згідно зі звітом за 2023 рік Lloyds Bank, виявивши, що шахрайство з квитками на футбольні матчі в соціальних мережах зросло більш ніж удвічі порівняно з попереднім роком.

Унікальна багатогранна природа спортивної індустрії — включаючи цифрові та фізичні події, широкий спектр конфіденційних даних клієнтів і гравців, а також часто міжнародний масштаб — вимагає від галузевих організацій бути в курсі широкого спектру загроз безпеці. Нижче ми висвітлюємо деякі з найбільш значущих проблем кібербезпеки, з якими стикається спортивна індустрія в усьому світі, а також ключові найкращі практики в галузі права та кібербезпеки, які допоможуть керувати цими ризиками, що розвиваються.

Цифрова трансформація

Цифрове перетворення спортивних об'єктів і досвіду глядачів — дедалі більше покладаються на інтелектуальні пристрої, онлайн-платежі та користувацький досвід на основі додатків — відкрило безліч нових точок доступу для проникнення хакерів. Наприклад, на початку 2019 року хакерам вдалося встановити зловмисне програмне забезпечення для сканування кредитних карток в онлайн-магазині Atlanta Hawks, щоб викрасти інформацію про платіжні картки клієнтів, що свідчить про вразливість платіжних даних клієнтів до таких атак.

Щоб допомогти у вирішенні цих проблем, Агентство з кібербезпеки та безпеки інфраструктури США (CISA) і Національний центр безпеки та безпеки глядацьких видів спорту (NCS⁴) випустили публікацію під назвою Stadium Spotlight: Connected Devices and Integrated Security Considerations, яка містить корисну діаграму цифрових вразливостей у типовому середовищі спортивного стадіону, а також принципи та ресурси зменшення ризиків кібербезпеки.

Корпоративне шпигунство

Професійні спортивні команди також все більше покладаються на безліч власних даних і аналітичних моделей, щоб визначити свій підхід до всього, починаючи від виборів драфту і закінчуючи внутрішньоігровою стратегією.

Ці дані є цінною мішенню для конкурентів у галузі та зловмисників, які прагнуть використати їх для отримання фінансової вигоди — як це сталося в 2015 році, коли директора скаутського відділу «Сент-Луїс Кардіналс» Крістофера Корреа було заарештовано та притягнуто до відповідальності за злом бази даних Houston Astros, яка містила конфіденційні звіти скаутів, деталі торгівлі та інші цінні статистичні дані. Пізніше Корреа був засуджений до 46 місяців тюремного ув'язнення, а MLB оштрафувала «Кардиналів» на 2 мільйони доларів і змусила віддати два драфт-піки «Астрос».

Загрози програм-вимагачів

Програми-вимагачі залишаються повсюдною загрозою в усіх галузях - і професійний спорт не є винятком. На початку минулого року Королівська футбольна асоціація Нідерландів (KNVB) повідомила, що заплатила нерозкриту

суму викупу процвітаючій банді LockBit, яка потенційно викрала персональні дані понад 1,2 мільйона співробітників і членів клубу.

У попередні роки значні інциденти з програмами-вимагачами також вплинули на «Сан-Франциско 49ерс», «Х'юстон Рокетс» і футбольний клуб «Манчестер Юнайтед».

Інсайдерські загрози

Окрім боротьби із зовнішніми загрозами, організації спортивної індустрії також повинні запроваджувати внутрішній контроль, щоб запобігти неправильному використанню або крадіжці даних інсайдерами.

Наприклад, італійський футбольний клуб «Лаціо» став жертвою фішингової афери у 2018 році, яка призвела до передачі шахрайських банківських інструкцій, за допомогою яких клуб відправив 1,75 мільйона фунтів стерлінгів, що мали стати частиною угоди про трансфер гравця з голландським клубом. У звіті зазначається, що хакери, ймовірно, мали інсайдерську інформацію про угоду, яку вони використали для здійснення атаки з використанням технології «людина посередині».

Національно-державні актори

Деякі великі спортивні події та спортивні організації мають значну міжнародну популярність, що робить їх основними цілями для національних державних акторів з геополітичними планами.

Візьмемо один резонансний приклад: у 2016 році хакери, імовірно пов'язані з російською групою «Fancy Bear», атакували облікові записи різних офіційних осіб Всесвітнього антидопінгового агентства (WADA) за допомогою фішингових атак, як повідомлялося на сайті WADA. Дивіться також «США звинуватили російських офіцерів ГРУ в міжнародних хакерських операціях і пов'язаному з цим впливі та дезінформації», Міністерство юстиції США, 4 жовтня 2018 р. Атака призвела до витоку медичних даних, що стосуються різних олімпійських спортсменів, включаючи інформацію про терапевтичне використання. винятки для заборонених речовин.

Багато хто сприйняв цей інцидент як політично вмотивовану помсту за доповідь WADA від липня 2016 року, яка закликала не допустити Росію на літню Олімпіаду в Ріо через докази організованого використання допінгу російськими спортсменами.

Найкращі методи управління та пом'якшення змінних ризиків

З огляду на ці виклики, існує низка широко поширених практик — як технічного, так і юридичного характеру — які можуть допомогти організаціям у всьому спектрі кіберрозвиненості зменшити свою вразливість до кіберризиків. Приклади цих передових практик, рекомендованих як урядами, так і експертами приватного сектору, включають:

• Дізнайтесь, які конфіденційні дані зберігає ваша організація та де вони зберігаються. Професійні спортивні команди зберігають широкий спектр конфіденційних даних, зокрема: конфіденційні ділові дані, власні драфтові та торгові дані, особисту та фінансову інформацію клієнтів, а також медичні записи гравців. Важливо розуміти, де ці дані, які засоби захисту їх охороняють і хто має дозвіл на доступ до них.

• Дізнайтеся про своїх сторонніх постачальників і про те, які дані вони отримують або до яких мають доступ. Сторонні постачальники та постачальники послуг стають все більш поширеним вектором атак для загроз кібербезпеці. Наприклад, атака 2021 року на консалтингову фірму Horizon Actuarial Services LLC скомпрометувала особисті дані з планів пільг багатьох гравців Вищої ліги бейсболу та їхніх сімей. Професійні спортивні організації повинні знати, якими даними вони обмінюються з постачальниками, і регулярно оцінювати адекватність своїх процедур управління ризиками третіх сторін.

• Запровадити багатофакторну автентифікацію та безпечні політики керування паролями. Багато кібератак відбуваються через погане керування паролями — наприклад, повторне використання паролів працівниками або відсутність багатофакторної автентифікації. Інцидент з корпоративним шпигунством у 2016 році, який торкнувся Houston Astros, наприклад, стався через те, що один із співробітників не повернув старий пароль, який був зламаний.

Широке впровадження багатофакторної автентифікації, особливо для привілейованих користувачів, і вимога надійних паролів із регулярною ротацією можуть уникнути низки дуже поширених моделей атак.

• Запровадження інструментів для моніторингу ваших мереж і виявлення підозрілої активності. Раннє виявлення може бути різницею між незначним інцидентом і серйозною подією, для відновлення якої потрібні місяці або роки. Спортивні організації можуть співпрацювати з охоронними фірмами для постійного моніторингу мережевого трафіку та впровадження інструментів виявлення кінцевих точок для значного підвищення безпеки та цілісності своїх мереж.

• Майте оновлений план реагування на кіберінциденти та регулярно проводите настільні навчання, щоб перевірити його. Наявність співробітників, які знайомі з поточним планом реагування та можуть швидко діяти в надзвичайних ситуаціях, має неоціненне значення для пом'якшення впливу швидкоплинних інцидентів кібербезпеки. Проведення щорічних настільних навчань з урахуванням профілю ризиків організації, які можуть допомогти виявити прогалини в політиці, брак досвіду чи необхідних інструментів, стає все більш невід'ємною частиною програм управління кіберризиками багатьох організацій.

• Заздалегідь запропонуйте постачальників реагування на кризові ситуації для підтримки в разі потреби. Підключення до нового постачальника реагування на інциденти, будь то юридична фірма, фахівець із відновлення програм-вимагачів чи експерт з цифрової криміналістики, у розпал кризи може зайняти багато часу. Завчасне залучення постачальників із привілеєм може виграти дорогоцінний час на початку інциденту.

Кібербезпека та правові основи для спортивних команд

Наведені нижче вказівки від установ США та Великобританії містять принципи та структуру для професійних спортивних команд та інших установ спортивної індустрії, які займаються ризиками кібербезпеки.

• NIST Cybersecurity Framework 2.0: Структура кібербезпеки Національного інституту стандартів і технологій (NIST), востаннє оновлена в лютому 2024 року,

надає спільну мову для організацій критичної інфраструктури для оцінки ризиків кібербезпеки та керування ними…

• Партнерство CISA: CISA співпрацює зі спортивними лігами, командами, стадіонами та іншими великими майданчиками по всій країні, щоб розробити плани реагування на інциденти та провести настільні навчання з кібербезпеки. Щороку CISA проводить понад 150 навчань у США з підприємствами, школами та іншими організаціями будь-якого розміру, щоб підвищити їх безпеку та стійкість. У вересні 2023 року CISA провела свої 10-ті щорічні настільні навчання з кібербезпеки в партнерстві з НФЛ для імітації нападу на стадіон Allegiant під час Super Bowl LVII. Чотиригодинні пробні вправи включали гіпотетичний вплив фішингу, програм-вимагачів, витоку даних і потенційної внутрішньої загрози, а також каскадний вплив на фізичні системи.

• PCI DSS: стандарт безпеки даних індустрії платіжних карток (PCI DSS) — це набір політик безпеки, які захищають дані кредитних і платіжних карток і транзакції для основних брендів карток. PCI DSS запобігає шахрайству з кредитними картками та крадіжкам у системах торгових точок, подібних до тих, які є на більшості великих спортивних майданчиків.

• Рекомендації NCSC: Звіт Національного центру кібербезпеки Великої Британії (NCSC) «Кіберзагроза спортивним організаціям», містить рекомендації з управління кіберризиками, а також інформацію про галузеві тенденції. NCSC також створив посібник «Кібербезпека для великих подій», присвячену питанням безпеки на великих спортивних заходах і майданчиках». ***(Karen M. Lent, Anthony J. Dreyer, David Simon. Cyber threat outlook for the sports industry // Reuters (https://www.reuters.com/legal/legalindustry/cyber-threat-outlook-sports-industry-2024-05-15/). 15.05.2024).***

***

«Загрози кібербезпеці для бізнесу не тільки численніші, ніж будь-коли, але зараз стають все більш витонченими через використання зловмисниками штучного інтелекту (ШІ) і небезпечнішими у геополітичних цілях.

У своєму щорічному огляді кібератак, опублікованому в січні, дослідник аналізу загроз Check Point виявив, що організації по всьому світу зазнавали в середньому 1158 щотижневих кібератак кожна протягом 2023 року, що на 1% більше, ніж у 2022 році.

Тим часом у квітні стало відомо, що половина підприємств (50%) у Великій Британії, 70% підприємств середнього розміру (70%) і майже три чверті великих підприємств (74%) зазнали певної форми кібератак у останні 12 місяців.

Аналітика GlobalData вказує на те, що компанії усвідомлюють важливість кібербезпеки, займаючи 13 місце. тис із понад 130 у списку тем, які найчастіше згадуються у заявках компаній у всьому світі та в різних галузях з травня 2023 року по квітень 2024 року.

Незважаючи на це, нещодавнє дослідження GlobalData Thematic Intelligence: ESG Sentiment Polls Q1 2024 показало, що лише 8,8% компаній вважають, що кібербезпека є темою, яка найбільше вплине на них протягом наступних 12 місяців. Висока інфляція (36,2%), геополітичний конфлікт (35,9%) і цифровізація (10,5%) вважаються більш актуальними проблемами.

Навпаки, нещодавнє опитування ClubCISO, членського форуму керівників інформаційної безпеки, показало, що 62% керівників інформаційної безпеки (CISO) погоджуються, що галузь у цілому не здатна боротися з кібератаками ШІ, а 63% % заявляють, що оцінюють серйозність загрози, яку створюють для їхніх компаній кібератаки ШІ, як критичну або високу. Дійсно, 40% респондентів сказали, що поява штучного інтелекту не змінила їхні пріоритети, а для більш ніж трьох чвертей (77%) ШІ не спричинив змін у витратах на кібербезпеку.

Про це Роб Робінсон, керівник Telstra Purple у регіоні EMEA, який керує ClubCISO, розповідає Verdict: «Переважна більшість організацій, які ми виявили в цих висновках, не зробили нічого, щоб збільшити своє фінансування, щоб збільшити свої витрати на кібербезпеку для вирішення проблем, очевидно, це прискорить тип складності, обсяг, складність і автономію загроз, з якими стикаються організації... Переважна більшість бачить це як загрозу, але переважна більшість не витрачає на це гроші».

Витонченість кіберзагроз

Примітно, що методи, за допомогою яких кіберзлочинці вчиняють атаки, майже не змінюються, а ШІ в основному використовується для полегшення та вдосконалення існуючих підходів.

«Я б сказав, що самі загрози не обов'язково змінюються», — каже Баррі О'Коннелл, старший віце-президент і генеральний менеджер компанії Trustwave з керованого виявлення та реагування на територію EMEA. «Методики, інструменти та підходи, які використовують люди, загалом однакові, але вони набагато складніші».

Річард Хаммел, керівник відділу аналізу загроз для платформи видимості мережі NetScout, погоджується, коментуючи: «Вони не атакують їх за допомогою нових методів. Вони не обов'язково використовують нові вектори атаки. Вони не використовують нульові дні. По суті, вони просто використовують те саме, що використовували десятиліття чи два, і просто використовують це по-новому, або вони переслідують інші активи, або вони вкладають трохи більш передбачливо в те, що вони повторна атака».

Робінсон також виявив, що, незважаючи на прогрес ШІ, він не змінив підходи кіберзлочинців. «Це саме те, що він ускладнив, прискорив і прискорив кількість загроз у цих технологічних сферах», — каже він.

Він додає: «Це зводиться до обсягу та адаптивності. ШІ може зробити це так, як людина не може. Замість того, щоб застосовувати якийсь підхід, заснований на сценаріях, або якийсь рівень людської витонченості та інтелекту, ці витонченість і інтелект застосовуються штучним інтелектом до все більш ефективного рівня, і, отже, захоплення або викриття стає набагато швидшим і набагато витонченіший».

У поєднанні з більшою витонченістю, з якою штучний інтелект може здійснювати типи атак, з якими бізнес знайомий, це визнання того, що самі зловмисники стають більш організованими. Хаммел припускає, що «підпілля» кіберзлочинців перейшло від індивіда, який займається індивідуальними справами, до більш організованої екосистеми.

«Я кодуватиму зловмисне програмне забезпечення, ти будеш розсилати спам, ти будеш писати спам-повідомлення, ти будеш розміщувати мою інфраструктуру», — говорить він, характеризуючи цю зміну. «І це була еволюція протягом п’яти чи шести років. Отже, вони вже почали цей перехід, і він триває лише донині. Зараз у вас є ціла кримінальна екосистема, де ви можете фактично передати багато аспектів кампанії на аутсорсинг».

Цей вищий рівень організації означає, що злочинці також більш вибірково підходять до бізнесу.

О'Коннелл пояснює: «Те, що [організації] зараз знаходять, це те, що поверхня атаки набагато, набагато більша, ніж вони думали спочатку. Це не лише ваші комп’ютери, це тепер і ваші операційні засоби керування, і ваші фабрики, або ваш нафтопереробний завод, чи будь-що інше – тепер це частина поверхні атаки».

Уточнюючи це, він додає: «Проблема полягає в тому, що багато з цих організацій – особливо коли ви дивитесь на охорону здоров’я, виробництво тощо – мають дуже, дуже довгі ланцюжки поставок. Те, що ми бачимо, це те, що є пара векторів атак, які дуже, дуже поширені. Є електронна пошта, про яку всі говорять, але інша — це ланцюжок поставок і здатність поганого актора увійти в найслабшу частину цього ланцюга поставок».

Кіберризики для організацій

У нещодавно опублікованому GlobalData про кібербезпеку звіті за 2024 рік зазначається, що фішинг, зловмисне програмне забезпечення, атаки на воду та експлойти нульового дня є основними нецільовими загрозами, з якими сьогодні стикаються організації, а головними є фішинг, розподілена відмова в обслуговуванні (DDoS) і атаки на ланцюги поставок. цільові форми.

Ланцюжки постачання – як фізичні, так і цифрові – стали мішенню для зловмисників, які бажають проникнути в системи компанії через сторонній доступ чи інтеграцію або просто хочуть спричинити збій.

Про цю проблему у звіті пояснюється: «Кібератаки, націлені на ланцюжки поставок програмного забезпечення, стають все більш поширеними і, як правило, нищівними. Ці атаки є ефективними, оскільки вони можуть зруйнувати весь

ланцюжок постачання програмного забезпечення та послуг організації, що призведе до серйозних збоїв у роботі. Відповідно до IBM Cost of a Data Breach за звіту 2023 рік, на виявлення порушень ланцюга поставок знадобилося в середньому 233 дні та 74 дні на локалізацію, а загальний життєвий цикл становив 307 днів. Цей середній життєвий цикл становив 37 днів, або на 13% більше, ніж середній життєвий цикл у 270 днів для порушень даних, пов'язаних з іншою причиною. У дослідженні 2023 року 15% організацій визначили компрометацію ланцюга постачання як джерело витоку даних».

У звіті також зазначається, що уряди в усьому світі починають серйозно ставитися до безпеки ланцюга поставок і тісніше співпрацювати, щоб запобігти таким атакам через їх потенційно серйозні наслідки. Дійсно, потенціал для створення хаосу та напруги є однією з таких причин, чому кібератаки, подібні до тих, що спрямовані на ланцюги поставок, зосереджені не лише на бізнесі, але й на геополітичних цілях.

Геополітичні кібератаки

«Я б сказав, що атаки, пов'язані з геополітичними подіями, є масштабнішими, ніж будь-коли раніше», — каже Хаммел. «Чесно кажучи, якщо мені довелося визначити переломний момент, то це був момент, коли Росія вторглася в Україну...»

«Це траплялося епізодично впродовж історії, але тепер здається, що майже кожен політичний крок, чи кожна велика річ, чи будь-хто починає говорити про те, як вони збираються надіслати гуманітарну допомогу в Україну чи Саудівську Аравію, і Німеччина разом координує рух зброї. і подібні речі – все це як основні міжнародні розмови, речі, які впливають на НАТО, речі, які впливають на Організацію Об'єднаних Націй – усе це виглядає як чудова можливість для цих хактивістів посіяти хаос або висловити свої плани.»

Одним із таких нещодавніх прикладів – фактично до вторгнення Росії в Україну – став момент, коли Швеція подала заявку на вступ до НАТО. Країна спостерігала натиск DDoS-атак, а у звіті NetScout зазначено: «Це сигналізує про сплеск небаченої напруги та помсти з боку кількох політично мотивованих

хакерських груп. Насправді російські хакери порушили урядові операції у Швеції за допомогою атак програм-вимагачів».

Відповідно Хаммел вказує на квазіурядові веб-сайти як на область, яка потребує більшого захисту.

«Якби мені довелося вибрати якусь одну сферу, якій, на мою думку, слід приділити трохи більше уваги, я б сказав, що це багато веб-сайтів, які стосуються політичних питань, які не обов'язково стосуються прямого уряду, вони не є державними адміністративними порталами або щось подібне, але це сайти, які обробляють державну інформацію або обробляють послуги чи повідомлення, які мають відношення до громадської аудиторії», – каже він.

«Візьмемо, наприклад, усі ці геополітичні конфлікти, які зараз тривають, і ви згадаєте Anonymous Sudans, NoNames і всіх цих інших загрозливих акторів. Я думаю, що за останні шість місяців ми бачили близько 1200 загрозливих осіб, скрізь, і кожного разу, коли ви віддаєте одну, повертається 1000 наказів. Ці хлопці хочуть посіяти розбрат, вони хочуть посіяти хаос, вони хочуть засмутити маси, вони хочуть створити параною та страх, і тому часто вони нападають на веб-сайти, які не обов'язково є критичними, але це змушує людей думати, «Ого, вони просто зняли це. Що ще вони можуть зробити?»

Кіберризики для організацій

У нещодавно опублікованому GlobalData про кібербезпеку звіті за 2024 рік зазначається, що фішинг, зловмисне програмне забезпечення, атаки на воду та експлойти нульового дня є основними нецільовими загрозами, з якими сьогодні стикаються організації, а головними є фішинг, розподілена відмова в обслуговуванні (DDoS) і атаки на ланцюги поставок. цільові форми.

Ланцюжки постачання – як фізичні, так і цифрові – стали мішенню для зловмисників, які бажають проникнути в системи компанії через сторонній доступ чи інтеграцію або просто хочуть спричинити збій.

Про цю проблему у звіті пояснюється: «Кібератаки, націлені на ланцюжки поставок програмного забезпечення, стають все більш поширеними і, як правило, нищівними. Ці атаки є ефективними, оскільки вони можуть зруйнувати весь

ланцюжок постачання програмного забезпечення та послуг організації, що призведе до серйозних збоїв у роботі. Відповідно до IBM Cost of a Data Breach за звіту 2023 рік, на виявлення порушень ланцюга поставок знадобилося в середньому 233 дні та 74 дні на локалізацію, а загальний життєвий цикл становив 307 днів. Цей середній життєвий цикл становив 37 днів, або на 13% більше, ніж середній життєвий цикл у 270 днів для порушень даних, пов'язаних з іншою причиною. У дослідженні 2023 року 15% організацій визначили компрометацію ланцюга постачання як джерело витоку даних».

У звіті також зазначається, що уряди в усьому світі починають серйозно ставитися до безпеки ланцюга поставок і тісніше співпрацювати, щоб запобігти таким атакам через їх потенційно серйозні наслідки. Дійсно, потенціал для створення хаосу та напруги є однією з таких причин, чому кібератаки, подібні до тих, що спрямовані на ланцюги поставок, зосереджені не лише на бізнесі, але й на геополітичних цілях.

Геополітичні кібератаки

«Я б сказав, що атаки, пов'язані з геополітичними подіями, є масштабнішими, ніж будь-коли раніше», — каже Хаммел. «Чесно кажучи, якщо мені довелося визначити переломний момент, то це був момент, коли Росія вторглася в Україну...»

«Це траплялося епізодично впродовж історії, але тепер здається, що майже кожен політичний крок, чи кожна велика річ, чи будь-хто починає говорити про те, як вони збираються надіслати гуманітарну допомогу в Україну чи Саудівську Аравію, і Німеччина разом координує рух зброї. і подібні речі – все це як основні міжнародні розмови, речі, які впливають на НАТО, речі, які впливають на Організацію Об'єднаних Націй – усе це виглядає як чудова можливість для цих хактивістів посіяти хаос або висловити свої плани.»

Одним із таких нещодавніх прикладів – фактично до вторгнення Росії в Україну – став момент, коли Швеція подала заявку на вступ до НАТО. Країна спостерігала натиск DDoS-атак, а у звіті NetScout зазначено: «Це сигналізує про сплеск небаченої напруги та помсти з боку кількох політично мотивованих

хакерських груп. Насправді російські хакери порушили урядові операції у Швеції за допомогою атак програм-вимагачів».

Відповідно Хаммел вказує на квазіурядові веб-сайти як на область, яка потребує більшого захисту.

«Якби мені довелося вибрати якусь одну сферу, якій, на мою думку, слід приділити трохи більше уваги, я б сказав, що це багато веб-сайтів, які стосуються політичних питань, які не обов'язково стосуються прямого уряду, вони не є державними адміністративними порталами або щось подібне, але це сайти, які обробляють державну інформацію або обробляють послуги чи повідомлення, які мають відношення до громадської аудиторії», – каже він.

«Візьмемо, наприклад, усі ці геополітичні конфлікти, які зараз тривають, і ви згадаєте Anonymous Sudans, NoNames і всіх цих інших загрозливих акторів. Я думаю, що за останні шість місяців ми бачили близько 1200 загрозливих осіб, скрізь, і кожного разу, коли ви віддаєте одну, повертається 1000 наказів. Ці хлопці хочуть посіяти розбрат, вони хочуть посіяти хаос, вони хочуть засмутити маси, вони хочуть створити параною та страх, і тому часто вони нападають на веб-сайти, які не обов'язково є критичними, але це змушує людей думати, «Ого, вони просто зняли це. Що ще вони можуть зробити?»

Сектори ризику

З іншого боку, зрозуміло, що типи організацій, які піддаються найбільшому ризику кібератак, – це ті, які можуть найбільше втратити, наприклад організації, що займаються фінансовими послугами та охороною здоров'я. Хаммел, однак, вважає, що фінансові послуги займають друге місце після уряду за своєю цифровою безпекою – і що необхідність у цьому через обробку грошей не є єдиним важливим фактором.

«Одна з причин, чому я твердо вірю, що вони такі, полягає не лише в грошах, адже ці хлопці діляться знаннями», — говорить він, згадуючи зокрема фінанси, банківську справу, комерційну банківську справу та страхування. «FS-ISAC, так? Це чудовий ресурс, і більшість основних гравців у банківській галузі є частиною FS-ISAC. Вони вільно діляться всією цією інформацією. «Гей, ми бачили цю

загрозу. Це надходить таким чином. Ось мережа. Ось деталі. Ось характеристики. Ось аналіз".

«І це групове мислення, і це спільні знання, щоб кожен знав, що там і що на них впливає. А це, у свою чергу, означає покращення стану безпеки для багатьох із цих організацій».

Центр обміну та аналізу інформації про фінансові послуги (FS-ISAC) — це міжнародна некомерційна членська організація, метою якої є «зменшення кіберризиків для сектора шляхом обміну розвідувальними даними».

Зазначаючи, що існують ISAC для різних інших галузей, Хаммел говорить про їхню цінність ширше: «Ви бачите, що рівень зрілості багатьох професіоналів із безпеки, які є частиною цих речей, набагато вищий, ніж тих, хто не є, оскільки [останні] не отримують вигоди від цієї частки групи. Я думаю, що це відіграє велику роль. Цей процес перевиховання, щоб переконатися, що всі знають про те, що там відбувається, безумовно, є рівні тих, хто готовий».

Часом охорона здоров’я була менш підготовленим сектором, ніж мав би бути. У Великій Британії, наприклад, застаріле програмне забезпечення інколи піддавало ризику Національну службу охорони здоров’я. Однак у більш широкому плані чутливість і, отже, цінність даних у сфері охорони здоров’я в усьому світі робить їх основною ціллю.

«Цінність, яка відбувається в охороні здоров’я, насправді полягає в даних пацієнтів і в можливості отримати їх», — говорить О'Коннелл. «Те, що ми бачимо зараз — і це, ймовірно, більше в США на даний момент, враховуючи тамтешню систему охорони здоров’я — це значні викупи, які в декілька разів перевищують середні, які сплачують організації охорони здоров’я, не кажучи вже про вплив втрати доходу.

«Ми побачимо сотні мільйонів доларів втрати прибутку в цих організаціях, тому що вони не можуть працювати, і тоді вони зрештою заплатять викуп. Отже, я думаю, що те, що відбувається, і знову ж таки, це не є чимось незвичайним для великої кількості злочинної діяльності, полягає в тому, що організації, які, ймовірно, найменш підготовлені або історично були найменш підготовленими,

саме там ми спостерігаємо збільшення кількість ряду кількість нападів. Охорона здоров'я, як правило, досить м'яка».

О'Коннелл також зазначає, що Trustwave вважає, що юридичні фірми та фірми, що надають послуги, піддаються дедалі більшому ризику атак.

«Юридичні фірми мають багато даних, у них часто є сховище даних — якийсь інструмент, який використовується спеціально для цієї галузі, — але багато з них передається електронною поштою, надсилається зовнішнім юрисконсультам і повертається знову», — каже він. «Ми бачимо цінність цієї інтелектуальної власності та вашу репутацію як юридичної фірми. Якщо я дізнаюся, що хтось перебуває в судовій справі, і я можу отримати інформацію, тоді, як юридична фірма, я можу почати запитувати умови, якщо ви хочете повернути цю інформацію, якщо ви не хочете розміщувати це громадськість».

У той час як деякі сектори та підприємства можуть бути більш схильні до ризику, ніж інші, реальність така, що всі піддаються ризику дедалі більше.

Про це Робінсон каже: «Я вважаю, що ми можемо точно визначити деякі ризики та ризики в певних ринкових вертикалях, це більше стосується розуміння цього комбінованого профілю загроз і цього комбінованого ризику».

Профілактика та захист

Небагато організацій сьогодні не мають заходів для захисту від кіберзагроз. Складність полягає в тому, щоб знати, що потрібно, скільки потрібно витратити та як бути в курсі загроз, що розвиваються.

«Одна з проблем, з якою ми стикаємося, полягає в тому, що визначення або визначення прибутку від інвестицій у кібербезпеку є дещо туманним», — говорить О'Коннелл. «Ви фактично намагаєтеся довести негатив. Це підхід страхового типу. Отже, це складно, коли підприємства мають дилеми щодо того, куди інвестувати, особливо з цифрової точки зору. «Чи варто мені інвестувати в покращення своєї платформи, визначаючи все більше й більше використання соціальних медіа, мої маркетингові кампанії чи щось інше?»

«А потім хтось каже: «Ну, вам тут виставили рахунок на 20 мільйонів, щоб розробити програму кібербезпеки». І виникає запитання: «Яка я від цього

віддамся?» Це складна розмова: «Ну, ви гарантуєте, що мене не зламатимуть, чи ви гарантуєте, що я буду в безпеці?» І відповідь така: якщо у вас є хоч якийсь глузд, відповідь така: «Ні, я взагалі не можу цього гарантувати!»

«То що, ви хочете, щоб я витратив 20 мільйонів на цю річ, за яку ви не можете гарантувати, що вона справді щось покращить?» «Ну, так, я знаю».

Незважаючи на труднощі з визначенням того, як розподілити інвестиції в кібербезпеку, це залишається критичним видатком. І, з часом, сам сектор розвивався.

«Тепер розмова про безпеку — це не обов'язково профілактика як наріжний камінь, а видимість», — каже Хаммел. «Ми хочемо якомога швидше виявити загрозу. Якщо ви зможете помітити це, перш ніж вони вас скомпрометують, чудово, чи не так? Зроби це. Якщо ви не можете, вам потрібно виявити їх у момент, коли вони входять, або дуже скоро після цього. Ви також повинні мати судово-медичні докази. Якщо вони скомпрометували вас, що вони зробили потім? Як вони повертаються вбік, убік? Вони щось викрали?»

Хаммел додає: «З точки зору відповідача, ми повинні переконатися, що кожен окремий фрагмент відкритої інфраструктури у вашій мережі перебуває в стадії виробництва. Недостатньо сказати: «Ну, просто мій важливий актив тут у безпеці, і я в порядку». Не обов'язково, тому що, навіть якщо ваші критичні активи залишаться на місці, якщо всі інші кісточки доміно навколо вас впадуть, ви все одно матимете яйце на обличчі, чи не так?

«Супротивники зроблять на цьому вигоду. І вони будуть цим хвалитися. І вони висуватимуть претензії. А потім, раптом, у вас є дуже наполегливий журналіст, який приходить і каже: «Чоловіче, це зняли, і ось доказ цього». І тепер у вас є ця стаття на CNN, і ця компанія каже: «Ну, привіт, наші критичні речі ніколи не знижувалися». Не має значення. Деякі частини вас опустилися. Отже, тепер у вас є шкода репутації, чи не так?

«Отже, нам просто потрібно думати про речі з такої точки зору — просто переконатися, що все, що вам належить, усе, що має мережевий слід, захищено. І зрозумійте, що супротивники використовують ті самі старі речі знову і знову, але

вони змінюють те, на що націлені. Вони обов’язково змінюють те, як вони збираються за цими активами».

«Стан кібербезпеки: штучний інтелект і геополітика означають більшу загрозу, ніж будь-коли» був створений і опублікований Private Banker International, брендом, що належить GlobalData». ***(Stu Robarts. The state of cybersecurity: AI and geopolitics mean a bigger threat than ever // yahoo! finance (https://finance.yahoo.com/news/state-cybersecurity-ai-geopolitics-mean-101744261.html?fr=sycsrp_catchall). 21.05.2024).***

***

«В епоху, коли загрози з кіберсфери стають все більш витонченими, бути проактивним більше не розкіш, а радше необхідність. Вирішальна роль, яку штучний інтелект і автоматизація відіграють у визначенні тенденцій кібербезпеки, стає все більш очевидною, ведучи трансформацію в різних вимірах операцій у сфері кібербезпеки. Від виявлення загроз до прогнозної аналітики, рішення на основі штучного інтелекту революціонізують методологію, що використовується для протидії цим цифровим загрозам.

Наш останній Всебічний щорічний звіт про моделі кіберзагроз висвітлює ландшафт загроз, що постійно змінюються, у кіберсфері. Була відмічена тривожна статистика: у 2023 році 66% організацій постраждали від програм-вимагачів, а кількість атак зловмисного програмного забезпечення Internet of Things IoT зросла в чотири рази, що чітко підкреслює нагальну потребу в надійних структурах кібербезпеки, як ніколи раніше.

У цьому документі розглядатимуться майбутні тенденції кібербезпеки та потенційні загрози, які очікуються на 2024 рік. У ньому розглядатиметься, як штучний інтелект та автоматизація змінюють парадигму кібербезпеки, і запропоновано стратегічний курс дій, який допоможе вам зберегти перевагу над кіберзлочинцями.

На арені кібербезпеки постійно з’являються нові тенденції та загрози. Це значні досягнення, які потребують ретельного вивчення у 2024 році.

Розвиток ШІ та машинного навчання в безпеці

Штучний інтелект і машинне навчання стають все більш помітними в ландшафті кібербезпеки. Вони забезпечують проактивне виявлення загроз і швидке реагування. Замість того, щоб просто реагувати на атаки після їх виникнення, системи ШІ та ML завчасно визначають потенційні загрози, що дозволяє вчасно вжити контрзаходів. Подумайте про штучний інтелект та машинне навчання як про авангард ваших зусиль у сфері кіберзахисту, які виявляють потенційних загарбників до того, як вони зруйнують вашу цифрову фортецю.

Переваги та проблеми квантових обчислень

Цим ми представляємо квантові обчислення, чудову, але складну тему щодо кібербезпеки. Один із аспектів цієї сфери має величезний потенціал щодо подолання кіберзагроз, революції в процесах шифрування та вдосконалення механізмів захисту даних. Водночас його майстерність також може зробити його непоборним інструментом для кіберзлочинців. Відсутність точного регулювання може спрямувати Quantum Computing на сприяння надзвичайно інтенсивним атакам, які переважають навіть наші найвідоміші системи захисту. З розвитком квантових обчислень стає необхідністю адаптувати стратегії кібербезпеки відповідно до неймовірних досягнень.

Підкреслено стурбованість безпекою Інтернету речей в Інтернеті речей

Повсюдність Інтернету речей (IoT) незаперечна. Він поширюється на різні аспекти, включаючи розумні будинки, розумні міста, охорону здоров’я, транспорт тощо. Згодом розширення IoT створює середовище, яке стає все більш вразливим до кіберзагроз. Очікуваний сценарій у 2024 році передбачає приділення більшої уваги безпеці IoT з наголосом на посиленні захисту цих взаємопов’язаних пристроїв. Ініціативи з кібербезпеки будуть спрямовані на пом’якшення цієї вразливості, тим самим зміцнюючи екосистему IoT від потенційних небезпек.

У світі, який поступово оцифровується, безпека полягає не лише в реагуванні, а й у підтримці проактивної позиції. Розуміння переважаючих тенденцій і загроз кібербезпеки, які визначатимуть 2024 рік, буде критично важливим. Відповідна адаптація оборонних стратегій і консолідація вашого

цифрового середовища є фундаментальними кроками, які мають бути пріоритетними.

Основні загрози кібербезпеці, які очікуються у 2024 році

Еволюція та вдосконалення програм-вимагачів

Очікуйте зростання складності атак програм-вимагачів у 2024 році, які вийдуть за рамки простого шифрування даних. Останні події підкреслюють цю еволюцію. BlackCat, сумно відома група програм-вимагачів, подала скаргу на програмну компанію MeridianLink за те, що вона не повідомила про свою атаку Комісії з цінних паперів і бірж США. За іншим сценарієм канадський державний постачальник послуг став жертвою атаки програм-вимагачів, яка скомпрометувала 14 мільйонів записів особистих даних. Хакери, як правило, націлені на файли резервних копій, шифруючи конфіденційні дані та вимагаючи жертв, часто погрожуючи оприлюднити інформацію. Оскільки страхування стає дорогим, а опір жертви сплаті зростає, ці кіберзлочинці починають агресивні дії. Підготуйтеся до цих загроз, покращивши свої протоколи кібербезпеки та стратегічні відповіді.

AI створює хвилі в кібербезпеці

Штучний інтелект (AI). Це викликає певний ажіотаж у світі кібербезпеки, і не завжди з найкращих причин. Як цього разу наші технічні майстри знайшли підступного хлопця зі зловмисним програмним забезпеченням, який ховався в пристроях віртуальної реальності (VR), непомітно переглядаючи приватні дані, як-от дані кредитної картки та паролі.

Час, коли хмарна система зберігання Samsung випадково розкрила особисту інформацію понад 100 000 користувачів? Так, не дуже. Ці інциденти лише показують, як зростання ШІ та високотехнологічних штуковин може призвести до більш складних і карколомних порушень безпеки.

Ці події справді підкреслюють необхідність для нас не відставати від темпу та постійно розробляти нові способи використання ШІ для захисту від цих хитрих цифрових загарбників. Ви не думаєте.

Вразливі місця в ланцюзі поставок

Питання вразливості в ланцюгах постачання стає надзвичайно важливим у 2024 році. Значний інцидент з витоком даних стався, коли незадоволені співробітники розкрили особисті записи відомої автомобільної корпорації Tesla німецькому медіа-агентству. Ці інциденти переконливо ілюструють важливість посилення протоколів кібербезпеки в усіх аспектах ланцюга постачання для забезпечення цілісності бізнес- операцій. Вкрай важливо залишатися пильним перед обличчям цих потенційних загроз і вживати профілактичних заходів для сприяння безпечному робочому середовищу.

Вплив нових технологій на кібербезпеку

Коли ви орієнтуєтеся в динамічному ландшафті кіберзагроз, дуже важливо визнати трансформаційний потенціал нових технологій. Тут у центрі уваги два таких досягнення: технологія блокчейн і біометрична безпека – основні елементи, що формують тенденції та загрози кібербезпеки у 2024 році.

Стратегічна інтеграція блокчейна

Стратегічна інтеграція Blockchain у протоколи кібербезпеки забезпечує безпрецедентний рівень безпеки, який захищає від підробки даних і незаконної діяльності. Використовуючи незмінну децентралізовану систему цифрового реєстру, Blockchain пропонує надійну безпеку за своєю конструкцією — усуває єдину точку збою та підтримує прозорість транзакцій. Ця революційна технологія протистоїть критичним загрозам, надійно шифруючи дані та забороняючи несанкціонований доступ. Запровадження Blockchain демонструє прогресивну тенденцію до 2024 року щодо зменшення ризиків витоку даних і підвищення цілісності цифрових транзакцій.

Удосконалення біометричної безпеки

З огляду на розвиток кіберзагроз, новаторські досягнення в біометричній безпеці висвітлюють відхід від традиційних систем на основі паролів. Забезпечуючи персоналізований, надійний рівень безпеки, Біометрична безпека використовує унікальні біологічні особливості, такі як відбитки пальців або розпізнавання обличчя, для автентифікації користувача. Поява безпарольних

технологій, прийнята учасниками Альянсу FIDO Alliance, підкреслює рух до стійких до фішингу рішень безпеки. Отже, ці досягнення розширюють можливості справжньої перевірки особи, протидіють крадіжці особистих даних і посилюють заходи кібербезпеки в 2024 році. Прогрес у біометричній безпеці є свідченням безперервних зусиль з протидії тенденціям і загрозам кібербезпеки.

Наслідки кібербезпеки в світлі

Після глобального переходу до віддалених робочих середовищ у 2024 році спостерігалося помітне зростання кількості порушень кібербезпеки. Перехід до протоколів розподіленої робочої сили та технологій дистанційної роботи розширив спектр потенційних можливостей кібератак, таким чином підвищивши вразливість суб'єктів господарювання до відповідних винних у кіберзлочинності.

Забезпечення розподіленої робочої сили

У нашу епоху віддаленої роботи введення ефективних заходів безпеки для розподілених робочих сил має першочергове значення. Швидкий перехід до децентралізованих операцій відкрив шляхи для безлічі загроз кібербезпеці. На щастя, проактивні організаційні стратегії можуть пом'якшити ці небезпеки.

Головною стратегією є інтеграція інтерактивного та захоплюючого навчального досвіду в навчання співробітників. Традиційна освіта з кібербезпеки, яка часто характеризується довгими лекціями та статичними презентаціями, більше не підходить. Багато прикладів організацій, які включають симуляції гейміфікації та сценарії реального світу в навчальні модулі. Цей метод сприяє активній участі, закріплюючи ключові концепції кібербезпеки в процесі захоплюючого навчання. Пам'ятайте, що культура обізнаності про безпеку є ключовою для захисту від кіберзагроз, що постійно виникають.

Необхідність проактивних стратегій кібербезпеки

У сфері кібербезпеки, що постійно розвивається. Технологічний прогрес, як правило, розвивається стрімко, часто випереджаючи нашу здатність повністю зрозуміти або передбачити потенційні кіберзагрози, пов'язані з цими вдосконаленнями.

Прогнозні технології безпеки

У 2024 році, коли ви зміцнюєте свою цифрову сферу, першочерговим буде впровадження технологій прогнозної безпеки. Використовуючи сильні сторони штучного інтелекту (ШІ), такі технології просіюють гори даних. Наприклад, алгоритми машинного навчання пропонують такі виняткові можливості, як виявлення загроз у реальному часі та реагування на них, аналіз поведінки та автоматизація рутинних завдань. Думайте про ці передові системи як про своїх цифрових ворожок, які завчасно попереджають про ймовірні загрози з різних точок зору.

ШІ — не єдиний гравець на арені прогнозної безпеки. Також подумайте про таку революцію, як Quantum Computing. Очікується, що організації, які не зможуть запровадити постквантову криптографію до 2024 року, можуть виявитися недостатньо готовими до загроз, коли квантові комп'ютери досягнуть зрілості. Таким чином, початок переходу на PQC у 2024 році може стати вирішальним кроком до готовності до квантово надійної безпеки.

Програми-вимагачі, атаки зловмисного програмного забезпечення Інтернету речей або загрози на основі штучного інтелекту для віртуальної реальності та хмарних сховищ, майбутнє рясніє викликами. Але не лякайтеся. Натомість сприймайте це як заклик до дії. Озбройтеся технологіями інтелектуальної безпеки, будьте в курсі глобальних законів про захист даних і добре навчайте свою команду. Пам'ятайте, що стійкість є ключовим у цьому кіберсвіті, що постійно змінюється. Адаптуйте, передбачте та захистіть свою цифрову сферу від кіберзагроз 2024 року.

Більше не хочеться, включаючи тайську мову до глобальних лінгвістичних програм навчання. Оскільки наш світ стає все більш зв'язаним, хвилювання від багатомовності є надто важливим, щоб ігнорувати його. І вгадайте, яка мова викликає хвилю в глобальних лінгвістичних навчальних програмах. Це тайська мова. Чарівна мова нашої приймаючої країни». ***(Kashish Sharma. Cybersecurity trends and threats in 2024 // The thaiger (https://thethaiger.com/news/national/cybersecurity-trends-and-threats-in-2024). 23.05.2024).***

***

«За останні роки обробна промисловість зазнала кардинальної трансформації, використовуючи цифрові технології для підвищення продуктивності, ефективності та інновацій. У той же час така підвищена залежність від підключених систем і пристроїв наразила виробників на зростаючу кількість загроз кібербезпеці.

Розвиток операційних технологій і впровадження пристроїв Інтернету речей значно розширили зону атаки виробничої промисловості. Кожна точка входу — це можливість для кіберзлочинців порушити виробництво та скомпрометувати критичні системи.

Атаки на ланцюги поставок стають дедалі витонченішими, і зацікавлені сторони у виробництві повинні бути готові до кіберзагроз, які, найімовірніше, вплинуть на їх діяльність. Наприклад, атаки програм-вимагачів ставлять під загрозу дані та можуть зупинити цілі виробничі лінії. Крадіжка інтелектуальної власності є ще однією потенційною проблемою, коли як зовнішні, так і внутрішні сторони можуть викрасти комерційні таємниці, патенти або неоприлюднені проекти.

Наслідки кіберінцидентів добре відомі, виходячи за рамки безпосередніх операційних невдач. Такі збої можуть мати далекосяжні наслідки, включаючи зниження довіри клієнтів і наслідки для безпеки для партнерів або інших зацікавлених сторін. Інциденти кібербезпеки можуть вплинути навіть на найвідоміші технологічно просунуті компанії, що підкреслює критичну важливість посилення заходів кібербезпеки у всьому виробничому секторі.

Виробники мають повноваження взяти під контроль свою кібербезпеку та створити стійкість до нових загроз. Впроваджуючи проактивний, багаторівневий підхід до кібербезпеки, вони можуть захистити активи, зберегти довіру зацікавлених сторін і позиціонувати себе для довгострокового успіху. Чотири основні елементи створюють потужний захист від кіберінцидентів.

Забезпечте раннє виявлення загроз і реагування. Для захисту від кіберзагроз виробники можуть впроваджувати системи, які дозволяють їм виявляти й запобігати потенційним проблемам. Дослідження IBM показали, що організаціям

потрібно в середньому 204 дні, щоб виявити порушення. Чим більше часу потрібно для виявлення проблеми, тим довше компанії залишаються вразливими до збитків.

Пам’ятаючи про це, виробники можуть розглянути можливість розгортання інструментів безпеки та управління подіями (SIEM) і розширеного виявлення та реагування (XDR). Вони пропонують моніторинг у реальному часі та можливості швидкого реагування. Інструменти SIEM і XDR можуть запобігти переростанню атаки в кризу, виявляючи аномалії та швидко реагуючи.

Розвивайте кіберпідковану робочу силу. Людські помилки залишаються критично слабкою стороною кібербезпеки: майже 75% атак є результатом простих помилок. Безперервна освіта та заглиблене навчання є незамінними для усунення цих вразливостей. Залучаючи співробітників до активного навчання, яке моделює реальні сценарії кіберзагроз, кожна особа в організації може навчитися виявляти та запобігати атакам, а організація може розвивати культуру, яка має більшу кіберобізнаність.

Комплексне навчання з кібербезпеки готує всю команду, від заводського цеху до керівного рівня, до знань, щоб виступати в якості першої лінії захисту компанії від онлайн-загроз. Беручи участь у регулярних реалістичних тренінгах, співробітники вдосконалюють свою здатність виявляти ризики безпеці та реагувати на них.

Навчання загальної робочої сили може включати щоденні найкращі практики кібербезпеки, такі як ідентифікація фішингових електронних листів і повідомлення про них, використання надійних паролів і застосування звичок безпечного перегляду. Інтерактивні модулі та вправи з імітації фішингу можуть допомогти співробітникам відточити свою здатність виявляти поширені загрози та реагувати на них.

ІТ-командам і командам безпеки потрібна додаткова технічна підготовка для запобігання, виявлення та ефективного реагування на кіберінциденти. Одним з ефективних підходів є проведення «настільних вправ», під час яких команди тренуються реагувати на гіпотетичні сценарії, такі як розподілена атака на відмову в обслуговуванні (DDoS), програмне забезпечення-вимагач або внутрішня загроза.

Ці тренування допомагають оцінити ефективність плану реагування на інциденти компанії та визначити сфери, які потрібно покращити.

Підготовка лідерів має включати все, що отримує загальна робоча сила, а також може охоплювати такі теми, як управління ризиками, відповідність та реагування на інциденти зі стратегічної точки зору.

Цілеспрямоване, цікаве навчання для всіх співробітників перетворює робочу силу на ефективну першу лінію захисту від онлайн-загроз.

Дотримуйтесь надійних систем управління ризиками. Навігація у сфері кібербезпеки вимагає не лише пильності; це вимагає стійкої та адаптованої структури. Дотримуючись вказівок ISO 27001, провідного глобального стандарту для системи управління інформаційною безпекою (ISMS), забезпечує виробників надійною інфраструктурою кібербезпеки.

ISO 27001 був представлений у 2005 році та оновлений у 2013 та 2022 роках на основі зміни цифрового ландшафту. Останній стандарт встановлює новий стандарт кібербезпеки. Оскільки кінцевий термін переходу від старої версії до 2025 року наближається, саме час розглянути наявні засоби захисту від цифрових загроз.

Важливо зазначити, що ISO 27001 містить правила та процедури, а не точний список справ. Нижче наведено кілька найкращих практик, які допоможуть організаціям підготуватися до відповідності стандартам ISO 27001:

Проведіть внутрішній аудит безпеки, щоб отримати кращий огляд систем безпеки, програм і пристроїв.

Визначте політику безпеки, зокрема те, як організація керує та впроваджує засоби контролю безпеки.

Контролюйте доступ до даних і подумайте про збереження записів про вхід для використання в майбутньому.

Впровадити заходи безпеки пристрою. Google Workspace і Microsoft 365 мають вбудовані конфігурації безпеки пристрою, які допоможуть.

Подумайте про безпеку виходу співробітника. Співробітник, який звільняється, не повинен мати доступ до систем організації.

Шифруйте організаційні дані для забезпечення цілісності та конфіденційності.

Створюйте резервні копії важливих даних і визначте місце резервного копіювання, частоту та період зберігання даних.

Розгорніть технологію для міцнішого захисту. Технологія може бути цінною для виробників, особливо для тих, хто має обмежені ресурси або не має спеціальної групи безпеки. Правильне програмне забезпечення для кібербезпеки може допомогти підвищити рівень безпеки, не обов'язково збільшуючи кількість персоналу. Вибираючи інструменти, важливо враховувати ті, які забезпечують комплексні функції безпеки, пам'ятаючи при цьому про навантаження та можливості вашої IT-команди.

Добре розроблена система може автоматизувати важливі завдання, надавати чітку інформацію та підтримувати відповідність. Однак важливо розуміти, що жодне програмне забезпечення для кібербезпеки не може зробити все. Процес інтеграції може вимагати коригування для забезпечення оптимальної продуктивності у вашому унікальному середовищі.

Зрештою, правильне рішення з кібербезпеки має дати змогу вашій команді зосередитися на основних бізнес-цілях, одночасно забезпечуючи надійний захист від нових загроз. Ретельно відбираючи та розміщуючи відповідні інструменти, виробники можуть посилити свою позицію в галузі кібербезпеки та створити стійкість до цифрових ризиків.

Перевіряючи рішення з кібербезпеки, виробники можуть ставити запитання щодо забезпечення безпечної та ефективної інтеграції, наприклад:

Як інструмент захищає як від відомих уразливостей, так і від нових загроз?

Який процес виявлення загроз у реальному часі та попередження?

Чи може це рішення бездоганно інтегруватися з нашою існуючою технічною інфраструктурою?

Маючи на увазі подібні запитання, лідери виробництва можуть переконатися, що обрана ними система забезпечить їм максимальний захист відповідно до їх унікальної ситуації.

Створення кіберстійкого виробничого сектору вимагає співпраці між виробниками, експертами з кібербезпеки, галузевими групами та іншими зацікавленими сторонами. Обмінюючись знаннями, інтелектуальними даними та ресурсами, компанії можуть покращити свою колективну здатність передбачати кіберзагрози, готуватися до них і реагувати на них.

Приймаючи культуру кіберстійкості та дотримуючись провідних галузевих практик, виробничий сектор може захистити свою діяльність і підтримувати свій важливий внесок у світову економіку». ***(Matt Warner. Four Cybersecurity Moves Every Manufacturer Can Make // Keller International Publishing Corp (https://www.supplychainbrain.com/blogs/1-think-tank/post/39645-four-cybersecurity-moves-every-manufacturer-can-make). 23.05.2024).***

***

«…Національна поліція Філіппін (PNP) знову стала жертвою кібератаки. Невловимий хакер, відомий як ph1ns, двічі зламав системи PNP, скомпрометувавши конфіденційні дані та виявивши потребу в надійних заходах кібербезпеки.

Спочатку зловмисник націлився на «Систему інформації та управління логістичними даними PNP» (PLDIMS), витоку понад 393 894 рядків особистої інформації. Серед постраждалих були високопоставлені посадовці, включно з головою ПНП і речником. Потім хакер продовжив свої дії, зламавши онлайн-систему PNP Управління з вогнепальної зброї та вибухівки. Відкриті дані включають повні імена, дати народження, цивільний стан, електронні адреси, номери мобільних телефонів, ІПН та найближчих родичів із детальною інформацією. Насторожує те, що хакер показав докази того, що він отримав доступ до інформації про 679 910 осіб, які зареєстрували свою зброю в агентстві.

Остання атака сталася, коли хакер скористався уразливістю локального включення файлів (LFI) і обійшов перевірку електронної пошти на онлайн-платформі ліцензій/дозволів Управління з питань вогнепальної зброї та вибухових речовин (FEO), викравши приблизно 1,6 терабайт даних.

Після злому дослідники з кібербезпеки запропонували кілька заходів для запобігання майбутнім інцидентам, наприклад розгортання брандмауерів веб-додатків (WAF), виправлення вразливостей і моніторинг підключень до конфіденційних служб.

Після порушення Департамент інформаційних і комунікаційних технологій (DICT) розпочав спільне розслідування з кількома правоохоронними та розвідувальними органами. Джеффрі Ян К. Дай, заступник секретаря DICT з управління інфоструктурою, кібербезпеки та підвищення кваліфікації, повідомив Manila Bulletin, що департамент зустрівся з Національним бюро розслідувань (NBI), Національною поліцією Філіппін (PNP) і Радою національної безпеки (NSC) Понеділок, 20 травня. За словами Дая, цей загальнодержавний підхід використовує сильні сторони та ресурси різних агенцій, забезпечуючи більш комплексну та ефективну відповідь на захист даних державних установ. Співпрацюючи, ці агенції можуть обмінюватися інформацією, координувати дії та застосовувати свій спеціалізований досвід, що призводить до надійного захисту від кіберзагроз і більш стійкої національної кібербезпеки.

«Ми підійдемо до цього колективно з правоохоронними та розвідувальними органами», — заявив Дай. «Ми вже ідентифікуємо кіберзлочинця, відомого як PH1NS, і впевнені, що зможемо знайти його/її та його співробітників. Ми виявили, як він проник у систему та переміщувався від однієї системи PNP до іншої. У нас також є його тактика, техніки та процедури (TTP)».

Дай наголосив на триваючих міжнародних репресіях проти кіберзлочинців. «ФБР зайняло Breachforums. Meta і YouTube розправляються з групами хакерів, спрямованих на урядові та цивільні комп'ютерні системи. Ми також координуємо роботу з нашими міжнародними партнерами, щоб обмінюватися інформацією, зібраною в результаті цих видалень, щоб затримати місцевих кіберзлочинців», — додав Дай.

Нещодавнє порушення є уроком для PNP та інших організацій. У цифрову епоху пильність і проактивний захист є найважливішими для захисту від постійно зростаючої загрози кібератак». ***(Art Samaniego. Double breach highlights critical***

cybersecurity lessons for PNP // Manila Bulletin Publishing Corporation (https://mb.com.ph/2024/05/23/double-breach-highlights-critical-cybersecurity-lessons-for-pnp). 23.05.2024).

***

«Постійний ризик кібератак є актуальною проблемою в сучасному взаємопов'язаному цифровому світі. Звичайно, це головний ризик для багатьох у юридичному секторі.

Кібератаки створюють значні ризики для конфіденційної клієнтської інформації, бізнес-активів, безперервності бізнесу та професійної репутації. Для юристів тут можуть бути дві ролі. По-перше, ті з нас, хто займається захистом власного бізнесу, повинні впровадити відповідні заходи кібербезпеки для захисту бізнесу та його активів. Для інших просто потрібно бути впевненим, що будь-яка інформація, якою ділиться, захищена, враховуючи, що вона може бути привілейованою, конфіденційною та/або ми зобов'язані дбати про наших клієнтів.

Враховуючи зростаючий кіберризик і після хвилі кібератак, які вплинули на адвокатів та їхні палати у 2021 році, Товариство юристів і Рада адвокатів скликали робочу групу з кібербезпеки. Ця група складалася з невеликої групи соліситорів, баристерів і співробітників інформаційної безпеки з усього юридичного сектора. Мені пощастило бути частиною групи, враховуючи мою роль і багаторічний досвід роботи спеціалістом із захисту даних у DAC Beachcroft, а також працюючи над інформаційною безпекою, кібербезпекою та безперервністю бізнесу.

Протягом останніх кількох років у зв'язку з появою кібератак багато адвокатських фірм відреагували, надіславши відповідні анкети щодо безпеки адвокатам та їхнім палатам. Це було зроблено для того, щоб фірми могли бути впевнені, що будь-яка спільна інформація належним чином захищена. У деяких випадках палати отримували анкети, які були різними за змістом і форматом, на заповнення яких знадобився значний час.

Перешкода для DAC Beachcroft, як і для багатьох юридичних фірм того часу, полягала в тому, що ми сиділи між клієнтом (який вимагав знати, щоб їхня

інформація була належним чином захищена) і палатами (які не були налаштовані так само, як юридична фірма, з відданою ресурс безпеки). Унікальна організація палат та їхній зв'язок із відповідним колективом самозайнятих адвокатів лише ускладнили орієнтування в ситуації.

Щоб вирішити цю проблему, навесні 2022 року спільна Робоча група з кібербезпеки Товариства юристів і Ради адвокатів опублікувала свою першу версію простої стандартизованої Анкети з інформаційної безпеки, яку можна було надіслати палатам для заповнення щодо загальних спільних IT-систем, які використовують їх адвокати. Хоча анкета не могла детально охопити всі аспекти захисту даних, кібернетичної та інформаційної безпеки, вона містила 24 питання, спрямованих на забезпечення відповідності ключовим сферам безпеки.

Хоча я не можу говорити про підхід інших юридичних фірм, DAC Beachcroft надіслала анкету до всіх палат, де її адвокати проходили інструктаж протягом наступного дворічного періоду. Після того, як анкета була успішно заповнена на рівні понад 90%, і, здавалося б, зменшилася кількість кібератак, які вплинули на адвокатів та їхні палати після випуску анкети на юридичний ринок, анкета, схоже, виконала свою роль. Звичайно, успіх опитувальника можна частково пояснити тим, що багато юридичних фірм і палат почали використовувати одну стандартну форму з моменту її випуску. Анкета не тільки допомогла палатам запровадити належний базовий контроль, але й виступила в якості освітнього посібника для усвідомлення важливості наявності належних заходів безпеки інформації.

У 2024 році Робоча група з кібербезпеки опублікувала другу версію анкети, яка розширює деякі нові сфери безпеки. добровільне підтвердження кібербезпеки та інформаційної безпеки. Разом з цим також було опубліковано, яке може бути автоматично додано (у системі керування справами) до інструкції для адвоката. Його мета — діяти як пам'ятна записка для забезпечення захисту даних, якими спільно користуються.

Хоча анкета та підтвердження не можуть зменшити всі ризики, вони є чудовими інструментами для забезпечення узгодженого базового розуміння та застосування засобів контролю для захисту інформації, що надається. По суті, це

дозволяє фахівцям у сфері права підтримувати довіру наших клієнтів не лише через захист їхньої інформації, але й завдяки високоякісному наданню юридичних послуг». ***(Mathew McGee. Cybersecurity in the legal sector // The Law Society (https://www.lawgazette.co.uk/commentary-and-opinion/cybersecurity-in-the-legal-sector/5119807.article). 23.05.2024).***

***

Діяльність хакерів та хакерські угруповування

«Хакерське угруповання Anonymous звернулося до прем'єр-міністра Грузії Іраклія Кобахідзе і пообіцяло здійснити кібератаки на урядові сайти, якщо влада й надалі нападатиме на протестувальників.

Про це повідомляє Sova, передає Укрінформ.

Хакери наголосили, що підтримують грузинський народ в його боротьбі за демократію, свободу і процвітання, і хочуть, щоб Грузія, «вільна від російського впливу, підтримала своє прагнення до світлого майбутнього».

Крім того, вони звернулись до прем'єр-міністра Грузії.

«Якщо ваш уряд і далі використовуватиме той самий стандарт застосування поліції для жорстоких нападів на протестувальників, ми відповімо ще більш дикими кібератаками на урядові сайти», - ідеться в повідомленні.

Хакери нагадали про свої попередні відповіді на дії силовиків під час акцій протесту проти закону про іноагентів, який правляча партія «Грузинська мрія2 намагається ухвалити.

«За цей період Anonymous здійснила кібератаки на вебсайти уряду Грузії - понад 30 сайтів, більшість із яких зараз відключено. Ці дії є відповіддю на насильство з боку поліції проти мирних протестувальників у Тбілісі та Батумі», - наголосили вони.

Хакери додали, що нападів зазнали і державні ЗМІ, які «виконують функцію пропагандистських каналів».

«Маріонетковий уряд Кремля в Грузії запровадив російський закон про «іноземних агентів», прагнучи примусити замовкнути інакомислення та незалежні ЗМІ, а також націлитися на організації, що критикують уряд», - написали Anonymous». ***(Хакери Anonymous пообіцяли прем'єру Грузії «дикі кібератаки» за напади на мітингувальників // Укрінформ (https://www.ukrinform.ua/rubric-world/3860940-hakeri-anonymous-poobicali-premeru-gruzii-diki-kiberataki-za-napadi-na-mitinguvalnikiv.html/). 07.05.2024).***

***

Вірусне та інше шкідливе програмне забезпечення

«Було помічено, що хакери націлювалися на пристрої Mac, що працюють на процесорах Intel і ARM, за допомогою нового шкідливого програмного забезпечення infostealer.

Провайдер безпеки Mac Kandji виявив шкідливе програмне забезпечення та назвав його Cuckoo. «Це зловмисне програмне забезпечення запитує конкретні файли, пов’язані з певними програмами, намагаючись зібрати якомога більше інформації з системи», — йдеться у звіті дослідників.

Серед інформації, яку він збирає, є інформація про апаратне забезпечення, поточні запущені процеси та встановлені програми. Крім того, Cuckoo здатний робити знімки екрана, збирати дані з iCloud Keychains, Apple нотаток, веб-браузерів, різних програм (Discord, Telegram, Steam тощо) і криптовалютних гаманців.

Росія чи Китай?

Для розповсюдження зловмисного програмного забезпечення зловмисники створили низку шкідливих сайтів, де код рекламується як програма для копіювання музики з потокових сервісів і перетворення її у.MP3. Також рекламується наявність як безкоштовної, так і платної версії.

Хоча дослідники прямо не приписували кампанію жодному конкретному учаснику загрози, вони зауважили, що інфокрадій не запускається, якщо заражений

пристрій знаходиться у Вірменії, Білорусі, Казахстані, Росії та Україні, що, можливо, натякає на приналежність до Росії. Однак вони також відзначили, що Cuckoo встановлює постійність через LaunchAgent, який уже був помічений у RustBucket, XLoader, JaskaGO та бекдорі, схожому на ZuRu – китайському акторі загрози.

Додаткову довіру до китайської теорії додає той факт, що зловмисне програмне забезпечення було підписано законним китайським ідентифікатором розробника:

«Кожна шкідлива програма містить інший набір програм у каталозі ресурсів», — сказали дослідники. «Усі ці пакети (крім тих, що розміщені на fonedog[.]com) підписані та мають дійсний ідентифікатор розробника Yian Technology Shenzhen Co., Ltd (VRBJ4VRP).» ***(Sead Fadilpašić. A dangerous new malware is targeting Macs of all kinds — here's how to stay safe // Future US, Inc. (https://www.techradar.com/pro/security/a-dangerous-new-malware-is-targeting-macs-of-all-kinds-heres-how-to-stay-safe?utm_source=flipboard&utm_content=rubertus%2Fmagazine%2FInnovation%2C+Business%2C+Tech+and+Creativity+%7C+Innovaci%C3%B3n+y+Creatividad). 06.05.2024).***

***

«У квітні Apple надіслала сповіщення користувачам iPhone у 92 країнах, попереджаючи їх про шпигунське програмне забезпечення. «Apple виявила, що ви стали мішенню для атаки найманців-шпигунів, які намагаються віддалено скомпрометувати iPhone, пов’язаний з вашим ідентифікатором Apple», — йдеться в повідомленні.

Користувачі швидко перейшли на сайти соціальних мереж, включаючи X, намагаючись зрозуміти, що означає сповіщення. Багато з тих, хто став мішенню, були в Індії, але інші в Європі також повідомили, що отримали попередження від Apple.

Через кілька тижнів про останні атаки на iPhone все ще мало що відомо. Колишній гігант смартфонів Blackberry, а тепер охоронна фірма, оприлюднив дослідження, яке вказує на те, що вони пов’язані з китайською кампанією шпигунського програмного забезпечення під назвою LightSpy, але речник Apple Шейн Бауер каже, що це неточно, а дослідники охоронної фірми Huntress кажуть, що проаналізований варіант Blackberry був версія macOS, а не iOS.

Квітневі попередження не були першим випадком, коли Apple надсилала повідомлення такого роду. З 2021 року виробник iPhone розіслав попередження людям у понад 150 країнах, оскільки шпигунське програмне забезпечення продовжує націлюватися на високопоставлених осіб у всьому світі.

Шпигунське програмне забезпечення може стати зброєю противників національних держав, але це відносно рідко і дорого. Його розгортання, як правило, спрямоване на дуже конкретну групу людей, включаючи журналістів, політичних дисидентів, державних службовців і підприємства в певних секторах.

«Такі атаки значно складніші, ніж звичайна діяльність кіберзлочинців і споживче зловмисне програмне забезпечення, оскільки зловмисники-шпигуни застосовують виняткові ресурси для націлювання на дуже невелику кількість конкретних осіб та їхніх пристроїв», — написала Apple у квітневому повідомленні. «Найманні шпигунські атаки коштують мільйони доларів і часто мають короткий термін придатності, тому їх набагато важче виявити та запобігти. Переважна більшість користувачів ніколи не стане ціллю таких атак».

Крім того, Apple каже, що її функція Lockdown Mode може успішно захистити від атак. «Як ми вже говорили раніше, ми не знаємо, щоб хтось, хто використовує режим блокування, був успішно атакований шпигунським програмним забезпеченням найманців», — говорить Бауер. Тим не менш, для тих, хто став мішенню і спійманий зненацька, шпигунське програмне забезпечення надзвичайно небезпечне.

Атаки без кліків

Шпигунське програмне забезпечення надає зловмисникам доступ до мікрофона смартфона та дозволяє їм переглядати все, що ви пишете, включаючи

повідомлення в зашифрованих програмах, таких як WhatsApp і Signal. Вони також можуть відстежувати ваше місцезнаходження, збирати паролі та інформацію з програм.

Раніше шпигунське програмне забезпечення доставлялося за допомогою фішингу, вимагаючи від жертви натиснути посилання або завантажити зображення. Сьогодні це можна зробити за допомогою так званих «атак з нульовим кліком» за допомогою зображення iMessage або WhatsApp, яке автоматично встановить шпигунське програмне забезпечення на вашому пристрої.

У 2021 році дослідники Google Project Zero розповіли, як експлойт без кліків на основі iMessage використовувався для націлювання на саудівського активіста. «Немає жодного способу запобігти експлуатації за допомогою експлойту з нульовим кліком, якщо не використовувати пристрій; це зброя, проти якої немає захисту», – попередили дослідники.

Ланцюжок зараження шпигунським програмним забезпеченням за допомогою експлойтів без натискання через iMessage був продемонстрований підрозділом безпеки Kaspersky в рамках свого дослідження Operation Triangulation минулого року.

Все, що має відбутися, — жертва отримає iMessage із вкладенням, що містить експлойт без натискання. «Без будь-якої подальшої взаємодії це повідомлення викликає вразливість, що призводить до виконання коду для підвищення привілеїв і забезпечення повного контролю над зараженим пристроєм», — каже Борис Ларін, головний дослідник безпеки в Kaspersky Global Research & Analysis Team.

Як тільки зловмисник встановлює свою присутність на пристрої, за його словами, повідомлення автоматично видаляється.

Підйом Пегаса

Найвідомішим і найвідомішим шпигунським програмним забезпеченням є Pegasus, створене ізраїльською фірмою NSO Group для виявлення вразливостей програмного забезпечення iOS і Android.

Шпигунське програмне забезпечення існує лише завдяки таким постачальникам, як NSO Group, яка стверджує, що продає експлойти урядам лише

для полювання на злочинців і терористів. «Будь-які клієнти, включаючи уряди в Європі та Північній Америці, погоджуються не розголошувати ці вразливості», — говорить Річард Вернер, радник з кібербезпеки в Trend Micro.

Незважаючи на заяви NSO Group, шпигунське програмне забезпечення продовжує націлюватися на журналістів, дисидентів і протестувальників. Дружина саудівського журналіста та дисидента Джамаля Хашоггі, Ханан Елатр, нібито була мішенню Пегаса перед його смертю. У 2021 році репортер New York Times Бен Хаббард дізнався, що його телефон двічі атакували Pegasus.

Пегас був тихо імплантований в iPhone Клода Маньїна, дружини політичного активіста Наами Асфарі, якого ув'язнили та ймовірно катували в Марокко. Pegasus також використовувався для націлювання на продемократичних протестувальників у Таїланді, російську журналістку Галину Тимченко та урядовців Великобританії.

У 2021 році Apple подала позов проти NSO Group та її материнської компанії, щоб притягнути її до відповідальності за «стеження та націлювання на користувачів Apple».

Справа все ще триває, NSO Group намагається відхилити позов, але експерти кажуть, що проблема не зникне, доки постачальники шпигунського ПЗ зможуть працювати.

Девід Руїз, старший захисник конфіденційності в охоронній фірмі Malwarebytes, звинувачує «нав’язливих і репресивних операторів, що стоять за шпигунським програмним забезпеченням, яке посилює його небезпеку для суспільства».

Вилив шпигунського ПЗ

Якщо ви вважаєте, що ви можете стати мішенню шпигунського програмного забезпечення, ви можете зробити лише кілька корисних речей. Apple По-перше, увімкніть режим блокування, який вимикає певні функції, але напрочуд зручний і може захистити ваш iPhone від зараження. По-друге, якщо ви підозрюєте, що ваш пристрій уже інфікований, доступні лінії довіри, які допоможуть вам у видаленні шпигунського програмного забезпечення, як-от лінія цифрової безпеки Amnesty International Access Now і лабораторія безпеки.

Виявлення шпигунського програмного забезпечення може бути надзвичайно складним завданням, а для таких складних шпигунських програм, як Pegasus, виявити зараження самостійно майже неможливо. Існують менш складні типи шпигунського програмного забезпечення, яке може спричиняти незвичайну поведінку, як-от швидке розрядження акумулятора, несподіване завершення роботи або високе використання даних, що може свідчити про деякі типи інфекцій, каже Джаввад Малік, провідний спеціаліст із питань безпеки в організації з навчання безпеки KnowBe4.. Хоча певні програми стверджують, що виявляють шпигунське програмне забезпечення, їх ефективність може бути різною, і для надійного виявлення часто потрібна професійна допомога, каже він.

Кріс Хаук, захисник конфіденційності споживачів у Pixel Privacy, погоджується, що розрядка акумулятора є вагомим показником наявності нехитрих шпигунських програм на вашому пристрої. «Більшість шпигунських програм не розроблено для ефективної роботи», — каже він.

Однак для складних найманців-шпигунських програм, таких як Pegasus, такі очевидні індикатори, як розряд батареї, випадкові вимкнення або проблеми з використанням даних, не були підтверджені, каже Бауер з Apple. «Ці симптоми більше стосуються стандартних шпигунських програм для Android, ніж цілеспрямованих шпигунських програм для найманців, які здатні залишатися непоміченими на пристроях користувачів», — говорить він.

Якщо ви вважаєте, що на вас може націлитися низькоякісне шпигунське програмне забезпечення, можливо, ви також шукаєте додатки, які вони не встановили, примусове переспрямування через захоплення веб-переглядача та змінені налаштування в їхньому браузері чи пошуковій системі за умовчанням.

На початку цього року команда Касперського представила метод виявлення індикаторів зараження від складних шпигунських програм iOS, таких як Pegasus, Reign і Predator. Це може бути ефективним, оскільки зараження Pegasus залишає сліди в неочікуваному системному журналі Shutdown.log, який зберігається в архіві sysdiagnose пристроїв iOS, повідомляє служба безпеки. Однак робота з такими професіоналами, як Access Now і Amnesty, є єдиним надійним способом розкрити

складне зараження шпигунським програмним забезпеченням. Також краще зберегти потенційно заражений пристрій для професійного аналізу.

Ще один крок, який ви можете зробити, щоб захистити свій пристрій, це переконатися, що ви перезапускаєте його принаймні раз на день. «Це змушує зловмисників неодноразово повторно інфікувати, збільшуючи шанси виявлення з часом», — каже Ларін. Але знову ж таки, це працює лише для нескладного шпигунського програмного забезпечення, оскільки високорозвинене шпигунське програмне забезпечення може залишатися на вашому пристрої.

Якщо ви можете бути ціллю, ви також можете вимкнути iMessage і FaceTime, щоб зменшити ризик стати жертвою атак без кліків. Водночас оновлюйте свій пристрій до останньої версії програмного забезпечення та не натискайте посилання, отримані в повідомленнях, наприклад електронних листах, каже Адам Прайс, аналітик Сujах з аналізу кіберзагроз.

«Оновіть програмне забезпечення до останньої версії для захисту від відомих вразливостей, використовуйте багатофакторну автентифікацію та встановлюйте програми лише з перевірених і законних джерел», — каже Прайс». ***(Kate O'Flaherty. Apple's iPhone Spyware Problem Is Getting Worse. Here's What You Should Know // Condé Nast (https://www.wired.com/story/apple-iphone-spyware-101/?utm_source=flipboard&utm_content=EllieElizab2015%2Fmagazine%2FIPhone)*** . 06.05.2024).

***

«Дослідники безпеки розкрили спосіб зробити будь-яку віртуальну приватну мережу (VPN) марною. І вони підозрюють, що їхній подвиг, можливо, був у дикій природі роками – і зловмисники вже могли про це знати.

Дослідники з Leviathan Security Group виявили метод викриття трафіку користувача, коли він використовує VPN, фактично дозволяючи зловмисникам стежити за їхнім незашифрованим трафіком і отримувати цінні дані від передачі. Дослідники називають свій експлойт TunnelVision і кажуть, що вони ще не натрапляли на VPN, який би не піддавався цьому трюку.

VPN відіграють вирішальну роль у безпечному трафіку та безпеці даних. Коли хтось використовує VPN, його інтернет-трафік шифрується, що дозволяє уникнути сторонніх очей хакерів. Але TunnelVision змінює це. Дослідники сказали, що якщо їм вдалося атакувати мережу, вони можуть запустити сервер DHCP, який призначає IP-адреси для пристроїв у тій же мережі та змушує трафік маршрутизуватися через нього. Роблячи це, вони можуть уникнути шифрування VPN і переглядати повністю незашифровані пакети трафіку. Що ще гірше, користувачі жодного разу не вірять, що їхній трафік надсилається через незашифроване з'єднання, а самі VPN ніколи не повідомляють їх про зміни.

Звісно, хакерам доведеться пройти певні перешкоди, щоб скористатися експлойтом, головним з яких є фактичний доступ до мережі. Але хакери часто можуть сидіти в зламаних мережах, не попереджаючи нікого, чекаючи можливості викрасти дані. І TunnelVision є лише однією з таких можливостей.

Але стає гірше. Дослідники безпеки заявили, що вони вважають, що зловмисники могли скористатися слабкістю функціональності VPN з 2002 року, припускаючи, що хакери могли знати про експлойт більше двох десятиліть. І хоча вони не підтвердили, що хакери скористалися експлойтом, вони повідомили виробників VPN про своє відкриття.

Тим не менш, незрозуміло, як вирішити проблему. Хоча видалення підтримки DHCP у VPN негайно вирішило б проблему, це також спричинило б низку проблем із підключенням до Інтернету поза межами використання VPN. І хоча дослідники змогли знайти один із способів вирішення проблеми лише в операційних системах на базі Linux, це виправлення створить «бічний канал», який все одно дозволить деанонімізувати трафік.

«У деяких місцях у світі сам по собі бічний канал може призвести до ув'язнення або смерті тих, хто покладається на VPN для забезпечення безпеки, наприклад журналістів або інформаторів, які є звичайними об'єктами стеження або шпигунського програмного забезпечення», — заявили дослідники.

Отже, єдине справжнє рішення — не мати VPN, що працює в мережі, яка була скомпрометована — це важка задача, враховуючи, як важко дізнатися, чи не

ховаються хакери. Тому наразі будьте обережні з VPN і пам’ятайте, що ваш приватний трафік може бути не таким приватним, як ви думаєте». ***(Don Reisinger. Security researchers say this scary exploit could render all VPNs useless // ZDNET (https://www.zdnet.com/article/security-researchers-say-this-scary-exploit-could-render-all-vpns-useless/?utm_source=flipboard&utm_content=user%2FZDNet). 07.05.2024).***

***

Програми-вимагачі

«Виробник датчиків зображення OmniVision надсилає листи людям, чиї дані потрапили під атаку програм-вимагачів у 2023 році, пропонуючи поради щодо того, як протистояти шахрайству та атакам соціальної інженерії.

Компанія OnniVision, заснована в 1995 році компанією Aucera Technology китайським напівпровідниковим гігантом Will Semiconductor, має кілька помітних технологічних досягнень, зокрема першу в історії інтегральну схему для конкретного застосування (ASIC) у 1999 році та Книгу рекордів Гіннеса за найменшу комерційно доступну датчик зображення, відомий як CameraCubeChip.

«OmniVision Technologies (OVT) пише, щоб повідомити вам про інцидент безпеки, який міг стосуватися вашої особистої інформації», — йдеться в листі. «Хоча у нас немає доказів того, що відбулося будь-яке фактичне зловживання вашою особистою інформацією, пов’язане з цим інцидентом безпеки, ми надаємо вам інформацію про інцидент і подробиці, пов’язані з тим, що ви можете зробити, щоб краще захистити свою інформацію, якщо ви вважаєте це за потрібне робити так."

OVT повідомляє, що 30 вересня 2023 року було виявлено «інцидент із безпекою, який призвів до шифрування певних систем OVT неавторизованою третьою стороною».

Компанія негайно найняла експертів з кібербезпеки для стримування інциденту, повідомила поліцію та почала розслідування.

«Це поглиблене розслідування встановило, що неавторизована сторона отримала деяку особисту інформацію з певних систем у період з 4 по 30 вересня 2023 року», — йдеться далі в листі. «3 квітня 2024 року, після завершення цієї всебічної перевірки, ми визначили, що була залучена частина вашої особистої інформації», — повідомляє компанія цифрових зображень.

Персоналізований лист, опублікований BleepingComputer, відредагований і не містить конкретних даних, скомпрометованих для кожної постраждалої особи.

Однак, згідно з даними сайту кіберновин, учасники програм-вимагачів під псевдонімом «Cactus» взяли на себе відповідальність за злом і злили архів, що містить скани паспортів, угоди про нерозголошення, контракти та конфіденційні документи. Іншими словами, злом призвів до крадіжки корпоративних даних і даних співробітників. Примітно, що хакери нібито пропонували дамп даних безкоштовно.

OVT збільшила кількість рішень для моніторингу у своїй мережі, щоб краще виявляти підозрілу активність і запобігати її повторенню, повідомляє компанія.

«Ми також перебуваємо в процесі оновлення нашої політики та процедур безпеки, переходимо певні системи до хмарних операцій і вимагаємо додаткових тренінгів з питань безпеки в нашій організації», — додається в листі.

Під час розслідування не було отримано жодних доказів того, що скомпрометована інформація була використана шахрайським шляхом, але OVT, незважаючи на це, пропонує постраждалим особам безкоштовний кредитний моніторинг та послуги відновлення ідентифікації протягом 24 місяців.

Компанія також пропонує кроки щодо пом’якшення спроб шахрайства та повідомляє одержувачам «остерігатися схем, у яких зловмисники можуть прикидатися представниками OVT або посилатися на цей інцидент».

Постраждалі особи можуть розглянути можливість використання служби моніторингу даних, наприклад Bitdefender Digital Identity Protection. DIP дозволяє миттєво дізнатися, чи стався витік ваших даних в Інтернет, який тип інформації було зламано, які ризики вам загрожують і чи продається ваша інформація в темній мережі.

Bitdefender нещодавно представив Scamio, безкоштовну службу виявлення та запобігання шахрайству для всіх, хто має обліковий запис Bitdefender. Ви підозрюєте певний телефонний дзвінок, електронну пошту чи SMS? Просто опишіть ситуацію нашому розумному чат-боту, і він допоможе вам у безпеці. Ви можете поділитися зі Scamio саме тим, що хочете перевірити, наприклад знімком екрана, PDF-файлом, QR-кодом або посиланням. Scamio за лічені секунди повідомить вам, чи це фальшивка». ***(Filip TRUȚĂ. OmniVision Confirms Hackers Made Off with Personal Data in 2023 Ransomware Incident // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/omnivision-confirms-hackers-made-off-with-personal-data-in-2023-ransomware-incident/?utm_source=flipboard&utm_content=other%2F). 21.05.2024).***

***

«Координатор з кібербезпеки Австралії каже, що масштабний злам даних програм-вимагачів постачальника електронних скриптів MediSecure був «ізольованою» атакою, хоча вона попереджає, що кіберзлочинці, ймовірно, знову націляться на індустрію охорони здоров'я.

Компанія, яка займається випискою електронних рецептів та їх відпуском, не повідомила, скільки австралійців постраждало.

Генерал-лейтенант Мішель МакГіннесс підтвердила, що «значна» витока даних минулого тижня містила особисту інформацію та інформацію про здоров'я австралійців.

Триває розслідування, щоб встановити, чи були скомпрометовані документи, що посвідчують особу, та картки Medicare.

«Ми вважаємо, що це одиничний випадок і що жодні інші організації не постраждали», — сказала вона в інтерв'ю ABC News Breakfast у п'ятницю вранці.

Коли її запитали, хто стоїть за атакою програм-вимагачів, генерал-лейтенант відповіла, що не буде надавати додаткових подробиць з цього приводу.

MediSecure закрила свій веб-сайт у вівторок, заявивши, що збирає більше інформації та що «перші ознаки свідчать про те, що інцидент стався через одного з наших сторонніх постачальників».

Генерал-лейтенант МакГіннесс сказав, що поки немає жодних ознак того, що будь-яка інформація про витік даних була розповсюджена чи опублікована.

«Поки що ми не бачили доказів того, що будь-кому потрібно замінити свою картку Medicare», — сказала вона в заяві.

Генерал-лейтенант МакГіннесс сказав, що влада тісно співпрацює з MediSecure, щоб бути «підготовленими та мати найкращу позицію» для підтримки будь-кого, чия інформація була скомпрометована.

Однак президент Австралійської медичної асоціації Стів Робсон сказав, що він був присутній на брифінгу в п'ятницю, і масштаб кіберзлому ще не повністю відомий.

«Ще рано», — сказав він.

«Незрозуміло, які саме дані були вкрадені, заблоковані або щось інше, і ці речі можуть бути складними.

«Я думаю, що масштаб того, що сталося, потрібен час, щоб повністю розкритися».

За його словами, за останні кілька років електронні рецепти пережили масовий вибух.

«Звичайно, MediSecure була значною частиною цієї групи», - сказав він.

«Тож ми очікуємо, що багато лікарів і багато пацієнтів по всій країні матимуть дані в базі даних».

Генерал-лейтенант МакГіннесс сказав, що ті, хто постраждав від порушення, не повинні вживати жодних дій прямо зараз і з ними зв’яжеться MediSecure, якщо їхня особиста інформація буде оприлюднена.

«Ми не рекомендуємо нікому платити викуп — це лише створює цикл із злочинцями», — сказала вона.

«Це забезпечує фінансування подальших викупів, і немає жодної гарантії, що ми повернемо дані або що даними все одно буде передано».

Дані про стан здоров'я «продовжуватимуть націлюватися»

Керівник відділу кібербезпеки сказав, що органи влади на державному та федеральному рівнях продовжують розслідувати порушення та стежать за ситуацією, щоб зменшити шкоду.

«MediSecure була неймовірно прозорою та дуже тісно співпрацювала з усіма зацікавленими сторонами, щоб забезпечити найкращий результат для австралійців», — сказала вона.

Але генерал-лейтенант попередив, що останній витік даних, ймовірно, не буде останнім.

«Ми були б наївними думати, що ми не будемо продовжувати об’єктом нападів, особливо галузь охорони здоров’я», – сказала вона.

«Він [має] велику інформацію, особливо конфіденційну, і злочинці продовжуватимуть реагувати».

Вона сказала, що деякі основні запобіжні заходи, які кожен австралієць може вжити, щоб запобігти витоку даних, включають оновлення програмного забезпечення, застосування багатофакторної автентифікації та використання унікальних і складних паролів.

«Це речі, які покращать нашу позицію в галузі кібербезпеки як нації та зроблять нас більш безпечними», — сказала вона.

Вона сказала, що уряд також працює над створенням своєї кібернетійкості проти атак і забезпеченням готовності швидко реагувати на будь-які витоки даних.

Уповноважений з питань конфіденційності Карлі Кінд сказала ABC, що цей інцидент є нагадуванням про захист конфіденційності в економіці Австралії не там, де він повинен бути.

«Для мене це нагадування про те, що це актуальна проблема і що австралійська спільнота глибоко вражена такими інцидентами, і що нам потрібна законодавча реформа, щоб відповідати викликам цієї нової ери».

Вона сказала, що Закон про конфіденційність необхідно розширити, щоб охопити малий бізнес, оскільки зараз 95 відсотків австралійських підприємств не мають жодних зобов’язань щодо конфіденційності.

«Це потрібно змінити, і моєму офісу потрібно більше повноважень для розслідування та забезпечення дотримання порушень конфіденційності», — сказала вона.

«Наразі ми обмежуємося вимогами цивільних санкцій у федеральному суді за конкретні випадки, коли є серйозні та неодноразові втручання в приватне життя.

«І ми хотіли б, щоб сфера цих повноважень була розширена, щоб ми могли застосовувати покарання нижчого рівня».

Вона сказала, що реформа конфіденційності є терміновою.

«Це тепер є частиною нашого повсякденного життя, і ми повинні переконатися, що захист особистої інформації відповідає цій новій загрозі».

Доцент кафедри права та юстиції Університету Нового Південного Уельсу Кетрін Кемп каже, що викликає занепокоєння те, що немає більше фінансування для боротьби з порушеннями конфіденційності.

«Викликає занепокоєння те, що в цьому останньому бюджеті фінансування OAIC було скорочено приблизно на 11 мільйонів доларів у той час, коли ризики та шкода конфіденційності лише зростають».

«Всі види ризиків»

Враховуючи поточне розслідування, поки неясно, який вплив матиме витік даних MediSecure на постраждалих австралійців.

Головний виконавчий директор Дослідницького центру споживчої політики Ерін Тернер заявила, що витік медичних даних може наражати людей «на всілякі ризики, якщо вони доступні зловмисникам».

«Це може бути все, починаючи від крадіжки особистих даних. Якщо там достатньо інформації, вони можуть, наприклад, взяти кредити на ваше ім'я», - сказала вона.

«Або в інших досить жахливих ситуаціях ваша інформація може бути використана проти вас або для маніпулювання вами, для обману, для того, щоб її звинуватили».

Пані Тернер сказала, що всім австралійським компаніям необхідно розробити кращі плани щодо повідомлення клієнтів про порушення даних.

За її словами, «розпливчастих і незрозумілих» заяв компаній недостатньо.

«Це ще один масштабний витік даних, про який постраждалі люди ще не знають. Вони не знають, які їхні дані можуть бути захоплені», — сказала вона.

«Вони просто залишилися в тривожному, жахливому стані, чекаючи, коли це підтвердиться».

Згідно з дослідженням центру, половина австралійців не знала, що робити, коли їхні дані були зламані.

«Якщо вас це спіткало, ви можете піти в компанію, а якщо ви незадоволені, ви можете піти в OAIC [Офіс комісара з інформації Австралії], регулятора з цього питання», — сказала пані Тернер.

Вона додала, що «справді розчаровує» те, що австралійські закони щодо витоку даних не вказують на те, які операції з обслуговування клієнтів мають відбуватися після інциденту.

«Ми знову і знову бачили, будь то Qantas, Optus, тепер MediSecure, що є дуже мало інформації про те, що постраждалі клієнти можуть робити або повинні знати».

ABC надіслав MediSecure докладні запитання, але був направлений на його веб-сайт для оновлень». ***(Audrey Courty, Michael Atkin. Cyber security chief says MediSecure data breach is an 'isolated' attack but warns health data a prime target for cybercrime // ABC (https://www.abc.net.au/news/2024-05-17/cyber-security-chief-says-medisecure-data-breach-isolated-attack/103860120). 17.05.2024).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Принаймні з 2019 року тіньова фігура, яка ховається за кількома псевдонімами, публічно зловтішається вимаганням мільйонів доларів у тисяч жертв, яких він та його спільники зламали. Тепер, вперше, «LockBitSupp»

було викрито міжнародною групою правоохоронних органів, і за його арешт призначено винагороду в 10 мільйонів доларів.

У розкритому у вівторок обвинувальному акті федеральні прокурори США викрили яскраву персону як Дмитра Юрійовича Хорошева, 31-річного громадянина Росії. Прокурори заявили, що протягом п’яти років перебування на чолі LockBit — однієї з найплідніших груп програм-вимагачів — Хорошев і його підлеглі виманили 500 мільйонів доларів у приблизно 2500 жертв, приблизно 1800 з яких перебували в США. Його скорочення доходу нібито склало близько 100 мільйонів доларів.

Збитки в мільярди доларів

«Крім виплат і вимог викупу, атаки LockBit також серйозно порушили операції їхніх жертв, спричинивши втрату доходів і витрат, пов’язаних із реагуванням на інциденти та відновленням», — написали федеральні прокурори. «З урахуванням цих збитків LockBit завдав у всьому світі збитків на мільярди доларів США. Більше того, дані, які викрали Хорошев і його філія LockBit, змовники, що містять дуже конфіденційну організаційну та особисту інформацію, залишалися незахищеними та скомпрометованими назавжди, незважаючи на помилкові обіцянки Хорошева та його співзмовників про протилежне».

Обвинувальний висновок інкримінує громадянину Росії одну звинувачення в змові з метою шахрайства, вимагання та пов’язану з ними діяльність у зв’язку з комп’ютерами, одну змову з метою вчинення шахрайства, вісім пунктів навмисного пошкодження захищеного комп’ютера, вісім пунктів вимагання щодо до конфіденційної інформації із захищеного комп’ютера та вісім пунктів звинувачення у здирництві щодо пошкодження захищеного комп’ютера. Якщо Хорошева визнають винним, йому загрожує максимальне покарання у вигляді 185 років позбавлення волі.

На додаток до обвинувального акту офіційні особи Міністерства фінансів США разом із колегами у Великій Британії та Австралії оголосили про санкції проти Хорошева. Серед іншого, санкції США дозволяють офіційним особам накладати цивільні покарання на будь-яку американську особу, яка здійснює або

сприяє платежам групі LockBit. Державний департамент США також оголосив винагороду в 10 мільйонів доларів за будь-яку інформацію, яка призведе до арешту або засудження Хорошева.

Дії у вівторок відбулися через 11 тижнів після того, як правоохоронні органи в США та 10 інших країнах завдали серйозного удару по інфраструктурі, яку учасники LockBit використовували для управління своїм підприємством з програм-вимагачів як послуг. Зображення, опубліковані федеральними органами влади на темному веб-сайті, де LockBit назвав і присоромив жертв, вказав, що вони взяли під контроль /etc/shadow, файл Linux, який зберігає криптографічно хешовані паролі. Файл, який є одним із найбільш чутливих до безпеки в Linux, може бути доступний лише користувачу з root, найвищим рівнем системних привілеїв.

Загалом, як заявила влада в лютому, вони захопили контроль над 14 000 обліковими записами, пов’язаними з LockBit, і 34 серверами, розташованими в Нідерландах, Німеччині, Фінляндії, Франції, Швейцарії, Австралії, США та Великобританії. У Польщі та Україні заарештовано двох підозрюваних у LockBit, висунуто п’ять обвинувальних актів і три ордери на арешт. Влада також заморозила 200 криптовалютних рахунків, пов’язаних з операцією з програмами-вимагачами. Національне агентство з боротьби зі злочинністю Великобританії у вівторок повідомило, що кількість активних філій LockBit скоротилася зі 114 до 69 після лютневої дії під назвою Operation Cronos.

У середині березня житель Онтаріо, Канада, засуджений за звинуваченням у роботі на LockBit, був засуджений до чотирьох років ув’язнення. Михайло Васильєв, якому на момент винесення вироку було 33 роки, був заарештований у листопаді 2022 року та звинувачений у змові з метою зараження захищених комп’ютерів програмами-вимагачами та надсиланні вимог викупу жертвам. У лютому він визнав себе винним за вісьмома пунктами звинувачення в кібервимаганні, хуліганстві та зброї.

Ідентичність альтер-его Хорошева LockBitSupp у реальному світі користується гарячим попитом протягом багатьох років. LockBitSupp процвітав завдяки своїй анонімності в частих публікаціях на російськомовних хакерських

форумах, де він хвалився майстерністю та проникливістю своєї роботи. Одного разу він пообіцяв винагороду в 10 мільйонів доларів тому, хто розкриє його особу. Після операції в лютому, яка знищила більшу частину інфраструктури LockBit, прокурори натякнули, що знають, хто такий LockBitSupp, але не назвали його імені.

LockBit працює принаймні з 2019 року, а в минулому також був відомий під назвою «ABCD». Протягом трьох років після заснування зловмисне програмне забезпечення групи було найпоширенішим програмним забезпеченням-вимагачем. Як і більшість аналогів, LockBit працював у так званому програмному забезпеченні-вимагачі як послуга, в якому він надає програмне забезпечення та інфраструктуру афілійованим особам, які використовують його для фактичного злому. Потім LockBit і філії ділять будь-який отриманий дохід». ***(Dan Goodin. Ransomware mastermind LockBitSupp reveled in his anonymity—now he's been ID'd // Condé Nast (https://arstechnica.com/security/2024/05/the-mastermind-of-the-prolific-ransomware-group-lockbit-has-finally-been-unmasked/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 07.05.2024).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«У сфері кібербезпеки важливо розуміти свої найбільші вразливості. Національний інститут стандартів і технологій (NIST) спочатку створив національну базу даних про вразливості (NVD), щоб забезпечити централізований центр для аналізу вразливостей кібербезпеки, але зробив це за припущенням, що раціональні актори приймають раціональні рішення та приходять до раціональних висновків.

Незважаючи на те, що NVD ніколи не мав на меті стати універсальним рішенням, наразі NVD є найпоширенішою базою даних уразливостей програмного забезпечення у світі, і багато сканерів, аналітиків і постачальників щодня залежать від неї, щоб визначити, яке програмне забезпечення було знищено. уражені вразливістю. Тим не менш, нещодавно було виявлено, що NIST не збагачує вразливості, перелічені в NVD з 12 лютого, тобто кожен, хто покладається на ці звіти, потенційно перебуває під загрозою протягом місяців.

Хоча на перший погляд це здається раптовим, цей збій насправді є системною проблемою, яка розвивалася з часом. З моменту створення майже 25 років тому три ключові фактори вплинули на здатність NVD належним чином класифікувати проблеми безпеки, які допомагають галузі визначати пріоритети вразливостей — і те, що ми відчуваємо зараз, є результатом.

Три фактори, що впливають на NVD

1. Вкладники, які шукають кредит

Спочатку вразливості, перелічені в NVD, були схвалені досвідченими дослідниками або досвідченими практиками, а призначення CVE (загальні вразливості та ризики) служило підтвердженням за добре виконану роботу. Однак, оскільки безпека програмного забезпечення з часом набула важливості, наплив дослідників-початківців, часто з мізерним досвідом, прагнув використовувати NVD і CVE як трамплін у галузі.

Вони хотіли відзначити нові відкриття як нагороду за їхній внесок у галузь — подібно до того, як розробник-початківець робить внесок у видатні проекти з відкритим кодом. На початкових етапах ця тенденція слугувала життєздатною стратегією складання резюме. Але оскільки все більше недосвідчених дослідників наводнили світ уразливими місцями, якість звітів почала падати.

2. Широка доступність

У той же час глобалізація Інтернету дозволила дослідникам у всьому світі брати участь і потенційно впливати на галузь значущим чином. Більше не лише кільці досвідчених дослідників із окремих регіонів приписували CVE, і ця друга

хвиля людей, які прагнуть визнання, ще більше збільшила кількість звітів низької якості.

Разом зі збільшенням числа недосвідчених дослідників широка доступність відкрила двері для монетизації вразливостей безпеки в Dark Web. Хоча виплата може бути не вартою ризику для когось із промислово розвиненої економіки, вона може змінити життя для когось в іншій частині світу. Замість того, щоб отримати заслугу у висновках, деякі учасники вирішили використовувати вразливі місця для вчинення злочину або продавати інформацію особам, які це зробили.

3. Грошове заохочення

У відповідь на вищезазначене винагороди за помилки з’явилися як стимул для дослідників розкривати вразливості постачальникам, а не використовувати їх для нанесення шкоди. Теорія полягала в тому, що це збалансує ринок і не дозволить людям переходити на «темну сторону» виявлення вразливостей.

Повідомлення про вразливості швидко перетворилося на гру чисел. Замість того, щоб зосереджуватися на виконанні доброї роботи та отриманні за неї кредиту, ця третя когорта зосередилася на висуненні якомога більшої кількості звітів із якомога меншими зусиллями, сподіваючись, що кілька отримають винагороду, щоб вони могли перевести чек у готівку та йти далі.

Вплив на постачальників

Тепер постачальники стикаються з натиском розкриття інформації про безпеку, що виникає через базове використання безкоштовних інструментів безпеки, які дають помилкові спрацьовування та неточні або нерелевантні результати. Увесь цей шум значно збільшив кількість звітів, які постачальники повинні переглядати щодня, і переважна більшість із них не надає жодної суттєвої інформації чи можливості використання. Коли всі витрачають стільки часу на сміття, залишається менше часу, щоб зосередитися на якісних дослідженнях

Хоча цей сплеск відображає поширення шахрайства електронною поштою наприкінці 1990-х і на початку 2000-х років, еволюціонуючи від складних схем до шаблонної тактики, оскільки опортуністи по всьому світу намагалися заробити на фінансових прибутках, важливо визнати, що це не звинувачення проти осіб з

обмеженими можливостями. доступ до освіти чи технологій. Кожен заслуговує на можливість зайняти свою нішу та отримати належну винагороду за свій внесок, але поточний стан справ є передбачуваним результатом структурованих «правил гри», які ми встановили.

Наслідки

Оскільки кількість повідомлених CVE різко зросла, програма CVE працювала над федеративною моделлю, запровадивши нову програму під назвою Центральні органи іменування (CNA). Це дозволило організаціям пройти процес сертифікації та отримати довіру для безпосередньої видачі CVE. Це дозволило програмі масштабуватися для обробки нового навантаження.

Навпаки, NVD залишалася по суті однопотоковою системою, де найняті дослідники проводили додаткові дослідження кожного CVE, щоб призначити йому оцінку (CVSS) і призначити ідентифікацію ураженого програмного забезпечення (Common Platform Enumeration або CPE).

Конвергенція цих факторів створила потік звітів низької якості, що загострило проблеми масштабування дослідників у програмі NVD. Нещодавнє припинення розширених уразливостей підкреслює необхідність удосконалення існуючих фреймворків для створення середовища, де визнається справжній внесок і мінімізується шум. Це також можливість переосмислити структуру цих систем. Об’єднана модель, така як CNA, розроблена для масштабування, і додавання оцінки та ідентифікації програмного забезпечення до CVE, які вони призначають, не повинно бути важким завданням.

Якщо ми хочемо забезпечити цілісність і ефективність наших колективних зусиль у сфері безпеки, співтовариство кібербезпеки має переглянути свою залежність від NVD і адаптувати свої процеси відповідно до динаміки управління вразливістю». ***(Brian Fox. The Fall of the National Vulnerability Database // Informa PLC (https://www.darkreading.com/vulnerabilities-threats/fall-of-national-vulnerability-database?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 16.05.2024).***

***

«Дослідники виявили серйозну вразливість до пошкодження пам'яті в утиліті хмарного журналювання, яка використовується на основних хмарних платформах.

Служба, Fluent Bit, є інструментом з відкритим кодом для збору, обробки та пересилання журналів та інших типів даних програми. Це одне з найпопулярніших програмних продуктів, яке станом на 2022 рік було завантажено понад 3 мільярди, а з кожним днем розгортається близько 10 мільйонів нових програм. Його використовують великі організації, такі як VMware, Cisco, Adobe, Walmart і LinkedIn, а також майже всі великі постачальники хмарних послуг, включаючи AWS, Microsoft і Google Cloud.

Проблема з Fluent Bit, яку в новому звіті Tenable назвали «Linguistic Lumberjack», полягає в тому, як вбудований HTTP-сервер служби аналізує запити трасування. Маніпулювання таким чи іншим способом може спричинити відмову в обслуговуванні (DoS), витік даних або віддалене виконання коду (RCE) у хмарному середовищі.

«Кожного розголошують про вразливість Azure, AWS, GCP, але ніхто насправді не дивиться на технології, які складають усі ці основні хмарні сервіси — звичайні основні частини програмного забезпечення, які зараз впливають на кожного великого хмарного постачальника», — каже Джимі Себрі, старший інженер-дослідник Tenable. «Вам потрібно шукати бомби безпеки програм і подобатися компонентам служб, а не лише самим службам».

Лінгвістичний ефект дроворуба

Дослідники Tenable спочатку розглядали абсолютно окрему проблему безпеки в нерозкритій хмарній службі, коли зрозуміли, що відбувається щось несподіване. З місця, де вони сиділи, здавалося, що вони мали доступ до широкого спектру власних внутрішніх показників і кінцевих точок реєстрації постачальника хмарних послуг (CSP). Серед них були екземпляри Fluent Bit.

Цей витік даних між клієнтами стався з кінцевих точок програмного інтерфейсу програми моніторингу (API) Fluent Bit, призначеного для того, щоб

користувачі могли запитувати та контролювати внутрішні дані. Однак після деякого тестування трохи витоку даних виявилося лише вступом до глибшої проблеми.

Для певної кінцевої точки — /api/v1/traces — типи даних, передані як імена вхідних даних, не були належним чином перевірені до аналізу програмою. Таким чином, передаючи нерядкові значення, зловмисник може спричинити будь-які проблеми з пошкодженням пам’яті у Fluent Bit. Дослідники випробували різноманітні позитивні та негативні цілі значення, зокрема, щоб успішно викликати помилки, через які служба призведе до збою та витоку потенційно конфіденційних даних.

Зловмисники також потенційно можуть використати цей самий прийом, щоб отримати можливості RCE у цільовому середовищі. Проте Тенабл зауважив, що розробка такого експлойта потребуватиме значних зусиль, оскільки він буде налаштований відповідно до конкретної операційної системи та архітектури цільової програми.

Що з цим робити

Помилка існує у версіях Fluent Bit від 2.0.7 до 3.0.3. Він відстежується відповідно до CVE-2024-4323, і різні сайти присвоїли йому «критичні» оцінки CVSS понад 9,5 з 10. Після того, як про це було повідомлено 30 квітня, супроводжувачі Fluent Bit оновили службу для належної перевірки типів даних у цій проблемній ситуації. поле введення кінцевої точки. Виправлення було застосовано до головної гілки проекту на GitHub 15 травня.

Організаціям, які розгорнули Fluent Bit у власній інфраструктурі та середовищі, рекомендується оновити якомога швидше. В якості альтернативи, Tenable пропонує, адміністратори можуть переглядати будь-які конфігурації, пов’язані з API моніторингу Fluent Bit, щоб переконатися, що лише авторизовані користувачі та служби можуть запитувати його — або навіть жодні користувачі чи служби взагалі». ***(Nate Nelson. Critical Bug Allows DoS, RCE, Data Leaks in All Major Cloud Platforms // Informa PLC (https://www.darkreading.com/cloud-security/critical-bug-dos-rce-data-leaks-in-all-major-cloud-***

platforms?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 20.05.2024).

***

«Цей тиждень був жахливим для Google і понад 2 мільярдів користувачів настільних ПК Chrome. Тепер уряд США додав третю серйозну загрозу безпеці нульового дня до свого центрального каталогу вразливостей Chrome, які, як відомо, стоять за активними атаками.

Вам потрібно переконатися, що ваш веб-переглядач успішно оновлено — ось що вам потрібно зробити...

Усі три вразливості додано до CISA — каталогу відомих використаних уразливостей (KEV) Агентства кібербезпеки та безпеки інфраструктури США. У цьому каталозі перераховано «вразливості, які використовувалися в дикій природі... Організації повинні використовувати каталог KEV як вхідні дані для своєї системи пріоритетів керування вразливостями».

Недостатньо дозволити веб-переглядачу оновлюватися автоматично — вам потрібно активно переконатися, що оновлення встановлено однією простою дією, як пояснюється нижче.

Перше попередження Chrome «оновити зараз» з'явилося 9 травня, коли Google попереджав, що «знав, що експлойт для CVE-2024-4671 існує в дикій природі». Уразливість полягала в проблемі «використання після звільнення», коли вказівники на звільнену пам'ять не видаляються, тому ними можна зловживати.

Як попереджає Касперський, «зловмисник може використовувати UAF для передачі довільного коду або посилання на нього в програму та переходу до початку коду за допомогою висячого покажчика. Таким чином, виконання шкідливого коду може дозволити кіберзлочинцю отримати контроль над системою жертви».

Але до того, як більшість користувачів навіть дізналися про проблему, прийшла атака номер два. саме 13 травня CVE-2024-4761 рекламував Google, щоб попередити про виявлення експлойту в дикій природі. Цього разу це була

вразливість пам’яті «поза межами», яка вплинула на двигун Chrome V8 Javascript. Цей тип проблеми дозволяє зловмиснику націлюватися на Chrome зі зловмисно створеними HTML-сторінками.

Проблема поза межами ризикує розкрити конфіденційну інформацію, яка не повинна бути доступною, а також загрожує збоєм системи чи програмного забезпечення, що може дозволити зловмиснику отримати доступ до цих даних.

А лише через 48 годин, 15 травня, Google також попередив, що «експлойт для CVE-2024-4947 існує в дикій природі». Це була ще одна проблема з пам’яттю, уразливість «тип плутанина», яка знову наражає користувачів на сфабриковану атаку на сторінку HTML.

Плутанина типів виникає, коли програмне забезпечення намагається отримати доступ до несумісних ресурсів без захисної мережі, щоб уловити ризик. Помилка може перевести систему в неочікуваний стан, відкриваючи загрозу безпеці.

Усі ці вразливості можуть дестабілізувати браузер або пристрій, що само по собі викликає занепокоєння, але також можуть бути використані для запуску інших експлойтів, коли система дестабілізується.

У більшості користувачів Chrome буде налаштовано на автоматичне оновлення, що завжди має робитися для оновлень безпеки такого типу. Але цього самого по собі недостатньо. Ви завжди повинні повністю закривати та перезапускати Chrome, щоб переконатися, що оновлення повністю встановлено.

Враховуючи тривожну оптику трьох нульових днів за шість днів і логістику розгортання кількох випусків програмного забезпечення для такої кількості систем за такий короткий проміжок часу, вам слід вручну закрити та перезапустити Chrome сьогодні, сподіваємося, що кошмарний тиждень веб-переглядача настане зараз. кінець.

Навіть якщо ви думаєте, що оновлення вже встановлено, це хороший захист від збоїв.

Насправді я б пішов далі цього тижня, а також запропонував би перезавантажити пристрій, якщо це не спричинить багато додаткових проблем з іншим програмним забезпеченням, яке ви використовуєте.

Що стосується Chrome, це не повинно викликати багато проблем. Як пояснює Google, Chrome «зберігає ваші відкриті вкладки та вікна та знову відкриває їх автоматично після перезапуску». Але це не включає квазіприватний режим перегляду Google. «Ваші анонімні вікна не відкриються знову після перезапуску Chrome».

CISA також попередила, що перші дві вразливості «можуть вплинути на кілька веб-браузерів, які використовують Chromium, включаючи, але не обмежуючись ними, Google Chrome, Microsoft Edge і Opera».

Федеральні агентства США мають до 3, 6 і 10 червня відповідно «застосувати пом’якшення відповідно до інструкцій постачальника або припинити використання продукту, якщо пом’якшення недоступні».

Отже, що робити з цим кошмарним тижнем для Google і величезної кількості користувачів Chrome. Не дивно, що Google зазнає стільки ударів, це складна платформа та приманка для атак, враховуючи всюдисущість його бази встановлення для настільних комп’ютерів.

Експлойти проти будь-якого програмного забезпечення, яке, як може припустити зловмисник, буде на цільовому пристрої, високо цінуються. Усе це означає значні зусилля хороших і поганих хлопців, щоб знайти будь-які вразливі місця. І ось ми тут.

Трохи іронічно, що саме тоді, коли кошмарний тиждень Chrome завершився, Google випустив білий документ під назвою «Більш безпечна альтернатива», критикуючи Microsoft і припускаючи, що «після значних інцидентів кібербезпеки з Microsoft, Google Workspace пропонує безпечніший вибір».

Chrome — це не робочий простір, і офіційний документ зосереджувався на складних кібератаках, а не просто на використаних уразливостях. Але пам’ятаймо, одне веде до іншого.

І, окрім деталей, візуально хронометраж, м’яко кажучи, дещо незручний. Можливо, PR-відділ міг би притримати це лише кілька днів. Ми ще не знаємо масштабів будь-яких атак і чи було виявлення експлойтів пов’язане з якоюсь конкретною кампанією.

Хороша новина полягає в тому, що екстрені оновлення від Google цього разу були дуже вчасними — до такої міри, що потрапили в заголовки газет у всьому світі. Тепер вам просто потрібно зробити свій внесок». ***(Zak Doffman. Google Chrome Under Attack—Do This One Thing Now // Forbes (https://www.forbes.com/sites/zakdoffman/2024/05/20/new-google-chrome-attacks-microsoft-windows-10-windows-11-free-upgrade/?sh=42ae1db06fe7). 20.05.2024).***

***

«Мова програмування Go, широко визнана своєю ефективністю та простотою, нещодавно стала предметом критичних оновлень безпеки.

Команда Go випустила патчі для двох значних уразливостей, які можуть дозволити зловмисникам виконувати довільний код і викликати збої в роботі через нескінченні цикли.

Ці вразливості, ідентифіковані як CVE-2024-24787 і CVE-2024-24788, становлять серйозну загрозу для систем, на яких запущено уражені версії Go.

Уразливість виконання довільного коду на Darwin (CVE-2024-24787)

У середовищі програмування Go було виявлено критичну вразливість, яка, зокрема, впливає на операційні системи Darwin.

Ця проблема, яка відстежується в CVE-2024-24787, виникає під час процесу збирання модулів Go, які включають CGO.

Уразливість спричинена неправильним використанням прапора `-lto_library` в директиві `#cgo LDFLAGS`, яка використовується з версією компонувальника (ld) від Apple.

Цей недолік може дозволити зловмиснику виконати довільний код, завантаживши шкідливу бібліотеку LTO (Link Time Optimization) під час процесу збирання.

Уразливості було присвоєно оцінку CVSS 9,8, що вказує на її серйозність.

Нескінченний цикл у функціях пошуку DNS (CVE-2024-24788)

Друга вразливість, CVE-2024-24788, впливає на функції пошуку DNS у Go. Спеціально створена відповідь DNS може призвести до нескінченного циклу цих функцій, що потенційно може призвести до стану відмови в обслуговуванні (DoS).

Ця вразливість насамперед загрожує веб-додаткам і службам, які покладаються на запити Go for DNS, причому оцінка CVSS 7,5 відображає її значний вплив.

Терміновий дзвінок для оновлення

Команда Go швидко відреагувала на ці загрози, випустивши версії Go 1.22.3 і 1.21.10, які усувають ці вразливості.

Розробників і системних адміністраторів закликають негайно оновити свої установки Go, щоб захистити свої системи від потенційних експлойтів.

Оновлення містять необхідні виправлення, які запобігають використанню цих вразливостей.

Ці недавні вразливості підкреслюють поточні проблеми, з якими стикаються під час захисту ланцюгів постачання програмного забезпечення та інфраструктури.

Оскільки використання Go продовжує зростати в різних програмах, дотримання суворих методів безпеки та регулярне оновлення стає все більш важливим.

Користувачам Go радимо дотримуватися найкращих практик безпеки та негайно оновлювати свої системи, щоб зменшити ці ризики». ***(Guru Baran. Golang Vulnerability Alert: Remote Code Execution & Infinite Loop DNS Lookup // Cyber Security News (https://cybersecuritynews.com/golang-vulnerability-alert/). 09.05.2024).***

***

«Несподіваний відхід IBM від програмного забезпечення для кібербезпеки цього тижня не просто змінив конкурентний ландшафт — він також змінив плани закупівель і відносини з постачальниками для багатьох CISO, які перебудовують свої центри безпеки (SOC).

IBM погодилася продати портфоліо QRadar SaaS компанії Palo Alto Networks за нерозголошену суму. У 2023 році після багатьох років розробки IBM почала розгортати QRadar Suite — хмарний набір спільних компонентів безпеки кінцевих точок, включаючи кілька продуктів виявлення та реагування (EDR, XDR і MDR). Він також представив можливості керування журналами, зокрема платформи управління інформацією про безпеку та подіями (SIEM) і оркестровки безпеки, автоматизації та реагування (SOAR).

На початку 2024 року IBM випустила QRadar SIEM, а на початку цього місяця випустила локальну версію на основі Red Hat OpenShift. План включав наступні поетапні випуски генеративного штучного інтелекту (ШІ) з моделями мов навчання (LLM) на основі нової платформи ШІ watsonx.

Очікується, що угода, яка базується на партнерстві між двома компаніями, яке було розширено наприкінці минулого року, завершиться до кінця вересня. Пакт також передбачає, що IBM Consulting стане «переважним постачальником керованих послуг безпеки» (MSSP) для існуючих і майбутніх клієнтів Palo Alto Networks, причому обидва постачальники мають спільний SOC.

Palo Alto Networks повідомила, що організації, які бажають продовжувати локальну інсталяцію QRadar, продовжуватимуть отримувати оновлення функцій, виправлення критичних помилок і оновлення існуючих роз’ємів. Не було зрозуміло, як довго це буде запропоновано.

Тим не менш, продаж IBM свого бізнесу QRadar SaaS є приголомшливим поворотом. Це слідує за амбітним планом IBM з турбонаддуву своїх застарілих пропозицій QRadar, включаючи широко розгорнуту платформу SIEM, пакетом програмного забезпечення як послуги (SaaS) у хмарі.

Потенційна плутанина для клієнтів

Тепер клієнти повинні визначитися, чи хочуть вони слідувати нещодавно оголошеним вибраним шляхом, який вимагає перенесення застарілих пакетів QRadar і SaaS на Cortex XSIAM від Пало-Альто, чи оцінити інші варіанти.

Згідно з дослідженням Omdia, QRadar від IBM є третім за величиною постачальником SIEM наступного покоління за доходом після Microsoft і Splunk (тепер частина Cisco).

«Це один із найдивовижніших кроків, які я бачив у сфері корпоративної кібербезпеки за багато років», — каже керуючий аналітик Omdia Ерік Парізо.

Парізо каже, що цей крок особливо дивний, оскільки протягом останніх трьох років IBM інвестувала мільйони доларів і вклала значні ресурси в перетворення QRadar на хмарну платформу. IBM придбала QRadar, локальну SIEM, у Q1 Labs у 2011 році.

«Те, що IBM потім розвернулась і продала QRadar компанії Palo Alto Networks, здавалося б, практично без попередження для клієнтів, шокує і, відверто кажучи, не відповідає орієнтованості на клієнта, якою відома IBM», — каже Парізо. «Я думаю, що [зараз] багато збентежених і розчарованих клієнтів QRadar шукають відповіді».

CISO стикаються з цими рішеннями в критичний момент. Основні постачальники та аналітики повідомили про об’єднання SIEM, SOAR і XDR в єдину операційну платформу SOC на чолі з хмарними гігантами AWS, Microsoft і Google, а також великими постачальниками платформ, включаючи CrowdStrike, Cisco і Palo Alto Networks.

Довіряючи цій прогнозованій консолідації, Exabeam і LogRhythm оприлюднили свої плани злиття всього за кілька годин до того, як новини IBM-Palo Alto Networks стали публічними. Об’єднана компанія планує інтегрувати застарілу технологію LogRhythm і нову хмарну технологію SIEM із платформою аналізу поведінки користувачів і об’єктів (UEBA) Exabeam.

«Як об’єднана організація, ми продовжуватимемо просувати інновації в сфері безпеки за допомогою рішень, які об’єднують штучний інтелект, автоматизацію,

SIEM, аналітику безпеки та UEBA, щоб забезпечити цілісний підхід до боротьби з кіберзагрозами», — сказав генеральний директор Exabeam Адам Геллер, у заяві.

«Усі застарілі гравці SIEM стикаються зі зростаючою конкуренцією з боку технічних титанів (так званих гіперскейлерів), а також постачальників XDR, які агресивно позиціонують себе як альтернативи SIEM», — зазначила головний аналітик Forrester Аллі Меллен.

Можливо, IBM натякала на свою остаточну стратегію, торік запустивши пакет QRadar SaaS як план міграції для своєї застарілої SIEM та інших пропозицій кібербезпеки. На момент запуску в листопаді IBM випустила хмарне оновлення своєї SIEM, але компанії все ще не вистачало повноцінної пропозиції XDR, заявив Меллен у своєму блозі.

«Більшість того, що вони надають, дуже, дуже орієнтована на EDR», — сказала вона.

Поштовх для Пало-Альто

Аналітики вважають, що QRadar принесе користь організаціям, які віддають перевагу Palo Alto Networks, оскільки він обіцяє розширити пропозицію Cortex XSIAM SIEM. Меллен підкреслив, що Palo Alto Networks XSIAM привернула увагу клієнтів завдяки своїм можливостям автоматизації та MDR, а також в комплекті з пропозицією Cortex XDR.

«Однак досягнення такого масштабу клієнтів, як у постачальників застарілих SIEM і деяких великих гравців, — довгий шлях», — написав Меллен. Придбання Palo Alto Networks IBM QRadar SaaS прискорить це, додала вона.

Palo Alto Networks повідомила, що існуючим клієнтам QRadar SaaS буде запропоновано безкоштовні шляхи міграції до Cortex XSIAM, які спільно нададуть IBM і Palo Alto Networks. IBM, співробітники якої не переходять на Palo Alto Networks, заявила, що залучить понад 1000 консультантів з безпеки для надання послуг з міграції та розгортання.

Примітно, що Меллен підкреслив, що можливість безкоштовної міграції також буде поширена на «кваліфікованих» локальних клієнтів QRadar. Вона

порадила клієнтам якомога швидше визначити, чи відповідають вони вимогам для цих безкоштовних міграцій.

Сумнівне майбутнє QRadar SaaS

Залишається побачити, яка технологія від QRadar SaaS запровадить свій шлях у XSIAM і Cortex. Проте, грунтуючись на оголошенні, вона сказала, що Меллен вважає, що придбання спрямоване на отримання клієнтської бази QRadar.

«PANW явно не має довгострокових планів щодо пропозиції QRadar SaaS», — зазначив Меллен. «Як тільки договірні зобов'язання закінчаться, існуючі клієнти QRadar SaaS повинні прийняти XSIAM або перейти до іншого постачальника».

Palo Alto Networks робить значні інвестиції в Cortex XSIAM, свою нову пропозицію SIEM, випущену на початку 2022 року, але не вірить, що вона на одному рівні з QRadar, додає Парізо з Omdia.

«Хоча рішення швидко еволюціонувало за останні два роки, воно все ще є відносно молодим і загалом менш зрілим і менш надійним з точки зору конкретних можливостей, ніж IBM QRadar», — каже Парізо. «Я не можу очікувати, що клієнти QRadar перейдуть на XSIAM у будь-який момент протягом наступних 12-24 місяців і отримають еквівалентний набір можливостей», зокрема для виявлення загроз, дослідження та реагування.

Він додає: «Зрештою, я вважаю, що Palo Alto Networks доведеться підтримувати клієнтів QRadar на існуючому рішенні протягом більш тривалого періоду часу та суттєво стимулювати клієнтів QRadar перейти на XSIAM, щоб подолати виклики, які виникнуть у цей поточний період невизначеності.»

Перенесення Watsonx AI в Cortex XSIAM

Хоча наміри Palo Alto Networks щодо стеку QRadar можуть бути невизначеними, угода передбачає включення IBM watsonx LLMs у Cortex XSIAM, який забезпечить його нові інструменти Precision AI.

«IBM має дуже хороший штучний інтелект; вони просто не мають великої частки ринку», — каже видатний аналітик Gartner Авіва Літан. «Можливо, це їм допоможе». ***(Jeffrey Schwartz. CISOs Grapple With IBM's Unexpected Cybersecurity Software Exit // Informa PLC (https://www.darkreading.com/cybersecurity-***

analytics/ciso-grapple-with-ibm-unexpected-cybersecurity-software-exit?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 18.05.2024).

***

«Linea, фірма з безпеки блокчейнів, перешкоджає атаці, спрямованій на обхід емітентів і отримання сертифікатів, підкреслюючи ескалацію загроз кібербезпеці в крипто-секторі.

Linea виявляє та нейтралізує загрози кібербезпеці

Linea, відоме ім'я в індустрії безпеки блокчейнів, успішно виявила та нейтралізувала значну загрозу кібербезпеці. Атака була спрямована на обхід емітентів і отримання сертифікатів, метод, який потенційно міг скомпрометувати цілісність транзакцій блокчейну. Швидкі дії фірми не тільки запобігли потенційній шкоді, але й підкреслили зростаючу потребу в надійних заходах безпеки в криптопросторі.

Зростання загроз кібербезпеці в секторі криптовалют

Оскільки криптовалюти продовжують набувати загального визнання, у секторі спостерігається відповідне зростання загроз кібербезпеці. Хакери та кіберзлочинці постійно розробляють нові методи використання вразливостей у блокчейн-мережах і криптогаманцях. У цьому контексті нещодавня атака, виявлена Linea, є яскравим нагадуванням про постійну загрозу. Згідно зі звітом CipherTrace, загальна сума крадіжок, шахрайства та шахрайства криптовалюти склала 1,9 мільярда доларів у 2020 році, що підкреслює терміновість посилених заходів безпеки.

Роль Linea у забезпеченні безпеки блокчейну

Linea була в авангарді блокчейн-безпеки, надаючи комплексні рішення для захисту від широкого спектру загроз кібербезпеці. Розширені системи виявлення та профілактичні заходи безпеки компанії відіграли важливу роль у захисті численних транзакцій блокчейну. Нещодавній інцидент є свідченням відданості Linea забезпеченню безпеки та цілісності криптосектору.

Висновок

Недавня атака, виявлена Linea, підкреслює ескалацію загроз кібербезпеці в криптосекторі. Оскільки криптовалюти продовжують отримувати широке визнання, потреба в надійних заходах безпеки є більш важливою, ніж будь-коли. Такі фірми, як Linea, відіграють вирішальну роль у забезпеченні безпеки та цілісності транзакцій блокчейну, сприяючи зміцненню довіри та впевненості в криптопросторі». ***(Gideon Wolf. Linea Thwarts Cyber Attack Aimed at Issuers and Attestations: A Major Win for Crypto Security (LINEA) // COINOTAG (https://en.coinotag.com/linea-thwarts-cyber-attack-aimed-at-issuers-and-attestations-a-major-win-for-crypto-security-linea/). 12.05.2024).***

***