**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

№ 12 (грудень)

Київ – 2023

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №12 (грудень) . – 354 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

«Київстар, найбільший мобільний оператор України, продовжить реалізацію плану з інвестування $600 млн у свою мережу по всій країні після того, як минулого тижня зазнав масштабного порушення безпеки і повного відключення зв'язку, заявив президент компанії Олександр Комаров на щорічному заході «Україна і світ попереду», організованому журналом НВ 21 грудня.

«Ми залишаємося відданими нашим планам інвестувати $600 млн в Україну, і ми збільшимо наші інвестиції в кібербезпеку, ми повністю її модернізуємо», - сказав Комаров.

«Виявилося, що цього було недостатньо. Ми повністю змінимо наш підхід до архітектури кібербезпеки нашої компанії».

Він також зазначив, що «Київстар» почав процес компенсації клієнтам незручностей, які вони зазнали через недавню масштабну кібератаку.

«Сьогодні ми анонсували програму компенсацій», — сказав глава компанії.

«Будь-який абонент «Київстар» може пропустити наступну абонентську плату та користуватися послугою протягом місяця безкоштовно». ***(Kyivstar to invest in cybersecurity after major hack // VYDAVNYCHYY DIM MEDIA-DK LLC (https://english.nv.ua/business/kyivstar-to-invest-in-cybersecurity-after-major-hack-50378502.html). 21.12.2023).***

***

«Аналітична компанія Recorded Future схвалила виділення 23 мільйонів доларів США на посилення кібербезпеки України. Гроші підуть на захист важливих розвідувальних даних і протидію можливим загрозам у Мережі.

Деталі

Подробиці 18 грудня повідомив міністр цифрової трансформації Михайло Федоров у Telegram. Гроші мають передати Україні 2024 року, уточнив керівник міністерства.

Інструменти компанії вже використовують, щоб виявити загрози та усунути атаки хакерів на ранніх стадіях. Їх впровадили:

Міністерство цифрової трансформації;

Державне агентствто спеціального зв'язку та захисту інформації;

Головне управління розвідки;

Служба безпеки України;

Міністерство оборони;

Генеральна прокуратура;

Кіберполіція.

За словами Федорова, 2023 року сервіси компанії допомогли виявити групу хакерів APT28, яка отримала доступ до урядових організацій України.

Також компанія працює з ключовими підприємствами в енергетичній та телеком-сфері, а її якісні та надійні розвіддані — це те, без чого неможливо виграти технологічну війну

Міністр наголосив, що після повномасштабного нападу рф, у Recorded Future допомагають Україні даними розвідувального характеру, щоб країна змогла посилити безпеку критично важливої інфраструктури…» ***(Олександр Воєйков. Україна отримає $23 млн на посилення кібербезпеки та захист від хакерів // META.UA (https://meta.ua/uk/news/economics/106371-ukrayina-otrimae-23-mln-na-posilennya-kiberbezpeki-ta-zahist-vid-hakeriv/). 18.12.2023).***

***

Правове забезпечення кібербезпеки в Україні

«Кабмін затвердив план заходів на 2023–2024 роки з реалізації стратегії кібербезпеки України.

Про це йдеться на сайті КМУ.

Одним із завдань стратегії є створення в системі Міноборони кібервійськ, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для

стримування збройної агресії в кіберпросторі та надання відсічі агресору. Реалізація цього завдання планується на І квартал 2024 року.

Відповідна стратегія також передбачає:

розроблення системи індикаторів стану кібербезпеки;

забезпечення проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав – членів НАТО для досягнення оперативної сумісності;

створення MIL.CERT-UA в інтересах Міноборони та Збройних Сил, налагодження на постійній основі співпраці з європейською військовою CERT-мережею;

посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-сфери.

Крім того, планується розроблення національного плану реагування на надзвичайні ситуації в кіберпросторі з визначенням механізмів реагування на кібератаки загальнонаціонального масштабу щодо об’єктів критичної інформаційної інфраструктури та заходів з подальшого відновлення; проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань і тренінгів за участю представників державного та приватного сектору тощо.

Нагадаємо: 26 серпня 2021 року президент України Володимир Зеленський ввів у дію рішення РНБО щодо невідкладних заходів із кібероборони держави, що передбачає створення кібервійськ». ***(Уряд планує створити кібервійська в системі Міноборони в І кварталі 2024 року // ТОВ «Фьючер Медіа» (https://mind.ua/news/20267240-uryad-planue-stvoriti-kibervijska-v-sistemi-minoboroni-v-i-kvartali-2024-roku). 21.12.2023).***

***

«Розвідка Міноборони України повідомила, що здійснила успішну атаку на Федеральне агентство повітряного транспорту Росії, відому як Росавіація, і отримала невстановлену кількість документів, що стосуються повсякденної діяльності агентства по всій країні.

Кібератаки стали частиною норми після російського вторгнення в Україну, причому одні були більш успішними, ніж інші. Росія постійно випробовує різні просунуті методи фішингу для зламу критичних систем в Україні та шукає вразливі місця.

З іншого боку, Україні допомагають хакери з усього світу, які постійно шукають вразливі цілі. Ця остання атака заслуговує на увагу, оскільки українська розвідка була відповідальною стороною.

«Головне управління розвідки Міноборони України повідомляє, що в результаті успішної комплексної спецоперації в кіберпросторі вилучено великий обсяг конфіденційної документації структурного підрозділу Мінтрансу Росії – Федерального агентства повітряного транспорту (Росавіація), української влади», - йдеться в прес-релізі.

«Зазначене відомство відповідає за безпеку польотів і фіксує всі випадки надзвичайних ситуацій під час експлуатації російської авіації. Дані, отримані в результаті злому та проникнення в інформаційні системи противника, включають перелік щоденних зведень Росавіації по всій Російській Федерації за понад півтора року», – додали в відомстві.

За словами українців, документи розкривають жахливий стан російської авіації, показуючи, що за один місяць у російській цивільній авіації було зафіксовано 185 аварій і що загроза безпеці польотів у Росії зросла втричі.

Крім того, Росія почала канібалізувати деякі зі своїх літаків, щоб інші літали.

Поки залишається незрозумілим, як це вдалося українцям, російські колеги ще не підтвердили порушення». ***(Silviu STAHIE. Ukraine Claims to Have Hacked Russian Air Transport Agency // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/ukraine-claims-to-have-hacked-***

russian-air-transport-agency/?utm_source=flipboard&utm_content=HamsterBoomer%2Fmagazine%2FHACKER%20-%20HACKED%2F). 04.12.2023).

***

«Українські фахівці очікують, що у 2024 році росіяни будуть проводити проти України набагато складніші кібератаки, зокрема з застосуванням штучного інтелекту. Про це під час виступу на конференції SANS CyberThreat 2023 у Лондоні розповів фахівець Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA Назар Тимошик, передає УНН.

За його словами, вже зараз окупанти залучають молодь і готують нове покоління хакерів...

Водночас він підкреслив, що рівень кіберзахищеності в Україні від 2022 року значно покращився. Зокрема завдяки технічній допомозі партнерів та обміну інформацією. Крім того, українські компанії почали більш фахово реагувати на кіберризики.

Тимошик розповів учасникам заходу про зміну моделей поведінки, цілей і можливостей російського уряду та підконтрольних йому груп хакерів, яка відбулася в першій половині 2023 року…» ***(У Держспецзв'язку прогнозують, що у 2024 росія вдасться до складніших кібератак // Українські Національні Новини (https://unn.ua/news/u-derzhspetszviazku-prohnozuiut-shcho-u-2024-rosiia-vdastsia-do-skladnishykh-kiberatak). 06.12.2024).***

***

«Провідний український оператор телефонного зв'язку «Київстар» повідомив про збої в містах на заході та півдні країни, повідомляє 20 грудня «Українська правда» з посиланням на прес-секретаря «Київстар» Ірину Леліченко.

Україна зазнала масової кібератаки 12 грудня, метою якої були Київстар і один із найбільших банків країни Monobank. Люди по всій країні повідомляли про

збої в Інтернеті та мережі, а також про проблеми з повідомленнями про повітряний наліт.

У «Київстар» станом на вересень цього року понад 24 мільйони абонентів мобільного зв’язку та більше 1 мільйона клієнтів домашнього інтернету.

Відповідальність за атаку взяла на себе російська хакерська група, імовірно пов'язана з російськими спецслужбами.

Леліченко не став коментувати причини цих збоїв і сказав, що компанія працює над якнайшвидшим відновленням роботи.

Росію неодноразово звинувачували в підтримці груп кіберзлочинців у атаках на своїх конкурентів. Москва також розгорнула свої кіберпотенціали проти України, включаючи атаки на державні установи, оборонний сектор та енергетичну інфраструктуру». ***(Nate Ostiller. Kyivstar reports outages in parts of Ukraine // The Kyiv Independent (https://kyivindependent.com/kyivstar-reports-outages-in-parts-of-ukraine/?utm_source=flipboard&utm_content=other). 20.12.2023).***

***

«ІТ-армія зупинила роботу російського хмарного сервісу «Бітрікс24».

Про це йдеться на телеграм-каналі IT ARMY of Ukraine у середу, 20 грудня.

Кібери пояснили, що внаслідок атаки «Роснафта» «має шалені проблеми у роботі з клієнтами, як і у 40%+ користувачів всіх CRM-систем в країні-агресорі».

«Це десятки чи навіть сотні мільйонів доларів збитків для економіки ворога, але залежить від того як довго ми їх протримаємо», – йдеться в дописі.

Мінцифри повідомило, що цим сервісом користуються найбільші компанії-спонсори війни в Росії». ***(Наші хакери «поклали» російський хмарний сервіс «Бітрікс24» // Новинарня (https://novynarnia.com/2023/12/20/nashi-hakery-poklaly-rosijskyj-hmarnyj-servis-bitriks24/). 20.12.2023).***

***

«Кібергрупа «Blackjack», яка, за попередніми висновками, може мати зв'язок з кіберспецслужбами СБУ, виконала атаку на інформаційну інфраструктуру «Росводоканалу», повністю блокуючи його роботу.

За інформацією «УП» від джерел в силових структурах, хакери здійснили атаку на понад 6000 комп'ютерів, вилучивши понад 50 ТБ даних.

Серед втрачених даних – внутрішні документи, корпоративна пошта, кіберзахистові сервіси, а також резервні копії. На даний момент робота «Росводоканалу» повністю припинена. Служба безпеки проводить аналіз вже завантажених 1,5 ТБ даних від «Росводоканалу»…» ***(Вікторія Горьова. Українські хакери знищили IT-інфраструктуру «Росводоканалу» – ЗМІ // ТОВ "Національні інформаційні системи" (https://podrobnosti.ua/2487022-ukransk-hakeri-znischili-it-nfrastrukturu-rosvodokanalu-zm.html). 20.12.2023).***

***

«Росія може переключити фокус своїх кібератак на західних союзників України, намагаючись підірвати їхню підтримку, передає Sky News із посиланням на експертів компанії з аналізу цифрових загроз для міжнародних корпорацій Сујах.

Кремль опирається на групи хакерів для підтримки своїх операцій. Сујах відзначив зростання активності проросійських UserSec, SiergedSec, NoName057, AnonymousSudan та AnonymousRussia. В опублікованій нині доповіді «Кіберзима невдоволення» компанія відзначила, що вони поки що не мали того згубного впливу, на який сподівався російський диктатор Володимир Путін.

Підтримка західних країн допомогла Україні зупинити атаки РФ в інформаційній сфері. Тому є ризик, що Росія атакує їх. Чимало з країн мають слабкий кіберзахист, відзначили експерти компанії. Тож Кремль спробує скористатися цим, аби порушити ланцюжки постачань допомоги Україні.

«Бізнес та експерти з кібербезпеки повинні бути насторожі щодо будь-якої несанкціонованої діяльності та зміцнювати свій захист у кібер- та інформаційному просторі», — зазначали в Сујах.

Кібератаки РФ на Україну

- Одна з останніх цілей - мережа "Київстар". СБУ відкрила кримінальне провадження за фактом кібератаки на оператора мобільного зв'язку за вісьмома статтями Кримінального кодексу. Одна із версій – за цією хакерською атакою можуть стояти російські спецслужби.
- Також відбулася масована DDoS-атака на Монобанк.
- Крім того, росіяни намагаються зламати український месенджер Signal
- Раніше мережа ботів намагалась завадити зустрічі Зеленського з Нетаньягу

Кібератаки Росії на союзників України

- Нещодавно Британія звинуватила Росію у кібератаках на високопоставлених політиків. Кібергрупа, підпорядкована ФСБ, збирала та "зливала" інформацію ще із 2015 року. Росіяни займались фішингом і збирали інформацію від значної кількості парламентаріїв із кількох політичних партій.
- Групи хакерів, тісно пов'язаних з РФ та Китаєм, зламали системи найбільшого ядерного об'єкта Великої Британії – Селлафілду.
- Минулого тижня Британія і США ввели санкції проти двох хакерів ФСБ, які розробляли цільові фішингові операції.
- У жовтні сайти уряду, парламенту, королівського палацу Бельгії зазнали кібератаки. Тоді підозрювали російських хакерів.
- Сайти МВС Чехії, поліції та рятувальників теж зазнали атаки з боку проросійських хакерів». ***(Віра Перун. Суjах: Росія може посилити свої кібератаки на союзників України // LB.ua (https://lb.ua/world/2023/12/13/588819_cyjax_rosiya_mozhe_posiliti_svoi.html). 13.12.2023).***

***

«Кіберпідрозділи Головного управління розвідки атакували податкову систему Росії, вдалося знищити всю базу даних і її резервні копії. Розвідники додають, що Росії не вдасться повністю реанімувати свою податкову систему.

Джерело: пресслужба ГУР

Дослівно: «Під час спецоперації воєнним розвідникам вдалось проникнути в один із добре захищених ключових центральних серверів фєдєральной налоґовой служби (ФНС РФ), а далі – у понад 2300 її регіональних серверів по всій росії, а також на території тимчасово окупованого Криму.

Внаслідок кібератаки усі сервери отримали шкідливе програмне забезпечення...

Відновити роботу податкової росіяни безуспішно намагаються уже четвертий день поспіль. За оцінками фахівців, параліч у роботі ФНС РФ триватиме щонайменше місяць. Водночас реанімація податкової системи держави-агресора у повному обсязі – неможлива».

Деталі: Також українські фахівці у такий же спосіб атаковали російську IT-компанію Office.ed-it.ru, яка обслуговувала ФНС РФ.

Повідомляється, що в результаті двох кібератак вдалося повністю ліквідувати конфігураційні файли, які роками забезпечували функціонування розгалуженої податкової системи РФ – знищена уся база даних та її резервні копії (backup).

Зв’язок між центральним офісом у Москві та 2300 російськими територіальними управліннями — паралізований, як і між ФНС РФ та Office.ed-it.ru, що була для податкової дата-центром (банком даних).

У ГУР зазначають, що фактично йдеться про повне знищення інфраструктури одного із основних держорганів Росії та численних супутніх даних податкової за великий часовий період.

Крім того, інтернет-трафік податкових даних у масштабах усієї Росії опинився в руках воєнної розвідки України». ***(Альона Мазуренко. ГУР атакувало податкову систему Росії // Українська правда (https://www.pravda.com.ua/news/2023/12/12/7432737/). 12.12.2023).***

***

«Російські хакери угруповання UAC-0050 використовують ситуацію з «Київстаром» при розсиланні українцям листів зі шкідливим програмним

забезпеченням – у вигляді архівних файлів із назвами «Заборгованість абонента», «Запит», «Документи» тощо, попереджає Держспецзв'язку.

Джерело: Державна служба спеціального зв'язку та захисту інформації України й урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA

Дослівно Держспецзв'язку: «Хакери продовжують використовувати проблеми, які хвилюють тисячі українців, для розповсюдження шкідливого програмного забезпечення. Цього разу фахівці Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA зафіксували масове розсилання електронних листів з тематикою «заборгованості за договором Київстар» і вкладенням у вигляді архіву «Заборгованість абонента.zip».

На електронні пошти українців приходили листи щодо «Заборгованості за договором Київстар», які містили вкладення у вигляді архіву «Заборгованість абонента.zip» з додатками у вигляді вкладених захищених паролем RAR-архівів.

Крім того, в CERT-UA зафіксовано розповсюдження листів за темою «Запит СБУ» та вкладенням у вигляді архіву «Документи.zip». Він містить захищений паролем RAR-архів «Запит.rar» з виконуваним файлом «Запит.exe». Відкриття архіву та запуск файлу, як і в попередньому випадку, призводять до ураження програмою віддаленого доступу RemcosRAT».

А 21 грудня команда CERT-UA зафіксувала масове розповсюдження електронних листів з тематикою «Заборгованості за договором Київстар» та вкладенням у вигляді архіву «Заборгованість абонента.zip».

Зазначений ZIP-архів містить розділений на 2 частини RAR-архів «Заборгованість абонента.rar», в якому знаходиться однойменний архів захищений паролем. В останньому знаходиться документ з макросом «Заборгованість абонента.doc».

У разі активації код макросу за допомогою оглядача файлів (explorer.exe) з використанням протоколу SMB здійснить завантаження на ЕОМ та запуск файлу «GB.exe».

У свою чергу, зазначений файл є SFX-архівом, що містить BATCH-скрипт для завантаження з сервісу bitbucket та запуску виконуваного файлу «wsuscr.exe», обфускованого за допомогою SmartAssembly.NET, призначенням якого є дешифрування та запуск програми для віддаленого управління RemcosRAT (ідентифікатор ліцензції: 5639D40461DCDD07011A2B87AD3C9EDD).

Окрім того, зафіксовано розповсюдженян листів з темою «Запит СБУ» та вкладенням у вигляді архіву «Документи.zip», що містить захищений паролем та розділений на 3 частини RAR-архів «Запит.rar». В останньому знаходиться виконуваний файл «Запит.exe». У випадку відкриття такого архіву та запуску виконуваних файлів ЕОМ може бути уражена програмою RemcosRAT (ідентифікатор ліцензії: 5639D40461DCDD07011A2B87AD3C9EDD).

Окрім типового для UAC-0050 розміщення серверів управління RemcosRAT на технічному майданчику малайзійського хостинг-провайдера Shinjiru, їх також розміщено в межах автономної системи AS44477 (STARK INDUSTRIES SOLUTIONS LTD).

За даними Держспецзв’язку, це не перша подібна атака угруповання UAC-0050.

Нещодавно кіберзловмисники здійснювали розсилання листів щодо «судових претензій» і «заборгованості». Об’єктом атаки стали користувачі з України та Польщі.

Група UAC-0050 також намагалася викрадати дані, маскуючись під МЗС України, робила шкідливі розсилки нібито від СБУ, Печерського райсуду Києва, «Укртелекому».

Минулого року також були зафіксовані розсилки електронних листів зі шкідливим вкладенням начебто від імені ДСНС, пресслужби Генштабу ЗСУ, СБУ, від імені Держспецзв’язку і навіть від CERT-UA». ***(Олена Рощіна. Російські хакери розсилають листи зі шкідливим софтом, користуючись збоєм «Київстару» // Українська правда (https://www.pravda.com.ua/news/2023/12/22/7434189/). 22.12.2023).***

***

«Експерти з кібербезпеки жваво обговорюють наслідки масованої хакерської атаки на інфраструктуру Київстара, що призвело до падіння як мобільної, так і фіксованої мережі.

Олександр Кардаков, власник Octava Defence, пише на ФБ-сторінці: “Судячи з масштабів, атака проведена зсередини мережі. Підключалися з Києва чи Амстердама (VEON) – нехай визначають відповідні органи”.

Висновки після кібератаки

На його думку, кібератака була ретельно підготовлена. Хакери мали всі дані про внутрішній устрій мережі та доступ до різних її частин, у тому числі – бекапів. Це була команда кількістю більше 10 чоловік, які могли використовувати спеціально створене програмне забезпечення.

«Те, як була «помічена» загроза та подальший кризовий менеджмент – абсолютно вразили! Неприємно вразили», – зазначає Кардаков.

Він робить наступні висновки:

Кібербезпека – це не лише захист ззовні, але й зсередини.

Бекапи також зберігаються на окремих носіях (так званий air-gap).

І головне – люди. За словами експерта, за останні роки в Київстарі були звільнені останні техспеціалісти, які насправді розуміли, як все побудовано та працює. Їх же замінили «гарними презентаторами».

Слід власників

Цей пост Кардакова активно коментується іншими користувачами. Дехто вважає, що мало місце «свідоме стирання даних». І це могли зробити фактичні власники Київстару з російським слідом.

«Допиз@ились – Фрідман і ко зачистили все нах. Від хазяїв кібербезпека не допомагає. Зараз актуальне питання – кому і що вони злили і що з цим робити», – вказує Михайло Комісарук, власник Укрнет.

«Так Маратовича (Фрідман Михайло Маратович – Г.Б.) ж загнали за Можай. З листопада він змушений був повернутися в РФ. Можливо, він і натиснув Велику Червону Кнопку. І також можливо, що це було умовою його безболісного

повернення, – пише Aleksandro Romanini, який вже встиг вилучити акаунт. – Також не слід забувати, що через сервери КС йшли терабайти даних, в т.ч. критичних. Плюс Хелсі. Тому треба було розуміти, що Маратович контролював критичну інфраструктуру держави. І ганяти його по всіх кутках було, як мінімум, недалекоглядно. Але хто ж про це думав. Думати у нас, як завжди, не на часі. Граблі наше все».

Також Ігор Шевченко, голова благодійного фонду «Успішна Україна», вважає, що «з великою вірогідністю це є диверсія спецслужб росії за сприяння російських власників КС, які досі контролюють компанію».

Внутрішній слід

Ще одна версія полягає у свідомому, або за недостатнім знанням впливом співробітників компанії.

«Часто після того як система налаштована і ідеально працює у керівництва компаній виникає “геніальна” думка про оптимізацію розходів на ІТ. Адже далі їм ніби достатньо енікейщика», – пише системний адміністратор Микола Солонін.

«Дуже прикро, але це тенденція в усьому. Керівництво вважає, що якщо система працює, то спеціаліст з усунення проблем не потрібен. Але воно не розуміє, що система працює завдяки цім спеціалістам», – зазначає Віталій Медведик.

Igor Khodorovskyi додає: «Самі співробітники і поклали. Або просто вимкнули тумблер…. і всьо…… Згорів сарай – гори і хата…»

Як би там не було, фахівці Київстар сьогодні докладають титанічних зусиль з повного відновлення. Тому побажаємо їм успіхів, а СБУ – розібратися з усіма можливими слідами у ході кібератаки». ***(Герман Богапов. Експерти вказують на внутрішній слід кібератаки на Київстар // HiTech.Expert (https://expert.com.ua/173373-eksperty-vkazuyut-na-vnutrishni-slidy-u-kiberataci-na-kyivstar.html). 16.12.2023).***

***

«Експерти із кібербезпеки радять українським військовим і членам їхніх родин не використовувати месенджер «Телеграм» для їхньої ж безпеки.

Про це йшлося під час пресконференції у Медіацентрі Україна-Укрінформ.

«Коли я їжджу на схід, то бачу, що деякі військові використовують Телеграм і що в ньому увімкнена геолокація, яка може привести до направлення зброї і вибухів у те місце, де знаходиться людина або скупчення людей з певними геолокаціями. І ці питання потрібно проговорювати і пояснювати військовим», - зазначив експерт ГО «Інститут дослідження кібервійни» Єгор Аушев.

За його словами, членам родини військовослужбовця також не варто спілкуватися з ним у Телеграмі.

Крім того, експерт вказав, що коли у російських військових вилучають телефони, то завжди виявляють два головних застосунки для комунікації – це Телеграм і «ВКонтакте».

«Це підтверджується і їхніми переписками - в Інтернеті є багато злитих переписок російських військових, і вони говорять про те, що наказовим характером їм вказують, щоб вони для комунікації використовували лише Телеграм і «Вконтакте», - розповів представник ГО.

Він закликав громадян порушувати цю тему і пояснювати своїм родичам та військовим, що не потрібно користуватися цим месенджером.

«Мені іноземні партнери, коли телефонують, кажуть: «Чому в Україні досі користуються російським месенджером?». Давайте хоча б по тих питаннях, які стосуються безпеки або роботи, не використовувати месенджер, до якого є дуже багато запитань», - порадив Аушев.

Співзасновник Інституту дослідження кібервійни Валентин Кучерук акцентував на тому, що при встановленні Телеграма на мобільний у користувача питають дозволи на доступ, зокрема, до контактної книги, мікрофону, фотогалереї тощо, і користувач погоджується і надає ці дозволи.

«І в ліцензійних умовах написано, що дані шифруються. Але це воно так написано. Ніхто не перевіряв це, зовнішніх аудитів цієї системи не було, вони не проходили. Це також закрита інформація. Ніхто не давав інформації, що якась

незалежна компанія проводила аудит коду чи чогось іншого. Таких свідчень ніде немає», - заявив наголосив Кучерук.

Відповідаючи на запитання про те, чи Телеграм є бізнесом, чи інструментом РФ як держави та російських спецслужб, Аушев зазначив, що якщо тут і йдеться про бізнес, то він є дуже неприбутковим.

«Але дійсно багато речей відбуваються, які нам невідомі, у тому числі і всередині РФ. Але те, що залучалися кошти з провідних російських інвестфондів та великих корпорацій саме у Телеграм, веде нас до думки, що це, власне, підтримується на федеральному рівні месенджер», - вважає представник ГО…» ***(Експерти з кібербезпеки радять військовим і членам їхніх родин не використовувати Телеграм // Укрінформ (https://www.ukrinform.ua/rubric-technology/3801668-eksperti-z-kiberbezpeki-radat-vijskovim-i-clenam-ihnih-rodin-ne-vikoristovuvati-telegram.html). 18.12.2023).***

***

«Кількість DDoS-атак на телекомунікаційну сферу держави-терористки російської федерації у жовтні-листопаді 2023 року збільшилася вчетверо у порівнянні з минулим роком. Найбільше страждають інтернет-провайдери у різних регіонах.

Хакери завдали проблем центральним та південним регіонам країни-агресорки, а також тимчасово окупованому Криму. Кібератаки були спрямовані на різні рівні та елементи інфраструктури, включно зі сайтами, мережами та системами інтернет-провайдерів.

Унаслідок DDoS-атак клієнти російських інтернет-провайдерів зіткнулися з недоступністю регіональних сайтів операторів зв’язку, туристичних компаній, онлайн-магазинів, фінансових установ та ЗМІ. Найтриваліші атаки, зазначають окупанти, тривали три дні, тоді як найкоротша тривала всього 20 хвилин. Аналітики підкреслили, що регіональні інтернет-провайдери та їхні клієнти зазнали значних збитків від кібератак.

Злами телеком-інфраструктури росіян продовжуються. Нагадаємо — наприкінці жовтня українські хакери здійснили потужну DDoS-атаку на російських інтернет-провайдерів. «Під кіберудар потрапили компанії «Кримтелеком», «Міранда-медіа» та «МирТелеком». Зараз комунікації окупаційних військ у Криму та на окупованих частинах Херсонської, Запорізької, Донецької й Луганської областей частково паралізовано», — розповів тоді очільник Мінцифри Михайло Федоров.

Додамо — одна з найвідоміших успішних операцій ІТ-армії України — злам сайтів російського оборонного концерну «Калашников». Завдяки масштабній DDoS-атаці, інтернет-ресурси головного постачальника зброї для армії російських окупантів наприкінці квітня були недоступними в жодній країні світу, навіть у росії». ***(Фахівці з кібербезпеки відзначили ефективність українських DDoS-атак на російську інфраструктуру // No worries! (https://noworries.news/fahivczi-z-kiberbezpeky-vidznachyly-efektyvnist-ukrayinskyh-ddos-atak-na-rosijsku-infrastrukturu/). 19.12.2023).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Естонія та ще 9 держав 20 грудня запустили Талліннський механізм для посилення кіберпідтримки України у цивільній сфері.

Джерело: «Європейська правда» з посиланням на заяву Міністерства закордонних справ Естонії

Деталі: Талліннський механізм, зазначили в естонському МЗС, був створений на першій зустрічі країн-донорів цієї весни. За допомогою цього механізму будуть систематизовані потреби України та співвіднесені з можливостями донорів таким чином, щоб підтримка різних країн становила єдине ціле, а Україна була здатна захистити себе в кіберсфері.

Донорами Талліннського механізму є Естонія, Нідерланди, Канада, Польща, Франція, Швеція, Німеччина, Данія, США та Велика Британія. НАТО і Європейський Союз є членами-спостерігачами у цьому механізмі.

Механізм має естонський фронт-офіс у Києві, польський бек-офіс у Варшаві та координаційну групу, яка об'єднує представників України та всіх донорів. Механізм відкритий для приєднання нових членів.

До участі в Механізмі залучені високотехнологічні компанії та неурядові організації країн-донорів.

Також, згідно з повідомленням, Естонія виділяє 500 тисяч євро для Талліннського механізму через свій бюджет співпраці у сфері розвитку на 2024 рік.

Талліннський механізм працює паралельно з ІТ-коаліцією, яка займається вирішенням кіберпроблем України у військовій сфері.

«Агресивна війна Росії проти України ведеться не лише на звичайному полі бою… Цілями Росії є кібернетичні можливості України, як військові, так і цивільні, і тому дуже важливо підтримувати кібернетичну оборону України та її здатність відновлювати і розвивати відповідну інфраструктуру», – прокоментував міністр закордонних справ Естонії Маргус Тсахкна.

«На жаль, цілком ймовірно, що кібератаки з боку Росії триватимуть в осяжному майбутньому. Саме тому за допомогою цього механізму ми надаємо шанс посилити системну готовність і стійкість України до кібератак у довгостроковій перспективі», – додав міністр…». ***(Естонія та ще 9 країн запустили Талліннський механізм для кібердопомоги Україні // Українська правда (https://www.pravda.com.ua/news/2023/12/20/7433891/). 20.12.2023).***

***

Світові тенденції в галузі кібербезпеки

«Оскільки технології відіграють ключову роль у сучасному бізнесі, організації не можуть дозволити собі залишатися в автономному режимі протягом тривалого періоду часу після нищівної кібератаки.

Щодо компаній, які пропонують цифрові продукти та послуги, користувачі швидко розчаруються й потенційно перекинуться до конкурентів, чим довше інтернет-продукт чи послуга перебувають у режимі офлайн.

А враховуючи те, що сьогодні так багато співробітників використовують пристрої та програмне забезпечення для роботи в Інтернеті, уся внутрішня діяльність компанії може призупинитися, якщо вона стане жертвою кібератаки.

Нещодавні приклади включають Раду Хакні в Лондоні та Британську бібліотеку, в обох системах через тривалий час перебували в автономному режимі через програми-вимагачі.

Зрозуміло, що компанії повинні зробити все можливе, щоб стримати та усунути кібератаки та якнайшвидше перезапустити порушені IT-системи. На жаль, це складний процес: підприємства часто розриваються між відновленням систем із чистої резервної копії чи їх повним відновленням.

Відновлення скомпрометованих систем після атаки також може призвести до нових кіберзагроз та IT-проблем для бізнесу. Але експерти з безпеки сходяться на думці, що дотримання простих найкращих практик може бути дуже корисним.

Відновлення кібератак непросте

За словами Азіма Алеема, керуючого директора компанії з кібербезпеки Sygnia у Великій Британії та Північній Європі, відновлення роботи IT-систем організації після кібератаки нічим не відрізняється від відновлення після торнадо.

«IT-команда та C-suite щойно пройшли розумовий марафон і тепер мають думати про те, як знову запустити бізнес. Керівництво має це усвідомлювати, щоб уникнути синдрому аналізу-паралічу», — каже він.

Алеєм каже, що ключ до відновлення систем і даних після кібератаки, а також уникнення будь-якої плутанини чи двозначності в процесі, полягає в тому, щоб передати чіткі очікування всієї організації та налаштувати «протокол розгортання відновлення».

У рамках цього процесу він радить IT-командам негайно розпочати відновлення та розслідування. Він каже: «Завдяки використанню середовища «захищеного острова», в якому ключові служби створюються заново до того, як

скомпрометований метод буде очищено, організація може повернутися до повноцінної роботи бізнесу набагато швидше. Зусилля з відновлення ідентифікують і закривають безпеку, а присутність зловмисника в середовищі знищується».

Алім також пропонує двоетапний процес виправлення, згідно з яким компанії спочатку вживають заходів для відновлення критичних програм і процесів, перш ніж звертатися до менш важливих елементів своєї діяльності.

Хоча перезапуск IT-систем, скомпрометованих кібератакою, життєво важливий, фірмам не слід нехтувати важливістю інформування персоналу, клієнтів та інших зацікавлених сторін про кіберзломи. Алім рекомендує, щоб керівники були повністю прозорими щодо кібератак, повідомляючи «про те, що трапилося, і попереджаючи про те, що процес відновлення може бути неприємним, оскільки багато програм і процесів потребують перебудови». Це допоможе організаціям «змінити мислення своїх співробітників на орієнтацію на рішення», коли вони просуваються вперед із відновленням.

Він додає: «У той же час може виникнути додатковий тиск, оскільки клієнти та партнери очікують тих самих послуг, що й раніше. Співробітники повинні бути в курсі ситуації в компанії, щоб вони могли адекватно розглянути, як порушення могло вплинути на зовнішніх сторін, і мати можливість повідомити про своє порушення відповідно до нормативних вимог».

Два варіанти відновлення

За словами Надера Завері, старшого менеджера з реагування на інциденти та усунення несправностей компанії Mandiant, спеціаліста з аналізу загроз, що підтримується Google Cloud, компанії часто стикаються з двома варіантами.

Перший варіант полягає у використанні непошкодженої резервної копії для початку відновлення. Або фірми з кібербезпеки мають можливість відтворити зламані системи з нуля. У будь-якому випадку, Завері каже, що компанії повинні створити комплексний план відновлення, зосереджений на управлінні ідентифікацією, сегментації мережі та перевірці кінцевих точок.

Під час створення нових облікових записів користувачів як частини зусиль із керування ідентифікацією, Завері каже, що організації повинні встановлювати надійні паролі. І якщо інцидент кібербезпеки все ще триває, він рекомендує скидати паролі щодня.

Завері каже, що сегментація мережі потребує трьох різних середовищ, включаючи «червону мережу» для скомпрометованих середовищ, «зелену мережу» для чистих середовищ і «жовту мережу» для розпізнавання компромісів, що впливають на системи, які тепер відновлені та працюють. Він додає: «Це жовте або проміжне середовище обмежує доступ до Інтернету та міжмережевий трафік, дозволяючи винятки лише для певних програм безпеки».

Нарешті, за його словами, компанії повинні звернути увагу на перевірку кінцевих точок, розглядаючи два важливі сценарії. Він рекомендує компаніям «використовувати чисте золоте зображення, сертифіковане групою реагування на інциденти», якщо їм потрібно відновити скомпрометовані системи.

Але якщо немає потреби перебудовувати систему, він каже, що компанії повинні ізолювати її всередині «жовтої мережі» та повторно активувати там. Це дозволить групі реагування на інциденти використовувати інструменти виявлення кінцевих точок, щоб переконатися, що індикатори компрометації не впливають на системи.

Відновлення даних є критичним

За словами керівника Rubrik Zero Labs Стіва Стоуна, фокусування на відновленні даних є ще одним важливим кроком у відновленні важливих систем після кібератаки. «Ці дії по відновленню керуватимуться видимістю, пріоритезацією та розумінням поточного доступу зловмисника, або вони виконуватимуться як «сліпі» події», — говорить він.

Він застерігає компанії від вибору сліпого відновлення, оскільки вони ризикують значною втратою даних через відновлення «протягом більш тривалого періоду, ніж потрібно» або «повторного введення зловмисників, якщо точка відновлення після того, як зловмисники отримали доступ».

На його думку, фірми повинні приймати обґрунтовані рішення на основі розуміння того, що «не можна відновити все відразу». Тому підприємства повинні прагнути забезпечити «зловмисникам втрату доступу, відновившись від того, що було до вторгнення», і вони можуть запобігти значним втратам даних, здійснюючи зусилля з відновлення «якнайближче до вторгнення».

Підприємства, які реалізують плани відновлення перед кібератакою, перезапустять системи набагато швидше, ніж ті, хто їх не має, каже він. Компанії, не готові відновитися після кібератаки, будуть обмежені «зниженою видимістю», оскільки вони виконають відкриття та відображають робочий процес під час події. Стоун додає: «Найуспішніші організації попередньо протестують відновлення, щоб переконатися в життєздатності своїх планів, і внесуть корективи на основі отриманих уроків».

Стоун зауважує, що підприємствам часто легше справлятися із загрозою шифрування атак програм-вимагачів, ніж з елементом вимагання. Він пояснює: «Це особливо складно, коли середовище активно зашифровано та/або зазнає вторгнення. Здатність оцінити, чи були дані вкрадені, що вони містять і як боротися з потенційною загрозою вимагання втрати даних, є критично важливою для сучасних вторгнень програм-вимагачів».

Успішне відновлення системи

За словами Кріса Денбі-Вайта, головного спеціаліста з безпеки платформи запобігання втраті даних Next DLP, є кілька факторів, які визначають, чи буде відновлення системи успішним чи ні у разі кібератаки.

По-перше, служби безпеки не повинні нехтувати основними бізнес-цілями, намагаючись відновити зламані системи. Денбі-Вайт каже, що такі цілі, як з’ясування особи кіберзлочинців і забезпечення того, щоб вони не могли повторно отримати доступ до систем у майбутньому, повинні бути узгоджені з основними цілями бізнесу. Він додає: «З точки зору бізнесу, головною метою є мінімізація збоїв і фінансових втрат, навіть якщо це суперечить деяким цілям IT і безпеки».

По-друге, компанії повинні бути дуже обережними після кібератаки. Таким чином, відновлення зламаної інфраструктури замість спроб очищення може бути найкращим рішенням для відновлення системи.

Денбі-Вайт пояснює: «Проблема підходу до очищення полягає в забезпеченні гарантій того, що система повністю вільна від компромісу. Доведення відсутності компромісу може бути важким і трудомістким. Парадоксально, але відновлення систем може бути більш ефективним і забезпечити більшу впевненість».

По-третє, фірми повинні використовувати можливості моніторингу, щоб переконатися, що система не матиме подальших компромісів після очищення чи перебудови. Denbigh-White рекомендує або проводити агрегацію журналів, або використовувати програмне забезпечення, яке фіксує всю діяльність, що відбувається в IT-мережах компанії.

«Крім того, вкрай важливо виділити ресурси, які мають як потужність, так і досвід, щоб зрозуміти дані посиленого моніторингу та діяти на основі них», – додає він. «Просте заповнення журналів системою управління інформацією про безпеку та подіями (SIEM) або сховищем даних за своєю суттю не покращує безпеку. Моніторинг має активно інтерпретуватися та діяти обізнаним персоналом».

Нарешті, компанії повинні переконатися, що вони вчаться з кібератак і подальших заходів з відновлення. Денбі-Уайт каже, що компаніям не слід нехтувати цим, оскільки кібератаки можуть надати «цінну можливість для організаційного зростання та навчання».

«Якщо поводитися з ним конструктивно, без звинувачень і вказівок пальцями, це може суттєво підвищити безпеку й обізнаність організації», — каже він. «Добре реалізований процес на основі отриманих уроків може допомогти пом’якшити певну шкоду, завдану бізнесу інцидентом, зрештою зміцнивши його загальну стійкість».

Кібератака може завдати великої шкоди бізнесу, спричинивши різноманітні проблеми від витоку даних до фінансових втрат. Тому вони повинні зробити все можливе, щоб швидко відновити роботу систем.

Хоча відновлення систем у разі кібератаки є нелегким процесом, створення добре продуманого плану відновлення, який відповідає найкращим галузевим практикам і узгоджує цілі безпеки з бізнес-цілями, відіграє важливу роль. І якими б жахливими не були кібератаки, вони можуть стати цінними уроками для всього бізнесу». ***(Nicholas Fearn. How to recover systems in the event of a cyber attack // TechTarget (https://www.computerweekly.com/feature/How-to-recover-systems-in-the-event-of-a-cyber-attack?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 05.12.2023).***

***

«Нове дослідження склало рейтинг країн світу за рівнем кібербезпеки з деякими потенційно несподіваними результатами.

Proxyrack використовував різні показники, щоб оцінити, наскільки кожна країна піддається ризику кібератак, включаючи її цифровий розвиток і кіберзаконодавство. Було зроблено висновок, що найбезпечнішою країною у світі є Данія з оцінкою ризику лише 1,87 з десяти, а найменш безпечною є Панама (9,70).

Скандинавія домінує у трійці найбезпечніших країн, а Швеція та Фінляндія займають друге та третє місце відповідно. Вісім найбезпечніших країн є європейськими, а Великобританія посідає шосте місце. США і Канада займають дев'яте і десяте місця відповідно.

Найбільш і найменш безпечні країни

Причина претензії Данії на перше місце пов’язана з її високим рівнем цифрового розвитку та низьким індексом ризику кібербезпеки. У звіті це принаймні частково пояснюється виконанням урядом Національної стратегії кібернетичної та інформаційної безпеки у 2022 році.

Між тим, Панаму вважали найменш безпечною через те, що вона найменш розвинена в цифровому відношенні країна та має один із найгірших показників індексу кібербезпеки. Крім того, він найбільше піддавався ризику відмивання грошей і фінансування тероризму.

Індекс ризику кібербезпеки вимірюється з урахуванням різних наборів даних, таких як Microsoft. частота виявлення зловмисного програмного забезпечення та програм-вимагачів, а також показники криптомайнінгу, дані про атаки хмарних провайдерів і відданість країни кібербезпеці

Таїланд і Білорусь були другою і третьою країнами за ризиком кіберзлочинності. Однак Об'єднані Арабські Емірати (ОАЕ) мають найнижчий національний рейтинг кібербезпеки, який оцінює, наскільки добре впроваджуються нормативні акти, пов'язані з кібербезпекою. ОАЕ також мають один із найвищих середніх показників збитків від кібератак: кожна атака в країні коштує в середньому 2,6 мільйона доларів.

Уругвай, Південна Корея та Швейцарія були країнами з найменшою кількістю кіберзаконів, лише по два закони в кожній. Уругвай також був визнаний шостою країною з найбільшим ризиком кіберзлочинності, тоді як Південна Корея та Швейцарія не опинилися ні в першій, ні в останній десятці». ***(Lewis Maddison. These are the countries most at risk from cyberattacks // Future US, Inc. (https://www.techradar.com/pro/security/these-are-the-countries-most-at-risk-from-cyberattacks?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 04.12.2023).***

***

«У постійно змінюваному ландшафті загроз кібербезпеці традиційний підхід «замок і рів» виявляється дедалі неадекватним. Середня світова шкода від витоку даних у 2023 році склала 4,45 мільйона доларів. Порівняно з 2020 роком, це зростання на 15%. Організації повинні зміцнювати свій захист за допомогою запобіжних та комплексних стратегій, оскільки кіберзлочинці стають дедалі витонченішими. У цю епоху ключем до стійкості є постійний моніторинг.

Розуміння цінності постійного моніторингу

За своєю суттю безперервний моніторинг — це не просто інструмент, а спосіб мислення — проактивний і комплексний підхід до кібербезпеки. Він виходить за рамки реактивних заходів минулого, наголошуючи на постійному

зборі, аналізі та кореляції даних. Це також не одноразова подія, а постійна система пильності, яка дозволяє організаціям бути на крок попереду кіберсупротивників.

Головною перевагою, звичайно, є раннє виявлення загроз. Крім того, використання розширеної аналітики та машинного навчання допомагає вийти за рамки виявлення на основі сигнатур і розпізнати аномалії, які можуть вказувати на потенційні загрози. Ця проактивна позиція має вирішальне значення в динамічному середовищі кіберзагроз, де швидкість часто є відмінною рисою між стримуванням і катастрофою.

Коли трапляються порушення, а вони неминуче відбуватимуться, система моніторингу відіграє ключову роль у ізоляції зламаних систем і утриманні зловмисного програмного забезпечення. Ця стратегія стримування обмежує радіус дії атаки, запобігаючи поширенню шкідливих об’єктів у мережі. Після порушення здатність швидко й ефективно пом’якшити вплив є свідченням стійкості, яку забезпечує постійний моніторинг.

Знання — це половина успіху, особливо у сфері кібербезпеки. Постійний моніторинг дає організаціям цінну інформацію про тактику, прийоми та процедури зловмисників (TTP). Організації можуть посилити контроль безпеки та створити адаптивну архітектуру захисту, розуміючи, як діють противники.

Крім стійкості, в епоху суворих правил і стандартів відповідності, моніторинг має вирішальне значення для демонстрації дотримання галузевих інструкцій. Забезпечуючи безперервну видимість стану безпеки та заходів моніторингу, організації можуть завчасно вирішувати вимоги відповідності, уникаючи пасток невідповідності.

Нарешті, фінансовий тягар кібератак виходить далеко за межі миттєвих витрат на усунення. Зведення до мінімуму впливу порушень та оптимізація реагування на інциденти значно зменшує загальні економічні втрати від кіберінцидентів. Він перетворює кібербезпеку з необхідних витрат на стратегічну інвестицію, яка захищає дані та кінцевий результат.

Здійснення постійного моніторингу у вашій організації

Щоб забезпечити повну видимість, комплексний план моніторингу повинен враховувати кожну кінцеву точку, мережу та програмне забезпечення, які використовує ваша компанія. Отже, першим кроком є оцінка кожного активу в корпоративній мережі. Однак не всі активи однакові. Щоб захистити найціннішу інформацію, важливо визначити пріоритети моніторингу. Дозволивши організаціям зосереджувати свої ресурси там, де вони найбільш важливі, це допомагає створити цілеспрямований захист, який зміцнює цифрові коштовності.

Архітектура моніторингу також повинна включати план реагування на інциденти. Звіти про інциденти мають важливе значення, оскільки вони дозволяють організаціям фіксувати кібератаки, реагувати на них і вивчати їх. Сприяння розробці чітко визначених процедур реагування на інциденти гарантує, що організації можуть швидко й рішуче реагувати, щоб пом’якшити потенційний збиток у разі виявлення загрози.

Вибір найбільш підходящої технології та інструментів моніторингу є вирішальним вибором. Щоб мати повну видимість, створена архітектура моніторингу повинна враховувати кожен вектор атаки, який може бути використаний для запуску кібератаки. Враховуючи те, що сьогоднішня поверхня атаки розширюється, вибір правильних інструментів має першочергове значення.

Наприклад, більшість підприємств починають із Інструменту моніторингу інформації про безпеку та подій (SIEM), за яким ідуть Виявлення та реагування на кінцеві точки (EDR) і рішення Уніфікованого керування кінцевими точками (UEM). SIEM шукає шаблони, які полегшують командам безпеки розпізнавання атак, зломів і технічних проблем. EDR, з іншого боку, збирає дані з кожної кінцевої точки та використовує ШІ для визначення загроз.

Хоча зовні SIEM і EDR пропонують видимість, EDR зосереджуються на кінцевих точках, а SIEM охоплює всю мережу. Однак EDR пропонує глибші можливості щодо реагування на інциденти, що дозволяє командам безпеки давати відсіч. UEM, з іншого боку, використовує свої віддалені можливості для відстеження відповідності пристрою. Крім того, невідповідні пристрої після

виявлення можна позначати та керувати ними віддалено. З появою нових національних і міжнародних нормативних актів наслідки невідповідності справді серйозні.

Вибрані інструменти повинні бездоганно інтегруватися в існуючу екосистему кібербезпеки, будь то моніторинг мережі, моніторинг кінцевих точок або платформи аналізу загроз. Наприклад, вибір SIEM із запобіганням втраті даних або UEM із можливостями керування виправленнями позбавляє IT-команд від керування кількома платформами.

Нарешті, припустімо, що ви реалізували надійну архітектуру. Однак це ще не кінець. У сфері кібербезпеки, що розвивається, завжди є нові ризики, про які слід пам’ятати. Щоб реагувати на мінливі загрози, необхідні постійні вдосконалення та вдосконалення. Регулярні перевірки та оновлення гарантують, що сторожова вежа залишається пильною та стійкою до кіберзагроз, що постійно змінюються.

Не в останню чергу — ваші співробітники. Проблема складних інструментів, таких як SIEM, полягає в тому, що для керування ними потрібні кваліфіковані фахівці з безпеки. Крім професіоналів із безпеки, кожен співробітник має бути в курсі останніх кіберзагроз і векторів атак на регулярних семінарах і тренінгах. Знання того, як злочинці порушують безпеку, допоможе їм помітити найдрібніші деталі та ознаки, які можуть допомогти їм визначити порушення. Крім того, це також впливає на те, наскільки добре вони реагують на дилему кібербезпеки.

Йти вперед

Оскільки кіберзагрози стають все більш витонченими, значення постійного моніторингу безпеки продовжує зростати. Не буде перебільшенням представити його як життєво важливий інструмент для компаній, які прагнуть захистити свої активи та забезпечити безперервність бізнесу — насправді це є стратегічною вимогою. Гнучкість і швидкість реагування, що забезпечуються безперервним моніторингом, є будівельними блоками стійкої стратегії кібербезпеки в епоху, коли цифрові збої є нормою». ***(Apu Pavithran. Cyber Attacks Are On the Rise — Here's How Your Business Can Continuously Prepare for Threats // Entrepreneur Media, LLC (https://www.entrepreneur.com/science-technology/cybersecurity-attacks-are-on-***

the-rise-is-your-business/465843?utm_source=flipboard&utm_content=user%2Fentrepreneur). 08.12.2023).

***

«Згідно з опитуванням 500 спеціалістів із безпеки, проведеним у 2023 році компанією Observe & CITE, 47% організацій мають стимули скоротити чисельність персоналу служби безпеки. Стільки ж, 47% респондентів, стверджують, що не мають ініціатив щодо зниження чисельності персоналу служби безпеки, тоді як відповідь «Не впевнений» підскочила з 1-2% до 6%

«Примітно, що організації, які планують скоротити чисельність персоналу, також мають більше місячних інцидентів у цілому, а також більше інцидентів, які вирішуються першими службами реагування, ніж автоматизація», — йдеться у звіті State of Security Observability 2023.

Серед організацій із сотнями інцидентів на місяць 62% респондентів підтвердили, що мають стимули скорочувати команди безпеки.

Observe зазначає, що організації з інженерними командами понад 100 (61%), більше половини свого IT-бюджету витрачають на безпеку (60%), використовують понад 6 інструментів для розслідування інциденту (58%) і мають доходи понад 100,1 мільйона доларів США. (57%) більш схильні до скорочення штату.

Дещо краща ситуація з видатками на інфраструктуру.

«Чотири з десяти планують зменшити витрати на інфраструктуру безпеки за рахунок скорочення інструментів або постачальників, і майже половина планують зменшити витрати на безпеку», — йдеться у звіті.

З організацій, які планують скоротити штат, 60% також планують обмежити витрати на інфраструктуру, показало опитування.

«Невеликим організаціям важко знайти відповідність поточному ринку засобів безпеки. Вони не можуть дозволити собі виділити людей або готівку на охорону, і їм важко використовувати інструменти, які вони купують. Іноді відповідь – аутсорсинг», – йдеться у звіті.

Понад дві третини (73%) опитаних спеціалістів сказали, що у їхній організації є як група реагування на інциденти, так і центр безпеки для відомих подій. Одна п’ята мала лише одну з команд, 5% передали функції безпеки аутсорсингу, а 2% працювали без цих можливостей. Зараз 95% респондентів використовують SIEM (Security Information and Event Management).

«Великі організації наймають багато людей і купують багато інструментів, але потім вони повинні інтегруватися. Вони можуть бути багатими на процес, людей і продукт, але це не означає, що всі ці частини оптимально поєднуються між собою», – зазначається у звіті.

Ще в листопаді останнє дослідження робочої сили з кібербезпеки, проведене ISC2, показало, що розрив між попитом на фахівців з кібербезпеки та їх доступністю зріс до безпрецедентного рівня. У всьому світі потрібно чотири мільйони кіберпрофесіоналів, щоб заповнити світовий дефіцит кадрів у сфері кібербезпеки, що є рекордним показником. Однак оцінка стосується не ринку праці, а ресурсів, необхідних для належного забезпечення організацій». ***(Ernestas Naprys. Cybersecurity downsizing: 47% of organizations planning to reduce teams // Cybernews https://cybernews.com/security/half-organizations-plan-reduce-cybersecurity-teams/). 08.12.2023).***

***

«Звіт EDUCAUSE Cybersecurity and Privacy Workforce in Higher Education, 2023, підтверджує те, що ми знаємо в галузі кібербезпеки: значні прогалини в кадровому забезпеченні кібербезпеки піддають вищі навчальні заклади ризику. Заголовки новин підтверджують, що кіберзагрози дедалі більше впливають на діяльність університетів, порушуючи навчання, дослідження та успішність студентів. Коледжі та університети перебувають під величезним тиском, а проблеми з кадрами сприяють глибокій нестачі стійкості. Шлях вперед вимагає інституційної відданості програмі кібербезпеки, яка включає ефективне забезпечення ресурсами, адаптованим до конкретних потреб вашої установи.

Ризики

Вища освіта має мішень на спині. У вересні 2022 року Агентство з кібербезпеки та безпеки інфраструктури США повідомило, що Vice Society, загроза програмного забезпечення-вимагача, непропорційно націлилася на сектор освіти. Дані показують, що програми-вимагачі є серйозною загрозою. Майже одна третина зломів у секторі освітніх послуг минулого року стосувалася програм-вимагачів.

Вища освіта також знаходиться під мікроскопом, посилюючи ці ризики. Цього року коледж у Нью-Йорку уклав угоду з генеральним прокурором Нью-Йорка або інвестувати 3,5 мільйона доларів у кібербезпеку, або отримати штраф за порушення у 2021 році. Загрози реальні, і керівники коледжів і університетів не можуть ігнорувати покарання за неврахування ризиків кібербезпеки.

Регуляторний тиск також підвищив вимоги до вищої освіти. Наприкінці 2021 року Федеральна торгова комісія (FTC) оновила свої Правила захисних заходів для відповідності Закону Грамма-Ліча-Блілі (GLBA). Більшість установ повинні дотримуватися GLBA, і, як багато хто дізнався, FTC вимагає більш зрілого та стратегічного програмування безпеки. Фактично, звіт EDUCAUSE Cybersecurity and Privacy Workforce вказує на те, що відповідність є справжньою проблемною точкою, оскільки 55 відсотків респондентів відзначили значне збільшення часу, пов’язане з відповідністю.

Виклики

Незважаючи на ці ризики, що швидко зростають, лише 46 відсотків респондентів вказали, що бюджети на кібербезпеку в їхніх установах зросли за минулий рік. Майже однакова кількість респондентів сказали, що їхні бюджети на кібербезпеку або зменшилися, або не змінилися. Фінансування кібербезпеки продовжує залишатися серйозною проблемою. Як наслідок, стає менше можливостей професійного розвитку, штат залишається незмінним (у кращому випадку), а зусилля з усунення ризиків призупиняються або відкладаються.

Підбір персоналу з кібербезпеки є проблемою для всіх галузей. Дослідження робочої сили з кібербезпеки ISC2 у 2023 році показало, що дефіцит робочої сили з кібербезпеки у всьому світі становить майже чотири мільйони працівників. Вища

освіта конкурує на агресивному ринку з організаціями, які платять вищу зарплату. Якщо ви сподіваєтеся на безкоштовне вирішення цих проблем, його немає. Обізнаність керівників і достатній бюджет необхідні для вирішення проблем робочої сили. Без підтримки виконавчої влади вам доведеться довести, що ризик бездіяльності набагато більший, ніж необхідні інвестиції. Після того, як ви отримаєте достатню підтримку, три ключові практики можуть допомогти вашій установі усунути прогалини у сфері кібербезпеки: інвестування зсередини, залучення зовнішнього досвіду та розробка майбутнього трубопроводу.

Зберегти, підвищити кваліфікацію, переоснастити

Якщо у вас є співробітники з кібербезпеки, інвестиції в них повинні бути центральними у вашому плані. Задоволення роботою має різні каталізатори: стабільність, сильні команди, гарне лідерство, баланс між роботою та особистим життям і приваблива робота. Однак достатньо конкурентоспроможні зарплати все ще необхідні, щоб утримувати та залучати життєздатних кандидатів. Інфляція та збільшення можливостей віддаленої роботи зробили це більш важливим. Звіт EDUCAUSE Cybersecurity and Privacy Workforce показує, що неконкурентоспроможні зарплати є проблемою багатьох вищих навчальних закладів. Загалом 85 відсотків респондентів сказали, що більш конкурентоспроможні зарплати значною мірою сприятимуть вирішенню кадрових проблем, і 96 відсотків тих, хто займає керівні посади, погодилися. Неконкурентоспроможні зарплати значною мірою сприяють неможливості заповнити вакансії. Більше половини (64 відсотки) респондентів не вірять, що вони можуть успішно найняти на існуючі посади. Можливо, вам не потрібно пропонувати найвищу зарплату, але ви повинні бути готові найняти й утримувати фахівців з кібербезпеки. Дані свідчать про те, що якщо ви не підвищите зарплати своїх найкращих виконавців, ви їх втратите (і їх буде важко замінити).

Головне – інвестувати свій час і інституційні долари в розумні способи. Почніть із детального плану, який ефективно передає вашу відданість благополуччю та професійному розвитку співробітників. Потім візьміть участь у їх зростанні та успіху.

Підтримка професійного розвитку та наставництво персоналу з кібербезпеки

Вища освіта традиційно підтримує професійний розвиток персоналу, і звіт EDUCAUSE Cybersecurity and Privacy Workforce підтримує цю тенденцію. Однак лише 37 відсотків закладів-учасників надають можливості наставництва, що свідчить про можливості для зростання. Пропонувати можливості наставництва – це недорога і ефективна інвестиція. Окрім передачі знань і досвіду, він повідомляє вашим співробітникам, що ви дбаєте про їхні кар'єрні траєкторії. Я отримав величезну користь від стосунків наставництва, яким сприяв EDUCAUSE. Як новому CISO, побудова навмисних відносин з досвідченим CISO в іншій установі була неоціненною. Це дозволяло мені орієнтуватися в складних ситуаціях за допомогою мудрих порад і уникати небезпечних пасток. Понад десять років потому ці стосунки продовжують бути надзвичайно цінними для мене як особисто, так і професійно. Якщо у вашому навчальному закладі немає програми наставництва, подумайте про її започаткування. Якщо ви не можете створити програму всередині себе, подумайте про те, що пропонують інші професійні організації, такі як EDUCAUSE, ISC2, ISACA та Асоціація безпеки інформаційних систем (ISSA).

Підвищення кваліфікації

Чудовим рішенням може стати заохочення наявного (не кібербезпекового) IT-персоналу до переходу на відкриті посади у сфері кібербезпеки та конфіденційності. Перехід із IT-організації може бути легшим, оскільки багато навичок можна передати, а будь-які прогалини в навичках можна усунути за допомогою навчання з кібербезпеки. Підвищення кваліфікації наявного співробітника сприяє професійному зростанню та утриманню та заповнює критичні прогалини в команді безпеки.

Переоснащення

Менш поширеним шляхом є найм співробітників, які не мають досвіду в IT. Ці люди являють собою невикористаний резерв талантів, оскільки більшість оголошень про роботу, як правило, вимагають попереднього досвіду або дуже спеціальних навичок. Проте ця практика поширюється. Згідно з дослідженням

робочої сили з кібербезпеки ISC2 2023 року, 39 відсотків респондентів працювали на посадах, не пов’язаних з IT, перш ніж прийти в кібербезпеку (один рік або менше в цій галузі). Замість того, щоб шукати точну відповідність, найміть на основі компетенцій, які призведуть до успішного переходу до кібербезпеки, а потім допоможіть у переобладнанні. У звіті EDUCAUSE Cybersecurity and Privacy Workforce визначено кілька важливих компетенцій для успішної кар’єри в галузі кібербезпеки та конфіденційності.

1. Навички побудови стосунків, спілкування та спілкування
2. Постійне навчання та адаптивність
3. Аналітичні навички та навички вирішення проблем

Погляд за межі звичайних шляхів — це чудовий спосіб заповнити прогалини, запровадити різноманітність (щодо досвіду та мислення) та інвестувати в турботу та розвиток вашого персоналу.

Використовуйте зовнішній досвід

У вашій установі може бути брак навичок, незаповнені вакансії або проект, який потребує спеціальних навичок. Якщо не усунути ці прогалини, вони можуть викликати у наявного персоналу відчуття перевантаження. Відповідно до звіту EDUCAUSE Cybersecurity and Privacy Workforce, більшість (80 відсотків) респондентів заявили, що їх робоче навантаження дещо або дуже надмірне. Якщо такі умови триватимуть, заклади зіткнуться із загостренням проблем, пов’язаних із утриманням, продуктивністю та пропуском термінів. Можливо, вже назріває криза утримання, оскільки 55 відсотків респондентів зазначили, що вони, ймовірно, подадуть заявку на іншу посаду протягом наступних дванадцяти місяців. Наймання сторонніх експертів може принести додаткову цінність вашій організації та знизити рівень стресу в існуючих співробітників.

Якщо ви плануєте залучити сторонніх експертів, важливо розробити план ресурсів, який відображатиме конкретні потреби та пріоритети вашої установи. Можливо, ви знаєте деякі ключові прогалини, але не встигли їх належним чином визначити, задокументувати та визначити пріоритети. Якщо це так, професійна оцінка програми кібербезпеки та індивідуальні рекомендації можуть налаштувати

вас на правильний шлях і позбавити вас від багатьох головних болів. Почніть з визначення досвідчених фірм з кібербезпеки, які знають вищу освіту та можуть надати вам індивідуальний і дієвий план (тобто, не просто довгий список нездійсненних цілей).

Якщо ви знаєте, куди прямуєте, консультанти з кібербезпеки можуть привнести цілеспрямований досвід і глибокий досвід, які потрібні сьогодні установам.

Віртуальний CISO (vCISO) стає все більш необхідним для багатьох вищих навчальних закладів. Ефективні програми безпеки вимагають надійної стратегії безпеки та ефективного керівництва. Хоча існує великий попит на досвідчених спеціалістів із безпеки з лідерськими навичками, їх недостатньо. CISO вимагає значних знань у сфері кібербезпеки, досвіду в IT та розуміння бізнесу вищої освіти. Укладання контракту з vCISO — це можливість для установи значно підвищити свій досвід і досягти своїх цілей (часто за менших витрат).

Дедалі частіше багато керівників вищих навчальних закладів у сфері кібербезпеки розглядають керований центр безпеки (SOC) як економічно ефективний засіб значного збільшення потужностей без збільшення персоналу. Майже половина (47 відсотків) тих, хто відповів на опитування фахівців з кібербезпеки та конфіденційності EDUCAUSE, повідомили про значне збільшення часу, пов’язаного з моніторингом і виявленням. SOC вирішує проблему моніторингу загроз цілодобово. У багатьох установах є співробітники служби безпеки, але вони не працюють цілодобово. Інші не мають офіційного персоналу служби безпеки та мінімальні заходи моніторингу. Для кожної ситуації є постачальники.

Наймання консультантів і постачальників керованих послуг заповнює прогалини, просуває програму кібербезпеки вперед і знімає тиск на наявний персонал. Знайдіть час, щоб визначити, як цей підхід може допомогти вам розробити комплексну стратегію управління інституційним ризиком.

Розробка майбутнього трубопроводу

Можливість формувати нове покоління фахівців з кібербезпеки та інвестувати в нього допомагає кожному. Навчальні заклади повинні пропонувати або розширювати освітні програми з кібербезпеки та акредитації, включно з аспірантами, бакалаврами, асоційованими ступенями, без ступеню та сертифікаціями. Ці програми можуть підтримати наявних співробітників, яким потрібно переоснастити свої навички, а також майбутніх спеціалістів з кібербезпеки.

Подумайте про залучення поточних студентів, щоб заповнити прогалини в кадрах з кібербезпеки. Це може вимагати більше часу та участі, ніж звичайна робота студентів IT; однак посади у сфері кібербезпеки є чудовим способом додати студентів до вашої команди, одночасно готуючи їх до вступу на роботу з бажаними навичками. Вам не потрібно (і, можливо, не можна) розробляти ці програми самостійно, але ви можете використовувати партнерські відносини. Ваші програми для студентів-працівників мають бути узгоджені з програмами інформатики та STEM, перевіреними постачальниками, які пропонують стажування з кібербезпеки, і можливостями, які надають EDUCAUSE, Internet2/InCommon та інші.

Вища освіта відіграє унікальну та життєво важливу роль у вирішенні прогалин у кадрах у сфері кібербезпеки в усіх галузях. Навіть якщо ваш навчальний заклад не пропонує освітніх програм з кібербезпеки, ви все одно можете залучити студентів, щоб покращити свою команду. Навички, яких вони отримують у класі, можна застосувати до викликів кібербезпеки у вашій команді.

Висновок

Документи EDUCAUSE Cybersecurity and Privacy Workforce in Higher Education, 2023, що стосуються тенденцій програм безпеки. Лідери інституцій повинні сприймати їх серйозно та вирішувати їх стратегічно. Немає срібної кулі. Проте вища освіта має потужну мережу інституційних партнерів, постачальників і професійних організацій, і нам усім потрібно працювати разом, щоб усунути прогалини та подолати ці виклики». ***(Adam Vedra. 3 Key Solutions to Higher Education Cybersecurity Workforce Challenges // EDUCAUSE***

(https://er.educause.edu/articles/sponsored/2023/12/3-key-solutions-to-higher-education-cybersecurity-workforce-challenges). 11.12.2023).

***

«Оскільки 2024 рік наближається, настав час подивитись на те, що цей рік може принести з точки зору кібербезпеки. Очікується, що до 2025 року витрати на кібербезпеку зростуть у всьому світі до 10,5 трильйонів доларів, оскільки кіберзлочинність стане все більш витонченою. Безсумнівно, ми побачимо, що штучний інтелект (ШІ) буде використовуватися для нечесних цілей, а атаки в стилі соціальної інженерії, такі як фішинг, також, ймовірно, зростуть. Ось п’ять прогнозів щодо того, що принесе 2024 рік.

1. Розширений фішинг

Ми вже бачили, як штучний інтелект почав використовуватися, але навряд чи він повністю розкрив свій потенціал. Як і будь-яка хороша технологія, це лише питання часу, коли злочинці заволодіють нею. Використання генеративного штучного інтелекту зробить шахрайство простішим і набагато витонченішим, а розширений фішинг — це перше місце для звернення. Generative AI можна використовувати для створення дуже переконливих фішингових електронних листів, повідомлень або веб-сайтів, які можна використовувати для імітації законної комунікації з надійних джерел, що ускладнює для користувачів розрізнення справжнього вмісту від шахрайського.

У 2023 році ми стали свідками атак на глобальні корпорації, такі як Clorox і MGM Resorts, з боку розробників атак соціальної інженерії Scattered Spider, які використовували численні методи та інструменти для отримання віддаленого доступу або обходу багатофакторної автентифікації, щоб зламати ці компанії. У випадку з MGM це була атака Vishing, яка призвела до витоку даних, підкреслюючи людський фактор ризику в цих атаках.

Просунуті методи фішингу, такі як фішинг, також стали простішими завдяки ШІ. Для учасників загроз продуктивність значно підвищується, і вони можуть збирати більше інформації про людей. Подібним чином ми можемо спостерігати

збільшення нападів на китобійних промислів, оскільки передові технології навчаться проривати багатофакторну автентифікацію. Нещодавня атака Okta змусила хакерів переглянути записані файли браузера, які завантажили її клієнти для усунення несправностей.

2. Шахрайство на основі ШІ

Генеративний штучний інтелект можна використати для створення інших шахрайств, таких як автоматизована служба підтримки клієнтів, за допомогою якої боти служби підтримки імітують стиль спілкування законних компаній, намагаючись отримати доступ до облікових даних. ШІ також можна використовувати для поширення фейкових новин і дезінформації шляхом створення реалістичних новинних статей, публікацій у блогах або вмісту соціальних мереж. Я очікую, що під час наступних президентських виборів з'являться шахрайські схеми deepfake, і, до речі, ці види шахрайства також можуть призвести до складних спроб крадіжки особистих даних.

Щоб зменшити ризики, пов'язані з генеративним штучним інтелектом у контексті онлайн-шахрайства, розробникам технологій, підприємствам і регуляторним органам вкрай важливо дотримуватися етичних принципів і впроваджувати запобіжні заходи в системах штучного інтелекту, щоб запобігти зловмисному використанню та підвищити обізнаність користувачів щодо безпеки. Підприємства також повинні впроваджувати надійні процеси автентифікації, щоб переконатися, що користувачі взаємодіють із законними об'єктами, і переконатися, що вони регулярно оновлюють протоколи безпеки.

3. Збільшення атак на ланцюги поставок

Зростання кількості атак на ланцюги поставок протягом багатьох років руйнує бізнес і призводить до витоку та продажу приватної інформації про клієнтів у темній мережі. Для зловмисника атаки на ланцюг поставок є ефективними, оскільки їм потрібно лише скомпрометувати окремий об'єкт у ланцюзі поставок, щоб мати далекосяжні наслідки. Широкий вплив цих атак поширюється на численні організації, впливаючи на кінцевих користувачів і клієнтів і збільшуючи потенціал шкоди.

Наприклад, злам MOVEit у 2023 році торкнувся лише понад 1000 організацій і понад 60 мільйонів осіб, демонструючи, наскільки швидко може посилитися атака на ланцюжок поставок. Координація захисту кібербезпеки у великих мережах може бути складною, що полегшує зловмисникам пошук вразливостей у ланцюгах постачання. Організаціям необхідно ще більше підвищити безпеку, проводити ретельну оцінку постачальників і стежити за ненормальною діяльністю в ланцюзі постачання, щоб уникнути цих порушень.

4. Розгортання шкідливих розширень браузера

Зловмисне програмне забезпечення, націлене на домашніх користувачів, різко зростає, і збільшення використання шкідливих розширень браузера є прекрасним прикладом. Нещодавно ми бачили, як у червні було видалено понад 30 шкідливих розширень із Веб-магазину Google Chrome, але лише після того, як їх було завантажено 75 мільйонів разів. На жаль, використання зловмисних розширень для веб-переглядачів є тенденцією до зростання — не лише за частотою, але й за складністю.

Погані гравці все краще вміють використовувати як відкриту архітектуру веб-браузерів, так і наївність користувачів. Організаціям необхідно вживати профілактичних заходів, щоб мінімізувати ризики, пов’язані зі зловмисними розширеннями браузера в майбутньому, зокрема регулярно оновлювати розширення, використовувати надійний захист кінцевих точок та інтегрувати захист розширень у свої ширші стратегії кібербезпеки.

5. Демографічна зміна несе більше загроз

Оскільки все більше молодих людей підключаються до Інтернету, кількість атак значно зростає. Життєво важливо, щоб молоді користувачі створили позицію кібербезпеки. Проте, можу сказати з власного досвіду, на це майже знизують плечима. Миттєве задоволення, а також помилкове переконання, що все одноразове, поширюється на те, як люди бачать свою онлайн-діяльність і цифрову безпеку.

Природною реакцією на зламаний обліковий запис не має бути «Я просто створю інший обліковий запис!» Натомість нам потрібно вирішити основну

проблему. Щоб це сталося, нам потрібно надати пріоритет освіті, обізнаності та навчанню з кібербезпеки. Незалежно від того, чи використовується настільний комп'ютер, мобільний телефон чи ігри, кожне нове покоління має розуміти вкрай важливу потребу у зміцненні своїх пристроїв і захисті своїх даних.

Ризики кібербезпеки споживачів

На даний момент найбільшим програшем від будь-якого порушення безпеки є споживач. Коли бізнес стає єдиним центром уваги, програє людина. Крім того, існує велика потреба в експертах з кібербезпеки для найму, що є іронією долі, оскільки стає очевидним, що з часом цей розрив зменшиться, оскільки ШІ замінить працівників. Зрештою, просуваючись у 2024 році, ми повинні наголошувати на безперервній співпраці між розробниками технологій, експертами з безпеки та регуляторними органами, яка є важливою для вирішення нових викликів і захисту користувачів від шахрайства». ***(Andrew Newman. 5 cybersecurity predictions for 2024 // Mansueto Ventures, LLC (https://www.fastcompany.com/90997838/5-cybersecurity-predictions-for-2024?utm_source=flipboard&utm_content=FastCompany%2Fmagazine%2FFast+Company). 15.12.2023).***

***

«Розглядаючи кіберризики, багато хто часто зосереджується виключно на технологічних ризиках, що випливають з інфраструктури інформаційних технологій (IT). Однак ця вузька перспектива охоплює лише частину ризику і може завдати шкоди через неадекватне визнання безлічі ризиків, з якими організація повинна зіткнутися. Кібербезпека створює справжній бізнес-ризик і стосується як малого, так і великого бізнесу в короткостроковій і довгостроковій перспективі. Нам потрібно змінити обговорення та розвивати культуру, вкорінену в системах управління кіберризиками, створених роками, не лише для інформування професіоналів IT/ІнфоСеку, але й для керівників і не тільки.

Організаціям різних розмірів і галузей слід звернутись до сторонніх експертів, щоб оцінити різні ризики. Звідти вони можуть запровадити

багаторівневий захист для їх вирішення. Це подорож, яка може сприяти зрілості організації та прищепити культуру стійкості. Якщо трапиться кіберінцидент, ваша організація буде готова та поінформована.

Наслідки кібертенденцій для бізнесу

Кіберризик проникає, розгортається непередбачувано та часто завдає суттєвої шкоди операційним і репутаційним фронтам. Складний ландшафт кіберзлочинців адаптувався, знайшовши нові шляхи отримання прибутку від проникнення як безпосередньо, так і через взаємозалежні програми третіх сторін. Це спричиняє значні наслідки для малих та середніх підприємств (МСП). Незалежно від того, чи є подія безпеки чи конфіденційності ненавмисною чи зловмисною, її вплив на бізнес у кожній галузі може бути суттєвим. Інциденти можуть призупинити роботу, порушити ланцюги поставок, призвести до значних фінансових витрат, завдати шкоди репутації та потенційно спровокувати судові процеси та регуляторні заходи.

Положення щодо конфіденційності продовжують розвиватися, і очікується посилення заходів щодо захисту даних, зокрема використання, збору та зберігання інформації третіх сторін.

МСП часто є привабливою мішенню для загроз, оскільки вони покладаються на дані та мережі, але мають менше ресурсів кібербезпеки, ніж великі організації. Вони часто залежать від сторонніх постачальників технологій (наприклад, постачальників хмарних послуг), де конфігурації безпеки та конфіденційності й елементи керування можуть бути неоптимальними, перевіреними або адаптованими до останніх уразливостей безпеки та правил конфіденційності.

У своєму звіті про глобальні загрози за 2023 рік (потрібна реєстрація) CrowdStrike визначив зростання використання хмарних технологій на 95%, що непропорційно вплинуло на МСП, враховуючи це загострене цільове середовище. NetDiligence Згідно з дослідженням кіберпретензій за 2022 рік (потрібна реєстрація), 98% претензій стосувалися малих і середніх підприємств або організацій із доходом 2 мільярди доларів США або менше. Програми-вимагачі були найбільшим джерелом кіберпретензій для малих і середніх підприємств, за ними йшли хакерські дії.

Дослідження 2022 року (потрібна реєстрація), проведене моєю материнською компанією, показало, що майже 75% організацій повідомили про принаймні один кіберінцидент за останні 12 місяців. Примітно, що лише 3% оцінили кібергігієну своєї організації як «відмінну», причому майже 3 з 4 респондентів вважають кібергігієну своєї організації «задовільною» або «потребує покращення».

Чому фінансові спеціалісти повинні піклуватися

Фінансові спеціалісти можуть відчувати себе приголомшеними та втомленими через зростаючі ризики безпеки та конфіденційності, з якими стикаються їхні організації, і те, як найкраще їх кількісно оцінити та керувати ними. Організації в усіх галузях відчувають зростаючу залежність від технологій у всіх аспектах свого бізнесу, і очікується, що ця тенденція посилиться з генеративним штучним інтелектом (ШІ). Цю залежність від технологій часто сприяють сторонні постачальники технологій та їхні субпідрядники. Постачальники не завжди можуть дотримуватись рекомендованих структур або стандартів кібербезпеки настільки, наскільки це хотілося б. Коли ці треті сторони стикаються з програмами-вимагачами, компрометацією корпоративної електронної пошти або іншими порушеннями безпеки чи системними збоями, це може спричинити хвильовий ефект у їхній клієнтській базі, вимагаючи відповіді.

Це напружує ІТ, інформаційну безпеку (ІБ), операційну службу, головного юрисконсульту та команди із закупівель, щоб забезпечити належну перевірку в процесі управління ризиками постачальника. Це все з метою отримання розумного прибутку від інвестицій з фінансової точки зору для залучених сторін.

Фінансовим фахівцям доручено збалансувати внутрішні інвестиції в кібербезпеку та управління своїми інтегрованими надійними партнерами. У міру того, як ландшафт загроз розвивається, їх моделі потрібно змінювати, щоб врахувати загальну вартість ризику. Фінансові спеціалісти можуть доповнити команду ІТ/ІБ організації, допомагаючи поставити складні запитання для фінансової оцінки безпеки та стійкості конфіденційності організації. Перевагою цього є те, що вони можуть робити це, не обов’язково перевантажуючись технічним жаргоном, який може стримувати деяких фінансових спеціалістів.

Акції для фінансових професіоналів

Фінансові спеціалісти повинні бути частиною групи планування реагування на інциденти, щоб розуміти різні сценарії, з якими організація може зіткнутися всередині організації та через треті сторони. Вони можуть спричинити перебої в роботі та завдати шкоди репутації на додаток до дорогих витрат на реагування на інциденти. Візьміть участь у настільній вправі/імітаційному моделюванні різних сценаріїв, щоб зрозуміти, як ваша організація та треті сторони відреагують.

Оцінка реакції критично важливих постачальників і третіх сторін може бути повчальною. Це може допомогти виявити додаткові гарантії та договірні механізми передачі ризиків, щоб обмежити час простою та фінансовий ризик вашої організації. Співпрацюйте з головним юрисконсультом, щоб скласти відповідніші угоди про відшкодування з цими третіми сторонами, щоб краще зрозуміти потенційне фінансове відновлення та внести поправки до їхніх вимог щодо ліміту страхування кібер/технічних помилок і упущень, наприклад.

Фінансові спеціалісти також повинні вимагати від свого страхового брокера моделі кількісної оцінки кіберризиків, щоб отримати уявлення про загальну вартість ризику за різними сценаріями збитків. Використання актуальних даних про галузеві кіберзбитки може допомогти точніше кількісно визначити та забезпечити адекватні ліміти кіберстрахування. Ваша організація може покладатися на них, щоб своєчасно та відповідально відповідати безпосередньо вашим зацікавленим сторонам. Організації, у яких критично важливий постачальник або постачальник постраждали від програми-вимагача, надзвичайно вразливі з операційної та нормативної точки зору. Страхове покриття може допомогти забезпечити своєчасне розслідування та звітність перед ключовими зацікавленими сторонами, клієнтами та регуляторними органами.

Попередня оцінка відповіді вашої організації на численні сценарії має вирішальне значення для обмеження фінансових зобов’язань у результаті кібератаки. Це також демонструє проактивну культуру для регуляторів, яка може обмежити дорогі штрафи та вимоги плану коригувальних дій.

За допомогою правильних інструментів і інформації бізнес може стати кіберстійким. Впровадження програми страхування, спрямованої на усунення вашої вразливості, може допомогти захистити ваш бізнес від потенційних ризиків, так само як і розгортання профілактичних служб кібербезпеки, які виявляють і усувають ризики. Однак це не зупиняється на досягнутому. Такі фактори, як інструменти кібер-бенчмаркінгу, узгодження з ключовими постачальниками засобів контролю за втратами в кіберпросторі та партнерство з досвідченим кібер-брокером, можуть змінити будь-яку організацію. Розуміння того, як вимірювати, зменшувати та керувати кіберризиками для вашої організації, може допомогти запобігти потенційним репутаційним, операційним і фінансовим катастрофам». ***(Denise Perlman. How Organizations And Financial Professionals Can Address Their Cyber Risk // Forbes (https://www.forbes.com/sites/forbesfinancecouncil/2023/12/15/how-organizations-and-financial-professionals-can-address-their-cyber-risk/?utm_source=flipboard&utm_content=user%2Fforbes&sh=80f5bf25fbf8). 15.12.2023).***

***

«Відповідно до нового опитування, проведеного компанією Integrity360, провідним загальноєвропейським фахівцем з кібербезпеки, майже дві третини осіб, які приймають рішення в IT, повідомляють, що скорочення бюджетів негативно вплинуло на психічне здоров'я в їхній галузі. Отримані результати представляють серйозний погляд на наслідки економічних обмежень для психічного здоров'я в галузі кібербезпеки.

Дослідження, засноване на відповідях 205 осіб, які приймають рішення з IT-безпеки, показує, що 60% учасників вважають, що бюджетні обмеження негативно вплинули на їх психічне здоров'я. Крім того, більше половини (55%) скаржаться, що поточні економічні умови зменшили доступність ресурсів психічного здоров'я та добробуту в їхніх організаціях.

Основні джерела стресу, названі опитаними, включають захист конфіденційних даних (48%), управління ризиками та відповідність вимогам (28%), захист особистих даних (26%), боротьбу з програмами-вимагачами (25%) і безпеку хмарних середовищ (23%). Меншими, але все ж значними причинами стресу є безпечні середовища IoT та OT (20%), розширені поверхні атак (19%) і консолідація безпеки (18%).

IT-директори виявляють особливу стурбованість щодо консолідації безпеки, що відображає їх безпосередню участь. Прагнення до консолідації інструментів безпеки для більш надійного контролю та видимості мережі призводить до того, що 30% IT-директорів повідомляють про вищий рівень стресу, порівняно з 18% технічних директорів і 14% аналітиків з інформаційної безпеки.

Хоча програмне забезпечення-вимагач було позначено як меншу проблему, ніж захист конфіденційних даних, його відродження суттєво вплинуло на психічне здоров'я та благополуччя осіб, які приймають рішення в IT, причому 57% респондентів назвали це фактором стресу.

Браян Мартін, керівник відділу розробки продуктів, інновацій і стратегії Integrity360, прокоментував мінливий ландшафт атак програм-вимагачів: «Оператори програм-вимагачів, які використовують вимагання, а не вимагають даних, означає, що їм більше не потрібно шифрувати дані, які вони викрадають».

«Підприємства повинні бути готові до того, що ці тактики продовжуватимуть розвиватися, і мати необхідні команди та процеси. Спеціальна команда IR зніме тиск і навантаження на підприємства, які намагаються йти в ногу зі зловмисниками», — сказав Мартін.

Опитування також виявило, що 63% вважають, що їхня робота в індустрії кібербезпеки підвищила рівень стресу та тривоги. Більше того, майже 70% вважають, що їхні роботодавці надають достатню підтримку для їх психічного здоров'я та благополуччя. Тим не менш, більшість респондентів (75%) бажають бачити збільшення інвестицій у ресурси охорони психічного здоров'я.

За словами Мартіна, «бюджети на кібербезпеку завжди були складними, і цей рік, безсумнівно, став випробуванням для багатьох компаній. Безліч проблем із

бюджетом, економічний спад і дефіцит навичок вплинули на робоче навантаження на тих, хто відповідає за боротьбу з кіберзагрозами та відповідність вимогам, і не дивно, що це згубно впливає на психічне благополуччя».

«Компанії повинні знайти рішення, щоб підтримати своїх співробітників і переконатися, що системи, над якими вони так старанно працюють, справляються зі своїм завданням. Залучення сторонньої допомоги або аутсорсинг MSSP може бути хорошим місцем для початку».

Це дослідження було проведено компанією Censuswide у період з 9 по 14 серпня 2023 року, націлене на осіб, які приймають рішення щодо IT-безпеки, віком від 18 років. Під час проведення своїх досліджень група суворо дотримується кодексу поведінки MRS, заснованого на принципах ESOMAR». ***(Kaleah Salmon. Cyber security budget cuts linked to mental health issues, survey reveals // TechDay (https://securitybrief.co.nz/story/cyber-security-budget-cuts-linked-to-mental-health-issues-survey-reveals). 20.12.2023).***

***

«…10 найкращих історій про кібербезпеку за 2023 рік від Computer Weekly.

1. NCSC викриває іранську та російську фішингову кампанію, націлену на Великобританію

Ближче до кінця січня NCSC попередив про постійну кампанію ворожих кібератак, підтримуваних державою, проти британських політичних цілей, журналістів та інших відомих осіб. Атаки, які походили з Ірану та Росії, мали на меті зібрати розвіддані та підірвати політичний процес. Пізніше того ж року NCSC зміг твердо приписати російську діяльність групі під назвою Star Blizzard.

2. NCSC попереджає щодо мовних моделей штучного інтелекту, але відкидає кібертривогу

Величезний суспільний інтерес до генеративного штучного інтелекту (ШІ) і великих мовних моделей (LLM), які їх ґрунтують, забезпечив домінування таких інструментів, як ChatGPT, у всьому порядку денному технічних новин у 2023 році.

Деякі швидко використали цей інтерес для поширення страху, невпевненості та сумнівів щодо ШІ намагався довести, що лише їхня організація має відповідь на потенційні кіберпроблеми, які вона створює, але NCSC закликав до більш збалансованого підходу.

3. Чого можуть навчитися служби безпеки за рік кібервійни?

Лютий 2023 року став похмурою віхою, оскільки минула перша річниця руйнівної війни Росії проти України. Українські кіберзахисники провели майстер-клас зі стійкості протягом 2022 та 2023 років, а Computer Weekly виміряв температуру спільноти безпеки, щоб дізнатися, які уроки ми всі можемо винести з їхнього досвіду.

4. Заборона TikTok у Великій Британії дає нам усім підстави задуматися про безпеку соціальних мереж

Ризики, притаманні платформам соціальних медіа, добре відомі вже кілька років тому, але у 2023 році ситуація змінилася на тлі сейсмічних змін у Twitter і зростаючого занепокоєння щодо передбачуваного впливу Китаю на TikTok, що призвело до заборони використання сервісу у Великобританії. урядових пристроїв, питання керування тим, чим ми ділимося в Інтернеті, як приватні особи, так і представники організацій, ніколи не здавалося більш актуальним.

5. Лінді Кемерон закликає до співпраці та застерігає від самовдоволення

Щорічна конференція NCSC завжди викликає заголовки, і цьогорічна подія в Белфасті розпочалася із заклику до співпраці в індустрії безпеки та нагадування не піддаватися самовдоволенню від генерального директора організації Лінді Кемерон. У своїй вступній доповіді Кемерон розповіла про безліч викликів, від нових технологій до незахищеного програмного та апаратного забезпечення, до кіберзлочинності та державних загроз, і закликала людей об’єднатися для їх вирішення.

6. Кіберрежим GovAssure запускається в уряді Великобританії

Загрози державним відомствам і пов’язаним з ними органам посилюються в останні роки. Цього року було запущено розширений режим кібербезпеки GovAssure, що вийшов з офісу Кабінету міністрів, який має на меті краще

захистити IT-системи, які лежать в основі державних послуг Великобританії. Серед іншого, ця схема передбачатиме проведення щорічних більш серйозних перевірок кібербезпеки.

7. Користувачам Barracuda ESG наказано викинути своє обладнання

Деякі були збентежені після того, як виправлення вразливості, знайденої в продукті шлюзу безпеки електронної пошти (ESG) Barracuda Networks, не працювало належним чином, а це означало, що користувачі підданого ризику обладнання були змушені вивести свої пристрої з експлуатації та шукати заміну. Згодом з'ясувалося, що цією вразливістю активно користуються китайські загрозливі особи.

8. Microsoft видає нове попередження про китайське кібершпигунство

Китай також був на думці Microsoft після того, як з'ясувалося, що розширена стійка загроза (APT) змогла зламати облікові записи електронної пошти уряду США за допомогою споживчого ключа підпису облікового запису Microsoft. Випадок став причиною жорсткої критики Microsoft з боку американських політиків.

9. Уразливі місця в управлінні центром обробки даних створюють загрозу для публічних хмар

У зв'язку з тим, що безпека ланцюга постачання все ще є ключовою проблемою для ділового світу, на хакерській конвенції DEF CON 2023 року було оприлюднено численні вразливості в ключових продуктах для електроживлення та керування центрами обробки даних, які лежать в основі світової загальнодоступної хмарної інфраструктури. Незважаючи на те, що ці продукти мало відомі неспеціалістам, вони настільки поширені, що якби їх прикували та експлуатували, деякі з найбільших гравців гіпермасштабування могли б побачити, як їхні послуги перекинуться.

10. Найважливішою кіберзагрозою для Великобританії є неправомірні державні актори

У річному звіті NCSC цього року детально описано появу нового класу суб'єктів кіберзагрози, які мотивовані радше ідеологічно, ніж фінансово. Такі

групи стають все більш сміливими діяти безкарно, мають більшу схильність до ризику та можуть бути не в змозі повністю зрозуміти чи контролювати вплив своїх дій, що робить їх надзвичайною загрозою». ***(Alex Scroxton. Top 10 cyber security stories of 2023 // TechTarget (https://www.computerweekly.com/news/366563092/Top-10-cyber-security-stories-of-2023). 19.12.2023).***

***

«…Дослідження EY 2023 Global Cybersecurity Leadership Insights Study було розроблено, щоб краще зрозуміти, як компанії підходять до кібербезпеки своїх організацій, щоб підготуватися до загроз кібербезпеці сьогодні та завтра. У лютому та березні 2023 року глобальна організація EY провела опитування 500 керівників відділу кібербезпеки в 19 різних секторах і 25 країнах. Результати стосуються міркувань респондентів про 2022 календарний рік.

Це ж дослідження було проведено спеціально на швейцарському ринку та базується на висновках 28 керівників інформаційної безпеки (CISO) і керівників інформаційних технологій (CIO) у восьми галузях промисловості влітку 2023 року.

Компанії в усьому світі стикаються з дедалі складнішими проблемами в управлінні кіберзагрозами сьогоднішнього та майбутнього. Тим не менш, більше половини (57%) CISO у Швейцарії вважають, що їх організація має хороші можливості для боротьби з майбутніми загрозами; у всьому світі 46% CISO сказали те саме…

Глобальне опитування виявило, що найбільшою внутрішньою проблемою в підходах респондентів до кібербезпеки є "занадто велика кількість поверхонь для атак", а також проблема балансу між безпекою та швидкістю. Це стосується і швейцарських компаній. Що стосується ризиків, то швейцарські компанії поділяють глобальну стурбованість щодо хмарних технологій, 39% з яких назвали їх першочерговим завданням. Штучний інтелект і машинне навчання також виділяються як основні ризики для безпеки швейцарських компаній: 36% вважають ці теми першочерговими, а 54% - другорядними. Це цікава дилема: нові технології сприяють трансформації багатьох організацій, але водночас створюють нові

можливості для кіберзлочинів. Це також підкреслює важливість узгодження бізнес-стратегій та стратегій кібербезпеки на кожному рівні організації…

Понад три чверті (76%) компаній у всьому світі займають у середньому більше шести місяців, щоб виявити кіберінциденти, і стикаються в середньому з 44 серйозними кіберінцидентами на рік. Швейцарські компанії мають менше щорічних інцидентів – у середньому лише 14 – і також реагують на ті, що стаються, швидше (у середньому менше п'яти місяців). Ці порівняно високі показники можуть пояснити, чому швейцарські CISO значно більше задоволені своїм загальним підходом до кібербезпеки (71% порівняно з 42% у всьому світі). Незважаючи на їхню порівняльну швидкість реагування, половина швейцарських учасників дослідження б'ють тривогу щодо здатності їхніх засобів кібербезпеки досить швидко протистояти кіберзагрозам, що розвиваються. Можливо, це відображається як на швидкості змін загалом, так і на здатності швейцарських компаній реагувати.

Люди і культура

Результати швейцарського опитування підкреслюють роль людей у темі, яка, на перший погляд, є технічною. Керівники служби безпеки широко визнають потенційну помилку людини як головну слабкість. Ось чому компаніям слід інвестувати в сильну культуру безпеки через навчання та інформаційні кампанії – і саме тому зловмисники так часто націлюються на людський інтерфейс.

Як і в глобальному опитуванні, шість із 10 швейцарських кібер-лідерів повідомили про відсутність дотримання найкращих практик кібербезпеки серед працівників, не пов'язаних з IT, як одну з найбільших внутрішніх проблем (посідає 4 місце з 8). Це відображає результати глобального опитування. Крім того, лише шість із 10 швейцарських компаній задоволені ефективністю своїх навчальних програм з кібербезпеки, що лише трохи більше, ніж середній світовий показник (50%).

Ці висновки знову вказують на необхідність кращої співпраці між IT та іншими бізнес-функціями...

Залишаючись на темі людей, компанії відчувають значну нестачу робочої сили, оскільки пропозиція кваліфікованого персоналу не встигає за попитом. На цьому фоні CISO виходять за рамки своєї поточної організаційної схеми, щоб задовольнити зростаючі потреби в кадрах у сфері кібербезпеки. У всьому світі багато фірм розглядають аутсорсинг як ключове рішення проблеми нестачі навичок і ресурсів. Швейцарські CISO віддають перевагу підвищенню кваліфікації поточної робочої сили в кіберпространстві та автоматизації процесів безпеки, щоб підвищити ефективність управління безпекою. Вони також інвестують в утримання та наймання співробітників із кібербезпеки. Ці заходи є основою їхньої стратегії розвитку кадрів, при цьому 71% вважають, що це важливі або головні пріоритети для підготовки до майбутніх загроз. Така відданість стійким рішенням, а не короткостроковим виправленням, свідчить про те, що швейцарські компанії прагнуть закласти міцну основу для задоволення постійних і нових кіберпотреб…

Цей підхід, орієнтований на людину, також поєднується з ідеєю, що лише технологія не може вирішити проблеми кібербезпеки – консенсус серед швейцарських CISO. Крім того, більшість погоджуються, що інциденти кібербезпеки більше вплинуть на фізичні активи в реальному світі в найближчі кілька років (89% погодилися). Більшість (86%) погодилися, що війну з кібербезпекою неможливо виграти. Натомість компанії можуть навчитися адаптуватися швидше, ніж зловмисники.

Кібербезпека по-швейцарськи

Швейцарія відома певною мірою обережності та перевагою «серединного шляху» в багатьох ситуаціях. Певною мірою ми бачимо це у відповідях швейцарських учасників на наше дослідження, які ще раз підкреслюють роль культури в просторі кібербезпеки…

Лише 43% швейцарських підприємств вважають себе першими запроваджувачами новітніх технологій порівняно із середнім глобальним показником (65%). Незважаючи на те, що вони готові використовувати передові технології, такі як AI або ML, SOAR, DevSecOps, а також хмарну оркестровку та автоматизацію, вони, як правило, чекають, поки технологія буде випробувана в

іншому місці, перш ніж застосовувати її самостійно. Вони також схильні зосереджуватися на технології, яка підтримує автоматизацію, спрощення та оптимізацію процесів.

Впроваджуючи кібербезпеку в усій організації та сприяючи спрощенню, швейцарські CISO підтримують позитивну поведінку, яка одночасно захищає та створює цінність для своєї організації. Окрім суто технологічного аспекту, багато хто також приймає спеціальні стратегії для керування складними поверхнями атак у хмарі, локальних і сторонніх.

Від захисників до творців цінностей

Ми віримо, що кібербезпека відіграє важливу роль у створенні цінності, чи то через більшу довіру з боку клієнтів і постачальників, чи через впевненість у використанні переваг екосистем і партнерства без ризику. Це означає, що CISO є творцями, а не просто захисниками цінностей. Їхній підхід до кібербезпеки позитивно впливає на здатність їхніх організацій швидко трансформуватися, реагувати на ринкові можливості та зосереджуватися на створенні вартості.

Ключові моменти дій, які випливають із глобального та швейцарського опитувань, включають:

Спростити та оптимізувати

Спростіть стек кібертехнологій, щоб зменшити ризик і покращити видимість. Автоматизація та оркестровка можуть зменшити безлад у технологічному середовищі, дозволяючи вам швидше виявляти сигнали та реагувати ефективніше.

Стандартизуйте та автоматизуйте

Стандартизація та автоматизація в ланцюгах постачання можуть покращити кіберпильність і постійно контролювати продуктивність без додавання зайвої бюрократії. Команди безпеки повинні бути залучені на ранніх етапах вибору постачальника.

Чітко спілкуйтеся

Найефективніші інформаційні менеджери перетворюють свою розповідь на сюжетну лінію, яка резонує з бізнесом з точки зору зниження ризику, впливу на бізнес і створення вартості.

Увімкніть людей

Людська помилка залишається основною причиною кіберзломів. Зрілі організації поєднують поступове та добре розроблене навчання з автоматизацією та інструментами запобігання, щоб зробити робочу силу кіберзахищеною за задумом.

Культивуйте культуру кібербезпеки

Кібербезпека має бути вплетена в структуру організації, а не розглядатися як гальмівник. Це підвищує вартість, вселяє впевненість, необхідну для впровадження інновацій, і відкриває нові прибутки та ринкові можливості.

Резюме

Лідери кібербезпеки в усьому світі борються з поточними та очікуваними загрозами кібербезпеці. Незважаючи на те, що швейцарські компанії працюють вище середнього за різними критеріями, вони все ще стикаються з постійними проблемами. Щоб збалансувати безпеку та швидкість, швейцарські CISO повинні зосередитися на простоті, цілісному мисленні та загальноорганізаційній інтеграції міркувань кібербезпеки…» ***(Tom Schmidt and Marc Minar. Will you see the next cyber risk coming? // EY Switzerland (https://www.ey.com/en_ch/cybersecurity/will-you-see-the-next-cyber-risk-coming). 12.12.2023).***

***

«Оскільки людські помилки спричиняють 95% усіх інцидентів кібербезпеки, співробітники неминуче є найслабшою ланкою в ланцюжку безпеки будь-якої організації. Від попадання на фішингові електронні листи до використання слабкого пароля чи обміну конфіденційними даними через незашифровані канали, навіть невелика помилка в судженні може відкрити двері для дорогих і руйнівних атак.

Як наслідок, компанії все більше віддають перевагу програмам навчання та підвищення обізнаності кінцевих користувачів з кібербезпеки. Регуляторні органи також втручаються, щоб дозволити ці ініціативи. У Великій Британії, наприклад, Управління інформаційного комісара (ICO) тепер очікує, що всі організації

продемонструють завершення навчання з кіберобізнаності всіма новачками, постійне навчання для всіх співробітників і керівництво тих, хто не відвідує.

Організації усвідомлюють необхідність інтегрувати кібербезпеку в досвід співробітників, але скільки з них проводять освітні та просвітницькі програми з питань безпеки, які дійсно пов'язані зі щоденними обов'язками та досвідом їхніх співробітників?

Часто навчання з кібербезпеки стає просто черговою вправою щодо дотримання вимог. Організації рік за роком дають співробітникам короткі презентації PowerPoint або одні й ті самі сухі навчальні матеріали, що призводить до незаангажованих співробітників, які виконують кілька завдань одночасно або просто відключаються, чекаючи вікторини наприкінці навчання.

Gartner, Inc. Як зазначив у своїх головних тенденціях кібербезпеки на 2023 рік, розробка безпеки, орієнтована на людину, стає все більш важливим фактором у програмах кібербезпеки. Без орієнтованого на користувача рольового підходу, який зосереджується на перспективах і проблемах співробітників і справді залучає їх, навіть найбільш добре продумані навчальні програми з кібербезпеки в кінцевому підсумку не запрацюють. Тоді створити культуру безпеки стає набагато складніше, роблячи організації більш уразливими до нових кіберризиків.

Боротьба з втомою безпеки

Кібербезпека – це картина, яка постійно змінюється. З розвитком нових технологій і додатків постійно з'являються нові вектори атак, а політики та процедури, що швидко змінюються, ще більше заплутують багатьох кінцевих користувачів. Це стимулює безперервний цикл вдосконалення та адаптації. Постійний вплив попереджень безпеки та правил політики на роботі може перевантажити працівників, і вся інформація згодом змішується з фоновим шумом.

Більше того, деякі заходи, які організації вживають для зменшення ризиків кібербезпеки, можуть перешкоджати продуктивності або навіть створювати нові вразливості безпеки.

Наприклад, компанія може запровадити багатофакторну автентифікацію (MFA), щоб зменшити ймовірність фішингових атак. Хоча більшість співробітників

поступово адаптуються до цієї нової технології, вони можуть зіткнутися з потоком push-сповіщень, призначених для того, щоб змусити їх перевірити автентичність шахрайських спроб входу. Ця постійна гра в «удар по кроту» може так само дратувати співробітників, як і керівників служби безпеки.

Кібербезпека також часто суперечить нашому природному людському інстинкту довіряти, спонукаючи нас прийняти більш скептичний спосіб мислення. Це може втомити співробітників, особливо коли вони вже врівноважують численні вимоги повсякденної роботи. Оскільки ми всі більш схильні до помилок під час стресу або втоми, не дивно, що можуть легко статися прогалини в безпеці.

Втома від безпеки становить серйозну проблему як для окремих осіб, так і для компаній. Щоб вирішити цю проблему та відновити пильність персоналу, фірми повинні ставити людський досвід на перше місце. Це включає надання співробітникам інформаційних ресурсів і підтримку керівництва.

Лідерські команди можуть заохочувати залучення працівників, активно пропагуючи важливість кіберсвідомої культури. Вони повинні адаптувати та впроваджувати захоплюючі навчальні програми з кібербезпеки, які адаптовані до конкретних посадових ролей і обов’язків, надаючи можливість співробітникам ефективно керувати ризиками кібербезпеки, не перевантажуючи їх.

Зміцнення культури та забезпечення безпеки

Недостатньо запланувати регулярні сесії з інформування про кібербезпеку. Навчання має бути переконливим, інтерактивним і актуальним для працівників та їхніх щоденних завдань, щоб сприяти кращому запам’ятовуванню знань. Засвоєні принципи та практики безпеки потім можуть укорінитися в повсякденній поведінці, підтримуючи розвиток кіберсвідомої культури в організації.

Компанії можуть додати фактор веселощів через гейміфікований досвід або вони можуть використовувати вражаючі історії, щоб проілюструвати далекосяжні наслідки натискання на фішингове посилання. Змодельовані атаки соціальної інженерії можуть бути особливо ефективними, оскільки вони точно імітують сценарії реального світу. Коли працівники безпосередньо стикаються з такими ситуаціями в контрольованому середовищі, вони глибше розуміють ризики, з

якими вони можуть зіткнутися у своїй повсякденній роботі, що спонукає їх відповідним чином адаптувати свою поведінку.

Розширення знань і навичок співробітників також позитивно підвищує їхню впевненість у розпізнаванні та пом'якшенні загроз кібербезпеці. Ключовим є використання сучасних, інтерактивних та персоналізованих методів навчання, які допомагають користувачам пов'язувати свої дії та загальну безпеку фірми.

Організації повинні постійно оновлювати навчання, щоб відображати зміну кібербезпеки та нормативно-правового ландшафту, а також зміну використання технологій працівниками. Фірмам, які покладаються виключно на застарілі веб-системи керування навчанням для проведення навчання з кібербезпеки, буде важко йти в ногу з впливом на безпеку додатків на основі чату, таких як Slack і Teams.

Важливо те, що організації повинні проактивно збирати постійні відгуки від користувачів, щоб гарантувати, що всі аспекти програми відповідають конкретним потребам, викликам і проблемам співробітників. Організації також повинні регулярно звітувати про прогрес у навчанні з кібербезпеки керівникам рівня С, щоб заохочувати бізнес-обізнаність і підзвітність.

Збалансування вимог до навчання та експлуатації

З огляду на безліч конкуруючих відволікаючих факторів і вимог повсякденного бізнесу, організаціям може бути складно збалансувати продуктивність співробітників з вимогами постійного навчання з безпеки. Однак фірми повинні досягти цього балансу. Кіберризик – це бізнес-ризик, і будь-яка успішна кібератака може мати руйнівні наслідки для бізнесу.

Компанії повинні включити навчання з кібербезпеки у свій бюджет безпеки, ретельно оцінюючи зони ризику, визначаючи відповідний розподіл часу та призначаючи спеціального персоналу для забезпечення ефективності. Вони також повинні розглянути можливість стратегічного партнерства зі сторонніми постачальниками, які спеціалізуються на навчанні з кібербезпеки, орієнтованому на людину, для підвищення якості та ефективності своїх програм.

Ставлячи досвід співробітників на перше місце, фірми можуть адаптувати свої тренінги з безпеки, щоб створити індивідуальні, відповідні та довгострокові

моменти навчання. Цей підхід, орієнтований на людину, дає змогу співробітникам активно зміцнювати кібербезпеку та загальну стійкість своєї організації. Компанії, які інвестують у багаторівневу навчальну програму безпеки, яка враховує ці унікальні потреби, вживають важливих заходів для створення міцної та стійкої культури безпеки». ***(Paul Ponzeka. Securing Success: Putting The Employee Experience First In Cybersecurity Training // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/12/22/securing-success-putting-the-employee-experience-first-in-cybersecurity-training/?sh=6194beebcecd). 22.12.2023).***

***

«У царстві кібербезпеки, що постійно розвивається, архітектура нульової довіри (ZTA) постає маяком інновацій та стійкості. Оскільки кіберзагрози стають все більш складними, традиційні моделі безпеки виявляються недостатніми для захисту конфіденційних даних і систем. У цьому глибокому зануренні ми досліджуємо основи, принципи та практичні наслідки архітектури нульової довіри, проливаючи світло на те, чому її вважають наступним рубежем у зміцненні цифрового захисту від нових кіберзагроз.

Розуміння архітектури нульової довіри:

Переосмислення парадигм безпеки:

Архітектура нульової довіри – це зміна парадигми від традиційної моделі безпеки на основі периметра. Традиційно організації покладалися на припущення, що опинившись у мережі, користувачам і пристроям можна довіряти. Однак у сучасному середовищі загроз, де кіберзлочинці використовують передову тактику, а внутрішні загрози викликають справжнє занепокоєння, це припущення більше не є обґрунтованим.

Фундаментальний принцип ZTA полягає в тому, щоб ніколи не довіряти та завжди перевіряти, незалежно від місцезнаходження чи контексту користувача чи пристрою. Цей підхід кидає виклик традиційному менталітету «замок і рів»,

наголошуючи на тому, що довіра не повинна надаватися автоматично на основі розташування користувача в мережі.

Основні принципи архітектури нульової довіри:

Перевіряйте кожного користувача та пристрій: у середовищі нульової довіри кожен користувач і пристрій повинні проходити постійну перевірку. Це передбачає надійні процеси автентифікації, включаючи багатофакторну автентифікацію (MFA) і перевірки працездатності пристрою, щоб гарантувати, що лише авторизовані та захищені об'єкти отримують доступ до конфіденційних ресурсів.

Найменший привілейований доступ:

ZTA працює за принципом найменших привілеїв, обмежуючи доступ користувачів і пристроїв до мінімуму, необхідного для їхніх конкретних ролей. Це обмежує потенційний збиток у разі порушення безпеки та мінімізує поверхню атаки, доступну для кіберзлочинців.

Мікросегментація:

Замість того, щоб покладатися на монолітну мережу, ZTA виступає за мікросегментацію, поділ мережі на менші ізольовані сегменти. Ця стратегія стримування запобігає бічному руху шляхом обмеження несанкціонованого доступу, навіть якщо відбувається початкове порушення.

Безперервний моніторинг і аналітика: Zero Trust не є одноразовим впровадженням; це безперервний процес. Розширені інструменти моніторингу та аналітики є невід'ємною частиною ZTA, забезпечуючи бачення в режимі реального часу дій користувачів і пристроїв. Будь-яка аномальна поведінка викликає сповіщення, що дозволяє швидко реагувати на потенційні інциденти безпеки.

Реалізація архітектури нульової довіри:

Практичні кроки:

Інвентаризація та класифікація. Першим кроком у прийнятті Zero Trust є створення всебічної інвентаризації активів і їх класифікація на основі їх важливості та чутливості. Цей фундаментальний крок закладає основу для наступних заходів безпеки.

Керування ідентифікацією та доступом (IAM):

Реалізація надійних політик IAM є центральною для ZTA. Це включає застосування надійних методів автентифікації, регулярне оновлення дозволів доступу на основі посадових ролей і швидке скасування доступу для співробітників, яким він більше не потрібен.

Сегментація мережі:

Мікросегментація є ключовим компонентом ZTA. Розділивши мережу на менші, ізольовані сегменти, організації можуть стримувати потенційні загрози та обмежувати бічний рух. Це особливо ефективно для запобігання поширенню шкідливих програм або несанкціонованому доступу в мережі.

Постійний моніторинг та реагування на інциденти:

Моніторинг мережевих дій у реальному часі та оперативне реагування на інциденти є критично важливими аспектами ZTA. Використання аналітики на основі штучного інтелекту може покращити здатність виявляти незвичайні шаблони або поведінку, які можуть вказувати на загрозу безпеці.

Переваги архітектури нульової довіри:

Посилена система безпеки:

ZTA значно посилює безпеку організації, усуваючи притаманну довіру, пов’язану з традиційними моделями. Такий підхід допомагає зменшити ризик як зовнішніх кіберзагроз, так і внутрішніх атак.

Адаптація до сучасного робочого середовища:

Оскільки традиційне офісне середовище зазнає трансформації, коли віддалена робота стає все більш поширеною, ZTA забезпечує систему безпеки, яка адаптується до динамічного характеру сучасної організації роботи. До користувачів і пристроїв ставляться скептично, незалежно від їх місцезнаходження.

Зменшена поверхня атаки:

Запроваджуючи доступ із найменшими привілеями та мікросегментацію, ZTA зменшує площу атаки, доступну для потенційних зловмисників. Ця проактивна стратегія обмежує шляхи та можливості для кіберзагроз, ускладнюючи зловмисникам використання вразливостей.

Відповідність і нормативне узгодження:

ZTA відповідає різноманітним стандартам відповідності та правилам, що робить його ідеальним вибором для організацій, які працюють у галузях із суворими вимогами до захисту даних. Постійний моніторинг і контроль доступу, властиві ZTA, допомагають організаціям виконувати нормативні зобов'язання.

Проблеми та міркування щодо прийняття без довіри:

Хоча переваги ZTA переконливі, важливо визнати проблеми та міркування, пов'язані з його впровадженням.

Організаційна культура:

Перехід від мислення, орієнтованого на довіру, до нульової довіри вимагає культурних змін в організації. Співробітники та зацікавлені сторони повинні зрозуміти та прийняти нову парадигму безпеки, щоб ZTA була ефективною.

Інтеграція з існуючими системами:

Впровадження ZTA може потребувати інтеграції з існуючими системами та технологіями. Застарілі системи, які не мають необхідних можливостей для постійного моніторингу та адаптивного контролю доступу, можуть створити проблеми під час переходу.

Ресурсомісткість:

Ретельне впровадження заходів Zero Trust вимагає виділених ресурсів, зокрема часу, персоналу та інвестицій у технології. Організації повинні оцінити свої можливості та відповідно розподілити ресурси для успішного впровадження ZTA.

Майбутнє кібербезпеки:

Нульова довіра як наріжний камінь:

Оскільки кіберзагрози продовжують ускладнюватися та витончуватися, впровадження архітектури нульової довіри стає не просто стратегічним вибором, а необхідністю. Адаптивність ZTA до динамічних робочих середовищ, його акцент на безперервному моніторингу та проактивне стримування потенційних загроз позиціонують його як наріжний камінь майбутніх інфраструктур кібербезпеки.

висновок:

Архітектура нульової довіри являє собою зміну парадигми кібербезпеки, кидаючи виклик традиційним моделям і пропонуючи проактивний, адаптивний і надійний захист від загроз, що постійно змінюються. Оскільки організації прагнуть захистити свої цифрові активи та конфіденційні дані, впровадження принципів і практик архітектури нульової довіри є не лише підвищенням безпеки, а й стратегічним імперативом у поточній боротьбі з кіберзагрозами». ***(Zero Trust Architecture: A Deep Dive into the Next Frontier of Cybersecurity // TechBullion (https://techbullion.com/zero-trust-architecture-a-deep-dive-into-the-next-frontier-of-cybersecurity/). 24.12.2023).***

***

«У сучасному взаємопов'язаному цифровому ландшафті важливість кібербезпеки неможливо переоцінити. Оскільки кіберзагрози зростають і стають дедалі складнішими, впровадження надійної гігієни кібербезпеки має першочергове значення як для окремих осіб, так і для компаній. У цій статті досліджується значення гігієни кібербезпеки та надається вичерпний посібник із найкращих практик, які можуть захистити вас від нових кіберзагроз.

Розуміння гігієни кібербезпеки:

Фонд цифрової безпеки:

Гігієна кібербезпеки стосується практик і заходів, які застосовують окремі особи та компанії для підтримки безпечного та стійкого цифрового середовища. Він охоплює ряд заходів, спрямованих на запобігання, виявлення та реагування на потенційні кіберзагрози. Подібно до того, як особиста гігієна має вирішальне значення для фізичного здоров'я, гігієна кібербезпеки є важливою для здоров'я та безпеки наших цифрових активів і конфіденційної інформації.

Ризики нехтування гігієною кібербезпеки:

Нехтування гігієною кібербезпеки може мати серйозні наслідки. Кіберзлочинці використовують уразливості, використовуючи слабкі місця в заходах безпеки, щоб отримати несанкціонований доступ до особистих і бізнес-

даних. Наслідки кібератаки включають фінансові втрати, шкоду репутації та потенційні правові наслідки. Тому інвестування часу та ресурсів у гігієну кібербезпеки є проактивною стратегією пом'якшення цих ризиків і забезпечення надійного захисту від кіберзагроз.

Найкращі практики для окремих осіб:

Захист вашої цифрової присутності:

Надійні паролі та багатофакторна автентифікація (MFA): почніть із основ. Створюйте надійні унікальні паролі для кожного онлайн-облікового запису, що містять поєднання літер, цифр і символів. Впровадження MFA додає додатковий рівень безпеки, вимагаючи другої форми перевірки, наприклад коду, надісланого на мобільний пристрій.

Регулярні оновлення програмного забезпечення:

Оновлюйте операційні системи, антивірусне програмне забезпечення та програми. Оновлення програмного забезпечення часто включають виправлення, які усувають вразливості, що ускладнює для кіберзлочинців використання слабких місць.

Будьте обережні зі спробами фішингу:

Кіберзлочинці часто використовують фішингові електронні листи, щоб оманою змусити людей розкрити конфіденційну інформацію. Будьте обережні з несподіваними електронними листами, особливо з запитами особистої чи фінансової інформації. Перевірте легітимність відправника, перш ніж натискати будь-які посилання.

Захищені мережі Wi-Fi:

Переконайтеся, що ваша домашня мережа Wi-Fi захищена паролем і використовує надійне шифрування. Уникайте використання публічної мережі Wi-Fi для конфіденційних транзакцій, оскільки ці мережі можуть бути вразливими до кібератак.

Регулярне резервне копіювання:

Регулярно створюйте резервні копії важливих даних. У разі атаки програм-вимагачів або втрати даних наявність останніх резервних копій гарантує, що ви зможете відновити свою інформацію, не піддаючись на вимагання.

Найкращі практики для бізнесу:

Посилення корпоративного кіберзахисту:

Програми навчання співробітників: інвестуйте в комплексні програми навчання співробітників з кібербезпеки. Розкажіть їм про останні загрози, тактику фішингу та важливість дотримання протоколів безпеки. Поінформована робоча сила є важливою лінією захисту.

Заходи безпеки мережі:

Застосуйте надійні заходи безпеки мережі, зокрема брандмауери, системи виявлення вторгнень і віртуальні приватні мережі (VPN). Регулярно оцінюйте вразливі місця мережі та негайно усувайте будь-які недоліки.

Безпека кінцевої точки:

Захистіть усі пристрої, підключені до корпоративної мережі. Встановіть антивірусне програмне забезпечення, проводите регулярне сканування та переконайтеся, що співробітники використовують безпечні, схвалені компанією пристрої для виконання робочих завдань.

Плани реагування на інциденти:

Розробляйте та регулярно оновлюйте плани реагування на інциденти. У разі кібератаки наявність чітко визначеного плану забезпечує швидку та ефективну відповідь, мінімізуючи вплив на операції та дані.

Контроль доступу та найменші привілеї:

Застосуйте суворий контроль доступу, надаючи працівникам найменші привілеї, необхідні для виконання їхніх ролей. Обмеження доступу зменшує потенційну шкоду в разі порушення безпеки.

Роль переходів у гігієні кібербезпеки:

Плавний перехід між найкращими практиками має вирішальне значення для створення комплексної стратегії гігієни кібербезпеки. Наприклад, надійні паролі

служать основою кібербезпеки, але вони найбільш ефективні в поєднанні з багатофакторною автентифікацією (MFA). Подібним чином програми навчання співробітників плавно переходять у плани реагування на інциденти, створюючи узгоджений підхід до кібербезпеки в бізнесі.

Нові технології та гігієна кібербезпеки:

З розвитком технологій зростають і кіберзагрози. Впровадження нових технологій у практику гігієни кібербезпеки має важливе значення для того, щоб випереджати потенційні ризики.

Штучний інтелект (AI) і машинне навчання:

ШІ та технології машинного навчання покращують можливості виявлення загроз. Ці технології можуть аналізувати величезні масиви даних, щоб ідентифікувати шаблони, що вказують на кіберзагрози, забезпечуючи проактивне реагування.

Технологія блокчейн:

На додаток до своєї ролі в забезпеченні фінансових операцій, блокчейн може підвищити цілісність даних і захистити процеси ланцюжка поставок. Впровадження технології блокчейн може стати стратегічним кроком у зміцненні кібербезпеки.

Хмарні заходи безпеки:

Оскільки компанії все більше використовують хмарні сервіси, стає обов'язковим впровадження надійних заходів безпеки в хмарі. По-перше, шифрування відіграє ключову роль у захисті даних, що зберігаються у хмарі. Крім того, суворий контроль доступу допомагає регулювати та обмежувати несанкціонований доступ. Крім того, регулярні перевірки мають вирішальне значення для моніторингу та підвищення загальної безпеки. Підсумовуючи, запровадження цих заходів забезпечує комплексний і стійкий підхід до захисту конфіденційних даних у хмарі».

Безперервна еволюція гігієни кібербезпеки:

Кібербезпека – це не разова спроба; натомість це постійний процес, який вимагає постійної адаптації до нових загроз. Крім того, важливі регулярні оцінки,

аудити та оновлення практики кібербезпеки. Ці заходи мають вирішальне значення для підтримки стійкого захисту від нових кіберзагроз. Крім того, вони сприяють проактивному підходу, забезпечуючи швидке виявлення та усунення потенційних вразливостей.

висновок:

Важливість гігієни кібербезпеки неможливо переоцінити. Незалежно від того, чи то для окремих осіб, які захищають особисту інформацію, чи для компаній, які захищають конфіденційні дані, прийняття та підтримка найкращих практик кібербезпеки є колективною відповідальністю. Завдяки інтеграції цих практик у повсякденні процедури та організаційні протоколи окремі особи та компанії можуть впевнено орієнтуватися в цифровому ландшафті, знаючи, що вони вжили проактивних заходів для зміцнення свого цифрового захисту від ландшафту загроз, що постійно змінюється. Вступаючи в епоху цифрових технологій, нехай гігієна кібербезпеки буде нашим керівним принципом для безпечного та стійкого майбутнього». ***(The Importance of Cybersecurity Hygiene: Best Practices for Individuals and Businesses // TechBullion (https://techbullion.com/the-importance-of-cybersecurity-hygiene-best-practices-for-individuals-and-businesses/). 24.12.2023).***

***

«У технологічному ландшафті, що постійно розвивається, один прорив виділяється як кардинальний фактор – квантові обчислення. Оскільки ця революційна парадигма набирає обертів, вона несе з собою хвилю наслідків для різних сфер, де кібербезпека займає центральне місце. У цій статті ми заглибимося в розквіт квантових обчислень і дослідимо їх глибокий вплив на світ кібербезпеки.

Розуміння квантових обчислень:

Щоб зрозуміти вплив квантових обчислень на кібербезпеку, важливо спочатку осягнути основи цієї нової технології. На відміну від класичних комп’ютерів, які покладаються на біти, квантові комп’ютери використовують кубіти. Це дозволяє їм виконувати складні обчислення з безпрецедентною швидкістю, роблячи традиційні методи шифрування вразливими.

Загроза для класичного шифрування:

Одне з найважливіших наслідків квантових обчислень для кібербезпеки полягає в їх здатності зламати широко використовувані алгоритми шифрування. Класичні методи шифрування, такі як RSA та ECC, покладаються на складність певних математичних задач для безпеки. Однак квантові комп'ютери з їхньою здатністю експоненціально швидше вирішувати складні проблеми становлять значну загрозу цим криптографічним методам.

Поява квантово-безпечної криптографії:

Оскільки привид квантового дешифрування нависає, спільнота кібербезпеки активно працює над розробкою квантово-безпечної або пост-квантової криптографії. Ці криптографічні алгоритми розроблені, щоб протистояти обчислювальним можливостям квантових комп'ютерів, забезпечуючи безперервну безпеку конфіденційної інформації в квантову еру.

Перехід до квантово-безпечних рішень:

Перехід від традиційних криптографічних систем до квантово безпечних альтернатив є складним процесом. Організаціям необхідно оцінити свою поточну інфраструктуру безпеки, визначити потенційні вразливості та запровадити квантово-стійкі алгоритми. Цей перехід є не лише технологічним, а й стратегічним викликом, який вимагає ретельного планування для захисту цифрових активів.

Квантовий розподіл ключів (QKD):

Серед квантової революції, яка триває, Quantum Key Distribution стає маяком надії на безпечний зв'язок. Використовуючи принципи квантової механіки, QKD створює нерозривний зв'язок між двома сторонами. Отже, будь-яка спроба перехопити зв'язок негайно виявляється. Цей квантовий підхід не тільки розглядає, але й представляє багатообіцяюче рішення проблем шифрування, пов'язаних з появою квантових комп'ютерів.

Проблеми та етичні міркування:

Хоча квантові обчислення мають величезні перспективи, вони також створюють низку проблем і етичних міркувань. Можливість квантових комп'ютерів зламати шифрування викликає питання щодо конфіденційності даних

і безпеки конфіденційної інформації. Встановлення балансу між технологічним прогресом і етичною відповідальністю стає обов'язковим, коли ми рухаємося цією незвіданою територією.

Підготовка до квантової революції:

Перед обличчям неминучості квантових обчислень організації повинні прийняти проактивний підхід до кібербезпеки. Це передбачає інвестиції в дослідження та розробки, щоб бути в курсі квантових досягнень, співпрацювати з експертами з квантово-безпечної криптографії, а також постійно оцінювати та покращувати протоколи безпеки.

Міжнародна співпраця та стандарти:

Враховуючи глобальний характер цифрового ландшафту, міжнародна співпраця має вирішальне значення для встановлення стандартів і протоколів квантових обчислень. Уряди, галузі та дослідницькі установи повинні працювати разом, щоб створити єдиний фронт проти потенційних загроз кібербезпеці, створених квантовими технологіями.

Навчання робочої сили:

Оскільки поширеність квантових обчислень продовжує зростати, виникає все більш нагальна потреба в кваліфікованій робочій силі, яка б володіла знаннями та пом'якшувала пов'язані з квантовою кібербезпекою ризики. Отже, визначення пріоритетів освітніх програм і навчальних ініціатив стає обов'язковим. Таким чином ми можемо гарантувати, що фахівці з кібербезпеки отримають необхідні знання та навички, необхідні для вмілого орієнтування в цю нову еру.

висновок:

Розвиток квантових обчислень знаменує собою ключовий момент в історії технологій, приносячи як можливості, так і виклики. У сфері кібербезпеки потреба в адаптації та інноваціях ніколи не була такою гострою. Застосовуючи квантово-безпечні рішення, сприяючи міжнародній співпраці та навчаючи робочу силу, ми можемо прокласти шлях до безпечного цифрового майбутнього в епоху квантових обчислень. Оскільки ми стоїмо на порозі цієї технологічної революції, рішення, які ми приймаємо сьогодні, формуватимуть ландшафт кібербезпеки для майбутніх

поколінь». ***(The Quantum Leap: Navigating the Rise of Quantum Computing and Its Impact on Cybersecurity // TechBullion (https://techbullion.com/the-quantum-leap-navigating-the-rise-of-quantum-computing-and-its-impact-on-cybersecurity/). 24.12.2023).***

***

«Звіт Forbes The Reputation Impact of IT Risk свідчить про те, що 46% компаній зазнали репутаційної шкоди через порушення правил кібербезпеки. Кібербезпека є одним із найважливіших проявів турботи про своїх клієнтів та відвідувачів веб-сайту, адже ви захищаєте цифрові системи, мережі та дані від несанкціонованого доступу, крадіжки і шахрайства.

Турбота про кібербезпеку є важливою для сучасного українського бізнесу. Усі ми знаємо, що війна точиться не лише на полі бою, а ще й у цифровому просторі. Так, 12 грудня один із найбільших мобільних операторів України «Київстар» став жертвою хакерської атаки, яку називають наймасштабнішою за всю історію мобільного зв'язку в Україні. Абоненти залишилися без зв'язку, доступу до телебачення, мобільного та домашнього інтернету.

Як уберегти свій бренд, веб-сайт та клієнтів від шкідливих наслідків? Першочергово варто ознайомитись із трендами кібербезпеки у 2024 році, які допоможуть зберегти репутацію, кошти та нерви.

Що таке кібербезпека і чому необхідно про неї дбати

Кібербезпека — це комплекс заходів і технологій для забезпечення конфіденційності, цілісності та доступності інформації, що зберігають й обробляють комп'ютерні системи. Найважливішими компонентами кібербезки є: запобігання несанкціонованому доступу, визначення потенційних загроз і вразливостей у системі та вживання необхідних заходів для пом'якшення наслідків.

Вживання заходів із кібербезпеки важливе для цифрового маркетингу, адже:

Ви оперуєте особистісними даними клієнтів. Адреси електронної пошти, імена, номери телефонів, історія покупок, платіжні дані неймовірно приваблюють

шахраїв. Прогалини у системі безпеці веб-сайту призведуть до витоку даних, погіршення репутації бренду, а також юридичних проблем.

Якщо компанія зазнає кібератаки, клієнти можуть поставити під сумнів її безпеку та компетентність. Так, колективна думка про репутацію бренду може змінитися у гіршу сторону, якщо виявиться, що у системі відсутні належні інструменти контролю безпеки.

Важливою є безпека будь-яких платформ, якими ви користуєтесь у повсякденній роботі. CMS-системи, інструменти аналітики, служби електронної пошти та особливо CRM-системи містять безліч особистих даних про клієнтів.

Кібератаки призводять до зниження трафіку і погіршення SEO-рейтингів. Збої в роботі сайту через спровоковані атаки на сервер або зловмисне програмне забезпечення суттєво впливають на трафік. Користувачі, які нічого не підозрюють про зловмисні дії, можуть несвідомо ввести свої дані в тимчасово незахищені системи, що ставить під загрозу їхню фінансову і особисту інформацію.

Отож, як убезпечити себе від кібершахрайства у 2024 році? Розповідаємо нижче.

Дотримання міжнародних стандартів безпеки

Це не тренд, це — база, якої має дотримуватись кожний відповідальний бізнес. Скоріш за все, ви вже чули про GDPR — загальний регламент захисту даних, який набув чинності 25 травня 2018 року. GDPR вимагає, щоб персональні дані користувачів оброблялися безпечно, тобто з використанням відповідних технічних та організаційних заходів. Так, підхід включає в себе управління ризиками, захист особистих даних користувачів від кібератак, вчасне виявлення загроз та мінімізацію їх впливу.

Зокрема важливим є провадження Стандарту безпеки даних індустрії платіжних карток (PCI DSS). Сертифікація PCI забезпечує безпеку платіжних даних завдяки набору вимог: установка брандмауерів, шифрування передачі даних, використання антивірусного програмного забезпечення тощо. Крім того, компанії повинні обмежувати доступ до даних власників карток і контролювати доступ до мережевих ресурсів.

Якщо компанія зазнала кібератаки, у неї є 72 години для того, щоб повідомити регуляторний орган про інцидент.

Наявність захищеного протоколу веб-сайту

Чому ми говоримо про захищений протокол HTTPS у першу чергу? Ваш обов'язок як власника веб-сайту — забезпечити безпеку даних своїх клієнтів, зокрема платіжних і особистих. У 2020 році Chrome випустив оновлення, у якому захищені веб-сайти стали позначатися відповідним значком. На сьогодні користувачі обізнані у цьому питанні, а тому мало хто стане здійснювати покупку на веб-сайті, який такий і кричить с пошукового рядка — «Не захищений».

Протокол HTTPS забезпечує цілісність і конфіденційність даних, що пересилаються між пристроєм користувача та веб-сайтом. Дані, що передаються через HTTPS, захищені на трьох різних рівнях:

Безпечне шифрування: передача даних шифрується не читабельними символами, щоб зловмисники не змогли їх прочитати.

Цілісність даних: запобігає зміні або викривленню даних під час передавання від пристрою до веб-сайту.

Автентифікація: запобігає хакерським атакам і підвищує довіру користувачів.

Саме тому у 2024 році радимо подбати про наявність SSL-сертифікату, що дозволяє безпечно передавати конфіденційну інформацію, таку як номери кредитних карток, дані для входу в обліковий запис тощо. Сертифікати SSL видаються центрами сертифікації (CA), які перевіряють особу власника веб-сайту та легітимність компанії. Також сертифікат можна придбати у реєстратора доменних імен або постачальника послуг хостингу веб-сайтів. Звичайно, що доведеться докласти трохи зусиль, однак це варте довіри і безпеки ваших клієнтів.

Двофакторна аутентифікація

Цей тренд є важливим не тільки на словах: так, на початку 2022 року двохетапна автентифікація стала обов'язковою для всіх облікових записів Google. Якщо такі світові гіганти запобігають вразливості своїх систем, то що вже казати про малий і середній бізнес?

У стандартному процесі входу до облікового запису або застосунку користувач отримує доступ до свого облікового запису без жодних додаткових дій. Двофакторна аутентифікація передбачає і другий крок для підтвердження особи: наприклад, у Telegram це хмарний пароль, який можна завчасно вигадати і встановити. Google надає кілька варіантів підтвердження: через інший пристрій, введення восьмизначного резервного коду або коду підтвердження на мобільний номер телефону.

Ви можете обрати один або кілька варіантів двофакторної автентифікації в залежності від потреб. Найпоширеніші способи:

Проходження двофакторної аутентифікації за допомогою електронної пошти є найбільш універсальним методом, оскільки більшість людей мають до неї доступ щодня. Як це працює: після того, як користувач введе необхідні дані для входу, йому надійде електронний лист. Код або посилання у листі дозволить отримати доступ до облікового запису швидко, безпечно та надійно.

Процес двофакторної автентифікації через SMS. Надсилання коду у текстовому повідомленні — чудовий спосіб переконатися, що особа, яка запитує доступ до облікового запису, є авторизованим користувачем. Погодьтесь, що навряд чи зловмисники зможуть отримати доступ до мобільного пристрою користувача.

Програми автентифікації паролів працюють подібно до двофакторної автентифікації SMS. Однак у цьому випадку одноразовий код генерується локально на смартфоні користувача.

Безпечна і надійна служба хостингу

Вашому бізнесу пощастило, якщо веб-сайт обслуговується безпечною службою хостингу. Це не тільки захищає ресурс від хакерів і атак зловмисного програмного забезпечення, але й означає, що робота веб-сайту завжди під контролем.

При виборі сервісу, що надає послуги із хостингу, важливо враховувати тип веб-сайту та його мету. Так, особистий блог матиме інші потреби в кількості необхідних ресурсів, ніж сайт електронної комерції. Варто брати до уваги

очікуваний обсяг трафіку: якщо заплановані показники є високими, тоді треба переконатися, що хостинг-провайдер зможе задовольнити ці потреби. Серед інших порад:

Доступна служба підтримки. В ідеалі провайдер хостингових послуг має забезпечувати цілодобову підтримку, щоб ви завжди могли звернутися за допомогою у разі виникнення потреби.

Зверніть увагу на заходи безпеки, які хостинг-провайдер використовує для захисту веб-сайту та його даних. Так, необхідними складовими є брандмауери, регулярне сканування шкідливих програм і сертифікати SSL для захисту конфіденційної інформації.

Переконайтесь, що служба хостингу забезпечує автоматичне резервне копіювання даних та має параметри для відновлення веб-сайту в разі атак і несправностей.

Гарантія безперебійної роботи хостинг-провайдера має вирішальне значення для того, щоб веб-сайт завжди був доступним для відвідувачів. Дізнайтеся, чи має сервіс резервні джерела живлення та систему резервного копіювання для мінімізації ризику простою та втрати даних.

Використання CSP

Ще однією поширеною загрозою, якої мають остерігатися власники сайтів, є атаки міжсайтового сценарію (XSS). Хакери знаходять спосіб додати шкідливий код на сторінки веб-ресурсу, який може заразити пристрій користувача.

Саме у 2024 році варто подбати про політику безпеки вмісту (CSP) — інструмент, який допоможе захистити сайт від XSS-атак. Як це працює: CSP дозволяє вказати, які домени браузер повинен розглядати як шкідливі джерела. Так, користувач знатиме, що саме за цим посиланням криється зловмисне програмне забезпечення, за яке ви не несете відповідальність.

Обмеження транзакцій

Якщо ви працюєте у сфері електронної комерції, тоді напевно ви чули про шахрайський метод тестування платіжних карток. Так, зловмисники відвідують інтернет-магазин із слабкою системою безпеки, додають недорогий товар у кошик і

підставляють різні CVV-коди, доки не знайдуть підходящу комбінацію для списання коштів. Зокрема для цього використовують спеціальних ботів, кількість спроб яких може сягати тисячі лише за одну хвилину.

Щоб уникнути спамової діяльності шахрайських ботів, можна встановити обмеження кількості транзакцій на веб-сайті:

Обмежте кількість разів, коли клієнт може спробувати ввести правильний CVV. За великої кількості відмов IP-адреса користувача блокується системою.

Встановіть обмеження на кількість транзакцій, які можуть надходити з однієї IP-адреси за годину, день, тиждень тощо.

Відстежуйте кількість відхилених транзакцій, і за їх різкого сплеску вживайте необхідних заходів.

Посилення ролі ШІ та технологій машинного навчання

Звичайно, що новітні та ШІ-технології не оминули і сферу кібербезпеки. У 2024 році розширені можливості штучного інтелекту з аналізу даних все частіше будуть використовувати для виявлення та прогнозування кіберзагроз. Окрім цього, ШІ забезпечуватиме аналіз загроз у реальному часі, що дозволить швидше та точніше реагувати на кіберінциденти. Зокрема, технології машинного навчання можна використовувати для автономного оновлення протоколів кібербезпеки та нейтралізації кіберзагроз.

Серед корисних інструментів, які варто протестувати у прийдешньому році:

Kriptos' AI відстежує трафік, щоб виявити підозрілі дії та спроби несанкціонованого доступу до веб-сайту. Інструмент підійде для ефективного визначення та класифікації кіберзагроз: ШІ збирає і аналізує великі обсяги даних, щоб визначити закономірності та тенденції кібератак, надаючи цінну інформацію для посилення заходів безпеки.

Darktrace DETECT аналізує тисячі показників, щоб виявити незначні відхилення системи в режимі реального часу. Головна перевага інструменту — самонавчання ШІ: для ефективної роботи моделі необхідно попрацювати із веб-сайтом близько тижня, щоб якнайкраще зрозуміти контекст.

Trellix пропонує прогнозування на основі штучного інтелекту: розумна й адаптивна платформа дозволяє передбачати загрози й вчасно ним запобігати. Зокрема, інструмент ознайомить вас із причинами порушення кібербезпеки веб-сайту, а також вирішить проблему в режимі реального часу.

Посилена увага до мобільної безпеки

Мобільні пристрої стали невід'ємною частиною як особистого, так і професійного життя людини, а тому увага до мобільної безпеки у 2024 році лише посилиться. У мобільних пристроях зберігається майже все наше життя: дані для навчання і роботи, платіжні картки, особисті листування — приваблива мішень для кібершахраїв, чи не так?

Як покращити рівень мобільної безпеки у прийдешньому році:

Наявність протоколів шифрування, які гарантують, що дані, що передаються між пристроями, залишаються захищеними від несанкціонованого перехоплення або доступу.

Багатофакторна автентифікація та функція реєстрації сеансів. Це допомагає при моніторингу будь-якої підозрілої діяльності, яка може виникнути під час сеансу користувача.

Безпека не має впливати на зручність користувацького досвіду. Так, доступ до веб-сайту або облікового запису має здійснюватись швидко, зрозуміло і без необхідності виконувати зайві дії.

Технологія блокчейну

Технологія блокчейну може значно посилити заходи із кібербезпеки. Це своєрідна база даних, яка використовується вузлами комп'ютерної мережі. Технологія найбільш відома своєю ключовою роллю в системах криптовалют для підтримки безпечного та децентралізованого запису транзакцій, однак це не єдина сфера застосування. Так, веб-сайту електронної комерції технологія дозволить відслідковувати велику кількість транзакцій та вчасно виявляти підозрілі дії.

Висновки: додаткові поради для бізнесу щодо кібербезпеки

У сучасному світі тренд на кібербезпеку є не тільки незмінним, а ще й обов'язковим. Передусім від гарантій безпеки залежить репутація бренду, а також

рівень довіри клієнтів. На жаль, у 2024 році тенденція до кібершахрайства збільшиться, а обізнаність у протидії цифровим злочинним діям лише зменшиться. Як цьому протистояти?

Регулярний перегляд, оновлення та підтримка політики щодо паролів.

Забезпечте навчання кібербезпеці для всієї команди. Кожний співробітник має знати, як захистити свої системи та що робити у разі атаки.

Переконайтеся, що команда використовує надійне і безпечне WI-FI з'єднання.

Встановіть контроль доступу до конфіденційних даних і систем, щоб мінімізувати ризик неавторизованого використання даних.

Шифруйте конфіденційні дані під час їх зберігання та передавання, щоб захистити їх від несанкціонованого доступу та потенційних атак.

Розробіть чітко визначений план реагування на інциденти, у якому описано кроки у разі порушення безпеки. План має містити чіткі протоколи зв'язку, ролі та обов'язки членів команди, а також інструкції щодо виправлення та відновлення системи». ***(Анастасія Кузнецова. ТОП-9 трендів кібербезпеки у 2024 році: як захистити свій веб-сайт від зловмисників? // Webpromo (https://web-promo.ua/ua/blog/top-9-trendiv-kiberbezpeki-u-2024-roci-yak-zahistiti-svij-veb-sajt-vid-zlovmisnikiv/). 25.12.2023).***

***

Сполучені Штати Америки та Канада

«…У сучасну епоху цифрових технологій канадська онлайн-індустрія ставок на спорт переживає величезне зростання. Хоча це надає вам більше можливостей і зручності, це також привертає увагу кіберзлочинців, які хочуть використовувати вразливості. Від витоку даних до атак програм-вимагачів – ставки на захист конфіденційної інформації високі.

Безпека ваших особистих і фінансових даних є однією з головних проблем ставок на спорт. Під час створення облікового запису онлайн-букмекерської контори ви повинні надати конфіденційну інформацію, таку як ваше ім'я, адреса та платіжні дані. Ця інформація має бути захищена від несанкціонованого доступу.

Крім того, ваші ставки та історія транзакцій містять цінні дані. Кіберзлочинці можуть спробувати перехопити ці дані та зловживати ними, що призведе до фінансових втрат і потенційної викрадення особистих даних. Беручи участь у ставках на спорт, ви повинні знати про ці загрози та заходи, які застосовуються для захисту ваших даних.

Найсучасніші засоби кібербезпеки

На щастя, індустрія ставок на спорт у Канаді серйозно ставиться до кібербезпеки. Авторитетні букмекерські заклади та онлайн-платформи ставок інвестують у найсучасніші засоби кібербезпеки, щоб гарантувати безпеку ваших даних.

Однією з ключових використовуваних технологій є шифрування. Коли ви передаєте дані до спортивної букмекерської контори, вони шифруються за допомогою розширених криптографічних алгоритмів. Це шифрування гарантує, що навіть у разі перехоплення ваші дані виглядатимуть неавторизованими сторонами як тарабарщина. Ця технологія є цифровим еквівалентом блокування ваших даних у безпечному сховищі.

Ще одним важливим заходом кібербезпеки є двофакторна автентифікація (2FA). Коли ви входите у свій обліковий запис ставок на спорт, 2FA вимагає від вас надати другу форму підтвердження, наприклад одноразовий код, надісланий на ваш мобільний пристрій. Це додає додатковий рівень безпеки, що значно ускладнює неавторизованим особам доступ до вашого облікового запису.

Крім того, спортивні букмекери проводять регулярні перевірки безпеки та оцінки вразливості, щоб виявити й усунути потенційні недоліки в своїх системах. Ці профілактичні заходи допомагають забезпечити безпеку ваших даних, поки ви насолоджуєтеся ставками на спорт.

Ваша роль у кібербезпеці: найкращі практики

Хоча канадські букмекерські контори використовують надійні технології кібербезпеки для захисту ваших даних, ваша роль у кібербезпеці є не менш важливою. Щоб підвищити безпеку в Інтернеті, подумайте про застосування таких найкращих практик:

– Використовуйте надійні унікальні паролі для своїх облікових записів ставок на спорт.

– Увімкніть 2FA, коли він доступний.

– Регулярно перевіряйте свій обліковий запис на наявність підозрілої активності.

– Будьте обережні зі спробами фішингу та підозрілими електронними листами.

– Оновлюйте свої пристрої та програмне забезпечення за допомогою останніх виправлень безпеки.

Поринаючи у захоплюючий світ спортивних ставок у Канаді, важливо пам’ятати про кібербезпеку. Галузь використовує передові технології та найкращі практики для захисту ваших даних, але ваша активна участь у підтримці онлайн-безпеки має вирішальне значення.

Будьте в курсі та вживайте профілактичних заходів, ви можете насолоджуватися гострими відчуттями від ставок на спорт, гарантуючи безпеку ваших даних. Отже, продовжуючи свій шлях до ставок на спорт, пам’ятайте про висновки цієї статті, щоб захистити свою цінну інформацію.

Правила конфіденційності даних у Канаді

Конфіденційність даних стала першочерговою проблемою для окремих осіб і організацій в епоху цифрових технологій. Канада запровадила жорсткі правила конфіденційності даних, щоб захистити особисту інформацію своїх жителів. Розуміння цих правил має вирішальне значення, особливо під час участі в таких видах діяльності, як спортивні ставки, які передбачають збір і обробку персональних даних.

Основним законом Канади про конфіденційність даних є Закон про захист персональної інформації та електронних документів (PIPEDA). PIPEDA встановлює правила збору, використання та розкриття особистої інформації організаціями приватного сектору. Він вимагає від організацій отримувати згоду на збір і використання персональних даних, надає особам право доступу до своєї інформації та вимагає заходів безпеки даних для захисту від порушень.

Коли ви співпрацюєте з онлайн-платформами спортивних ставок, ви довіряєте їм свою особисту інформацію. Важливо переконатися, що ці платформи відповідають PIPEDA та іншим відповідним нормам конфіденційності даних. Авторитетні спортивні букмекери серйозно ставляться до конфіденційності даних і мають чітку політику конфіденційності, яка інформує вас про те, як збираються, використовуються та захищаються ваші дані.

Як користувачу, радимо переглянути політику конфіденційності платформ ставок на спорт, якими ви користуєтеся. Переконайтеся, що вони є прозорими щодо своїх методів роботи з даними, мають заходи для захисту вашої інформації та забезпечують необхідні засоби контролю для керування вашими налаштуваннями даних. Знаючи правила конфіденційності даних і вибираючи платформи, які їм відповідають, ви можете спокійно насолоджуватися ставками на спорт.

Нові технології ставок на спорт

Світ ставок на спорт постійно розвивається, частково завдяки технологічному прогресу. Оскільки технології продовжують змінювати індустрію, для учасників ставок на спорт з’являються нові можливості та досвід. Тут ми досліджуємо новітні технології, які викликають хвилю в ландшафті спортивних ставок.

1. Мобільні програми для ставок: мобільні технології змінили ставки на спорт, дозволяючи зручно робити ставки зі свого смартфона чи планшета. Програми для ставок забезпечують зручний інтерфейс, оновлення коефіцієнтів у реальному часі та трансляцію подій у прямому ефірі, покращуючи загальний досвід ставок. Доступність і зручність мобільних додатків для ставок зробили їх популярним вибором серед любителів спорту.

2. Штучний інтелект (ШІ) і аналітика даних: штучний інтелект і аналітика даних роблять революцію в стратегіях ставок на спорт. Розширені алгоритми аналізують величезні обсяги даних, включаючи статистику гравців, ефективність команди та історичні тенденції, щоб надавати точніші прогнози. Інструменти на основі штучного інтелекту можуть допомогти вам приймати обґрунтовані рішення щодо ставок, пропонуючи статистику на основі даних і рекомендовані ставки.

3. Віртуальна реальність (VR) і доповнена реальність (AR): технології VR і AR виводять спортивні ставки на новий рівень занурення. Деякі платформи досліджують досвід віртуальної реальності, де ви можете віртуально відвідувати спортивні події та робити ставки у віртуальній спортивній точці. Програми AR накладають інформацію про ставки на прямі трансляції, покращуючи ваші враження від перегляду та роблячи ставки під час гри більш інтерактивними.

Ці новітні технології підвищують зручність і точність спортивних ставок і відкривають нові захоплюючі можливості для гравців. З розвитком технологій ви можете очікувати ще більше інновацій у спортивних ставках, які запропонують вам динамічний і захоплюючий досвід ставок…». ***(Shivam. Is Your Sports Betting Data Safe? Exploring Cybersecurity Tech in Canada // What's Trending (https://whatstrending.com/is-your-sports-betting-data-safe-exploring-cybersecurity-tech-in-canada/?utm_source=flipboard&utm_content=MichaelPetej5jk%2Fmagazine%2FProactive+Cyber+Security). 05.12.2023).***

***

Майже через рік, наприкінці березня 2023 року, C-26 пройшов у другому читанні. Зараз законопроект знаходиться на розгляді Постійного комітету з громадської та національної безпеки для розгляду та можливого внесення змін.

Зміст статті

Те, що цей закон продовжує лежати в комітеті через 16 місяців після того, як він уперше побачив світло, свідчить про одну з його основних недоліків, яка, чесно кажучи, не є унікальною для цього законодавчого акту: незважаючи на ознаки того, що він був написаний поспішно., мабуть, у надії встигати за технологічними змінами, він з’являється надто повільно.

До того моменту, коли він проходить третє читання, а потім петляє своїм шляхом через Сенат до Королівської згоди, C-26 цілком може бути наздогнаний

подіями. Загрози, яким він покликаний протистояти, множаться набагато швидше, ніж льодовиковий темп законодавчого процесу, здається, здатний відповідати.

Що це за погрози? Остання Національна оцінка кіберзагроз від Канадського центру кібербезпеки містить їх у виразі, який для урядового документа є надзвичайно прямим.

Кіберзлочинці швидко збільшуються, перетворюючи програмне забезпечення-вимагач та інші атаки на транснаціональну компанію, тоді як державні суб'єкти — зокрема Китай, Росія, Іран і Північна Корея — розгортають величезні ресурси для нападу та підриву відкритих економік і суспільств, підриваючи довіру до них. державні інституції та фактичну основу, на якій ґрунтується довіра до них. «У вас може виникнути спокуса припинити читання на півдорозі, — пише керівник CCSE Самі Хурі у передмові, — від'єднайте всі свої пристрої та викиньте їх у найближчий смітник».

Щоб протистояти цьому, проект закону пропонує два стовпи : по-перше, перегляд Закону про телекомунікації, що надає федеральному міністру інновацій, науки та промисловості широкі повноваження наказувати компаніям забороняти певні продукти, клієнтів або постачальників послуг із можливими щоденними штрафами в розмірі до 15 мільйонів доларів на день, якщо вони не дотримуються; і по-друге, Закон про захист критичних кіберсистем (CCSPA), який дозволить міністру та призначеній посадовій особі розпоряджатися про кіберзаходи в регульованих на федеральному рівні частинах приватного сектора, які вважаються важливими для національної безпеки.

До них належать телекомунікаційна та енергетична інфраструктура, як-от трубопроводи, атомні станції, регульований на федеральному рівні транспорт, банківська справа, кліринг і розрахунки.

Дивлячись з висоти 10 000 футів, широка сфера дії законодавства декому здасться виправданою; зрештою, чи значні загрози не виправдовують драматичні дії? Але є різниця між актуальною дією та такою прогалиною, що потребуватиме перезавантаження того дня, коли вона стане законом.

Крістофер Парсонс у аналізі для The Citizen Lab окреслює шість основних проблем, кожна з яких повинна бути підставою для дискваліфікації. До них належать надлишок свавільних повноважень, занадто велика секретність, неадекватний контроль над обміном інформацією в уряді, потенційно непомірні витрати для менших фірм (законодавство не проводить відмінностей на основі масштабу чи галузі), розпливчасті формулювання та відсутність визнання Хартії або права на конфіденційність.

Бренда Макфейл у жовтневому 2022 році в аналізі для Канадської асоціації громадянських свобод повторює багато критики Парсонса, іронізуючи, зауважуючи, що закон доповнює «все більш довгий ряд законодавства, яке задовольнило б очевидну потребу, якби воно було кращим».

Якщо метою в цілому є управління, яке сприяє процвітанню, безпеці, підзвітності, різноманітності та справедливості в демократичному суспільстві, тоді C-26 у його проекті не має бути прийнято.

Чи терміново потрібен закон? Абсолютно. Але чи правильно зрозуміли його розробники? Ні. Враховуючи блискавичну швидкість зростання векторів кіберзагроз, має сенс продовжувати керувати цими загрозами на тимчасовій основі, як це робив міністр, за допомогою The Communications Security Establishment (CSE) і CCCS, і знайдіть час, необхідний для того, щоб законодавчі акти були правильними». ***(Michael Den Tandt. Den Tandt: Canadian government must take the time needed to get its cyber security bill right // Ottawa Citizen (https://ottawacitizen.com/opinion/den-tandt-canadian-government-must-take-the-time-needed-to-get-its-cyber-security-bill-right). 04.12.2023).***

***

«Канадський центр кібербезпеки, який є частиною організації Communications Security Establishment, опублікував свою публікацію Cyber Threats to Canad's Democratic Process: 2023 Update. Ця оцінка стосується глобальної кіберзагрози, спрямованої на вибори та наслідків для демократичного процесу в Канаді, і визначає чотири глобальні тенденції:

Активність кіберзагроз, націлених на вибори, зростає в усьому світі, у 2022 році це стосується понад чверті національних виборів. Виходячи з цієї тенденції, CSE оцінює, що кіберзагрози більш імовірні на наступних федеральних виборах у Канаді, ніж у минулому.

Росія та Китай продовжують здійснювати більшість приписуваних кіберзагроз, спрямованих на вибори за кордоном.

Організатори кіберзагроз все краще замітають сліди, і більшість кіберзагроз, спрямованих на вибори, залишаються невідомими.

Організатори кіберзагроз все частіше використовують генеративний штучний інтелект (ШІ) для посилення дезінформації в Інтернеті. Цілком ймовірно, що іноземні супротивники або хактивісти використовуватимуть генеративний ШІ, щоб вплинути на виборців напередодні наступних федеральних виборів у Канаді.

CSE прагне захищати канадців від будь-якого кібервтручання в демократичний процес Канади. Будучи членом робочої групи із загроз безпеки та розвідки виборам (SITE), CSE допомагає відслідковувати загрози виборам і усунути їх. Канадський центр кібербезпеки CSE (Cyber Centre) тісно співпрацює з Elections Canada, щоб захистити свою інфраструктуру, а також з основними політичними партіями, щоб підвищити їхню обізнаність про кібербезпеку. Це включає проведення брифінгів, навчальних ресурсів, консультацій та індивідуальних порад, а також послуги з кібербезпеки.

Постійні відносини Cyber Centre з Elections Canada включають послуги моніторингу для виявлення кіберзагроз, співпрацю з ними для захисту їхніх комп’ютерних мереж і допомогу в реагуванні на інциденти, якщо це необхідно. CSE оцінює, що малоймовірно, що конфіденційна інформація, яку зберігає Elections Canada, буде скомпрометована учасниками кіберзагроз, і малоймовірно, що кіберактивність порушить інфраструктуру голосування під час національних виборів.

Після призначення федеральних виборів Cyber Center готовий створити спеціальну гарячу лінію для федеральних політичних партій, яка пропонує цілодобову підтримку кібербезпеки. Крім того, поза виборчим періодом у

Кіберцентрі є спеціальна контактна особа, до якої політичні партії можуть звертатися з питань кібербезпеки.

Кіберцентр CSE та кампанія Get Cyber Safe продовжують надавати поради та вказівки всім канадцям, щоб допомогти їм залишатися в безпеці в Інтернеті, включаючи інформацію про те, як ідентифікувати дезінформацію, дезінформацію та зловмисну інформацію, а також інформаційний бюлетень для виборців щодо діяльності впливу в Інтернеті…» ***(Communications Security Establishment releases 2023 update on cyber threats to Canada's democratic process // Government of Canada (https://www.canada.ca/en/communications-security/news/2023/12/cyber-threats-to-canadas-democratic-process-2023-update.html). 06.12.2023).***

***

«У серпні 2023 року Білий дім оголосив про план посилення кібербезпеки в школах K-12 – і не без причин. У період з 2018 року до середини вересня 2023 року було зафіксовано 386 кібератак на освітній сектор США, і вони коштували цим школам 35,1 мільярда доларів. Основною метою були школи K-12.

Нова ініціатива Білого дому передбачає співпрацю з федеральними агентствами, які мають досвід у сфері кібербезпеки, такими як Агентство з кібербезпеки та безпеки інфраструктури, Федеральна комісія зі зв'язку та ФБР. Такі технологічні компанії, як Amazon, Google, Cloudflare, PowerSchool і D2L, пообіцяли підтримати ініціативу навчанням і ресурсами.

Хоча кроки, вжиті Білим домом, позитивні, як людина, яка викладає та проводить дослідження з кібербезпеки, я не вважаю, що запропонованих заходів достатньо для захисту шкіл від кіберзагроз. Ось чотири причини, чому:

1. Школи стикаються з більшою кількістю кіберзагроз, ніж інші сектори

Кібератаки на школи K-12 зросли більш ніж у вісім разів у 2022 році. Навчальні заклади привертають увагу кіберзлочинців через свою слабку кібербезпеку. Ця слабка кібербезпека дає можливість отримати доступ до мереж, що містять дуже конфіденційну інформацію.

Злочинці можуть використовувати інформацію студентів, щоб подавати заявки на шахрайські державні пільги та відкривати неавторизовані банківські рахунки та кредитні картки. Даючи свідчення підкомітету із питань соціального забезпечення Палати представників Федеральної торгової комісії зазначив, що номери соціального страхування дітей є винятково цінними, оскільки вони не мають кредитної історії та можуть бути пов'язані з будь-яким іменем і датою народження. Було виявлено, що понад 10% дітей, які навчаються в службі захисту особи, мають кредити.

Кіберзлочинці також можуть використовувати таку інформацію для здійснення атак програм-вимагачів проти шкіл. Атаки програм-вимагачів включають блокування комп'ютера або його файлів і вимогу оплати за їх звільнення. Рівень віктимізації програм-вимагачів у секторі освіти перевершує показники в усіх інших досліджуваних галузях, включаючи охорону здоров'я, технології, фінансові послуги та виробництво.

Школи особливо вразливі до кіберзагроз, оскільки все більше шкіл електронні пристрої позичають учням. Зловмисники ховають зловмисне програмне забезпечення в онлайн-підручниках і есе, щоб змусити студентів завантажити їх. Якщо учні або вчителі випадково завантажать шкідливе програмне забезпечення на шкільні пристрої, зловмисники можуть здійснити атаку на всю шкільну мережу.

Зіткнувшись з такою атакою, школи можуть відчайдушно намагатися виконати вимоги злочинців щодо забезпечення доступу учнів до навчання.

2. Школам не вистачає персоналу з кібербезпеки

Низькі показники кібербезпеки шкіл K-12 можна пояснити, частково, браком персоналу. Близько двох третин шкільних округів не мають штатної посади спеціаліста з кібербезпеки. Ті, хто має штат із кібербезпеки, часто не мають бюджету на посаду головного спеціаліста з інформаційної безпеки, який би контролював та керував стратегією округу. Часто IT-директор бере на себе цю роль, але він несе ширшу відповідальність за IT-операції без особливого акценту на безпеці.

3. Школам бракує навичок кібербезпеки

Відсутність навичок кібербезпеки серед наявного персоналу перешкоджає розробці потужних програм кібербезпеки.

Лише 10% викладачів кажуть, що мають глибоке розуміння кібербезпеки. Більшість студентів кажуть, що мають мінімальні знання про кібербезпеку або взагалі не мають їх. Поінформованість про кібербезпеку, як правило, ще нижча в районах з більшою бідністю, де студенти мають менший доступ до освіти з кібербезпеки.

Агентство з кібербезпеки та безпеки інфраструктури планує провести навчання з кібербезпеки для додаткових 300 шкіл K-12, шкільних округів та інших організацій, залучених до освіти K-12 У наступному навчальному році. Маючи 130 930 державних шкіл K-12 і 13 187 державних шкільних округів у США, план CISA обслуговує лише крихітну частину з них.

4. Недостатнє фінансування

FCC запропонувала пілотну програму, яка передбачає виділення 200 мільйонів доларів протягом трьох років на посилення кіберзахисту. З річним бюджетом у 66,6 мільйона доларів це не покриває повних витрат на кібербезпеку, враховуючи, що належний захист шкіл K-12 країни коштуватиме приблизно 5 мільярдів доларів.

Витрати охоплюють закупівлю обладнання та програмного забезпечення, консультації, тестування та наймання експертів із захисту даних для боротьби з кібератаками. Для реагування на нові загрози також необхідні часті навчання. З розвитком технологій кіберзлочинці адаптують свої методи для використання вразливостей у цифрових системах. Вчителі повинні бути готові до вирішення таких ризиків.

Витрати значні

Скільки повинні витрачати школи та округи на кібербезпеку? Інші сектори можуть слугувати моделлю для керівництва школами K-12.

Один зі способів визначення фінансування кібербезпеки – це кількість працівників. Наприклад, у сфері фінансових послуг ці витрати коливаються від 1300 до 3000 доларів США на одного штатного працівника. понад 4 мільйони

вчителів У США. Встановлення витрат на кібербезпеку на рівні 1300 доларів США на вчителя – найменший кінець того, що витрачають фінансові компанії – вимагало б від шкіл К-12 витратити загалом 5 мільярдів доларів.

Альтернативний підхід полягає у визначенні фінансування кібербезпеки відносно витрат на ІТ. За оцінками, підприємства США витрачають у середньому 10% своїх ІТ-бюджетів на кібербезпеку. Оскільки школи К-12, за оцінками, витратять понад 50 мільярдів доларів на ІТ у 2020-21 фінансовому році, виділення 10% на кібербезпеку також вимагатиме від них витрат 5 мільярдів доларів.

Інший підхід полягає у розподілі витрат на кібербезпеку як частки від загального бюджету. У 2019 році витрати на кібербезпеку становили 0,3% федерального бюджету. Федеральний уряд, уряд штату та місцеві органи спільно виділяють 810 мільярдів доларів на освіту К-12. Якщо школи встановлять витрати на кібербезпеку на рівні 0,3%, за прикладом федеральних агентств, це потребуватиме річного бюджету в 2,4 мільярда доларів.

Навпаки, п’ята частина шкіл виділяє менше 1% своїх ІТ-бюджетів, а не весь бюджет, на кібербезпеку. У 12% шкільних округів взагалі не виділяються кошти на кібербезпеку». ***(Nir Kshetri. Why federal efforts to protect schools from cybersecurity threats fall short // The Conversation Media Group Ltd (https://theconversation.com/why-federal-efforts-to-protect-schools-from-cybersecurity-threats-fall-short-216866?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 14.12.2023).***

***

«Державні компанії повинні дотримуватися нового набору нормативних термінів протягом наступного тижня, які вимагатимуть швидкого розкриття зловмисних кібератак на їхні мережі та діючих процесів, щоб запобігти їх повторенню.

Згідно з новими правилами SEC, що набувають чинності 18 грудня, суб’єкти, які підпадають під дію Комісії з цінних паперів і бірж, повинні будуть подавати

звіти про порушення даних у скорочений термін і містити додаткову інформацію про обсяг будь-яких інцидентів. Управління кібербезпекою компанії також вимагатиметься в щорічному розкритті інформації, починаючи з 15 грудня.

Оновлені зобов'язання набувають чинності, оскільки SEC порушує справу проти розробника програмного забезпечення SolarWinds Corp., яка може свідчити про те, наскільки агресивно агентство застосовуватиме ймовірні порушення розкриття інформації. Нові вказівки також з'явилися в той час, коли державні службовці намагаються впорядкувати понад 50 вимог звітності про інциденти, що збігаються між федеральними агентствами.

Агентство почало оновлювати правила в жовтні 2021 року, а в березні 2022 року запросило відгук громадськості щодо запропонованих правил.

«Фірми повинні приймати рішення в режимі реального часу, реагуючи на кіберподії та пов'язані з ними розкриття інформації, особливо коли тривають атаки або навіть тривають внутрішні та кримінальні розслідування», — сказав директор SEC із забезпечення дотримання прав людини Гурбір С. Гревал під час виступу в червні, в якому він підкреслив, що ці рішення впливають на клієнтів, чиї дані були скомпрометовані. «Ці рішення також можуть бути суттєвими для інвесторів у публічні компанії».

1. Як розкриваються порушення?

Згідно з остаточним правилом, опублікованим 4 серпня, оновлені вимоги до звітності мають на меті інформувати інвесторів про стан кібербезпеки компанії, «одночасно уникаючи конфіденційних деталей безпеки», якими можуть скористатися зловмисники.

Протягом чотирьох днів після визначення того, що інцидент кібербезпеки вплинув на бізнес, компанії повинні повідомити про вплив злому за допомогою форми 8-K. Для розкриття інформації потрібна інформація про час і масштаби інциденту, зокрема про те, коли було виявлено порушення та чи були якісь дані викрадені чи зашифровані.

Регулятори не надали конкретного визначення суттєвості щодо кібербезпеки, але сказали, що аналіз цієї фрази є узгодженим у законодавстві про цінні папери.

Інциденти слід вважати суттєвими, якщо вони можуть вплинути на інвестиційні рішення «розумного акціонера», – йдеться в правилі, вказуючи на вплив на фінанси та сприйняття бренду як приклади суттєвості.

Згідно з правилом, інвестори також повинні знати, як жертва намагалася пом'якшити інцидент і чи зазнає компанія будь-яких фінансових або операційних наслідків злому. Компанії повинні подати змінену форму 8-K протягом чотирьох днів після отримання будь-якої нової інформації про інцидент.

Незважаючи на запевнення агентства, що ці розкриття інформації не загрожуватимуть внутрішній безпеці, організації, зокрема Software Alliance та American Gas Association, у публічних коментарях висловили стурбованість тим, що ці деталі можуть стати дорожньою картою для атак для суб'єктів загрози. AGA підкреслила важливість обміну інформацією та даними після того, як Colonial Pipeline Co. була скомпрометована у 2021 році групою програм-вимагачів, що призвело до дефіциту палива на східному узбережжі США.

Згідно з остаточними правилами, регуляторні органи врахували занепокоєння галузі, видаливши запити щодо технічних деталей про інцидент і замість цього зосередившись на його матеріальному впливі.

Крайній термін виконання вимог щодо звітності – 18 грудня для більшості компаній, на які поширюється дія SEC. Менші компанії, які отримують менше 100 мільйонів доларів річного доходу або мають менше 250 мільйонів доларів публічних акцій, мають розпочати розкриття інформації до 15 червня 2024 року.

2. Що потрібно для управління?

Відділ корпоративних фінансів SEC виявив, що більшість компаній не розкривають інформацію про нагляд за кібербезпекою, повідомляючи про інцидент, йдеться в правилі. Агентство стверджує, що більш детальний нагляд «зменшить інформаційну асиметрію» на ринку та краще надасть інвесторам важливі знання про рівень готовності бізнесу до вирішення кіберризиків, які можуть вплинути на його стратегію чи фінансові перспективи.

Нове розкриття інформації, яке компанії повинні вносити у форму 10-K, спрямоване на досягнення цього шляхом опису процесів оцінки та управління

значними ризиками кібербезпеки. Згідно з правилом, розкриття оцінки ризиків може включати інформацію про перевірки систем безпеки або загрози, створені сторонніми постачальниками.

Згідно з правилом, у звітах про нагляд слід назвати будь-які комітети ради директорів, які контролюють кібербезпеку, і пояснити, як члени залишаються в курсі загроз. SEC також просить розкрити інформацію у формі 10-K про те, які ролі компанії відповідають за моніторинг кібербезпеки та як інциденти передаються до правління.

Вітчизняні компанії, фінансові роки яких закінчуються 15 грудня або пізніше, повинні розкривати нову інформацію в річних звітах. Регульовані компанії, зареєстровані за межами США, повинні повідомляти подібні дані в пункті 16K форми 20-F.

3. Чи є винятки?

Правило дозволяє відкладене розкриття суттєвих кіберінцидентів у випадках, які можуть загрожувати національній або громадській безпеці. Відповідно до вказівок, виданих 12 грудня Міністерством юстиції, компанії, які бажають отримати 30-денну початкову відстрочку, повинні спочатку зв’язатися з ФБР, щоб надати інформацію про інцидент і пояснити наслідки публічного розголошення.

Затримки можуть бути дозволені, якщо публічне визнання злому може призвести до нових інцидентів або підірвати спроби компанії пом’якшити його вплив, йдеться в інструкції. Виправданнями для затримки також є порушення системи, що містить конфіденційні дані уряду США.

ФБР має передати запит генеральному прокурору разом із аналізом того, чи становить розголошення ризики для національної чи громадської безпеки. Генеральний прокурор має той самий чотириденний термін, щоб задовольнити або відхилити запит на відстрочку. Якщо генеральний прокурор надає початкову затримку, компанії можуть вимагати більше часу, якщо ризики триватимуть, максимум до 90 днів після початкової затримки. Запити на затримку після цього періоду вимагають звільнення від SEC у кожному конкретному випадку, йдеться в інструкції.

Емітенти цінних паперів, забезпечених активами, звільнені від цього правила, оскільки Комісія з цінних паперів і цінних паперів дійшла висновку, що ці організації зазвичай не використовують онлайн-інформаційні системи, які регулюються цим положенням.

4. Як захищаються порушення?

SEC має «нульову толерантність до ігор», коли йдеться про розкриття інформації про кібербезпеку, сказав Гревал, директор агентства з правозастосування, під час червневої промови, коли він застеріг компанії від пріоритету репутації над прозорістю, навмисно мінімізуючи інциденти або не повідомляючи про них.

Агентство може накласти грошові штрафи на будь-яку регульовану установу, яка порушить будь-який новий мандат щодо розкриття інформації. Страхова компанія First American Financial Corp. виплатила агентству майже 500 000 доларів США в червні 2021 року після того, як нібито місяці чекала, щоб розкрити порушення безпеки, незважаючи на те, що знала про це.

Інші наслідки невиконання можуть включати накази про припинення та відмову від них або скасування реєстрації цінних паперів.

Нещодавно SEC продемонструвала свою готовність притягнути керівників служби безпеки до особистої відповідальності за неналежне розкриття інформації, висунувши звинувачення проти керівника відділу безпеки SolarWinds Тіма Брауна за те, що він здійснив історичну кібератаку. Брауна звинувачують у навмисному нерозкритті вразливостей кібербезпеки у формі 8-K до та після того, як російські кіберзлочинці використали їхній доступ до SolarWinds для проникнення в десятки приватних і державних мереж. Компанії загрожує цивільне покарання на суму до 100 000 доларів США. Агентство також звернулося до суду із запитом про заборону Брауну працювати на посаді виконавчого директора в державній компанії». ***(Skye Witley. Cyberattack Victims Must Abide New SEC Disclosures: Explained // Bloomberg Industry Group, Inc. (https://news.bloomberglaw.com/privacy-and-data-security/cyberattack-victims-must-abide-new-sec-disclosures-***

explained?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity%20Stuff). 15.12.2023).

***

«Британська розвідка похвалила канадську електронну шпигунську службу за те, що вона є «спритною» та більш просунутою в деяких сферах, ніж вони, зокрема в кібербезпеці, де Канада є «головою зграї».

У п’ятирічному дослідженні Комітету з розвідки та безпеки Британської палати громад сказано, що Канада відіграє «провідну роль» у сфері кібербезпеки в розвідувальному партнерстві Five Eyes, яке також включає Великобританію, США, Австралію та Нову Зеландію.

У звіті комітету з міжнародного партнерства, який використовує свідчення шпигунських агентств і опублікований цього місяця, зазначається, що Британія прийняла канадську систему захисту від кібератак.

Однак ці висновки були зроблені після попередження Ділової ради Канади на початку цього року про те, що Канада ризикує бути сприйнятою її союзниками як «слабка ланка», якщо вона швидко не вживе заходів для пом’якшення загроз економічній безпеці. У звіті групи, яка представляє великих роботодавців Канади, йдеться про те, що «вже є тривожні ознаки того, що найближчі союзники Канади звертають увагу на наше небажання протистояти зростаючим загрозам безпеці».

Британський комітет під головуванням депутата від Консервативної партії сера Джуліана Льюїса мав доступ до секретних матеріалів і заслуховував свідчення керівників британських спецслужб, у тому числі MI5, яка займається внутрішньою розвідкою та національною безпекою; MI6, відповідальна за зовнішню розвідку; і Штаб урядового зв'язку (GCHQ), агентство електронного шпигунства; а також підрозділ оборонної розвідки Великобританії.

У звіті йдеться, що MI5 і MI6 «мають тісні робочі стосунки з CSIS», а зв’язки між шпигунськими службами двох країн є «сильними та надійними».

Комітет заявив, що докази свідчать про те, що партнерство між канадськими кібершпигунами, установою безпеки зв’язку (CSE) і GCHQ «процвітає».

GCHQ засвідчив перед парламентським комітетом, що «Канада справді спритна, і вони дуже зосереджені на кібербезпеці».

У звіті говориться, що GCHQ відзначив «зрілу та провідну роль Канади в кібербезпеці в межах П’яти очей».

«Канада була з нами на чолі з кібербезпеки, і наші стосунки з кібербезпеки надзвичайно міцні та глибокі», — сказав GCHQ комітету. «Насправді це найглибше з «П’яти очей», і вони були першопрохідцями в деяких речах, які ми використовуємо, включно з тим, як ви відстежуєте загрози в уряді, і так само ми поділилися можливостями в іншому напрямку».

У 2020 році Британський національний центр кібербезпеки оприлюднив, що «наші друзі з Канадського центру кібербезпеки» дозволили йому використовувати канадську технологію Host Based Sensor для захисту британських державних систем замість того, щоб витрачати роки на розробку власних.

Канадська система розміщує датчики на комп’ютерах уряду Канади, які можуть автоматично виявляти та зупиняти незвичайну активність, зокрема спроби встановлення зловмисного програмного забезпечення. Він також збирає дані про шкідливі дії для аналізу. Центр кібербезпеки, що є частиною CSE, встановив систему на понад 850 000 урядових пристроїв Канади в 85 федеральних установах.

Альянс «П’ять очей», учасники якого погоджуються не шпигувати один за одним, обмінюються розвідданими та проводять спільні операції, працюючи разом у деяких областях для розвитку можливостей.

Збір і обмін «метаданими» або перехопленими телекомунікаційними слідами може розширити операції зі збору розвідувальної інформації.

Але в минулому CSE стикався з критикою з боку свого спостерігача за те, що він незаконно передавав дані іноземним союзникам. CSE заборонено шпигувати за канадцями без ордера.

У британському звіті йдеться, що в деяких випадках завдання оборонної розвідки передаються «П’яти очим», щоб забезпечити цілодобове охоплення, за допомогою того, що відомо як «слідувати за сонцем», щоб скористатися перевагами різних часових поясів, йдеться у звіті.

Голова британської оборонної розвідки навів як приклад операцію, коли аналітики зображень, які працюють на базі Королівських ВПС, передають місію Вашингтону, округ Колумбія, а потім канадським партнерам, «які потім передадуть австралійським і новозеландським партнерам, які потім передадуть її назад нас."

У звіті виявлено, що розвідувальне командування збройних сил Канади також приносить додаткову цінність альянсу «П’ять очей», «а не дублює можливості та аналізи, проведені іншими».

У звіті говориться, що Великобританія планує розвивати свої космічні активи, дозволяючи більше супутникового спостереження, дозволяючи їй «платити більше в котел Five Eyes».

Комітет дійшов висновку, що в середньостроковій перспективі «П’ять очей» розширить своє членство, наприклад, до Японії, «невеликі», оскільки рівень взаємної довіри, необхідний кожному партнеру, «щоб поділитися своїми найбільш чутливими та ретельно охоронюваними секретами», таким чином, що поріг для вступу має бути дуже високим.

У доповіді висловлено занепокоєння з приводу того, що Великобританія працює з країнами з нижчими етичними стандартами, заявивши, що «відносини Великобританії та США були напруженими через дії США, пов’язані з жорстоким, нелюдським і таким, що принижує гідність, поводженням (CIDT), тортурами та видачею підозрюваних у тероризмі» на початку 2000-х років. У звіті йдеться про ув'язнення в Гуантанамо.

Комітет розкритикував колишнього міністра закордонних справ Великої Британії Домініка Рааба, який, на їхню думку, ввів його в оману, сказавши, що він ніколи не дозволяв дії, які становили ризик тортур.

У звіті говориться, що пізніше була отримана інформація, яка «виявила, що тодішній міністр закордонних справ фактично дозволив дію одного разу, яка мала реальний ризик катувань – навіть якщо були запрошені гарантії, вони не зменшили ризик до меншого, ніж реальний ризик тортур».

Він також санкціонував дії, як зазначено у звіті, які становили реальний ризик жорстокого, нелюдського та такого, що принижує гідність, поводження –

тричі протягом 12 місяців – і дії, які несли ризик іншого неприйнятного поводження, наприклад, під час арешту та затримання, у 22 випадках. протягом 12 місяців». ***(Marie Woolf. British intelligence says Canada's cyberspies are 'at the head of the pack' // The Globe and Mail Inc. (https://www.theglobeandmail.com/politics/article-canada-cybersecurity-five-eyes/?utm_source=flipboard&utm_content=Len2ikm%2Fmagazine%2FCanada+). 12.12.2023).***

***

«15 грудня набули чинності розширені правила кібербезпеки Комісії з цінних паперів і бірж (SEC), які вимагають від публічних компаній розкривати інциденти протягом чотирьох робочих днів. Це означає, що резонансні порушення, як-от той, який торкнувся всіх користувачів системи підтримки клієнтів Okta, або злом 23andMe, який включав інформацію майже 7 мільйонів клієнтів, матимуть навіть більші наслідки, ніж будь-які дані, які були зламані. І правила SEC – лише верхівка айсберга змін до нормативної відповідності.

З невеликою помпою та майже непоміченим пресою, інституційними інвесторами чи будь-ким іншим федеральний уряд тихо керує сейсмічними змінами в економіці, вимагаючи суворої відповідності кібербезпеці в усіх 16 секторах критичної інфраструктури.

Ці сектори включають добре відомі та дуже відсунуті ринки, такі як оборонно-промислова база, фінансові послуги та енергетика, які регулюються відповідно Міністерством оборони (DoD), SEC та Міністерством енергетики (DoE). Однак часто не звертають уваги на підгалузі, що знаходяться під цими 16 секторами, які, по суті, об'єднуються, щоб охопити майже кожну компанію та компонент нашої економіки, завдяки чому майже кожен бізнес потрапляє під дію нових нормативних актів у сфері кібербезпеки, які поширюються федеральним урядом із дедалі швидкішими темпами. Сектор комерційних об'єктів, наприклад, складається з восьми підсекторів, включаючи нерухомість, роздрібну торгівлю,

спортивні ліги та розважальні заклади. Ніде сховатися від регулювання кібербезпеки та обов'язкових мінімальних вимог до кібербезпеки.

Благо для галузі

Хоча дехто стверджує, що уряд перевиконує свої дії, стає зрозуміло, чому ці правила діють швидко та люто. Росія становить величезну кіберзагрозу – вона навіть порушила Міністерство оборони – і представники розвідки попереджали про потенційні загрози з боку Китаю.

Ця посилена революція в галузі кібербезпеки почалася минулого року з виконавчого указу Білого дому та розгортається як рух, що долає кордони. Кілька десятків країн приєдналися до зусиль США в галузі кібербезпеки, що відображає колективне прагнення до зміцнення глобальної цифрової економіки.

Ми прямуємо до зростаючого ринку відповідності вимогам кібербезпеки, коли шахрайські претензії щодо кібербезпеки потрапляють під контроль судового сканування. Належний контроль безпеки більше не буде вибором, а юридичним і економічним імперативом, що знаменує нову епоху цифрової стійкості та зміцнення економічної структури.

Це вже вимагається для підрядників Міністерства оборони через Доповнення щодо федеральних закупівель Міністерства оборони (DFARS), а незабаром і через програму сертифікації моделі зрілості кібербезпеки (CMMC) 2.0. Ймовірно, що через кілька років державні підрядники, які не входять до сфери оборони, також повинні будуть відповідати обов'язковим мінімальним вимогам щодо кібербезпеки як умови для отримання будь-якого федерального контракту.

Виконавчий наказ вимагає обов'язкових базових стандартів для всіх федеральних підрядників, щоб замінити непослідовну та невиконувану політику окремих установ, яка існує сьогодні. Окремі департаменти та агенції не чекають цього дня і люто видають власні нормативні вимоги.

Ми вже бачили, як Управління транспортної безпеки (TSA) видає нові вимоги до операторів аеропортів і літаків, Міністерство внутрішньої безпеки (DHS) діє щодо захисту контрольованої несекретної інформації (CUI), EPA) прагне захистити Агентство з охорони навколишнього середовища (водного сектору та

Закон про звітність про кіберінциденти для критичної інфраструктури 2022 року (CIRCIA).

Перетягування всіх важелів

Уряд використовує всі доступні регуляторні важелі, щоб тихо визначити та забезпечити дотримання обов'язкових мінімумів кібербезпеки для всієї економіки так само, як він зобов'язує використовувати ремені безпеки, подушки безпеки та інші засоби безпеки в автомобілях.

Це адресне розширення ринку не зупиняється на кордоні: Канада нещодавно прийняла CMMC для своєї оборонної промислової бази, а Японія також вимагатиме від державних підрядників відповідати правилам кібербезпеки США.

Тиск щодо виконання обов'язкових мінімумів кібербезпеки полягає не лише в отриманні федеральних контрактів. Міністерство юстиції активно шукає випадки шахрайства, використовуючи Закон про неправдиві заяви, щоб переслідувати шахрайство, пов'язане з кібербезпекою, державними підрядниками та одержувачами грантів. Справи почали накопичуватися, оскільки співробітники, які повідомляють про викривачі, вимагають великих винагород.

У жовтні минулого року на Університет штату Пенсільванія подав до суду колишній директор з інформації (CIO) за нібито неспроможність захистити CUI та фальсифікацію звітів про відповідність безпеці. Справа триває, але прецедент вже є. У липні минулого року Aerojet Rocketdyne погодилася заплатити 9 мільйонів доларів за вирішення подібної справи. Минулого року було виплачено понад 2,2 мільярда доларів США в рамках мирових угод і судових рішень у справах щодо неправдивих позовів, а понад 1,7 мільярда доларів США стосувалися галузі охорони здоров'я.

Щоб ще більше зміцнити рішучість уряду дотримуватись цих правил, він почав судитися з окремими компаніями та співробітниками за обман інвесторів, вводячи їх в оману щодо кібер-вразливості, як це робили SolarWinds та її колишній віце-президент із безпеки Тім Браун.

Кожна галузь економіки перебуває під дією трансформаційної директиви для зміцнення цифрового захисту. Позиція безпеки еволюціонувала з найвищого

ступеня до вирішального фактора, який впливає на кінцевий результат. Це не просто зміна політики – це зміна парадигми, яка робить дотримання кібербезпеки юридичним імперативом, оскільки його наслідки є більш далекосяжними, ніж будь-коли раніше». ***(Eric Noonan. A quiet cybersecurity revolution is touching every corner of the economy as U.S., allies 'pull all the levers' to face new threats // Fortune Media IP Limited (https://fortune.com/2023/12/20/quiet-cybersecurity-revolution-economy-us-allies-new-threats-regulation-politics-tech-eric-noonan/?utm_source=flipboard&utm_content=fortune%2Fmagazine%2FPersonal+finance). 20.12.2023).***

***

«Підприємства в енергетичній галузі підпадають під дію величезної кількості нормативних актів щодо звітності. На початку цього року Комісія з цінних паперів і бірж (SEC) завершила роботу над правилами щодо розкриття кібератак, додавши ще один рівень звітності для енергетичних компаній. Однак перед цим Конгрес прийняв Закон про звітність про кіберінциденти для критичної інфраструктури від 2022 року, який встановлював додаткові вимоги до звітності для певних охоплених суб'єктів, а також створив нову раду, доручену узгодити федеральні вимоги щодо звітності про інциденти.

Нові правила SEC щодо розкриття інформації про кібербезпеку

26 липня 2023 року SEC ухвалила остаточні правила та поправки (Остаточні правила) щодо обов'язкового розкриття інформації щодо управління ризиками кібербезпеки, стратегії, управління та звітування про інциденти. Починаючи з 5 вересня 2023 року, правила вимагають розкриття в режимі реального часу суттєвих інцидентів кібербезпеки, а також поточного розкриття інформації щодо управління ризиками кібербезпеки компанії, стратегії та управління, а також експертизи ради директорів з кібербезпеки.

Правила були прийняті для вирішення проблеми зростання поширеності кіберінцидентів, а також постійної залежності компаній від інформаційних систем і

значних і потенційно суттєвих витрат як на кіберзахист, так і на кіберінциденти, які в перспективі можуть вплинути на ціни акцій і акціонерна вартість.

Ключовим наслідком Остаточних правил є те, що компанії повинні мати процеси не лише для управління ризиками подій у сфері кібербезпеки, але й для оцінки суттєвості таких подій у короткий термін після їх виникнення. Важливо, що аналіз суттєвості повинен включати як кількісні, так і якісні оцінки. Крім того, Остаточні правила підтверджують, що «аналіз суттєвості більшості компаній включатиме розгляд фінансового впливу інциденту кібербезпеки».

Дати відповідності Остаточним правилам починаються в середині грудня 2023 року. Керівники кібербезпеки постраждалих компаній повинні враховувати наступне:

Достатність існуючої політики та практики кібербезпеки.

Адекватність і частота звітів ради з питань кібербезпеки.

Оцінка керівних принципів корпоративного управління компанії та статутів комітетів правління (і розгляд можливостей постійного навчання, якщо це необхідно)

Оцінка досвіду ради з питань кібербезпеки (і розгляд можливостей постійного навчання, якщо це необхідно)

Координація з керівництвом планування реагування на інциденти

Довгоочікуваний федеральний закон про повідомлення про кіберінциденти

У березні 2022 року президент Байден підписав закон про звітність про кіберінциденти для критичної інфраструктури 2022 року (CIRCIA), який вимагає від власників і операторів критичної інфраструктури повідомляти про кіберінциденти та виплати викупу Агентству з кібербезпеки та безпеки інфраструктури (CISA). CIRCIA встановлює 72-годинний термін для охоплених кіберінцидентів і 24-годинний термін для виплати викупу.

CISA було доручено розробити нормативні акти для заповнення прогалин у законі, який він розпочав із запиту на інформацію (RFI), опублікованого у Федеральному реєстрі у вересні 2022 року. RFI висвітлив кілька відкритих питань впровадження, зокрема застосовність, терміни звітності, гармонізацію з існуючими

нормативними вимогами, наслідками для третіх сторін, а також питаннями правозастосування та відповідальності. Варто зазначити, що CIRCIA надає CISA повноваження щодо виклику до суду та інші інструменти примусового виконання.

Тепер, коли CISA завершила свої «сеанси прослуховування» для отримання відгуків від громадськості та інших зацікавлених сторін, вона формалізує свою нормотворчу діяльність. Офіційне повідомлення про запропоновану нормотворення (NPRM) має бути надіслано до березня 2024 року, але, як повідомляється, воно випереджає графік. Остаточна норма має бути видана протягом 18 місяців після публікації НПРМ.

Гармонізація вимог до звітності про кіберінциденти

Підприємства в енергетичній галузі вже підпадають під численні вимоги щодо звітування про кіберінциденти, що збігаються, що призводить до розрізнених вимог, що обумовлені різними нормативними та політичними цілями, зокрема національною безпекою, громадською безпекою, захистом споживачів і акціонерів, а також прозорістю ринку. Вимоги до звітності також встановлюються на всіх рівнях влади — федеральному, штатному та місцевому — і включають як обов'язкову, так і добровільну звітність.

Щоб вирішити цю складну мережу правил, Конгрес у CIRCIA створив Раду зі звітування про кіберінциденти (CIRC) для координації, усунення конфліктів і узгодження федеральних вимог щодо звітування про інциденти. У своєму звіті CIRC всебічно оцінив 52 чинні або запропоновані федеральні вимоги до звітності про кіберінциденти. Було виявлено, що 45 вимог наразі діють у 22 установах.

Крім того, CIRC виявив значне дублювання для певних організацій, посилене застосуванням міжгалузевих нормативних вимог і добровільним звітуванням. Крім того, різні часові рамки та тригери для звітування про кіберінциденти становлять значні проблеми. Щоб упорядкувати звітність, CIRC надав кілька рекомендацій, зокрема такі:

Прийняти типове визначення кіберінциденту, про який можна повідомити, де це можливо.

Використовуйте типові терміни звітування про кіберінциденти та тригери, де це можливо.

Агентствам слід розглянути можливість затримки сповіщень.

Прийняти типову форму звітності для звітів про кіберінциденти, де це можливо.

Оптимізуйте отримання та обмін звітами про кіберінциденти та інформацією про кіберінциденти.

Вимоги до звітності повинні передбачати оновлення та додаткові звіти.

Застосовуйте спільну термінологію щодо звітування про кіберінциденти, де це можливо.

Удосконалення процесів взаємодії з особами, які звітують, після первинного звіту про кіберінцидент.

Примітка про штучний інтелект та майбутнє звітування про кіберінциденти

Організаціям, які відстежують кібератаки, часто важко відсіювати шум, включаючи атаки низького рівня, «помилкові спрацьовування» та просто величезну кількість даних. Це створює труднощі для отримання значущої та своєчасної інформації про потенційні кіберінциденти. Хоча історично для ініціювання заходів реагування на інциденти покладалися на людей-аналітиків і координацію SOC, деякі рішення на основі штучного інтелекту (AI) уже використовують моніторинг і машинне навчання для оптимізації операцій безпеки. Така розширена інтеграція штучного інтелекту в діяльність сортування та реагування на інциденти повинна призвести до більшої ефективності та допомогти у виявленні аномалій та автоматизованих реакціях.

Однак 30 жовтня 2023 року президент США Джозеф Байден видав розпорядження, яке вимагає від Національного інституту стандартів і технологій (NIST) розробити стандарти штучного інтелекту, щоб гарантувати, що системи є «безпечними, безпечними та надійними». Хоча остаточні стандарти ще належить визначити, вони, ймовірно, введуть застереження щодо використання штучного інтелекту в критичній інфраструктурі, особливо у спосіб, який може завдати шкоди

цій інфраструктурі через неправильне використання або непередбачуваність». ***(J. Daniel Skees, Celia A. Soehner and Arjun Prasad Ramadevanahalli. How New Cyber Incident Reporting Regulations Impact Energy Companies // Morgan, Lewis & Bockius LLP. (https://www.morganlewis.com/pubs/2023/12/how-new-cyber-incident-reporting-regulations-impact-energy-companies). 21.12.2023).***

***

«З 2021 року Міністерство юстиції (DOJ) дедалі більше зосереджується на розгляді справ, пов'язаних із Законом про неправдиві заяви (FCA) щодо недосконалих методів кібербезпеки. Оскільки уряд посилює контроль за конфіденційністю даних і кібербезпекою, стає все більш важливим розробляти та підтримувати надійні системи кібербезпеки, навчати працівників і забезпечувати належне управління ризиками. Витративши час на захист конфіденційності та кібербезпеки своїх даних, ви допоможете уникнути труднощів FCA в майбутньому.

Тенденції застосування кібербезпеки FCA

У 2021 році Міністерство юстиції оголосило про свою ініціативу щодо цивільного кібершахрайства. За допомогою FCA Міністерство юстиції розправляється з державними підрядниками та одержувачами грантів, які намагаються приховати порушення та не дотримуються необхідних стандартів кібербезпеки. Міністерство юстиції цитує наступне як частину своєї ініціативи:

Створення широкої стійкості до вторгнень у кібербезпеку в уряді, державному секторі та ключових галузевих партнерах;

Дотримання підрядниками та грантодавцями своїх зобов'язань щодо захисту державної інформації та інфраструктури;

Підтримка зусиль державних експертів щодо своєчасного виявлення, створення та оприлюднення виправлень уразливостей у широко використовуваних продуктах і послугах інформаційних технологій;

Забезпечення того, щоб компанії, які дотримуються правил і інвестують кошти у відповідність вимогам кібербезпеки, не знаходилися в невигідному конкурентному становищі;

Відшкодування уряду та платникам податків збитків, понесених через невиконання компаніями своїх зобов'язань щодо кібербезпеки;

Покращення загальної практики кібербезпеки принесе користь уряду, приватним користувачам і американській громадськості.

Ініціатива швидко призвела до активізації примусових дій згідно з FCA.

Примітно, що в березні 2022 року Міністерство юстиції швидко використало нову ініціативу в претензіях за участю Comprehensive Health Services LLC (CHS). CHS працювало з Державним департаментом і Військово-повітряними силами, щоб створити та підтримувати безпечну систему електронних медичних записів. Збережені записи включали особисту ідентифікаційну інформацію військовослужбовців, дипломатів і підрядників, які працюють в Іраку та Афганістані. Інколи CHS не вдавалося належним чином захистити записи, що робило їх доступними для персоналу поза клінікою. Незважаючи на занепокоєння, висловлене співробітниками CHS, компанія не вжила жодних заходів щодо забезпечення доступу до документів лише персоналу клініки. CHS отримав відносно невеликий штраф FCA ($930 000), щоб вирішити цю проблему.

Після CHS Міністерство юстиції звернулося до судового переслідування компанії Aerojet Rocketdyne, Inc. за її неадекватність кібербезпеки. Aerojet надав неправдиву інформацію щодо дотримання чинних правил придбання. Родич подав позов після того, як його звільнили за відмову підписати документи про те, що Aerojet відповідає вимогам. Aerojet врегулював претензії qui tam на 9 мільйонів доларів.

А в березні 2023 року Міністерство юстиції врегулювало звинувачення FCA проти Jelly Bean Communications Design LLC та її власника Джеремі Спінкса на 239 771 долар. Jelly Bean забезпечив дизайн та обслуговування веб-сайту для флоридського постачальника коштів Medicaid. Як підрядник, Jelly Bean підтримував веб-сайт, на якому батьки могли подати заявку на отримання страхового покриття для своїх дітей. Протягом шести років Jelly Bean не надавав оновлень і виправлень для свого програмного забезпечення для захисту даних. Їхня невдача призвела до компрометації понад 500 000 файлів і угоди FCA.

Кроки, які потрібно зробити

Поселення показують кілька тенденцій, щоб уникнути пасток FCA. По-перше, важливо мати спеціальну команду фахівців з кібербезпеки та конфіденційності даних, щоб переконатися, що системи та методи відповідають відповідним нормам. Відповідно, освіта всього персоналу є життєво важливою. Відповідність — це командна робота, і всі співробітники повинні знати нормативні стандарти, щоб залишатися сумісними. Ознайомтеся зі структурою кібербезпеки Національного інституту стандартів і технологій. Структура регулярно використовується агенціями як стандарт відповідних практик кібербезпеки. Виконання цих простих кроків може значно допомогти уникнути пасток FCA». ***(Peter Strickland. Avoiding the False Claims Act with Good Cyber Practices // Husch Blackwell LLP (https://www.contractorsperspective.com/false-claims-act/avoiding-the-false-claims-act-with-good-cyber-practices/). 21.12.2023).***

***

«Крадіжка інтелектуальної власності викликає серйозне занепокоєння для всіх компаній, але особливо для організацій оборонно-промислового комплексу, оскільки їхня інтелектуальна власність життєво важлива для національної безпеки. Загроза проникнення іноземних супротивників у внутрішні організації з метою досягнення власних цілей привернула увагу протягом останніх кількох років завдяки резонансним справам, таким як атака на ланцюжок поставок SolarWinds і звинувачення китайського бізнесмена у змові з метою викрадення комерційних секретів General Electric.

Ці загрози особливо неприємні для малого та середнього бізнесу, якому, як правило, не вистачає ресурсів кібербезпеки, щоб захистити себе. На щастя, існує все більше ресурсів, які ці компанії можуть використати для захисту своєї інтелектуальної власності.

На жаль, загрози оборонно-промисловій базі, або DIB, продовжують зростати. Цього року корпорація Майкрософт виявила досвідченого китайського загрозливого агента під назвою «Вольт Тайфун», який проникав у критично

важливу інфраструктуру США для збору інформації та шпигунства. Це лише один із багатьох прикладів китайських загроз кібербезпеці для американських компаній із спільною метою викрадення інтелектуальної власності іншої країни для отримання економічної вигоди китайським підприємствам.

У міру прискорення технологічного роз'єднання технологічних екосистем США та Китаю організаціям на всіх рівнях DIB доведеться посилити безпеку, щоб захистити свою інтелектуальну власність від цілеспрямованих вторгнень і атак на ланцюги поставок.

За деякими оцінками, для окремої компанії ІВ може становити до 80% її вартості. Це означає, що успішна кібератака, яка призведе до крадіжки IP-адреси, може призвести до кінця бізнесу, особливо для малого бізнесу. Крім того, за оцінками, індустрії з інтенсивним використанням ІВ забезпечують понад 45 мільйонів робочих місць у США, а крадіжка ІВ обходиться економіці США в 600 мільярдів доларів на рік, що свідчить про масштаби та вплив проблеми.

На щастя, уряд почав усвідомлювати серйозність цієї загрози та вжив заходів для її пом'якшення. У січні 2023 року був підписаний Закон про захист американської інтелектуальної власності. Цей закон має на меті накласти додаткові санкції на неамериканських суб'єктів, які займаються крадіжкою ІВ, але це стосується лише випадків викрадення ІВ. У червні 2023 року, визнаючи зростаючу загрозу кіберзлочинності проти компаній США, Міністерство юстиції отримало схвалення Конгресу на створення нового відділу національної кібербезпеки, який надає додаткові федеральні ресурси для виявлення та знищення сучасних постійних загроз кібербезпеці, націлених на DIB.

Хоча США інвестують у федеральні ресурси для пом'якшення кіберризиків, США також надають безкоштовні послуги з кібербезпеки підрядникам Міністерства оборони, які пропонуються через Агентство національної безпеки. Крім того, Агентство з кібербезпеки та безпеки інфраструктури, підрозділ Міністерства внутрішньої безпеки, надає різноманітні безкоштовні послуги з кібербезпеки для організацій, такі як сканування вразливостей і оцінка кібербезпеки (вони також доступні для компаній за межами DIB).

Нарешті, Центр боротьби з кіберзлочинністю Міністерства оборони має цілий підрозділ, який надає безкоштовну підтримку DIB, включаючи можливості кібербезпеки як послуги та аналіз кібервідмовостійкості для дозволених оборонних підрядників. Ці три послуги є особливо цінними для малого та середнього бізнесу в DIB, яким часто не вистачає надійних власних ресурсів кібербезпеки.

Через надлишок доступних ресурсів і незліченну кількість загроз може бути важко зрозуміти, з чого почати або що робити далі. На щастя, CISA також надає чудові рекомендації для малого бізнесу, які також виявилися найкращими кроками для будь-якого малого та середнього бізнесу в DIB.

По-перше, переконайтеся, що у вашій організації є призначена особа або команда з кібербезпеки, які можуть негайно визначити пріоритетність чотирьох заходів:

Переконайтеся, що багатофакторна автентифікація повністю реалізована для входу у ваші IT-системи, включаючи електронну пошту.

Переконайтеся, що всі технологічні системи регулярно оновлюються програмним забезпеченням.

Постійно створюйте резервні копії бізнес-даних і періодично перевіряйте, чи резервні копії дійсні, а відновлення працює.

Увімкніть шифрування даних на всіх IT-активах, включаючи ноутбуки, настільні комп’ютери та сервери.

По-друге, компанії в DIB повинні забезпечити розробку плану реагування на інциденти, який періодично переглядається та виконується. Цей крок допомагає гарантувати, що в разі неминучого інциденту підприємства зможуть швидко відновити роботу та з мінімальним впливом на бізнес. CISA надає ресурси про те, з чого почати розробку плану реагування на інциденти.

По-третє, організації в DIB повинні брати участь у періодичних настільних навчаннях з кібербезпеки. Знову ж таки, це підготовка, яка гарантує, що компанії найкраще підготовлені до якнайшвидшого відновлення після кіберінциденту, щоб мінімізувати наслідки. Федеральне агентство з управління надзвичайними

ситуаціями проводить постійні безкоштовні віртуальні настільні навчання з кібербезпеки, якими DIB може і повинен скористатися.

Підсумовуючи, загрози крадіжки інтелектуальної власності є постійними та зростають, особливо в DIB. Резонансні атаки на кібербезпеку, такі як злам SolarWinds і вторгнення Volt Typhoon, підкреслюють необхідність термінових дій для захисту ІВ — ІВ, яка є основою валового внутрішнього продукту США та національної безпеки США.

Хоча уряд вжив помітних заходів для протидії цим загрозам, компанії в DIB не можуть покладатися лише на законодавство та регулювання. На щастя, є багато ресурсів, якими компанії в DIB можуть скористатися, щоб зміцнити свій захист і захистити свої коштовності». ***(Noah Rivers, Jimmy Benoit. How to bolster security against intellectual property theft // Defense News (https://www.defensenews.com/opinion/2023/12/20/how-to-bolster-security-against-intellectual-property-theft/). 20.12.2023).***

***

Країни ЄС та Великобританія

«Щорічне опитування Softcat серед понад 4000 клієнтів-посередників у 2900 організаціях у Великобританії та Ірландії показало, що кібербезпека є головним пріоритетом для більш ніж половини.

Це другий рік поспіль, коли кібербезпека стала домінуючим напрямком, і 56 відсотків респондентів визнали її своїм головним пріоритетом.

Головний технолог з кібербезпеки Softcat Кірон Ньюшем сказав, що для організацій важливо не тільки визнавати важливість кібербезпеки, але й використовувати нові технології для відновлення та нормалізації після кіберінцидентів.

Цифровий робочий простір займає друге місце за пріоритетністю.

Опитування показало, що третина організацій (39 відсотків) наголошують на пристроях і обчисленнях кінцевих користувачів у наступному році.

Ця зміна визнає важливість оптимізації цифрових робочих просторів, використання генеративного штучного інтелекту для підвищення продуктивності, безпеки та стійкості в цифровому ландшафті, що постійно змінюється.

Дані займають третє місце в списку пріоритетів: 28 відсотків клієнтів приділяють їм увагу протягом наступних 12 місяців.

Мережі та підключення (25 відсотків), а також центри обробки даних і приватні хмари (18 відсотків) є найбільшими сферами інвестицій у технології.

Більше 48 відсотків опитаних хвилюють проблеми, пов'язані з людьми. Люди та культура лідирували в 70 відсотках, за ними йшли стійкість (68 відсотків) та різноманітність та інклюзивність (55 відсотків).

Примітно, що сталий розвиток значно зріс: порівняно з 2022 роком кількість респондентів, які визнають його головним пріоритетом, зросла більш ніж утричі (19 відсотків у 2022 році до 68 відсотків у 2023 році).

Комерційний ризик (40 відсотків), процеси (31 відсоток), технологічний досвід (30 відсотків) і закупівлі (26 відсотків) завершують список очікуваних проблем, демонструючи ландшафт, де організації повинні адаптуватися та впроваджувати інновації, щоб залишатися попереду.

Комерційний директор Softcat Річард Він Гріффіт сказав, що, застосовуючи виважений і стратегічний підхід, компанії можуть керувати ризиками, пов’язаними з новими технологіями, використовуючи можливості, які вони надають.

«Ми повинні залишатися проактивними в наших зусиллях із захисту від кіберзагроз, інтегрувати штучний інтелект у наші операції та створити цифрову стійкість», — сказав він». ***(Nick Farrell. Softcat’s annual survey talks up cyber security // Channel EYE (https://channeleye.co.uk/softcats-annual-survey-talks-up-cyber-security/). 04.12.2023).***

***

«Оскільки наступного місяця наближається остання сесія переговорів, приватний сектор і громадянське суспільство дедалі більше сумніваються в

сумісності проекту Конвенції ООН про кіберзлочинність із цінностями ЄС і стандартами прав людини.

Конвенція про кіберзлочинність, ініційована Росією та спочатку відхилена західними ліберальними демократіями, увійде в останній раунд переговорів на заключній сесії, запланованій на січень-лютий 2024 року в Нью-Йорку.

Поки що країни-члени ООН досягли консенсусу лише щодо кількох пунктів, тобто остаточне рішення, ймовірно, буде прийнято шляхом голосування.

Правозахисні організації стурбовані тим, що Спеціальний комітет, відповідальний за переговори щодо проекту тексту, не розглянув занепокоєння громадянського суспільства, про які вже було відомо у квітні.

«Ми не вважаємо, що позиція ЄС на переговорах сумісна з європейськими цінностями чи його інтересами», — сказав Нік Ештон-Харт, старший директор APCO Worldwide і представник Digital Trade Network (DTN) і делегат Великобританії на засіданнях ITU. Euractiv.

Єврокомісія на момент публікації не коментувала.

«Її нинішня позиція дозволяє кожному уряду в усьому світі вимагати доступу до особистої інформації громадян у всьому світі, включаючи стеження в режимі реального часу, щодо будь-якого злочину будь-якого роду онлайн або офлайн, з невеликими гарантіями та в умовах постійної повної секретності», – додала Ештон-Харт.

Оскільки проект тексту залишається нечітким за обсягом і формулюваннями, які посилаються на численні кримінальні злочини, пов’язані зі змістом, він не захищає права людини та вираження думки, попереджає громадянське суспільство.

«Поточний проект, який можна було б ухвалити шляхом голосування або серії голосувань, більше нагадує мрію авторитарного режиму, ніж інструмент для боротьби з онлайн-злочинністю та захисту жертв», — Ян Теннант, голова Віденського багатостороннього представництва Глобальної ініціативи проти Транснаціональна організована злочинність, повідомив Euractiv.

За словами Теннанта, це може призвести до придушення критиків уряду чи дисидентів і шпигування державними установами за людьми, які здійснюють

законну діяльність, яка нібито захищена міжнародним правом у сфері прав людини, наприклад дослідження, журналістика та адвокація.

Поточний стан переговорів

У поточній версії проекту тексту, з якою ознайомився Euractiv, зазначено, щодо яких параграфів країни-члени досягли консенсусу. Наприклад, держави погодилися зміцнювати «міжнародну співпрацю у запобіганні та боротьбі з кіберзлочинністю», нарощувати потенціал і утримуватися від втручання у внутрішні справи інших країн.

«Викликає розчарування той факт, що після кількох років і багатьох сесій над проектом Конвенції все ще пов'язаний із фундаментальними проблемами – не меншою мірою тому, що він досі не містить узгодженого визначення того, що є або не є кіберзлочином», – Барбора Буковська, ARTICLE 19 старший директор з права та політики, розповів Euractiv.

Наразі держави також досягли консенсусу щодо більшості частин юрисдикції, включаючи застосовність кримінальної юрисдикції відповідно до національного законодавства та конфіскації, заморожування або арешту активів за рішенням суду запитуючої іноземної держави.

Так само країни прийняли вимоги щодо запиту від іноземної держави на збереження комп'ютерних даних і розкриття даних трафіку, які стосуються кримінального розслідування. Вони погодилися, що користувач не повинен бути повідомлений про такий запит.

«У ньому також пропонуються положення, які дозволять широкий і нав'язливий обмін персональними даними між державами, фактично узаконюючи транскордонне спостереження», – додала Буковська.

Механізми перегляду та допоміжні органи для реалізації також були прийняті всіма державами.

Euractiv розуміє, що ЄС зараз намагається відтворити Будапештську конвенцію 2001 року, регіональну конвенцію про кіберзлочинність, підписану багатьма ліберальними демократіями та державами-членами ЄС.

Порівняно з Конвенцією двадцятиріччя тому, у версії на рівні ООН відсутні пояснювальні примітки, що детально описують права людини та зобов'язання щодо належної процесуальної процедури.

У той час як держави досягли консенсусу щодо механізмів перегляду та допоміжних органів для імплементації, експерти не вважають цю систему настільки ефективною, як це передбачено Будапештською конвенцією.

«Документ має бути повністю доопрацьований. Інакше, замість вирішення проблеми кіберзлочинності, це лише поставить під загрозу права людини», – підсумувала Буковська.

Однак, оскільки все ще існують розбіжності щодо багатьох частин проекту тексту, цілком імовірно, що якщо консенсусу не буде досягнуто, остаточне рішення вимагатиме голосування країн-членів ООН. Якщо досягнуто простої більшості, проект тексту приймається.

Наслідки

Хоча Конвенція ООН проти кіберзлочинності має на меті сприяти транскордонному співробітництву у відповідь на зростаючу кількість інцидентів кіберзлочинності, російська ініціатива здається простою та менш чутливою порівняно з Конвенцією ООН проти транснаціональної організованої злочинності, яка зайняла майже подвійну кількість сесій.

Враховуючи, що угода була ініційована країною-джерелом кіберзлочинності в усьому світі, «спрощення доступу до особистих даних для Росії та інших недемократичних держав — означало б для Росії велику дипломатичну перемогу. Здається, це прямо суперечить зовнішній політиці ЄС і цілям у сфері прав людини», – пояснила Ештон-Хард.

Переговори про кіберзлочинність розцінюють як намір Росії переформатувати міжнародний форум.

«Ця остання сесія переговорів може призвести до того, що Організація Об'єднаних Націй буде тихо переформована, щоб протистояти універсальним цінностям, на яких вона була заснована. Настав час для тих делегацій, включаючи ЄС та його держави-члени, які підтримують ці цінності, переконатися, що ми не

дійти до цього моменту», – підсумував Теннант». ***(Alina Clasen. UN Cybercrime Convention calls EU values into question, civil society warns // EURACTIV MEDIA NETWORK BV. (https://www.euractiv.com/section/cybersecurity/news/un-cybercrime-convention-calls-eu-values-into-question-civil-society-warns/?utm_source=flipboard&utm_content=EURACTIV%2Fmagazine%2FEURACTIV). 19.12.2023).***

***

«Європейська комісія оприлюднила 762,7 мільйона євро на фінансування цифрових рішень, включаючи кібербезпеку та штучний інтелект, у рамках своєї програми «Цифрова Європа».

Програма «Цифрова Європа» спрямована на зміцнення технологічного суверенітету Європи та виведення на ринок цифрових рішень для громадян, державних адміністрацій і підприємств, одночасно сприяючи досягненню цілей Європейської зеленої угоди.

За словами законодавців ЄС, через цю схему протягом наступних семи років буде інвестовано 7,5 мільярда євро…

Згідно з новим бюджетом на 2024 рік, майже 549 мільйонів євро буде спрямовано на проекти, які використовують цифрові технології, такі як суперкомп'ютери, дані, AI, хмара, кібербезпека та передові цифрові навички.

Це включатиме підтримку різних проектів у країнах, спрямованих на розвиток спільної європейської інфраструктури даних і послуг, надійних процесорів наступного покоління з низьким споживанням енергії та загальноєвропейського розгортання коридорів 5G.

Гроші також охоплюють придбання суперкомп'ютерів і квантових комп'ютерів, пов'язаних з Європейським високопродуктивним обчисленням (EuroHPC), а також розробку та розгортання надзахищеної квантової та космічної комунікаційної інфраструктури та розгортання мережі центрів безпеки.

У рамках цього пакету також буде нова підтримка для імплементації Закону ЄС про штучний інтелект та розвитку європейської екосистеми штучного інтелекту, включаючи фінансування для малого та середнього бізнесу (SMB).

Крім того, програма 2024 року запровадить нове початкове фінансування для пілотного проекту, спрямованого на демонстрацію повної інтеграції та сумісності Industrial IoT Edge із розробками Telco Edge, створення 3D-центру компетенції для сектору культурної спадщини та надання квантової бази метаболічні датчики МРТ для діагностики та лікування раку.

Другий фінансовий пакет, 214 мільйонів євро, спрямовується на кібербезпеку з метою підвищення колективної стійкості ЄС проти кіберзагроз.

Це фінансування підтримає загальноєвропейське виявлення кіберзагроз та обмін ними, імплементацію законодавства ЄС у сфері кібербезпеки, надзвичайну готовність до кібератак і взаємодопомогу, а також підтримку існуючих і нових національних координаційних центрів.

Роботу на цьому фронті виконуватиме Європейський центр компетенції з кібербезпеки, а національні координаційні центри виступатимуть у якості контактної точки між державами-членами та зацікавленими сторонами.

«Програма «Цифрова Європа» забезпечує лідерство та суверенітет Європи в цифрових технологіях. Вона спиратиметься на нещодавню угоду щодо Закону ЄС про штучний інтелект та сприятиме розвитку процвітаючої європейської екосистеми стартапів зі штучного інтелекту», — сказав комісар Тьєррі Бретон…» ***(Emma Woollacott. EU's Digital Europe Programme eyes major funding boost for AI, cyber security innovation // Future US, Inc. (https://www.itpro.com/business/policy-and-legislation/eus-digital-europe-programme-eyes-major-funding-boost-for-ai-cyber-security-innovation). 18.12.2023).***

***

Визнаючи мінливий характер кіберзагроз, інструкції спрямовані на те, щоб допомогти довіреним особам і менеджерам схем виконувати свої

обов'язки «оцінювати ризики, забезпечувати наявність засобів контролю та реагувати на інциденти».

Зокрема, TPR вперше закликав довірених осіб і постачальників схем добровільно повідомляти про значні кіберінциденти. Це демонструє зміну очікувань, оскільки TPR прагне до проактивної співпраці галузі для покращення розуміння та стійкості до кіберзагроз. Однак керівництво нагадує довіреним особам, що звітність до TPR доповнює, а не замінює існуючі юридичні зобов'язання, зокрема звітування про порушення персональних даних до Управління комісара з інформації (ICO).

Ці нові інструкції з кібербезпеки є бажаним оновленням від TPR, враховуючи, що попередні принципи кібербезпеки TPR датуються 2018 роком, з того часу зміни в ландшафті кібербезпеки для пенсійної галузі значно.

Нове керівництво стосується ключових аспектів запобігання, виявлення та реагування на кіберінциденти, наголошуючи на необхідності чітких структур управління, політики безпеки даних і технічного контролю. У подальшому він має на меті заохотити довірених осіб активно співпрацювати з відповідними сторонами, включаючи саму TPR, щоб забезпечити вжиття необхідних заходів для зменшення кіберризиків. У прес-релізі TPR від 11 грудня 2023 року Луїза Дейві, тимчасовий директор з питань регуляторної політики, аналізу та консультацій Пенсійного регулятора, прокоментувала, що:

«Ми хочемо, щоб індустрія відкрито та спільно співпрацювала разом і з нами, щоб протистояти викликам кіберзагроз і мати чіткий план, коли щось піде не так. Це зробить нас усіх більш стійкими до атак. У рамках цього ми хочу почути про кіберінциденти, щоб наше розуміння проблем покращилося в реальному часі»…» ***(Richard Pettit and Samantha Howell. An early Christmas present for pension scheme trustees: updated cyber security guidance from the Pensions Regulator // Burges Salmon (https://blog.burges-salmon.com/post/102iv5w/an-early-christmas-present-for-pension-scheme-trustees-updated-cyber-security-gu). 13.12.2023).***

***

«Міністерство юстиції Великобританії прагне зробити кожну критично важливу службу правосуддя стійкою до кібератак, забезпечивши «безпеку за дизайном» у всьому, що вона робить.

Воно висвітлило це як стратегічне бачення та мету своєї нової Стратегії кібербезпеки на 2023-2028 роки разом із вісьмома основними напрямками своєї роботи, щоб зробити їх досяжними.

У документі йдеться, що технологічний ландшафт Міністерства юстиції є складним і фрагментованим, із понад 1000 IT-сервісів, з яких менше 100 вважаються сучасними цифровими сервісами. Крім того, застарілі служби мають багато різних моделей підтримки, комерційних домовленостей і покладаються на різні основні технології; і містить понад 100 мільйонів файлів і понад 350 Тб неструктурованих даних.

Це створює потребу в деяких складних пріоритетних рішеннях щодо експлуатації існуючих систем, створення необхідних функцій і впровадження покращень безпеки.

Міністерству також доводиться вирішувати питання, характерні для його маєтку, наприклад підтримання безпеки разом із програмою In-Cell Technology для в’язниць.

«Ми знаємо, що для досягнення відмінної кібербезпеки потрібен час і потрібні узгоджені зусилля в цьому середовищі», — йдеться в документі.

Розвиток професії

Перший із восьми стовпів полягає у створенні та розвитку професії кібербезпеки всередині міністерства відповідно до визначень Урядової групи безпеки з програмами професійного розвитку та навчання для суміжних посад, таких як технічні архітектори та персонал DevOps.

Він також розглядатиме потенціал допомоги людям у в’язницях або на випробувальному терміні для розвитку кібернавички.

Друга складова передбачає створення позитивної культури безпеки шляхом подальшого розвитку мережі «чемпіонів безпеки», об’єднаних навчальних та

просвітницьких кампаній, які відповідають усім посадовим особам, і продовження роботи над відкритою політикою безпеки та вказівками.

По-третє, він прагне забезпечити «безпечні за дизайном» послуги з архітектурою безпеки, яка мінімізує довіру, необхідну для окремих компонентів, гарантуючи, що цифрові команди дотримуються цього підходу, і застосовує існуючі загальні моделі безпеки з автоматизованими огорожами. Він також братиме участь у підході «захищатися як один», продовжуючи обмінюватися матеріалами з іншими відділами.

Четвертий стовп полягає в тому, щоб продовжувати зміцнювати корпоративну власність Міністерства юстиції, покращуючи ідентифікацію та керування доступом, щоб більшість співробітників могли отримати доступ до критично важливих систем через єдину ідентифікацію, що забезпечується керуванням без пароля. Міністерство також перегляне свої можливості корпоративної безпеки та практики управління доступом, а також запровадить технічні рішення для персоналу, щоб керувати власною безпекою

Це супроводжуватиметься міграцією невеликої кількості вищевказаних ОФІЦІЙНИХ систем на міжурядову платформу Rosa.

Тестування, процеси, політики

П’ятий компонент полягає в забезпеченні ефективних операцій безпеки із заходами, включаючи оновлення підходу до регулярного тестування безпеки систем, а також процесів і політик щодо інцидентів. Також буде докладено зусиль, щоб підтвердити, що всі критично важливі системи часто резервуються в автономному режимі, а плани аварійного відновлення всебічно тестуються.

Шістий: мати впевненість у заходах безпеки шляхом покращення гарантій постачальників і партнерів, оновлення політик і процедур для підтримки безперервної гарантії та створення пілотних проектів GovAssure міністерства.

Сьомий, це ефективне управління ризиками кібербезпеки, включаючи визначення старшого відповідального власника для кожної IT-системи, гарантуючи, що вони разом із керівниками агентства та функціональними керівниками мають чітку відповідальність за безпеку. Також будуть оновлені

процеси та вказівки щодо ризиків, а також автоматизовано аналіз ефективності безпеки.

Восьмою опорою є забезпечення безпеки судової спільноти через розробку дорожньої карти та створення невеликої команди з політики в галузі кібернетики та правосуддя для співпраці з іншими департаментами.

Зміна ландшафту

«Важливо, щоб ми пам’ятали, що ландшафт не залишається статичним», – додається в документі. «Кіберзагрози будуть приходити і зникати, відділ адаптуватиметься до нових викликів і можливостей, технології, які ми використовуємо, будуть розвиватися, постачальники та партнери, з якими ми працюємо, змінюватимуться, як і наші люди.

«Рівень ризику кібербезпеки, який ми готові терпіти, також зміниться, як в агентствах і незалежних органах, так і на рівні підприємства. Тому важливо, щоб ми ефективно контролювали нашу кіберстійкість і прогрес у вдосконаленні». ***(Mark Say. MoJ highlights ‘secure by design’ for cyber security // Informed Communications Ltd. (https://www.ukauthority.com/articles/moj-highlights-secure-by-design-for-cyber-security/). 13.12.2023).***

***

«У Великобританії хронічно не вистачає кібернавичок. Компанії та навчальні заклади повинні працювати разом, щоб розпалити пристрасть дітей, пропонуючи нові можливості для навчання та практичне розуміння програм STEM. Це життєво важливо, якщо ми хочемо побачити довгострокове зростання сектору кібербезпеки.

У звіті про навички кібербезпеки на ринку праці Великобританії, опублікованому минулого року, було виявлено, що близько половини всіх підприємств мали прогалину в базових навичках кібербезпеки. Кількість оголошень про роботу в сфері кібербезпеки зросла на 30 відсотків до 160 000, хоча кіберробоча сила у Великобританії стикається з дефіцитом близько 11 200 осіб. Жінки складають лише 17 відсотків працівників у цьому секторі, тоді як на

керівних посадах зазвичай не представлено гендерне чи етнічне розмаїття в суспільстві.

Міністр кібернетики Віконт Кемроуз сказав: «Зростаючий кіберсектор Великої Британії — це місце, де почнуться технологічні інновації та цифрові відкриття майбутнього. Ось чому ми зосереджені на подоланні бар'єрів для входу та створенні нових можливостей для молодих людей отримати навички та знання, які могли б дати старт захоплюючій кар'єрі в кіберпросторі. Понад 2000 шкіл по всій країні вже підписані на Cyber Explorers, а це означає, що десятки тисяч учнів можуть скористатися пропонованими ресурсами – і ми хочемо переконатися, що цього року таку можливість отримають ще більше». Однак існує дефіцит кваліфікованих і впевнених учителів, і залишення навчання навичкам кібербезпеки середнім школам може не збільшити різноманітність абітурієнтів. Це повинно бути включено в початкову навчальну програму, щоб бути справді ефективним. Один проект в Ейлсбері показує, як це можна зробити.

Red Helix, провідний у Великій Британії постачальник послуг із керування кібербезпекою, заохочує дітей і дівчат розвивати кар'єру в галузі STEM і кібербезпеки через запуск клубу кодування в початковій школі. Він призначений для того, щоб дати їм першочерговий досвід реального застосування науки, технологій, інженерії та математики (STEM).

Клуб, який спочатку проводився для учнів 5-го та 6-го класів школи Елмхерст, пов'язаної з Great Learners Trust, був запущений влітку, щоб викликати у дітей інтерес до STEM з раннього віку. Однією з цілей було покращити соціальну мобільність, націливши програму на дітей початкових шкіл з вищими ставками учня. Діти початкової школи були одними з найбільше постраждалих від закриття шкіл через Covid-19, і збій мав значний вплив на дітей з нижчого соціально-економічного становища». ***(Anna Meyer. We Need To Take A Different Approach To Attract Young Talent To Cyber Security // Imaginative Minds Ltd. (https://www.teachingtimes.com/we-need-to-take-a-different-approach-to-attract-young-talent-to-cyber-security/). 11.12.2023).***

***

«…Кабмін Молдови сьогодні схвалив створення Національного агентства з кібербезпеки, повідомляє департамент комунікації уряду.

Установа матиме місію впровадження державної політики у сфері кібербезпеки з метою забезпечення високого рівня безпеки мереж та ІТ-систем постачальників послуг.

Буде сформовано групу реагування на кіберінциденти на національному рівні та створено єдиний національний контактний пункт, який забезпечуватиме взаємодію національних органів державної влади та установ з аналогічними органами в інших державах.

Установа відповідатиме за захист критичної інформаційної інфраструктури, ідентифікацію та фіксацію провайдерів послуг, запровадження обов'язкового механізму повідомлення про кіберінциденти, а також нагляд і державний контроль за дотриманням провайдерами послуг нормативної бази у сфері кібербезпеки.

Зі створенням Агентства стане можливим реалізовувати стратегії та політику, які зміцнюють національну безпеку та сприяють підвищенню рівня обізнаності та освіти громадян у кібербезпеці». ***(National Cyber Security Agency to be set up in Moldova // I.P. MOLDPRES A.I.S. (https://www.moldpres.md/en/news/2023/12/21/23010354). 21.12.2023).***

***

«Організаціям потрібно підготуватися, оскільки через 10 місяців наближається термін виконання переглянутої директиви на національному рівні.

Переглянута Директива про мережеві та інформаційні системи (NIS2), яка набула чинності 16 січня 2023 року та замінила Директиву про мережеві та інформаційні системи (NIS1), спрямована на усунення розбіжностей у реалізації скасованої NIS1.

Оновлена директива спрямована на все більш цифровий світ, у якому кібербезпека стала першорядною проблемою: із розвитком технологій зростають і

загрози, тому для організацій надзвичайно важливо зміцнювати захист кібербезпеки та забезпечувати відповідність нормам, що розвиваються.

NIS2 є значним кроком вперед у зміцненні стійкості кібербезпеки в Європейському Союзі (ЄС). Завдяки більш широкому охопленню, підходу, що ґрунтується на оцінці ризиків, і акценту на безпеці ланцюга поставок, NIS2 визнає цю загрозу, що розвивається, і критичну роль основних послуг і цифрової інфраструктури.

21-місячний період впровадження NIS2 у національне законодавство розпочався 16 січня 2023 року, протягом якого NIS2 має бути включено в національне законодавство. Країни-члени ЄС мають до 17 жовтня 2024 року транспонувати директиву у свої національні закони. Який прогрес був досягнутий серед держав-членів?

Нідерланди

У Нідерландах було оголошено, що проект акта про імплементацію NIS2 стане доступним десь у першому кварталі 2024 року. Після публікації проекту акта розпочнеться шеститижневий період консультацій в Інтернеті, який дозволить громадянам, організаціям та державним установам прокоментувати проект та запропонувати можливі вдосконалення.

Крім того, уряд Нідерландів опублікував інструмент на своєму веб-сайті, який дозволяє організаціям визначати, чи NIS2 застосовується до їхньої організації, чи є їхня організація «основною» або «важливою» організацією; і чи підпадає їх організація під голландський нагляд.

Інструмент також надає інформацію про кожну категорію секторів-підсекторів та організацій, до яких може застосовуватися NIS2. Незважаючи на те, що більшість інформації, включеної в інструмент, уже викладено в додатках до NIS2, він надає додаткову інформацію, яка може бути корисною для визначення того, чи вплине NIS2 на організацію.

Уряд Нідерландів у нещодавньому листі підтвердив, що всі рівні влади будуть визначені основними суб’єктами відповідно до закону про впровадження NIS2. Це включає незалежні адміністративні органи та регіональні органи влади,

такі як автономні адміністративні органи (zelfstandige bestuursorganen). Урядові організації, що належать до судової системи, парламенту та центрального банку, не підпадають під дію акта про впровадження NIS2.

Уряд Нідерландів радить організаціям почати впроваджувати заходи, пов'язані з кібербезпекою та NIS2.

Німеччина

Федеральне міністерство внутрішніх справ опублікувало дві версії проекту закону про впровадження NIS2 у законодавство Німеччини. Останній проект імплементаційного акту, опублікований у липні, пропонує зміни до кількох німецьких правових актів.

Його центром є нові версії Закону про Федеральне відомство з інформаційної безпеки – BSI Act – і кілька адміністративних постанов (Verordnungen), які додатково конкретизують BSI Act (адміністративні норми та BSI Act вже служать для імплементації керівних принципів NIS1). У вересні 2023 року Міністерство внутрішніх справ опублікувало неофіційний документ для обговорення розділів нового проекту закону BSI.

Судячи з поточного Закону про імплементацію, схоже, що німецький законодавець вирішить застосовувати NIS2 суворіше, ніж цього вимагають самі керівні принципи (тобто, поза межами мінімальної гармонізації).

Німеччина розширить сферу регульованих організацій порівняно з NIS2; наразі Німеччина визначила організації, які регулюються NIS1, залежно від того, чи надають вони «критично важливі» послуги приблизно 500 000 людей у Німеччині. Він регулював більше суб'єктів, ніж вимагає NIS1.

З NIS2 деякі з тих раніше регульованих організацій у Німеччині теоретично можуть випасти з-під регулювання. Однак поточні німецькі проекти вводять третю категорію на додаток до «суттєвих» і «важливих» суб'єктів, які регулюються NIS2. У цій категорії проекти планують продовжити регулювання колишніх «критичних інфраструктур». Більше суб'єктів підпадає під дію зобов'язань щодо IT-безпеки в Німеччині, ніж вимагає сфера NIS2.

Нинішні проекти дозволяють Міністерству внутрішніх справ вимагати обов'язкову сертифікацію кібербезпеки для певних послуг. NIS2 лише дозволяє, але не вимагає від держав-членів запроваджувати обов'язкову сертифікацію.

Реалізація в Німеччині міститиме вимогу до суб'єктів третьої категорії («критичні об'єкти») кожні три роки надавати Федеральному відомству з інформаційної безпеки відповідні докази відповідних технічних та організаційних заходів безпеки ІТ.

Однак проект Акту впровадження ще може бути суттєво змінений. Зараз він перебуває на ранній стадії законотворчого процесу як внутрішній документ, який проходить обговорення у відповідних міністерствах (Referentenentwurf). Він ще не був схвалений федеральним урядом і не поданий до парламенту як офіційний проект, який би розпочав офіційну законодавчу процедуру. Навіть після прийняття Закону про імплементацію Закон BSI залишатиметься абстрактним. Міністерство внутрішніх справ повинно буде визначити важливі деталі нового Закону BSI в кількох адміністративних постановах (Verordnungen) після того, як він набуде чинності.

Франція

Французьке національне агентство з безпеки інформаційних систем (ANSSI) відповідає за NIS2 у Франції. ANSSI зазначив, що законопроект про транспозицію у Франції все ще розробляється, і щоб вкластися в крайній термін 17 жовтня 2024 року, він розпочав консультації із зацікавленими сторонами в другій половині 2023 року. ANSSI наполягав на умовах «спільного будівництва» із зацікавленими сторонами щодо впровадження заходів безпеки та намагався обговорити методи, терміни, механізми припущень тощо.

ANSSI зазначив, що підприємства, які вже регулюються NIS1, повинні продовжувати свої зусилля, щоб підготуватися, тоді як нові організації можуть почати готуватися, звернувшись до посібників, уже доступних на його веб-сайті, де є спеціальна сторінка NIS2 із запитаннями та відповідями. Рекомендації базуються на загальних рекомендаціях ЄС і стосуються управління, захисту та стійкості ІТ.

Італія

Італія запровадить NIS2 законодавчим указом, ухваленим урядом, який буде уповноважений парламентом через закон про делегування. 27 липня 2023 року новий проект Закону про європейське представництво на 2022-2023 роки був поданий до парламенту.

У проекті зазначені критерії, якими має керуватися уряд при прийнятті законодавчого указу. Вони включають параметри для ідентифікації державних установ, на які поширюється дія NIS2, а також конкретних державних і приватних організацій, що надають послуги державним установам у секторах, звільнених від застосування NIS2. Вони також включають механізми реєстрації «важливих» або «важливих» суб'єктів, а також повноваження Агентства цифрової Італії та Національного агентства кібербезпеки.

Оскільки проект ще обговорюється, критерії можуть бути змінені. Уряд має прийняти законодавчу постанову до 17 червня 2024 року, якщо закон про делегування не набуде чинності після цієї дати. На цьому дуже ранньому етапі не можна виключати, що фактичне впровадження NIS2 може відбутися після 17 жовтня 2024 року.

Іспанія

Хоча NIS2 також має бути запроваджено в Іспанії до 17 жовтня 2024 року, наразі немає проектів законодавчих актів чи офіційних керівних документів щодо транспонування директиви. Цей процес транспонування все ще перебуває на дуже попередніх стадіях, і конкретні деталі щодо термінів і введення в дію очікують на подальший розвиток законодавства.

Польща

У Польщі в останні роки проводилася законодавча робота щодо внесення змін до Закону про національну систему кібербезпеки (NCSS), який є польською реалізацією NIS1.

Поправка також розглядає деякі вимоги та рішення, введені в NIS2. Однак повна імплементація не відбудеться до наступної ітерації Закону про NCSS, яка запланована на кінець 2024 року. Проект, разом з іншими законами про нові

технології, наразі знято з подальшого розгляду. Ймовірно, це пов’язано з парламентськими виборами в Польщі, які відбулися 15 жовтня 2023 року.

Впровадження NIS2 призупинено, але очікується, що воно відновиться на новому терміні польського парламенту, Сейму, на початку 2024 року.

Бельгія

Під керівництвом Центру кібербезпеки Бельгії (CCB) бельгійська влада представила проект закону, який встановлює основу для NIS2, і імплементаційний королівський указ про транспонування цієї директиви. Пропозиції вже отримали початкове схвалення від Ради міністрів Бельгії та пройдуть подальший розгляд Державною радою та Бельгійським органом із захисту даних. Крім того, прем’єр-міністр доручив CCB організувати публічні консультації щодо попереднього проекту закону разом із супровідним проектом імплементаційного королівського указу. CCB опублікував проект пояснювальної записки, а консультації завершилися для коментарів 21 грудня 2023 року.

Швеція

У 2018 році Швеція перетворила NIS1 на власне законодавство через «Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster». NIS2 знаходиться в процесі впровадження в шведське законодавство. 23 лютого 2023 року уряд Швеції призначив спеціального слідчого в Міністерстві оборони, щоб запропонувати адаптації шведського законодавства, необхідні для імплементації директиви.

Спеціальний слідчий звітуватиме перед урядом Швеції до 23 лютого 2024 року. Слідчий запропонує, як має регулюватися ідентифікація та вимоги до суб’єктів, які охоплюються NIS2, а також як розподілятимуться ролі між органами влади Швеції щодо обов’язків та обов'язки, передбачені в NIS2.

Також буде проведено аналіз того, як NIS2 має працювати разом із шведськими правилами захисту безпеки та запропонованими змінами для досягнення більш узгодженої системи між правилами. Слідчий розгляне необхідність більш сильного та комплексного захисту конфіденційності даних, які

можуть оброблятися відповідно до NIS2, і подасть пропозиції щодо необхідних конституційних поправок.

До звіту спеціального дослідника в лютому не надходило жодних оновлень щодо статусу реалізації NIS2.

NIS2 покращує NIS1

NIS2 вносить важливі зміни та вдосконалення в NIS1. Він ширший за обсягом і має підхід, що ґрунтується на оцінці ризику. Він наголошує на безпеці ланцюга постачання та запроваджує суворіше звітування про інциденти та відповідальність керівництва за недотримання вимог кібербезпеки згідно з NIS2. Це також посилює національний регуляторний нагляд.

Більш широкий діапазон

У той час як NIS1 в основному зосереджена на безпеці мережевих та інформаційних систем для основних і життєво важливих послуг, NIS2 розширює сферу діяльності на такі організації, як сектор водопостачання та розподілу (наприклад, оператори стічних вод), послуги з виробництва продуктів харчування та цифрові послуги, такі як хмарні обчислення. Крім того, уряди можуть призначати мікро- або малі організації, такі як служби, які мають життєво важливе значення для національної економіки чи суспільства.

Ризик-орієнтований підхід

NIS2 використовує підхід до кібербезпеки, який більшою мірою ґрунтується на ризиках, вимагаючи від організацій ефективної оцінки та управління ризиками, а не дотримання універсальних заходів безпеки. Це вимагає від основних і важливих суб’єктів принаймні впровадження:

Процедури врегулювання інцидентів.

Процедури управління резервним копіюванням та управління кризовими ситуаціями.

Використання багатофакторної аутентифікації.

Політики аналізу ризиків та безпеки інформаційних систем.

Політика та процедури використання криптографії та шифрування.

Безпека ланцюга поставок

NIS2 наголошує на важливості безпеки ланцюга постачання, зобов'язуючи компанії забезпечувати безпеку своїх цифрових ланцюгів постачання та оцінювати кібербезпеку своїх постачальників.

Суб'єкти, які підпадають під дію NIS2, повинні запровадити відповідні та пропорційні технічні, організаційні та операційні заходи для забезпечення безпеки ланцюга постачання.

Звіт про інцидент

Суворіші вимоги щодо звітування про інциденти передбачають коротші терміни подання серйозних інцидентів до компетентних органів, щоб забезпечити швидке реагування на кіберзагрози.

Організації повинні повідомляти про всі значні інциденти кібербезпеки призначеній національній групі реагування на інциденти комп'ютерної безпеки або компетентному національному органу (залежно від того, як це влаштовано відповідно до національних імплементаційних актів).

Управлінська відповідальність

Керівники організацій, до яких застосовується NIS2, можуть бути притягнуті до особистої відповідальності, якщо буде виявлено, що вони не вжили належних заходів для забезпечення відповідності вимогам кібербезпеки згідно з переглянутою директивою.

Відповідальність може виникнути, якщо директори недбало виконують свої обов'язки щодо безпеки мережевих та інформаційних систем, і це призводить до серйозних інцидентів або порушень. Це також може виникнути, коли директори не гарантують, що їхня організація відповідає конкретним зобов'язанням, викладеним у NIS2, таким як оцінка ризиків, звітування про інциденти та співпраця з національними органами.

Особиста відповідальність зазвичай виникає лише у випадках серйозної недбалості або навмисної неправомірної поведінки. Таким чином, директори повинні бути старанними у нагляді за зусиллями своєї організації щодо кібербезпеки та забезпечувати дотримання NIS2, щоб мінімізувати ризик особистої відповідальності.

Посилений регуляторний нагляд

Директива наділяє національні регуляторні органи розширеними можливостями нагляду та правозастосування, забезпечуючи дотримання бізнесом її положень.

До яких підприємств застосовується NIS2?

NIS2 застосовується до широкого кола підприємств і організацій і охоплює як державні, так і приватні установи, які працюють в ЄС, класифіковані як «необхідні» або «важливі».

Оператори основних послуг надають послуги, необхідні для забезпечення критичної соціальної та економічної діяльності. Вважається, що основні суб'єкти мають більш руйнівний вплив на економіку та суспільство, якщо їхні послуги не працюють порівняно з важливими суб'єктами.

Організація вважається важливою юридичною особою, якщо вона є великою та працює в секторі, викладеному в додатку 1 NIS2, наприклад, енергетика, транспорт, охорона здоров'я та фінансові послуги. Організація є великою, якщо вона має щонайменше 250 співробітників або річний обіг понад 50 мільйонів євро, а загальний баланс понад 43 мільйони євро або обидва.

Якщо організації визначено як критично важливу юридичну особу відповідно до Директиви щодо стійкості важливих юридичних осіб, вони також автоматично вважаються основними юридичними особами відповідно до NIS2. Це організації середнього розміру, які працюють у секторах, зазначених у додатку 1, і мають щонайменше 50 співробітників або річний оборот і загальний баланс понад 10 мільйонів євро або те й інше.

Середні та великі організації, що працюють у секторі, викладеному в додатку 2 NIS2, також кваліфікуються як важливі організації. До них належать, наприклад, управління відходами, поштові та кур'єрські послуги, а також виробники медичних приладів.

Уряд Нідерландів опублікував інструмент для підприємств, щоб визначити, чи застосовується до них NIS2, і надає більше інформації про категорії підгалузей і організацій. Очікується, що інші країни ЄС з часом нададуть подібні інструменти

чи рекомендації…» ***(Joanne Zaaijer, Doddy Wolfs, Adrian Schneider, Gregoire Dumas, Benjamin Docquir, Margo Cornette, Roger Segarra, Rafael García del Poyo, Antonio Cabrera, Henrik Bergström, Szymon Ciach and Gianluigi Marino. What EU businesses need to know about NIS2 and cybersecurity compliance // Osborne Clarke (https://www.osborneclarke.com/insights/what-eu-businesses-need-know-about-nis2-and-cybersecurity-compliance). 21.12.2023).***

***

«Постійні представники держав-членів Європейського Союзу в середу досягли попередньої згоди щодо регламенту про кіберсолідарність, який передбачає посилене реагування на кіберінциденти й кіберспівпрацю в ЄС.

Про це, як пише «Європейська правда», сповістила пресслужба Ради ЄС.

Проєкт регламенту передбачає створення «Європейського кіберщита» – загальноєвропейської інфраструктури, що складається з національних і транскордонних оперативних центрів безпеки по всьому ЄС. Їхнім завданням буде виявлення кіберзагроз та реагування на них.

У своїй роботі учасники «кіберщита» використовуватимуть найсучасніші технології, такі як штучний інтелект та передову аналітику даних. А органи влади та відповідні організації зможуть ефективніше й оперативніше реагувати на серйозні інциденти, кажуть у Раді ЄС.

Проєкт регламенту також передбачає створення механізму реагування на кібернетичні надзвичайні ситуації для підвищення готовності та посилення можливостей реагування на інциденти в ЄС.

Пропозиції постпредів до проєкту Єврокомісії стосувались насамперед уточнення термінології та функцій, наголосі на добровільній участі держав-членів у «Європейському кіберщиті», а також узгодження з іншими актами ЄС у сфері кібербезпеки.

Тепер Рада ЄС буде вести переговори з Європейським парламентом для узгодження остаточної версії регламенту.

Загальний бюджет усіх заходів, передбачених регламентом ЄС про кіберсолідарність, становить 1,1 мільярда євро, з яких близько двох третин будуть профінансовані через програму «Цифрова Європа»…» ***(У ЄС попередньо погодили створення «Європейського кіберщита» // Європейська правда (https://www.eurointegration.com.ua/news/2023/12/20/7175945/). 20.12.2023).***

***

«30 листопада 2023 року ЄС зробив рішучий крок до посилення кібербезпеки в ланцюжку постачання Інтернету речей (IoT), досягнувши політичної угоди щодо Закону про кібернетостійкість (CRA). CRA накладе низку зобов'язань щодо кібербезпеки на виробників, імпортерів і дистриб'юторів «продуктів із цифровими елементами», включаючи радіоняні, розумні годинники, комп'ютерні ігри, брандмауери, маршрутизатори та багато іншого.

Класифікація продукції: гранулярний підхід до оцінки ризику

CRA запроваджує систему класифікації продуктів, яка поділяє продукти з цифровими елементами на класи критичності на основі їх потенційного впливу на кібербезпеку:

Клас критичності I: цей клас охоплює продукти, які потенційно можуть завдати значної шкоди людям, майну чи навколишньому середовищу, якщо вони піддані розповсюдженню. Приклади включають операційні системи, менеджери завантаження, мікропроцесори, системи керування ідентифікацією, мікроконтролери з функціями безпеки та спеціальними схемами програм, системи керування мережею, мережеві пристрої, менеджери паролів, маршрутизатори, програмне забезпечення для видачі цифрових сертифікатів, програмне забезпечення для виявлення шкідливих програм, системи для керування інформацією та подіями безпеки, споживчими продуктами та віртуальними приватними мережами (VPN).

Клас критичності II: цей клас складається з продуктів, які створюють ще більші ризики для кібербезпеки через їхню функціональність, пов'язану з кібербезпекою, і призначене використання в чутливих середовищах, таких як

промислові установки. Приклади включають системи виконання контейнерів, брандмауери, гіпервізори та мікропроцесори та контролери із захистом від несанкціонованого доступу.

Клас критичності III: дуже критичні продукти, що підпадають під цей клас, можуть бути визначені Європейською комісією шляхом делегованих актів. Цей клас призначений для охоплення продуктів, які використовуються основними суб'єктами згідно з Директивою NIS2 2022/2555, або продуктів, які мають велике значення для стійкості загального ланцюга постачання продуктів із цифровими елементами до руйнівних подій. Система класифікації гарантуватиме, що продукти з вищими потенційними ризиками піддаються суворішим заходам, особливо коли мова йде про демонстрацію відповідності продуктів основним вимогам безпеки CRA.

У той час як відповідність основним вимогам безпеки CRA в основному можуть оцінювати виробники (на основі процедури внутрішнього контролю виробництва), така самосертифікація може застосовуватися лише до продуктів, що належать до класу критичності I, якщо гармонізовані стандарти, спільні специфікації або європейська кібербезпека схеми сертифікації будуть повністю доступними та застосованими. Якщо це не так, уповноважений орган повинен бути залучений до процедури оцінки відповідності. Така участь третіх сторін у будь-якому випадку буде обов'язковою для продуктів класу критичності II. Нарешті, для дуже критичних продуктів виробники повинні будуть отримати європейський сертифікат кібербезпеки за європейською схемою сертифікації кібербезпеки.

Основні вимоги безпеки

CRA встановлює набір важливих вимог безпеки, яких виробники повинні дотримуватися для своїх цифрових продуктів. Ці вимоги спрямовані на мінімізацію ризиків кібербезпеки шляхом усунення ключових вразливостей безпеки з самого початку. Основні вимоги безпеки включають:

Захищена конфігурація за замовчуванням: продукти повинні постачатися з конфігурацією захищеної за замовчуванням, що дозволяє користувачам легко скинути їх до початкового стану, якщо це необхідно.

Захист від несанкціонованого доступу: мають бути встановлені відповідні механізми контролю, включаючи автентифікацію, ідентифікацію або системи керування доступом.

Конфіденційність: дані, які зберігаються, передаються або обробляються продуктом, повинні бути захищені за допомогою шифрування, як у стані спокою, так і під час передачі, щоб забезпечити їх конфіденційність.

Цілісність: Дані, що зберігаються, передаються або обробляються продуктом, а також команди, програми та конфігурація повинні бути захищені від маніпуляцій або модифікацій, не дозволених користувачем.

Мінімізація даних: продукти мають збирати та обробляти лише ті дані, які суворо необхідні для їхнього використання за призначенням, зводячи до мінімуму кількість особистих чи інших даних, які обробляються.

Доступність: основні функції мають бути стійкими до атак типу «відмова в обслуговуванні».

Обмеження поверхні атаки: продукти мають бути розроблені з обмеженою поверхнею атаки, мінімізуючи потенційні точки входу для кібератак.

Управління вразливими місцями. Повинні існувати механізми для своєчасного й ефективного виправлення вразливостей для вирішення нових загроз кібербезпеці.

Безпека за проектом: впровадження кібербезпеки протягом усього життєвого циклу продукту

CRA наголошує на принципі «безпеки за проектом», вимагаючи від виробників включати питання кібербезпеки на кожному етапі життєвого циклу продукту, від планування та проектування до розробки, виробництва, доставки та обслуговування. Цей цілісний підхід спрямований на те, щоб у першу чергу запобігти вразливостям у продуктах, зменшуючи загальний ризик кібербезпеки.

Крім того, виробники будуть зобов’язані постійно та систематично визначати та документувати відповідні аспекти кібербезпеки. Вразливості необхідно ефективно усунути протягом усього життєвого циклу продукту, що включає пов’язане з ризиком зобов’язання негайно усунути вразливі місця в безпеці

(зокрема, шляхом надання оновлень). Щоб забезпечити це, CRA вимагатиме від виробників впровадження відповідних внутрішніх процесів для обробки та усунення потенційних вразливостей, включаючи встановлення контактної точки.

Зобов'язання щодо звітності: сприяння прозорості та своєчасному реагуванню

Щоб підвищити прозорість і сприяти своєчасному реагуванню на загрози кібербезпеці, CRA вводить зобов'язання щодо звітності для виробників. Виробники зобов'язані повідомляти про активно використовувані вразливості відповідному національному органу та Агентству Європейського Союзу з кібербезпеки (ENISA). Цей механізм звітування призначений для швидкої координації та реагування на критичні вразливості, мінімізуючи потенційну шкоду для користувачів.

Програмне забезпечення з відкритим кодом: індивідуальні вимоги до підвищеної безпеки

Усвідомлюючи складність і різноманітність моделей розробки програмного забезпечення з відкритим кодом, CRA прийняла диференційований підхід до вирішення проблем кібербезпеки. Програмне забезпечення з відкритим вихідним кодом, розроблене під егідою допоміжної організації, такої як Linux Foundation або Apache Software Foundation, підпадає під спрощені вимоги, включаючи спрощені процедури оцінки відповідності та режим пом'якшених санкцій.

Щоб відрізнити програмне забезпечення з відкритим кодом, розроблене під егідою організації, що підтримує, та інше програмне забезпечення з відкритим кодом, CRA вводить концепцію «спільно розробленого під егідою організації, що підтримує». Цей термін застосовується до програмного забезпечення з відкритим кодом, яке відповідає таким критеріям:

Програмне забезпечення розробляється групою осіб або організацій, які співпрацюють над проектом.

Програмне забезпечення випускається за безкоштовною ліцензією з відкритим кодом.

Організація підтримки надає ресурси та підтримку для розробки програмного забезпечення.

Програмне забезпечення з відкритим кодом, яке не відповідає цим критеріям, підлягатиме тим самим вимогам, що й інші продукти з цифровими елементами. Ця відмінність має на меті знайти баланс між безпекою та сприянням сприятливого середовища для розробки з відкритим кодом.

Терміни та впровадження: стандартизація та адаптація до нового ландшафту

Завершення розробки тексту CRA має прокласти шлях для прийняття та публікації CRA в Офіційному журналі Європейського Союзу до виборів до Європейського парламенту в червні 2024 року. Після набуття чинності виробники, імпортери та дистриб'ютори матимуть три роки, щоб адаптуватися до нових вимог. Коротший 21-місячний перехідний період застосовується до зобов'язань звітувати про інциденти та вразливості.

Є надія, що керівні документи та, перш за все, гармонізовані стандарти для охоплених категорій продукції будуть доступні з достатнім часом до того, як нові вимоги стануть застосовними. Це навіть важливіше, оскільки гармонізовані стандарти є обов'язковою умовою для самостійної сертифікації продуктів, які входять до класу критичності I.

З огляду на широку сферу застосування CRA, ймовірно, буде розпочато стандартизаційний марафон, у рамках якого поточні зусилля зі стандартизації відповідно до Делегованого регламенту 2022/30 до Директиви про радіообладнання можна, принаймні частково, використати». ***(Márton Domokos, Dóra Petrányi, Tom De Cordier, Anna Horvath, Michael Biendl, Deven Dobbelaere, Valeska De Pauw and Thomas Dubuisson. With EU Cyber Resilience Act, EU gets tough on IoT supply chain cybersecurity // CMS Legal (https://cms-lawnow.com/en/ealerts/2023/12/with-eu-cyber-resilience-act-eu-gets-tough-on-iot-supply-chain-cybersecurity?utm_source=lawnow-realtime&utm_medium=email&utm_campaign=With%20EU%20Cyber%20Resilience%20Act,%20EU%20gets%20tough%20on%20IoT%20supply%20chain%20cybersecurity&utm_id=2535&utm_term=read_more&utm_content=664828). 13.12.2023).***

***

«Недавнє дослідження, проведене Apple (NASDAQ: AAPL) з Массачусетського технологічного інституту (MIT), підкреслило тривожну тенденцію в кібербезпеці, особливо в Австралії.

Незважаючи на значне розширення Apple практик шифрування даних і запуск Advanced Data Protection для iCloud, кібератаки не вщухають.

Насправді витоки даних посилилися, і у вересні цього року їх стало більше, ніж за весь 2022 рік.

Австралія - чотири головні глобальні цілі

Дослідження Массачусетського технологічного інституту поміщає Австралію в четвірку найбільших глобальних цілей для хакерів, поступаючись лише Сполученим Штатам, Великобританії та Канаді.

Відомі кібератаки в Австралії скомпрометували такі великі компанії, як Medibank, Optus, Latitude Financial і Australian Clinical Labs.

Серйозність цих порушень підкреслюється розголошенням конфіденційної інформації про клієнтів, включаючи записи про стан здоров’я та особисті дані, у темній мережі.

Прихильники зашифрованого зберігання персональних даних

Стюарт Меднік, професор інформаційних технологій Массачусетського технологічного інституту, наголосив на ризиках, пов’язаних з компаніями, які зберігають конфіденційні дані в незашифрованому, читабельному форматі: «Поки організації продовжують збирати незашифровані особисті дані, хакери мотивовані продовжувати знаходити нові способи отримати це", - сказав він.

Він виступає за зменшення обсягу особистих даних, що зберігаються в читабельному форматі, і збільшення зусиль із захисту конфіденційних даних споживачів.

Звіт Массачусетського технологічного інституту показує, що з 2013 по 2022 рік кількість витоків споживчих даних зросла в три рази, лише у 2023 році було зламано 2,6 мільярда особистих записів.

Кількість атак на хмарну інфраструктуру з 2021 по 2022 рік майже подвоїлася, і на них припадає понад 80% зломів.

Без бекдорів для Apple

Apple у відповідь на ці загрози посилила захист даних, що засмутило правоохоронні органи.

Компанія стверджує, що вона ніколи не створювала бекдор для своїх продуктів або послуг, а також не дозволяла уряду прямий доступ до своїх серверів.

Цей суворий підхід до безпеки ускладнює виконання запитів правоохоронних органів на доступ до даних.

Мобільні телефони - основна ціль

Мобільні телефони, головна мішень для хакерів, містять велику кількість особистої інформації.

iCloud від Apple за замовчуванням використовує наскрізне шифрування для 14 категорій конфіденційних даних і для 23 категорій із увімкненим розширеним захистом даних.

Джулі Інман Грант, уповноважений з електронної безпеки, визнає складність проблеми, заявляючи, що, хоча компанії, які надають послуги з наскрізним шифруванням, не звільняються від відповідальності, від них не очікується створення систематичних уразливостей у своїх службах.

Вона навела WhatsApp від Meta як приклад служби, яка активно працювала над боротьбою з онлайн-зловживаннями без порушення шифрування.

Ця ситуація підкреслює нагальну потребу в надійних заходах кібербезпеки та відповідальних методах управління даними для захисту від зростаючої загрози кібератак». ***(Australia's cybersecurity crisis: unencrypted data creates a haven for hackers, says Apple // Fusion Media Limited (https://au.investing.com/news/stock-market-news/australias-cybersecurity-crisis-unencrypted-data-creates-a-haven-for-hackers-says-apple-3058586?utm_source=flipboard&utm_content=InvestingAus%2Fmagazine%2FAustralia+Financial+Markets). 08.12.2023).***

***

«У Новому році кібербезпека спостерігатиме найбільше збільшення інвестицій у технології серед IT-директорів і керівників Австралії та Нової Зеландії.

Згідно з дослідженням Gartner, 87 відсотків IT-директорів і керівників технологій у A/Новій Зеландії найбільше інвестують у простір кібербезпеки, особливо в умовах посилення регулювання та розширення загроз.

«Хоча цього року значну увагу було приділено генеруючому штучному інтелекту (GenAI), кібербезпека знову залишається на першому місці в списку інвестицій, враховуючи широко розголошені витоки даних, які ми бачили в A/Новій Зеландії за останні 12 місяців», Про це заявив аналітик Gartner Енді Роуселл-Джонс.

«Комітети з ризиків і аудиту кожної організації стурбовані потенційними наслідками для кібербезпеки, і більшість галузевих регуляторів активно наполягають на покращенні компетенції».

Опитування Gartner CIO and Technology Executive Survey 2024 зібрало дані від 2457 респондентів у 84 країнах, у тому числі 87 у A/Новій Зеландії, у державному, приватному та некомерційному секторах.

За кібербезпекою очікується, що 79 відсотків IT-директорів Нової Зеландії спрямують найбільшу суму нового або додаткового фінансування у 2024 році на хмарні платформи, за якими слідує аналітика даних (78 відсотків).

Незважаючи на недавній ажіотаж, штучний інтелект і машинне навчання посіли шосте місце (62 відсотки), а інвестиції були спрямовані на підвищення операційної ефективності та подолання прогалини в IT-кваліфікації.

«Однак це зміниться, коли організації пройдуть стадію перевірки концепції, особливо для GenAI», — сказав Роуселл-Джонс.

«Наразі лише невелика кількість організацій переходять до виробництва зі своїми випробуваннями GenAI — розгортання — це час, коли починаються справжні інвестиції».

Згідно з опитуванням, IT-директори Нової Зеландії та Нової Зеландії заявили, що трійкою найбільших технологій, у які вони зменшать інвестиції наступного року, є застаріла інфраструктура та технології центрів обробки даних (50 відсотків), ERP та обчислювальна технологія наступного покоління (обидві по 10 відсотків) і модернізація додатків. (9 відсотків).

«Хоча дивно бачити, що інвестиції в модернізацію додатків наступного року зменшаться, малоймовірно, що це вичерпано», — сказав Роуселл-Джонс. «Швидше за все, його пріоритети просто втратили перед лицем інших більш нагальних проблем для IT-директорів A/NZ».

Демократизація цифрової доставки з GenAI

IT-директори Нової Зеландії та Нової Зеландії вже заклали основу для демократизованої цифрової доставки за допомогою таких технологій, як платформи з низьким кодом, 68 відсотків зазначили, що вони розгорнули або планують розгорнути протягом наступних 24 місяців.

За словами Gartner, IT-директори Нової Зеландії та Нової Зеландії заявили, що GenAI стане найкращою технологією наступного року, яка змінить правила гри, яка також швидко просуне демократизацію цифрової доставки за межі IT-функцій.

У той час як лише 10 відсотків IT-директорів уже розгорнули технології GenAI, більше половини (58 відсотків) кажуть, що вони розгорнуть їх протягом наступних 24 місяців.

«Платформи GenAI зменшують перешкоди для впровадження для розробників програмного забезпечення, що означає, що технологія готова до швидкого розгортання наступного року», — сказав Роуселл-Джонс.

«IT-директори A/NZ повинні використовувати цю можливість і забезпечити захист для підтримки та сприяння бізнес-технологам, які прагнуть впровадження GenAI у ширшій організації».

Згідно з опитуванням, бізнес-пріоритети наступного року змішатимуть клієнтів і регулятори з фінансовими показниками.

IT-директори Австралії та Нової Зеландії вказали, що найважливішими результатами інвестицій у цифрові технології є відмінний досвід роботи з

клієнтами або громадянами (70 відсотків), забезпечення відповідності та мінімізація ризиків (57 відсотків) і підвищення операційної рентабельності (48 відсотків).

«Інтерес до цифрових технологій не зменшується, але організації в А/Новій Зеландії стали більш реалістичними у своєму ставленні до цього», — сказав Роуселл-Джонс.

«Замість того, щоб намагатися стати наступним цифровим гігантом, організації інвестують у цифрові можливості або для підвищення вартості та ефективності роботи, або для розширення традиційного набору продуктів цифровими можливостями, щоб вони могли пропонувати більше послуг».

Інші провідні новітні цифрові технології, які підприємства в А/Новій Зеландії вже розгорнули або планують розгорнути протягом наступних 24 місяців, включають штучний інтелект/машинне навчання (76 відсотків), розподілену хмару (62 відсотки) і 5G (57 відсотків)». ***(Julia Talevski. Cyber security and cloud top A/NZ spending list for 2024 // IDG Communications, Inc. (https://www.arnnet.com.au/article/709675/cyber-security-cloud-top-nz-spending-list-2024/?fp=2&fpid=1). 05.12.2023).***

***

«Нещодавно у другій за величиною телекомунікаційній мережі Австралії стався збій, який тривав 14 годин. Пізніше того ж тижня великий портовий оператор зазнав багатоденної атаки на кібербезпеку, яка залишила тисячі вантажних контейнерів заблокованими в портах країни. Ці інциденти вплинули на мільйони австралійських клієнтів і суттєво обмежили телекомунікаційні та важливі вантажні операції.

Хоча збій телекомунікаційної мережі не був результатом кібератаки, обидві події підкреслюють крихкість «секторів критичної інфраструктури» (до яких входять зв’язок і транспорт) і служать посиленню значення Закону про безпеку критичної інфраструктури 2018 року («Закон SOCI»).

Ось як Закон SOCI спрямований на вирішення та реагування на інциденти кібербезпеки

Закон SOCI охоплює «сектори критичної інфраструктури», створюючи нормативну базу для захисту, зміцнення та пом’якшення ризиків, пов’язаних із критичною інфраструктурою, яка вважається надзвичайно важливою для національної безпеки Австралії. Його метою є захист активів критичної інфраструктури шляхом створення позитивних зобов’язань безпеки для власників активів і прямих власників інтересів.

Наразі Закон SOCI поширюється на 11 секторів критичної інфраструктури, а саме:

сектор зв'язку;

сектор зберігання або обробки даних;

сектор фінансових послуг і ринків;

сектор водопостачання та водовідведення;

енергетичний сектор;

охорона здоров'я та медичний сектор;

сектор вищої освіти та досліджень;

продуктовий сектор;

транспортний сектор;

сектор космічних технологій;

сектор оборонної промисловості.

Потім ці сектори поділяються на 22 категорії активів. Наприклад, 5 класів активів, які належать до транспортного сектору, включають авіацію, вантажну інфраструктуру, вантажні послуги, портовий і громадський транспорт.

Закон SOCI загалом накладає зобов’язання на «відповідальних суб’єктів» (тих, хто несе кінцеву оперативну відповідальність за актив) і «власників прямої участі» (тих, хто володіє принаймні 10 відсотками активу або має частку в активі, що ставить його в прямий/опосередкований вплив або контроль над активом – розділ 8). Однак визначення «відповідальних осіб» і «прямих власників інтересів» змінюється залежно від активу, про який йдеться.

Хоча зобов'язання Закону про SOCI є широкими, не всі зобов'язання застосовуються до всіх секторів критичної інфраструктури чи класів активів – навіть якщо організація підпадає під дію Закону SOCI, вона може не нести відповідальності за дотримання всіх зобов'язань, що містяться в Законі про SOCI. Конкретні зобов'язання, яких повинен виконувати відповідальний суб'єкт або власник прямої частки, залежать від задіяного активу.

Таким чином може бути складно визначити, чи зобов'язана організація дотримуватися Закону SOCI і які саме зобов'язання має організація, що призводить до плутанини або відсутності роз'яснень. Якщо є сумніви, доцільно звернутися за порадою щодо того, чи може Закон SOCI вплинути на вашу організацію.

Підвищення ставок із позитивними зобов'язаннями безпеки

Після реформ наприкінці 2021 року та на початку 2022 року Закон про SOCI відмовився від пасивного підходу до встановлення вимог до суб'єктів господарювання щодо дотримання позитивних зобов'язань щодо безпеки («PSO»). Дотримання PSO буде обов'язковим лише після того, як їх буде «ввімкнено» для конкретного активу, про який йдеться. Залежно від PSO, про який йдеться, це відбувається через Правила безпеки критичної інфраструктури (додаток) (LIN 22/026) 2022 або Правила безпеки критичної інфраструктури (програма управління ризиками критичної інфраструктури) (Lin 23/006) 2023.

Суть SOCI стосується:

Реєстрація активів критичної інфраструктури (надання деталей щодо власності на активи та операційної інформації);

Обов'язкове повідомлення про інцидент кібербезпеки; і

Розробка програми управління ризиками критичної інфраструктури.

Інші зобов'язання Закону SOCI стосуються:

Повідомлення про сторонніх постачальників, які зберігають або обробляють «важливі для бізнесу дані» для активу; і

Повноваження уряду щодо поточних, минулих або неминучих інцидентів кібербезпеки (вказівки щодо збору інформації, запити на втручання та вказівки).

Наслідки невідповідності – штрафи та міжнародні санкції

Невиконання суб’єктом господарювання своїх зобов’язань (включно з ініціюванням інциденту кібербезпеки) відповідно до Закону про SOCI може призвести до серйозних штрафних санкцій, залежно від форми суб’єкта господарювання та рівня невиконання. Наприклад, суб’єкт господарювання, який не приймає, не підтримує, не виконує або регулярно переглядає свій план управління ризиками, може зіткнутися зі штрафом у розмірі 200 штрафних одиниць (наразі 62 600 доларів США) за кожну діяльність, яку він не виконує, а суб’єкт господарювання, який не повідомляє Регулятор, коли стався кіберінцидент, може зіткнутися зі штрафом у розмірі 50 штрафних одиниць (наразі 15 650 доларів).

Звичайним регулятором, відповідальним за забезпечення відповідності, є Центр кібербезпеки та безпеки інфраструктури, який знаходиться в Міністерстві внутрішніх справ (далі — Департамент). Вони мають звичайний набір повноважень щодо забезпечення виконання, включаючи цивільні покарання (штрафи), зобов’язання, судові заборони та повідомлення про порушення. Проте Резервний банк Австралії здійснює регулятивний нагляд за класом активів платіжної системи.

Але, визнаючи, що не всі кіберінциденти відбуваються на батьківщині, існують значні повноваження щодо санкцій, якими може скористатися міністр закордонних справ, спрямованих на іноземних гравців за певних обставин.

Якщо вважається, що організація спричинила «значний кіберінцидент», сприяла його спричиненню або була причетною до нього, міністр закордонних справ може накласти цільові фінансові санкції на цей суб’єкт і, зокрема, на осіб, які підпадають під режим санкцій за значні кіберінциденти. Коли юридична чи фізична особа підпадає під санкції, до них можуть бути застосовані правила про замороження активів і, у відповідних випадках, заборона на поїздки.

На винос

Якщо ці нещодавні події в кібернетичному просторі свідчать про те, що зосередженість уряду на захисті критично важливої інфраструктури Австралії, швидше за все, стане більшим пріоритетом, ніж будь-коли. Підвищення рівня освіти та дотримання відповідних норм у цій сфері, ймовірно, буде на першому місці порядку денного. Дійсно, лише минулого місяця Центр кібербезпеки та

безпеки інфраструктури запустив свій перший Місяць безпеки критичної інфраструктури – місячний захід для підвищення обізнаності про структуру критичної інфраструктури Австралії. Готуючись до подальшої уваги уряду, організації повинні знати про свої зобов'язання та виконувати їх. Ті, хто підозрюють або не знають, чи має Закон SOCI якийсь вплив на їх діяльність, повинні звернутися за порадою достроково, щоб уникнути дорогих дій пізніше». ***(Alistair Bridges and Emily Schilling. Responding to cyber incidents - the Security of Critical Infrastructure Act 2018 has never been more critical // Moulis Legal (https://moulislegal.com/knowledge-centre/responding-to-cyber-incidents-the-security-of-critical-infrastructure-act-2018-has-never-been-more-critical/). 05.12.2023).***

***

Китай

«Інтернет-оператори повинні будуть повідомляти про основні інциденти кібербезпеки – в тому числі хакерські атаки, збої в інфраструктурі та витоки ключових даних – передати владі Китаю протягом години після того, як це сталося, інакше загрожує суворе покарання, згідно з проектом правил нагляду за Інтернетом країни.

Адміністрація кіберпростору Китаю (CAC) опублікувала нові правила в п'ятницю, щоб зацікавити громадську думку. CAC заявив, що регулювання звітності про інциденти кібербезпеки може зменшити збитки та збитки, які вони спричинили, а також захистити національну безпеку в Інтернеті.

Відповідно до проекту, усі оператори повинні повідомляти про інциденти в місцеві або національні офіси кіберпростору, а ті, хто працює з «ключовою інформаційною інфраструктурою» або стикається з інцидентами, пов'язаними зі злочинністю, також повинні повідомляти про порушення в поліцію.

Інциденти кібербезпеки визначаються як «інциденти, які завдають шкоди мережам, інформаційним системам або даним через людський фактор, збої програмного чи апаратного забезпечення або стихійні лиха».

Оператори зобов’язані повідомляти про збитки, заподіяні інцидентами, і вжиті заходи, ймовірну причину, поради щодо розслідування, включаючи все, що відомо про зловмисника, шлях атаки та наявні лазівки, йдеться в проекті.

У проекті особливо наголошувалося, що про серйозні інциденти необхідно повідомляти протягом години.

У ньому описано три рівні інциденту, причому найсерйозніший рівень включає витік особистих даних понад 100 мільйонів людей, «що впливає на роботу та життя понад 30 відсотків населення провінції», «ключову інформаційну інфраструктуру відключено для шість годин» та шкідливу інформацію, яку переглядали понад 1 мільйон разів або відображали більше шести годин у ЗМІ чи на державних веб-сайтах.

Після періоду громадського обговорення проект буде повернуто до CAC для редагування.

В останні роки влада Китаю неодноразово наголошувала, що країна стикається зі зростаючим ризиком кібератак, витоків даних, дезінформації та когнітивної війни, керованої штучним інтелектом, із швидким розвитком технологій.

У статті, опублікованій у вересні в China Internet and Information, офіційному журналі CAC, міністр державної безпеки Чень Ісінь написав: «Найбільший прихований ризик полягає в тому, що наша важлива базова інформаційна інфраструктура може бути вразливою до атак.

«Наші фінансові, енергетичні, електричні, комунікаційні та транспортні операційні мережі стали ключовими цілями кібератак з-за меж країни.

«Будуть жахливі наслідки, такі як збої в транспорті, хаос на фінансових ринках і параліч постачання електроенергії, якщо ці системи будуть зламані, захоплені, підроблені або саботовані».

Не наводячи конкретних прикладів, Чень назвав нові технології, які можуть внести більшу невизначеність у безпеку, включаючи штучний інтелект, квантовий зв’язок, технологію блокчейн і супутниковий Інтернет.

У нещодавньому прикладі збій у додатку для замовлення поїздок Didi Chuxing минулого місяця вплинув на тисячі людей і спричинив приблизно 100 мільйонів юанів (14 мільйонів доларів США) збитків. Тим часом, у Alibaba Cloud стався другий збій, який торкнувся клієнтів у материковому Китаї, Гонконзі та Сполучених Штатах.

Ці інциденти викликали дискусію серед експертів, медіа-коментаторів та користувачів Інтернету про те, як інтернет-інфраструктура стала нормальною частиною суспільного життя, так само як газ і вода, і її безпеку потрібно наголошувати та регулярно підтримувати.

У 2016 році Китай прийняв Закон про кібербезпеку, наголошуючи на необхідності збереження контролю над суверенним кіберпростором країни та національною безпекою.

Спираючись на цю основу, Закон про безпеку даних був запроваджений у вересні 2021 року, щоб обмежити способи обробки даних. Закон також наголошує на необхідності захисту національної безпеки та інтересів, роблячи захист даних пріоритетом національної безпеки». ***(Phoebe Zhang. Under China's new security rules, internet operators must report hacks and cybercrimes within an hour // South China Morning Post Publishers Ltd. (https://www.scmp.com/news/china/article/3244358/under-chinas-new-security-rules-internet-operators-must-report-hacks-and-cybercrimes-within-1-hour?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 08.12.2023).***

***

«Міністерство промисловості та інформаційних технологій Китаю (МІІТ) опублікувало вичерпну класифікацію для керівництва місцевими органами влади та компаніями щодо вирішення інцидентів безпеки даних. У плані описано процедури, яких суб'єкти повинні дотримуватися під час оцінки та вирішення таких інцидентів.

Класифікація запроваджує чотирирівневу систему з кольоровим кодуванням, яка базується на масштабі шкоди національній безпеці, онлайн- та інформаційній мережі компанії або загальній економіці.

Відповідно до плану, інциденти, які призведуть до збитків, що перевищують 141 мільйон доларів і вплинуть на особисту інформацію понад 100 мільйонів людей або на «делікатну» інформацію понад 10 мільйонів людей, будуть класифікуватися як «особливо серйозні», що призведе до червоного попередження.

У відповідь на червоні та помаранчеві попередження план передбачає, що залучені компанії та відповідні місцеві регуляторні органи встановлюють 24-годинний графік роботи для усунення інциденту. Крім того, МІІТ має бути повідомлено про порушення даних протягом десяти хвилин після його виникнення, серед інших визначених заходів.

Запровадження цього нового плану підкреслює побоювання Пекіна щодо значних витоків даних і кібератак, які відбуваються в його юрисдикції.

Виклики кібербезпеці загострюються на тлі глобальної напруженості

Запровадження плану дій у надзвичайних ситуаціях МІІТ збігається із загостренням геополітичної напруженості за участю Сполучених Штатів та їхніх союзників. Ця подія сталася після інциденту минулого року, коли хакер заявив, що отримав від поліції Шанхаю значну кількість особистої інформації, що належить мільярду китайців…

У динамічному ландшафті технологій, що керуються даними, захист особистої інформації та оперативне реагування на інциденти безпеки є критично важливими вимогами для урядів та організацій. Останнє оголошення МІІТ підкреслює зобов’язання Китаю захищати конфіденційну інформацію населення, сигналізуючи про проактивну позицію проти несанкціонованого доступу та потенційних порушень». ***(Alisa Davidson. China’s MIIT Unveils Data Security Incident Plan to Protect Companies from Cyber Threats // CRYPTOMERIA LABS PTE. LTD. (https://mpost.io/chinas-miit-unveils-data-security-incident-plan-to-protect-companies-from-cyber-threats/). 15.12.2023).***

***

«Управління телекомунікацій Пакистану (PTA), визнаючи зростання складності кібератак, оприлюднило Стратегію кібербезпеки для сектору телекомунікацій, яка забезпечує стратегічну основу та дорожню карту для реалізації національної політики кібербезпеки протягом наступних п'яти років (2023-2028).

Стратегія передбачала створення безпечної, стійкої та надійної цифрової екосистеми для телекомунікаційного сектора Пакистану.

У PTA заявили, що останніми роками сталася хвиля серйозних порушень безпеки, які виявили вразливі місця як у складних міжнародних, так і в національних мережах.

Подібні експлойти Solar Wind, Microsoft Exchange і Moveit служать яскравими нагадуваннями, порушуючи навіть найдосконаліші рівні безпеки та поширюючись у широкому масштабі.

Недавнім доповненням до них є доступ хакерів до складних інструментів штучного інтелекту, таких як ChatGPT або його шкідливих варіантів, таких як WormGPT або FraudGPT, використання яких може дозволити навіть сценаристам створювати складні корисні навантаження для успішного зламу багаторівневого кіберзахисту.

За останнє десятиліття Пакистан опинився на місці подібних кібератак, спонсорованих державою.

Це викликає значне занепокоєння, особливо враховуючи низьку позицію Пакистану в глобальному рейтингу кібербезпеки, що робить країну вразливою для своїх супротивників, які прагнуть порушити національну стабільність.

Ці загрози кібербезпеці є не просто викликом для наших цифрових мереж; вони становлять серйозний ризик для нашої національної безпеки, економіки та соціальної структури.

Стратегія кібербезпеки для телекомунікаційного сектору спрямована на забезпечення безпеки та стійкості телекомунікаційного сектору перед обличчям

кіберзагроз, що постійно розвиваються. Він окреслює різноманітні проблеми та можливості, пов’язані із захистом критично важливої телекомунікаційної інфраструктури, і забезпечує основу для спільних дій для вирішення цих проблем.

Стратегія наголошує на необхідності інтегрованого підходу до кібербезпеки, заснованого на оцінці ризиків, і визначає ключові сфери дій, включаючи управління ризиками та управління, кіберзахист і реагування на інциденти, дослідження та розробки, а також державно-приватне партнерство.

Стратегія складається з шести основ, кожна з яких стосується певної сфери кібербезпеки. У стратегії зазначено, що вона спрямована на вирішення проблем, пов’язаних із зростаючою взаємозв’язністю телекомунікаційних мереж, кіберзагрозами, з якими вони стикаються, і необхідністю захисту їхніх даних та інформації про клієнтів.

Стратегія фокусується на таких сферах, як управління ризиками та управління; кіберзахист і реагування на інциденти; дослідження та розвиток; та державно-приватне партнерство.

Він наголошує на необхідності комплексного та інтегрованого підходу до кібербезпеки в телекомунікаційному секторі та закладає основу для спільних зусиль із захисту критичної телекомунікаційної інфраструктури та послуг.

Стратегія також визначає ключові виклики та можливості для сектора та містить дорожню карту для дій для забезпечення безпеки сектору телекомунікацій.

Стратегія також окреслює кілька ініціатив і заходів, які будуть здійснені для захисту національної критичної інфраструктури. Це, зокрема, посилення державно-приватного партнерства, інвестиції в дослідження та розробки та розробка єдиної національної системи кібербезпеки.

На високому рівні, нижче є очікування від телекомунікаційних компаній щодо досягнення цілей цієї стратегії: a. Телекомунікаційні компанії повинні забезпечити, щоб увесь персонал був навчений і навчений практикам і процедурам кібербезпеки, особливо щодо обов’язків співробітників щодо запобігання внутрішнім загрозам. b. Телекомунікаційні компанії повинні переконатися, що їхні мережі та системи відповідають положенням і директивам PTA, особливо CTDISR і

Framework Cyber Security. в. Телекомунікаційні компанії зобов'язані забезпечити постійний моніторинг і своєчасне оновлення своїх мереж і систем, щоб зменшити ризик кібератак.

Зокрема, цього можна досягти шляхом створення CERT/SOC та сприяння цілодобовому моніторингу. Залучення кваліфікованих ресурсів рівня 1, 2 і 3 разом із чітко визначеними процесами є найважливішими для цих зусиль.

Крім того, для цих компаній вкрай важливо забезпечити інтеграцію своїх SOC з nTSOC, що забезпечить ефективну, синергетичну відповідь на будь-яку потенційну кібератаку.

Цей проактивний уніфікований підхід має вирішальне значення для підвищення загальної кіберстійкості телекомунікаційного сектора. d. Телекомунікаційні компанії повинні впроваджувати надійні заходи для захисту даних клієнтів від несанкціонованого доступу.

Пріоритет конфіденційності даних є важливим для збереження довіри між користувачами. д. Телекомунікаційні компанії повинні переконатися, що їхні системи розроблені таким чином, щоб швидко виявляти інциденти кібербезпеки та реагувати на них. f. Телекомунікаційним компаніям слід часто оцінювати свої системи та мережі, щоб гарантувати виявлення та усунення недоліків безпеки.

У зв'язку з цим їм необхідно розробити та практикувати чітко визначений трирівневий процес аудиту, кульмінацією якого стане перевірка командою кібербезпеки PTA.

Оператори повинні позитивно підходити до цих зусиль, співпрацюючи із зовнішніми командами, щоб покращити свою безпеку. g. Телекомунікаційні компанії повинні співпрацювати з іншими організаціями в галузі та PTA для обміну відповідною інформацією про загрози кібербезпеці та інциденти. Замість того, щоб приховувати кіберінциденти, ми повинні працювати над моделлю взаємної довіри, щоб спільно боротися з цією загрозою. I, ч. Телекомунікаційні компанії повинні надавати клієнтам інформацію про загрози кібербезпеці та способи захисту від таких загроз». ***(Tahir Amin. PTA unveils 'Cyber Security Strategy' // Business***

Recorder (https://www.brecorder.com/news/40278325/pta-unveils-cyber-security-strategy). 13.12.2023).

***

«Цифрова трансформація, яка охопила світ, не оминула Латинську Америку та Карибський басейн. Однак, оскільки уряди, компанії та окремі особи в регіоні все більше використовують цифрові інструменти, ризик кібератак також зростає.

У цьому звіті ми проаналізуємо стан кібербезпеки в країнах Латинської Америки та країнах Карибського басейну. Особливу увагу буде приділено найбільшим з них — Бразилії, Мексиці та Аргентині, — які відіграють ключову роль в економічному та технологічному розвитку регіону та які, що важливо для цього дослідження, стикаються з найбільшою кількістю кібератак. Мета цього звіту – визначити ключові загрози та запропонувати рекомендації щодо посилення цифрової безпеки регіону.

Ключові цифри та висновки

В останні роки країни Латинської Америки зазнали швидкої цифрової трансформації, яка вплинула на всі аспекти життя громадян і кожен сектор економіки. Як наслідок цієї трансформації зріс ризик кіберзагроз, до яких регіон не був готовий.

На Латинську Америку припадало 12% від загальної кількості атак у всьому світі у 2022 році. Зловмисники в основному були націлені на організації та окремих осіб у Бразилії, Мексиці та Аргентині — атаки на ці три країни становили 44% усіх атак.

Більшість успішних атак на організації були спрямовані на державні установи (31%), промислові підприємства (11%), фінансові установи (9%) і компанії роздрібної торгівлі (9%).

Найбільш серйозною кіберзагрозою для організацій і держав у регіоні є атаки програм-вимагачів. Завдяки діяльності операторів програм-вимагачів частка всіх успішних атак (52%), які призвели до збою в роботі компанії — призупинення

бізнес-процесів або втрати доступу до інфраструктури чи даних — є вищою за середньосвітовий показник. Примітно, що атаки програм-вимагачів у цьому регіоні часто націлені на державні структури: відсоток постраждалих державних установ (31%) у 2,2 рази перевищує середній світовий показник за той же період.

У 61% випадків успішні атаки на організації призвели до витоку конфіденційної інформації. Основна мотивація зловмисників у цих випадках, швидше за все, фінансова — вони продають викрадену інформацію (переважно особисті та облікові дані) у темній мережі або використовують її для подальших атак і вимагання.

На тіньових форумах зловмисники активно торгують та обмінюються вкраденими даними, хакерськими послугами та доступом до мереж латиноамериканських організацій. Більше половини списків (53%), які вказують на певну країну в регіоні, згадують Бразилію, Аргентину чи Мексику. Найчастіше в темній мережі продається доступ до мереж фінансових установ, державних установ, ІТ-компаній, промислових підприємств і сервісних організацій.

Високий рівень проникнення мобільного Інтернету, використання мобільних пристроїв та електронних платежів в регіоні призвели до збільшення кількості атак на мобільні пристрої громадян. Зловмисне програмне забезпечення використовується частіше, ніж у будь-якому іншому регіоні світу: 78% атак стосуються зловмисного програмного забезпечення, насамперед шпигунського ПЗ (40%) і банківських троянів (32%). Низький рівень кіберграмотності серед населення означає, що такі атаки часто є успішними.

Країни Латинської Америки мають посилити регіональне співробітництво у боротьбі з кіберзлочинністю та гармонізувати своє законодавство у сфері кібербезпеки, використовуючи накопичений досвід і кращі практики розвинених країн.

Рекомендації щодо покращення кібербезпеки на державному рівні також включають розробку національних стратегій кібербезпеки, зміцнення зв’язків між організаціями та національними центрами реагування на кіберінциденти,

підтримку освітніх програм з кібербезпеки та сприяння міжнародній співпраці та обміну даними.

Рекомендації щодо підвищення кіберстійкості організацій включають визначення неприпустимих подій і захист критичних активів, моніторинг і реагування на кіберзагрози за допомогою передових інструментів безпеки, оцінку ефективності впроваджених заходів і навчання співробітників.

Питання цифровізації та кібербезпеки

Розвиток цифрових технологій в регіоні

Латинська Америка та Карибський басейн мають різноманітні економіки, кожна зі своїми унікальними історичними, культурними та географічними характеристиками. Деякі країни, такі як Бразилія та Мексика, демонструють динамічний економічний розвиток і мають потужні промислові сектори. Водночас інші країни, особливо невеликі держави Центральної Америки та Карибського басейну, стикаються з економічними труднощами та більше залежать від туризму та сільського господарства. Сукупний ВВП регіону становить 6% світового ВВП, що підкреслює його важливість у глобальному економічному контексті.

Розвиток цифрової економіки є одним із ключових чинників подальшого економічного зростання. Перехід до цифрової економіки може покращити економічні показники, підвищити продуктивність і створити нові робочі місця, що є критично важливим для регіону, який характеризується відносно високим рівнем безробіття та соціальної нерівності. Незважаючи на те, що регіон традиційно відставав від більш розвинутих економік, коли йдеться про цифровізацію, останніми роками країни Латинської Америки активно впроваджують і розвивають цифрові технології та послуги. Особливо це помітно в державних послугах, фінансових технологіях, охороні здоров’я та роздрібній торгівлі.

Рівень проникнення інтернету в регіоні станом на початок 2023 року оцінюється в 75%, що перевищує середньосвітовий показник у 65%. У Бразилії цей показник становить 84%; в Аргентині 87%; а в Мексиці – 77%.

Цифровізація регіону передбачає не лише розширення доступу до Інтернету, а й інтеграцію нових технологій у повсякденне життя громадян — від мобільного

банкінгу та онлайн-магазинів до систем розумного дому. Близько 66% дорослого населення робить покупки онлайн, а в Аргентині, Бразилії, Чилі та Колумбії цей відсоток перевищує 80%. Електронна комерція в регіоні зростає: за оцінками експертів, у 2023 році обсяг транзакцій зросте на 27% і досягне $509 млрд.

У багатьох країнах, зокрема в Бразилії, Аргентині, Мексиці, Колумбії та Чилі, створено національні програми стимулювання розвитку цифрової економіки. Ці стратегії спрямовані на інтеграцію нових технологій у кожен сектор, насамперед на оптимізацію державних послуг і розвиток електронної комерції та цифрових платежів. Відповідно до різних оцінок, таких як Індекс розвитку електронного уряду та Індекс зрілості GovTech, більшість державних послуг у регіоні мають високий або дуже високий рівень цифрового розвитку.

Проблеми кібербезпеки

Незважаючи на активний технологічний розвиток, багато країн все ще не мають достатньої законодавчої бази та інфраструктури для боротьби з кіберзлочинністю. Питання кібербезпеки стали особливо актуальними в Латинській Америці через відсутність чітких стандартів і правил, дефіцит кваліфікованих фахівців, відсутність культури інформаційної безпеки серед користувачів і обмежені ресурси для інвестування в технології безпеки — усе це робить регіон особливо вразливі до кіберзагроз.

За оцінками експертів, збиток від кібератак країнам регіону становить близько 1% ВВП, а якщо постраждає критична інфраструктура, то може досягати 6%. У дослідженні Fortinet 31% латиноамериканських організацій повідомили, що наслідки кібератак коштують їм понад 1 мільйон доларів.

Результати звіту Global Cybersecurity Index 2020 показують, що Латинська Америка має найнижчий рівень кібербезпеки порівняно з іншими регіонами.

Лише 10 із 33 країн Латинської Америки мають індекс кібербезпеки, вищий за середньосвітовий, причому Бразилія (96,60) і Мексика (81,68) мають найвищий показник. У більшості країн проблема полягає у нестачі ресурсів; Природно, багатші країни можуть інвестувати більше в розвиток інфраструктури та кібербезпеки.

Регіон стикається з численними перешкодами на шляху до кіберстійкості. В першу чергу це пов’язано з браком фінансування. За даними Організації економічного співробітництва та розвитку, більшість підприємств регіону (99%) є малими та середніми підприємствами, що робить їх основою економіки. Такі компанії можуть не мати достатніх ресурсів для захисту своїх активів і найму кваліфікованого персоналу з кібербезпеки, що робить їх уразливими до нових загроз. Згідно з даними ESET Security Report, 65% фахівців вважають, що їхнім організаціям потрібно більше інвестувати в кібербезпеку.

Також в регіоні не вистачає кваліфікованих фахівців з кібербезпеки. За оцінками ISC2, у 2022 році лише в Мексиці та Бразилії не вистачало 516 000 співробітників. Навпаки, 94% організацій планують збільшити штат працівників із кібербезпеки. На жаль, країни регіону відчувають відтік мізків через відносно низькі зарплати порівняно з іншими регіонами — багато фахівців з Латинської Америки переїжджають до Північної Америки чи Європи в пошуках кар’єри та можливостей для навчання. За даними e-Governance Academy, лише 12 країн регіону пропонують бакалаврські програми з інформаційної безпеки, а 15 країн мають спеціальні магістерські програми.

Є й політичні проблеми. Підхід до кібербезпеки залишається переважно реактивним — дії вживаються лише у відповідь на інциденти, які вже відбулися. Такий підхід може не помічати нових загроз. Ставлення до безпеки в законодавстві також позбавлене почуття відповідальності. Наприклад, не всі країни регіону прийняли національні стратегії кібербезпеки. У листопаді 2022 року було опубліковано план цифрового розвитку для країн Латинської Америки та Карибського басейну, спрямований на впровадження національних стратегій кібербезпеки для 20 із 33 країн регіону до 2024 року. Критичні питання безпеки інфраструктури також розглядаються лише в стратегіях деяких держав. У країнах Латинської Америки немає єдиного законодавства щодо кібербезпеки чи захисту даних. З’являються окремі ініціативи щодо приведення законів у відповідність до передового досвіду; наприклад, Бразилія та Аргентина оновили своє законодавство щодо захисту персональних даних відповідно до європейського GDPR. Однак

правові вимоги відрізняються в кожній країні, що може створити додаткові труднощі в транскордонній передачі даних і боротьбі з кіберзлочинністю. Деякі країни регіону, такі як Бразилія, Аргентина, Колумбія, Чилі та Коста-Ріка, підписали Будапештську конвенцію про кіберзлочинність. Але на регіональному рівні зусилля з уніфікації законодавства та протидії кіберзагрозам просуваються дуже повільно.

У 24 країнах регіону існують національні групи реагування на кіберінциденти. Але навіть у країнах, де існують процедури звітування про кіберінциденти та взаємодії з CERT або CSIRT, фахівці з кібербезпеки не завжди знайомі з цими процесами. У звіті про кібербезпеку LATAM CISO 2023 зазначається, що хоча більшість респондентів розуміють процедуру взаємодії з CERT, 32% заявили, що не знають, куди та як повідомити про кіберінцидент. Крім того, 35% респондентів висловлюють низьку довіру до національних CERT.

Цілі та наслідки кібератак

Згідно зі звітом IBM, на країни Латинської Америки припадало 12% від загальної кількості атак у 2022 році. Існує чітка кореляція між розміром економіки країни, розвитком цифрових технологій і кількістю атак. Цілями зловмисників були організації та окремі особи в Бразилії (22% усіх атак у регіоні), Мексиці (12%), Аргентині (10%), Коста-Ріці (9%), Колумбії (9%) та Чилі (8%).

Відповідно до опитування в LATAM CISO 2023 Cybersecurity Report, 71% керівників кібербезпеки відзначили, що кількість атак на їхні організації зросла за останній рік, тоді як лише 8% повідомили про зменшення. В опитуванні ESET 69% респондентів сказали, що стикалися з інцидентом безпеки в минулому році. Дослідження Fortinet повідомляє, що 58% респондентів очікують збільшення кількості атак найближчим часом.

З початку 2022 року до кінця першого півріччя 2023 року більшість успішних атак на організації в регіоні були спрямовані на державні установи (31%), промислові підприємства (11%), фінансові установи (9%) та компанії роздрібної торгівлі. (9%).

На частку приватних осіб припадає 13% успішних атак у регіоні, що трохи нижче середнього світового показника (17%). Однак у таких країнах, як Мексика та Бразилія, цей відсоток був вищим — 23% і 20% відповідно.

Успішні атаки на організації найчастіше призводили до витоку конфіденційної інформації (61%) і збою в роботі (52%). Ці наслідки спостерігалися частіше, ніж у середньому по всьому світу, ймовірно, через високий рівень активності програм-вимагачів у регіоні.

Основним мотивом зловмисників, ймовірно, є фінансова вигода. Існують численні атаки, пов’язані з крадіжкою даних, але зловмисників не цікавить сама викрадена інформація (переважно особисті дані та дані облікових записів) — дослідження показують, що вони в основному продають її в темній мережі або використовують для подальших атак і вимагання. Це підтверджується частим використанням програм-вимагачів — 63% від загальної кількості атак на організації.

Найгучнішим інцидентом у регіоні за останні два роки стала безпрецедентна серія атак програм-вимагачів на урядові організації в Коста-Ріці, що вплинуло на ІТ-системи 27 установ. Через неробочість значної частини ІТ-інфраструктури в країні було оголошено надзвичайний стан. Лише за перші 48 годин атаки злочинці завдали збитків на 125 мільйонів доларів, а процес відновлення інфраструктури Коста-Ріки тривав кілька місяців.

Державні установи

Найчастіше об’єктами атак ставали державні установи. Вони цікаві кіберзлочинцям з кількох причин. Ці інституції ведуть широкі бази даних, включаючи персональні дані громадян, інформацію про національну безпеку та економічні дані. Ця інформація може бути використана для вимагання, шпигунства або продана на тіньовому ринку.

Урядові системи зазнають оцифрування, і все більше послуг надається онлайн, щоб миттєво стати мішенню для хакерів. Наприклад, щойно уряд Ямайки запровадив електронну систему для заповнення митних та імміграційних форм, її

зламали — зловмисники вимагали від нічого не підозрюючих користувачів 35 доларів за доступ до системи.

Деякі державні установи в регіоні також використовують застарілі або недостатньо захищені інформаційні системи, що робить їх легкою мішенню для кібератак. Недостатнє фінансування та низький рівень підготовки персоналу з кібербезпеки також можуть зіграти свою роль. Наприклад, у вересні 2022 року група Guacamaya проникла на сервери державних структур у Мексиці, Чилі, Перу, Колумбії та Сальвадорі через уразливість ProxyShell у сервісі Exchange. Офіційне оновлення безпеки було випущено на початку 2021 року, але скомпрометовані організації не встановили цей патч. У разі атаки на мексиканський Секретаріат національної оборони зловмисники скористалися уразливістю безкоштовного поштового сервера Zimbra — імовірно, це програмне забезпечення було використано через скорочення бюджету.

Кібератаки можуть бути інструментом політичного тиску, дестабілізації чи демонстрації влади. Вони також можуть бути використані для втручання у вибори чи інші урядові процеси. Деякі групи можуть націлюватися на державні установи, щоб просувати свої ідеологічні переконання. Наприклад, вищезгадана Guacamaya — це група хактивістів, які стверджують, що підтримують захист навколишнього середовища в Південній Америці. Вони викрадають і публікують дані державних установ і промислових компаній. З 2022 року ці хактивісти опублікували понад 20 ТБ вкрадених даних.

Промислові та енергетичні компанії

Виробництво та енергетична промисловість, зокрема нафтова промисловість, мають важливе значення для економічного зростання та розвитку Латинської Америки. Збої в цих секторах можуть перетворитися на економічні та соціальні проблеми. Успішні атаки призвели до збоїв в IT-інфраструктурі промислових підприємств у 58% випадків.

Промислові організації часто володіють цінною інтелектуальною власністю. У 77% успішних атак зловмисникам вдалося викрасти дані, а в половині випадків ця викрадена інформація містила комерційну таємницю. Гуакамая був особливо

активним у цьому плані: у 2022 році група опублікувала понад 2 ТБ інформації, викраденої з гірничодобувних компаній Центральної та Південної Америки.

Приблизно 6% усіх дарк-веб-листингів, пов’язаних із регіоном, пов’язані з продажем доступу до мереж компаній у виробничому та енергетичному секторах. Середня ціна такого доступу коливається від 600 до 800 доларів в залежності від розміру компанії та рівня привілеїв доступу. Один виключний список продав доступ до енергетичної компанії в Аргентині за 1700 доларів.

Фінанси

Фінансовий сектор залишається основною мішенню для кіберзлочинців у Латинській Америці через масштабну цифрову трансформацію та потенційні прибутки для зловмисників. Проте фінансові організації відносно добре захищені; за останні два роки не було жодної серйозної атаки, яка призвела б до значних збоїв у роботі або великомасштабної крадіжки коштів. Найбільше злочинців цікавить викрадення конфіденційних даних і вимагання: у 70% успішних атак на фінансові організації вони викрадали конфіденційну інформацію про клієнтів жертв.

Програми-вимагачі використовувалися в 45% атак, найчастіше з сімейств LockBit і BlackCat. Наприклад, у жовтні 2022 року група програм-вимагачів атакувала банк у Бразилії за допомогою шкідливого програмного забезпечення LockBit і попросила викуп у розмірі 50 біткойнів, що на той час становило близько 1 мільйона доларів. Атака призвела до витоку даних і тимчасових збоїв у роботі клієнтських сервісів.

У 2023 році шкідливе ПЗ для банкоматів під назвою FiXS почало поширюватися в Латинській Америці, зокрема в Мексиці. Ця шкідлива програма дозволяє зловмисникам знімати готівку в банкоматах. Хоча останніми роками кількість атак на банкомати неухильно зменшувалася, на початку цього року відновилося використання таких шкідливих програм.

Крім того, зловмисники націлені не лише на банки, а й на їхніх користувачів, особливо клієнтів бразильських банків, які використовують популярну систему миттєвих платежів PIX. Кілька банківських троянів з'явилися спеціально для атаки на цю систему. Загалом, оскільки електронні платежі та цифровий банкінг

продовжують розвиватися, ми можемо очікувати збільшення кількості загроз для користувачів, які недбало ставляться до своєї безпеки та, отже, більш уразливі до фішингових атак. Отже, банки повинні зосередитися на захисті своїх додатків і підвищенні обізнаності своїх клієнтів щодо кібербезпеки.

Роздрібна торгівля

Серед атак, спрямованих на організації, 9% припало на сектор роздрібної торгівлі. В основному це були компанії з найбільших країн регіону: Бразилії, Аргентини та Мексики — наприклад, Mercado Libre, Fast Shop і Rede Top.

IT-системи таких компаній обробляють і зберігають величезну кількість даних користувачів — інформації, яка дуже цікавить кіберзлочинців. Крім того, різноманітні платіжні системи пов’язані з інтернет-магазинами, створюючи можливості для крадіжки коштів і перехоплення даних банківських карт. Протягом звітного періоду 68% успішних атак призвели до витоку даних, в основному особистої інформації клієнтів.

Програми-вимагачі становлять основну загрозу для роздрібної торгівлі, адже вони беруть участь у 84% успішних атак. У той же час онлайн-платформи дуже чутливі до збоїв — один день простою може коштувати компанії мільйони доларів. Наприклад, бразильський конгломерат Americanas.com повідомив про збитки в 184 мільйони доларів через кібератаки, які зупинили онлайн-продажі на кілька днів. Загалом 58% успішних атак порушили діяльність компаній.

Електронна комерція є одним із найбільш швидкозростаючих секторів у Латинській Америці, причому роздрібна торгівля становить значну частину (53%). Прогнози передбачають середньорічне зростання онлайн-роздрібної торгівлі на 21% з 2023 по 2026 роки з відповідним збільшенням атак на цей сектор.

Основні загрози

Атаки на організації в основному пов'язані з компрометацією комп'ютерів, серверів і мережевого обладнання (87%). Успішні атаки на веб-ресурси становили 15%, причому 54% цих інцидентів пов’язані з використанням відомих уразливостей і загальнодоступних експлойтів.

Більше третини атак на фізичних осіб (34%) спрямовані на мобільні пристрої — цей показник вище середнього світового показника (22%) і близький до показників у країнах Азії (37%). Популярність цього вектора атаки пояснюється високим рівнем проникнення мобільного Інтернету та використанням мобільних пристроїв у регіоні. У звіті щодо електронної комерції в Латинській Америці за 2023 рік зазначається, що у 2023 році 70% онлайн-покупок та інших платежів здійснюються за допомогою смартфонів, і ця цифра щорічно зростає. Більше того, кількість користувачів мобільних пристроїв зростає з кожним роком і, як очікується, досягне 74% населення до 2025 року. Відповідно, кількість атак на мобільні пристрої також зросте.

Кожна друга успішна атака на організації використовує соціальну інженерію (53%). Експлуатація вразливості була зафіксована в 27% випадків, а компрометація облікових даних – в 19% атак. Зловмисне програмне забезпечення однаково часто використовується для атак на організації (80%) і на окремих осіб (78%).

Шкідливе програмне забезпечення

Країни Латинської Америки демонструють найвищий відсоток використання програм-вимагачів для атак на організації (79%) порівняно із середнім світовим показником (53%).

Зловмисне програмне забезпечення використовується частіше, ніж у будь-якому іншому регіоні світу: 78% атак стосуються зловмисного програмного забезпечення, насамперед шпигунського ПЗ (40%) і банківських троянів (32%). Цій тенденції сприяє кілька факторів: широке використання піратського програмного забезпечення, використання неперевірених програм VPN для доступу до заблокованих ресурсів і загалом низький рівень обізнаності з кібербезпекою.

Основними методами розповсюдження зловмисного програмного забезпечення в організаціях є електронна пошта (54%) і компрометація комп’ютерів і серверів (35%). Зловмисне програмне забезпечення потрапляє на пристрої людей, коли користувачі відвідують заражені веб-сайти (55%) або відкривають вкладення та посилання в електронних листах (29%). Офіційні

магазини додатків також можуть стати джерелами зараження, якщо зловмисникам вдається обійти системи безпеки та видавати свої програми за законні.

Атаки програм-вимагачів

Хоча загалом у світі спостерігається тенденція до зниження кількості атак програм-вимагачів, ця загроза зростає в Латинській Америці. Згідно з індексом IBM X-Force Threat Intelligence Index, у 2022 році кількість інцидентів, пов'язаних із програмами-вимагачами, у Латинській Америці зросла на 3%. Крім того, методи злочинців розвиваються — середня тривалість атаки скоротилася з двох місяців до чотирьох днів. Якщо порівнювати перші півріччя 2022 і 2023 років, то зростання атак програм-вимагачів в регіоні залишається на тому ж рівні, 3%.

Майже третина атак програм-вимагачів (31%) була спрямована на державні установи. Цей відсоток значно вищий, ніж в інших регіонах — у 2,2 рази перевищує середній світовий показник (14%). У топ-5 категорій постраждалих від програм-вимагачів також увійшли промислові підприємства, роздрібна торгівля, медичні та навчальні заклади.

Компанії ще не повністю готові самостійно боротися з наслідками атак програм-вимагачів. Наприклад, в опитуванні, проведеному Veeam у країнах Латинської Америки, 58% респондентів сказали, що їхня організація заплатила викуп і змогла відновити дані, а 14% заплатили викуп, але не змогли отримати дані. Лише 21% респондентів сказали, що не заплатили викуп, тому що змогли відновити дані з резервних копій. За даними Veeam, організації платили викуп через страховку в 77% випадків. Однак останнім часом умови страхування від кіберризиків змінюються: страхові компанії почали збільшувати франшизи та премії. Деякі страхові компанії зараз виключають атаки програм-вимагачів зі свого покриття, про що заявили 20% респондентів.

Можливо, через велику кількість організацій, які стають жертвами атак програм-вимагачів та інших загроз, які безпосередньо впливають на дані, найпоширенішою технологією безпеки в корпоративних мережах стали системи резервного копіювання — ними користуються 88% організацій. Однак, згідно з іншим дослідженням Thales Data Threat Report, лише 60% респондентів сказали, що

їхня організація має план реагування на випадок атаки програм-вимагачів (що вже є значним покращенням порівняно з 2021 роком, коли лише 42% респондентів повідомили, що мали такий план).

У регіоні працює багато груп програм-вимагачів, найактивнішими з яких за останні два роки були такі:

LockBit

Група програм-вимагачів LockBit, яка працює з 2019 року, націлена на урядові та приватні організації в Південній Америці. Не всі атаки були здійснені безпосередньо групою: LockBit поширює своє однойменне шкідливе програмне забезпечення за допомогою моделі програм-вимагачів як послуги (RaaS).

Чорний кіт (ALPHV, UNC4466, Noberus)

Група програм-вимагачів BlackCat працює з 2021 року. Ці кіберзлочинці націлені як на приватні, так і на державні організації в Південній Америці та в усьому світі.

Cl0p

Групу програм-вимагачів Cl0p було вперше виявлено в 2019 році. Зловмисники націлені на широкий спектр галузей у всьому світі, але в Латинській Америці вони зосередилися на атаках на університети та фінансові організації в Мексиці, Колумбії та Пуерто-Ріко.

BlackByte

Групу програм-вимагачів BlackByte вперше помітили в 2019 році. Кіберзлочинці діють по всьому світу, а в Латинській Америці вони націлилися на промислові та урядові організації в Мексиці, Аргентині та Перу. Як і LockBit, вони поширюють програмне забезпечення-вимагач за допомогою моделі RaaS.

Рисида

Кіберзлочинне угруповання Rhysida з'явилося в травні 2023 року. Вони маскуються під команду кібербезпеки, яка пропонує допомогу жертвам. У Південній Америці Rhysida атакувала урядові та медичні організації. У травні 2023 року група атакувала IT-інфраструктуру чилійської армії, що призвело до значних збоїв у системі та витоку конфіденційної інформації.

Облікові записи

Група програм-вимагачів Conti здійснювала атаки на приватні та державні організації по всьому світу. У квітні 2022 року вони запустили кампанію, націлену на урядові установи Коста-Ріки. Серія кібератак призвела до відключення багатьох державних систем майже на місяць, витоку 672 ГБ даних і оголошення надзвичайного стану в країні. Але наприкінці червня 2022 року група Conti закрила свої веб-сайти та припинила існування, імовірно розділившись на кілька менших організацій.

Розвиток тіньових ринків

На тіньових платформах злочинці торгують та обмінюються доступом до організаційних мереж, викраденими даними, інструментами та послугами для здійснення атак. Інтерес до організацій з країн Латинської Америки зростає: кількість повідомлень у темній мережі, що стосуються цього регіону, протягом перших трьох кварталів 2023 року вже на 32% перевищила загальну кількість повідомлень у 2022 році. У більш ніж половині списків (53%) із зазначенням певної країни в регіоні вказується Бразилія, Аргентина або Мексика.

Більшість повідомлень в темній мережі (70%) містять оголошення про продаж або купівлю доступу до інфраструктури організацій. Одна п'ята (22%) лістингів стосується продажу, купівлі або розповсюдження баз даних, що містять конфіденційну інформацію. Приблизно 6% повідомлень стосуються новин про зламані ресурси.

Найчастіше в темній мережі продається доступ до мереж фінансових установ, державних установ, IT-компаній, промислових підприємств і сервісних організацій. Бази даних, які продаються чи розповсюджуються безкоштовно, як правило, містять інформацію, виточену з державних установ, телекомунікаційних компаній, інтернет-магазинів і фінансових установ.

Вартість доступу залежить від кількох факторів: характеристик самої організації, таких як галузь і річний дохід, а також від типу пропонованого доступу та рівня привілеїв облікового запису. Середня вартість становить близько 600 доларів. Найдорожчим видом доступу є облікові дані для входу в інфраструктуру

фінансових організацій: доступ до банку пропонується в середньому за 1400 доларів, а ціни досягають 18 000 доларів.

Соціальна інженерія

Атаки з використанням соціальної інженерії є однією з головних загроз для регіону, як для організацій, так і для приватних осіб. Наприклад, програми-вимагачі проникали в корпоративні мережі через електронну пошту в 53% успішних атак. У звіті KPMG Fraud Outlook виявилося, що 32% респондентів у Латинській Америці спостерігали збільшення спроб фішингових атак у 2022 році, тоді як у звіті LATAM CISO Report: Cybersecurity Insights From Industry Leaders зазначається, що 88% лідерів у сфері кібербезпеки вважають різноманітні форми соціальної інженерії основними. головна загроза для компаній.

Дослідження, проведене KnowBe4, показує, що рівень обізнаності співробітників латиноамериканських організацій нижчий порівняно з іншими регіонами: 41% користувачів не можуть розпізнати фішингову атаку. Це означає, що четверо з десяти співробітників можуть завантажувати та запускати вкладення з фішингових електронних листів, натискати шкідливі посилання або передавати облікові дані зловмисникам. В інших регіонах цей показник не перевищує 35%.

Атаки соціальної інженерії часто спрямовані на людей через соціальні мережі, програми обміну повідомленнями та кампанії електронною поштою. Однак найчастіше такі атаки відбуваються через фішингові або зламані веб-сайти (58%). Найбільше фішингових сайтів зафіксовано в Бразилії. За даними SocRadar, з жовтня 2022 року по жовтень 2023 року було зареєстровано понад 2600 потенційних фішингових доменів з метою підробки веб-сайтів бразильських організацій. Бразильський щорічник громадської безпеки повідомляє про зростання випадків онлайн-шахрайства на 66% у 2022 році. Ця загроза також актуальна для інших країн регіону: близько 1000 фішингових доменів було зареєстровано в Колумбії, понад 800 в Аргентині та понад 500 у Мексиці та Перу в той же період. Зловмисники здебільшого імітують сайти криптовалютних бірж, фінансових установ та державних служб.

У травні 2023 року дослідники виявили масштабну фішингову кампанію, націлену на окремих осіб і організації в Мексиці. Зловмисники надсилали електронні листи з вкладеним файлом, що імітував формат податкової квитанції CFDI, який зазвичай використовується в Мексиці. Після відкриття вкладення пристрій користувача було заражено шкідливим програмним забезпеченням, здатним захоплювати облікові дані для входу в банківські рахунки. Експерти вважають, що ця кампанія почалася в 2021 році, за останні два роки шахраї обдурили понад 4000 жертв, назбиравши понад 55 мільйонів доларів.

Банківські трояни

Банківські трояни становлять значну загрозу для громадян у Латинській Америці, становлячи третину (32%) усіх виявлених шкідливих програм. У регіоні поширюються численні банківські трояни, такі як BBTok, GoatRAT, PixBankBot і Grandoreiro. Жителі Бразилії та Мексики особливо вразливі; ці країни, ймовірно, будуть більш зацікавлені зловмисниками через їхню кількість населення та широке використання онлайн-банкінгу.

У вересні 2023 року банківський троян BBTok почав поширюватися Латинською Америкою, націлившись на жителів Мексики та Бразилії. Він імітує інтерфейси понад 40 мексиканських і бразильських банків, включаючи Citibank, Scotibank, Banco Itaú і HSBC. Це дозволяє шахраям обманом змушувати користувачів вводити коди двофакторної автентифікації та таким чином отримувати контроль над обліковими записами. Крім того, ця шкідлива програма може викрадати номери платіжних карток.

У Бразилії нещодавно атаки були спрямовані на системи миттєвих платежів PIX. Наприклад, троян GoatRAT націлений на користувачів трьох бразильських банків: Nubank, Banco Inter і PagBank. Цей троян перехоплює ключ PIX, необхідний для грошових переказів, і викрадає кошти з банківського рахунку жертви.

Витік даних

За даними IBM, середня вартість збитків від витоку інформації в країнах Латинської Америки зросла за рік на 32% і на початок 2023 року склала $3,69 млн. Більшість атак, які призвели до витоку даних, припали на урядовий сектор (27%),

далі йдуть обробна промисловість (15%), фінансовий сектор (10%), роздрібна торгівля (10%) та освіта (7%).

При атаках на організації зловмисники викрадали насамперед особисті дані (40% від загального обсягу викраденої інформації) та інформацію, що містить комерційну таємницю (21%). Найчастіше витік персональних даних громадян відбувався з систем державних органів, фінансових організацій, навчальних закладів. Основною причиною витоку даних в організаціях були атаки програм-вимагачів, які вимагали оплату в обмін на нерозголошення викраденої інформації. Атаки на фізичних осіб призвели до викрадення облікових і персональних даних (38% і 25% відповідно) і даних платіжних карток (25%).

Зловмисники можуть продавати скомпрометовані дані в темній мережі або робити їх загальнодоступними. Наприклад, дані з аргентинської лікарні Garrahan, яка постраждала від кібератаки у 2022 році, були виставлені на продаж у темній мережі за 1500 доларів.

Серед баз даних, знайдених у темній мережі, 28% були вкрадені в державних установах, 20% у IT-компаніях і 8% у фінансових організаціях.

Висновки та рекомендації

За останні роки країни Латинської Америки зазнали низки атак, які вплинули на функціонування критичних секторів і навіть цілої держави. Регіон виявився дуже неготовим до кіберзагроз через економічні та соціальні фактори, а також швидке впровадження цифрових технологій без забезпечення необхідного захисту. Ми вважаємо, що співпраця між країнами, інвестиції в безпеку, політична підтримка змін і покращення освіти є вирішальними кроками. Ми пропонуємо низку заходів для посилення кібербезпеки для окремих організацій, секторів і всього регіону.

Рекомендації для урядів

Прийняти стратегії інформаційної безпеки на національному рівні

Лише частина країн Латинської Америки прийняла національні стратегії кібербезпеки. Хоча прийняття стратегії саме по собі не гарантує підвищення рівня безпеки, ці документи визначають напрямок подальшого розвитку та підкреслюють

важливість кібербезпеки на державному рівні. Уряди повинні розробляти, впроваджувати та регулярно оновлювати національні політики та стратегії кібербезпеки, залучаючи до процесу широкий спектр зацікавлених сторін. Розробка цих стратегій повинна мати необхідне фінансування та політичну підтримку для забезпечення ефективної координації та чіткого розподілу відповідальності.

Національна стратегія інформаційної безпеки повинна включати оцінку загроз і перелік чітко визначених цілей і кроків, необхідних для їх досягнення. До розробки стратегії мають бути залучені представники державних організацій, бізнесу та сектору кібербезпеки, а проекти мають бути розглянуті та публічно обговорені.

Гармонізувати законодавство щодо кібербезпеки та захисту персональних даних

Країни регіону повинні розглянути питання про узгодження спільних стандартів кібербезпеки для більш ефективної співпраці або створення спільних механізмів для обміну інформацією про міжнародні кіберзагрози та боротьби з ними.

Законодавство щодо кібербезпеки та захисту даних необхідно регулярно оновлювати, щоб йти в ногу з останніми кіберзагрозами та технологічними досягненнями. Це також має сприяти ефективній координації між різними правоохоронними органами та органами безпеки.

Захист критичної інформаційної інфраструктури

Уряди повинні визначити неприпустимі події на галузевому та національному рівнях. Такий підхід допомагає ефективно розподіляти ресурси для забезпечення захисту найбільш критичних систем. Пріоритет має бути наданий інфраструктурі таких секторів, як уряд, телекомунікації, виробництво та фінанси, а також інших секторів, життєво важливих для економіки та національної безпеки, таких як електронна комерція та сільське господарство. Слід також враховувати швидкість цифрової трансформації та рівень зрілості інформаційної безпеки в країні.

Створити національні та галузеві центри реагування на кіберінциденти та вдосконалити механізми співпраці з організаціями

Національні групи реагування на кіберінциденти відповідають за моніторинг загроз і допомогу організаціям у відновленні після серйозних кібератак. Створення таких структур має бути пріоритетним при реалізації стратегії безпеки національної безпеки та критичної інфраструктури. У 2023 році лише 24 країни регіону мали національні CERT/CSIRT. Країни, які вже мають такі структури, повинні створити галузеві CERT і співпрацювати для підтримки створення регіональних центрів реагування. Слід також зазначити, що механізми звітування про інциденти можуть бути недостатньо зрозумілими для спеціалістів із безпеки. Необхідно розробити прості та прозорі механізми звітування про кіберінциденти, що виникають в організаціях, а також докласти зусиль для підвищення довіри до національних CERT та взаємодії з державними структурами. Покращений обмін інформацією між організаціями та центрами кібербезпеки може допомогти запобігти атакам і своєчасно реагувати на нові загрози.

Реагування на кіберзагрози має бути інтегровано в загальну стратегію захисту та відновлення критичної національної інфраструктури.

Підвищувати обізнаність і сприяти освіті з питань кібербезпеки

Уряди повинні інвестувати в кампанії з інформування громадськості про поточні загрози та способи захисту від них. У цьому регіоні, як і в усьому світі, не вистачає кваліфікованих фахівців з кібербезпеки. Тому популяризація цієї галузі та суміжних професій, розробка навчальних програм у навчальних закладах має бути пріоритетом держави.

Співпрацювати на міжнародному рівні

Кіберзлочинність давно вийшла за межі окремих держав, що робить надзвичайно важливим для країн співпрацювати одна з одною у боротьбі з кіберзагрозами. Обмінюючись інформацією, ресурсами та досвідом, країни можуть спільно зміцнити свій захист і зменшити ризики, створені кіберзлочинцями в різних юрисдикціях. Національні стратегії кібербезпеки повинні включати цілі розвитку міжнародних відносин у сфері кібербезпеки.

Рекомендації для підприємств

Визначте неприйнятні події та критичні активи

Щоб забезпечити кіберстійкість компанії, необхідно насамперед проаналізувати основні ризики та скласти перелік недопустимих подій, які можуть завдати суттєвої шкоди її діяльності. Цей крок допоможе визначити важливі активи та зосередитися на захисті найцінніших ресурсів. Необхідно розробити стратегію запобігання неприйнятним подіям, включаючи необхідні заходи безпеки та моніторинг мережевої активності за допомогою сучасних інструментів безпеки.

Відстежуйте інциденти та реагуйте на кіберзагрози

Системи моніторингу та виявлення інцидентів необхідні для своєчасного реагування на потенційні загрози та атаки. Для цього ми рекомендуємо використовувати системи SIEM, які збирають і аналізують інформацію про події безпеки з різних джерел у режимі реального часу. Разом із рішеннями XDR (розширене виявлення загроз і реагування) і NTA (аналіз мережевого трафіку) це допоможе виявити атаки на ранніх стадіях і забезпечить швидке реагування, зменшивши ризики для організації.

Оцінити ефективність кібербезпеки

Ефективність прийнятих заходів кібербезпеки слід регулярно перевіряти для оцінки ефективності стратегії та захисту. Рекомендуємо звернути особливу увагу на перевірку нестерпних для організації подій.

Також варто брати участь у програмах винагороди за помилки, щоб зовнішні дослідники безпеки могли знайти нові вразливості. Ці програми допоможуть виявити та усунути вразливості до того, як зловмисники зможуть ними скористатися.

Навчати співробітників і розвивати фахівців з інформаційної безпеки

Важливо навчати співробітників основам кібербезпеки та проводити тренінги, щоб підвищити обізнаність про поточні кіберзагрози та захистити від методів соціальної інженерії.

Для ефективної боротьби з кіберзагрозами організації повинні інвестувати в розвиток своїх експертів з кібербезпеки. Регулярне навчання та сертифікація

співробітників у сфері кібербезпеки дозволить підвищити їхні навички та знання, посиливши компанію експертною підтримкою у запобіганні та реагуванні на кібератаки. Одним із найефективніших способів зробити це є участь у кібервправах на спеціальних платформах, де спеціалісти з інформаційної безпеки можуть практикувати розпізнавання методів атак та протидію їм.

Методологія

Дані та висновки, представлені в цьому звіті, базуються на власному досвіді Positive Technologies, а також на аналізі загальнодоступних ресурсів, включаючи урядові та міжнародні публікації, дослідницькі статті та галузеві звіти.

За нашими оцінками, більшість кібератак не оприлюднюються через ризики для репутації. Як наслідок, навіть компанії, що спеціалізуються на розслідуванні інцидентів та аналізі хакерської діяльності, не можуть кількісно визначити точну кількість загроз. Це дослідження має на меті привернути увагу компаній та осіб, яким не байдужий стан інформаційної безпеки, до ключових мотивів і методів кібератак, а також висвітлити основні тенденції у мінливому ландшафті кіберзагроз.

У цьому звіті кожна масова атака (наприклад, фішингові листи, надіслані на кілька адрес) розглядається як один інцидент, а не кілька. Пояснення термінів, які використовуються в цьому звіті, дивіться в глосарії Positive Technologies». ***(Cybersecurity threatscape for Latin America and the Caribbean: 2022–2023 // Positive Technologies (https://www.ptsecurity.com/ww-en/analytics/latam-cybersecurity-threatscape-2022-2023-en/). 21.12.2023).***

***

Кіберстрахування

«Велика Британія продовжує залишатися прибутковою мішенню для кіберзлочинців, оскільки зловмисні атаки на цифрові системи та технології впливають на організації в різних секторах. За даними уряду Великобританії, понад 37% великих компаній стали жертвами кіберзлочинців.

У контексті все більш витончених атак і розширення ландшафту загроз британський ринок кіберстрахування у 2023 році зазнав припливу нових покупців, які виграють від стабілізації ставок після постпандемічних максимумів. Нові учасники ринку викликали конкуренцію, і в результаті клієнти отримали вигоду від посилення покриття та потужності.

Щомісяця у Великій Британії відбуваються сотні кібератак, і дедалі витонченіші методи загрози означають, що вони зазнають впливу на організації будь-якого розміру. Про резонансні кібератаки у 2023 році повідомили різноманітні організації: від державних установ і роздрібних торговців до ЗМІ.

Деякі постраждали через уразливості в ланцюгах постачання IT, що посилило потребу в пильності щодо засобів контролю кібербезпеки, таких як ретельний моніторинг заходів, вжитих продавцями та постачальниками. Події включали програми-вимагачі серед інших атак, які регулярно відкривали дані клієнтів, втручалися в ланцюги поставок тощо.

Тенденції ринку кіберстрахування Великобританії у 2023 році

На цьому тлі у 2023 році на страховому ринку відбулися зрушення, зокрема:

Ціноутворення: ціни на кіберстрахування продовжували знижуватися в середньому протягом року. У третьому кварталі ціни впали на 8% для клієнтів із річним доходом понад 250 мільйонів фунтів стерлінгів, порівняно з річним зростанням у середньому на 38% у тому ж кварталі минулого року. З цих клієнтів 71% відчули зниження цін цього року. Зниження ціни на надлишкові шари, як правило, було більш значним.

Обмеження та потужність: у другому кварталі 2023 року страховики зазвичай продовжували знімати деякі обмеження щодо існуючого покриття. Потужність зросла на тлі постійної підтримки Lloyd's кіберринку. Понад 9% клієнтів збільшили своє утримання в третьому кварталі, що може свідчити про підвищення довіри до їхніх заходів кібербезпеки.

Претензії: у 2023 році кількість претензій зросла порівняно з минулим роком, причому програмне забезпечення-вимагач залишається ключовим фактором. Зловмисники продовжують використовувати інноваційні та витончені способи,

щоб викликати збої. Майже половина всіх претензій на сьогоднішній день у 2023 році походить від атак на ланцюг постачання IT. Однак тенденції свідчать про те, що модель програм-вимагачів стає все складніше монетизувати.

Андеррайтинг: системні кіберризики залишаються головною проблемою. Страховики, як правило, включають конкретні військові та територіальні виключення в поліси, з формулюванням виключень війни відповідно до вимог Ллойда. Страховики ретельно вивчають сфери, які мають безпосереднє відношення до ландшафту загроз, наприклад методи збору даних і управління постачальниками. Незважаючи на це, вливання капіталу на ринок кіберстрахування призвело до розширення можливостей для клієнтів.

Пошкодження кібермайна та переривання діяльності (PDBI): Відповідно до мандату Управління пруденційного регулювання (PRA) від 2017 року, страховики повинні чітко вказати, чи покривається кібернебезпека як ризик у страховому полісі, щоб уникнути «тихого кібер» (кіберризик у некібернетичні політики). Це призвело до виключення кібернебезпек, зокрема в політиці «усіх ризиків» і власності. Це ключовий фактор у розвитку кіберринку PDBI, але не єдиний фактор, який розглядають покупці.

Розповсюдження операційних технологій (для критичної інфраструктури, транспорту, виробництва, морських суден, енергетики та комунальних послуг), високотехнологічних будівель із притаманним ризиком PDBI та підключених пристроїв також сприяло зростанню цього сектору. Наразі рекламована потужність PDBI становить понад 200 мільйонів фунтів стерлінгів, і ставки загалом знизилися у 2023 році. Хоча традиційний ринок нерухомості та постраждалих часто пропонує покриття для нешкідливих кіберподій, кіберринок PDBI заповнює порожнечу для зловмисні події, такі як атака програм-вимагачів.

Прогноз на 2024 рік

Кібератаки на ланцюжок поставок IT, ймовірно, залишаться фокусом у 2024 році. У 2023 році 44% заяв клієнтів стосувалися атак на постачальників IT-послуг або програмний продукт. Крім того, дедалі помітнішим стало викрадання даних — як частина атак програм-вимагачів. Ми очікуємо, що протягом 2024 року

страховики продовжуватимуть зосереджуватися на управлінні постачальниками IT-технологій і зборі даних.

Хоча очікується, що програми-вимагачі та інші події триватимуть, є оптимізм щодо того, що страхові можливості залишаться доступними у 2024 році.

Деякі клієнти, ймовірно, зіткнуться з новими проблемами щодо ризику, пов'язаного з операційною технологією. Лондонський ринок страхування забезпечує можливість відшкодування майнової шкоди, спричиненої зловмисною кіберподією.

Протягом 2023 року штучний інтелект був гарячою темою, і багато організацій досліджували способи, за допомогою яких генеративний ШІ може підтримувати повсякденну бізнес-діяльність. Дискусії щодо того, як такі інструменти будуть керуватися, тривають, і для клієнтів важливо усвідомлювати пов’язані з цим ризики.

Як Marsh може допомогти вам зрозуміти, виміряти та керувати кіберризиками

Управління кіберризиками — це безперервна робота, і для організацій важливо прийняти проактивний підхід. Як ваш консультант з кіберризиків, Марш може допомогти організаціям кількома способами:

Управління інцидентами: наша команда управління кіберінцидентами може допомогти сформулювати вашу реакцію на кіберінциденти та підтримати вас під час і після інциденту.

Консультації щодо ризиків: наша команда консультантів може співпрацювати з вами, щоб підвищити стійкість кібербезпеки з огляду на прогрес технологій і постійну зміну ландшафту загроз.

Аналіз ризиків: наші інструменти економічного моделювання та кількісної оцінки (такі як Blue[i]) можуть інформувати про передачу ризиків і прийняття рішень щодо кібербезпеки.

Страхування. Наші власні програми страхування дозволяють ефективно передавати кіберризики». ***(Ellis Nicholson and Daniel Lewsley. Five trends in the UK***

cyber insurance market // Marsh (https://www.marsh.com/uk/services/cyber-risk/insights/five-trends-in-uk-cyber-insurance-market.html). 18.12.2023).

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Найнебезпечніший ядерний об'єкт Великобританії, Селлафілд, був зламаний кібергрупами, тісно пов'язаними з Росією та Китаєм, повідомляє Guardian.

Розслідування показало, що це дивовижне розкриття інформації та її потенційні наслідки постійно приховувалися старшим персоналом великого сховища ядерних відходів та зняття з експлуатації.

The Guardian виявив, що влада не знає точно, коли IT-системи були вперше скомпрометовані. Але джерела повідомили, що вперше злам було виявлено ще в 2015 році, коли експерти зрозуміли, що в комп'ютерні мережі Селлафілда було вбудовано зловмисне програмне забезпечення – програмне забезпечення, яке може приховуватися та використовуватися для шпигунства чи атаки на системи.

Наразі невідомо, чи вдалося знищити шкідливе програмне забезпечення. Це може означати, що деякі з найбільш чутливих видів діяльності Селлафілда, як-от переміщення радіоактивних відходів, моніторинг витоків небезпечних матеріалів і перевірка пожеж, були скомпрометовані.

Джерела припускають, що, ймовірно, іноземні хакери отримали доступ до найвищих ешелонів конфіденційних матеріалів на сайті, який розкинувся на 6 квадратних кілометрах (2 квадратних милях) на узбережжі Камбрії та є одним із найнебезпечніших у світі.

За словами джерел, повний масштаб будь-якої втрати даних і будь-яких поточних ризиків для систем стало важче кількісно оцінити через те, що Селлафілд протягом кількох років не повідомляв ядерних регуляторів.

Викриття стало результатом Nuclear Leaks, річного розслідування Guardian щодо кіберзлому, радіоактивного забруднення та токсичної культури на робочому місці в Sellafield.

На цьому місці знаходиться найбільше сховище плутонію на планеті, і це розгалужене сміттєзвалище для ядерних відходів від програм озброєння та десятиліть виробництва атомної енергії.

Охороняється озброєною поліцією, він також містить документи планування на випадок надзвичайних ситуацій, які будуть використані, якщо Сполучене Королівство зазнає іноземного нападу або зіткнеться з катастрофою. Побудований більше 70 років тому і раніше відомий як Windscale, він виробляв плутоній для ядерної зброї під час холодної війни та приймав радіоактивні відходи з інших країн, включаючи Італію та Швецію.

The Guardian також може розкрити, що за даними джерел в Управлінні ядерного регулювання (ONR) і службах безпеки, минулого року до Селлафілда, який налічує понад 11 000 співробітників, було застосовано певні «спеціальні заходи» за постійні порушення кібербезпеки.

Вважається, що наглядовий орган також готується притягнути до відповідальності осіб за кіберпровали.

ONR підтвердив, що Sellafield не відповідає кіберстандартам, але відмовився коментувати порушення або заяви про «приховування».

Речник сказав: «Деякі конкретні питання є предметом поточних розслідувань, тому ми не можемо наразі коментувати».

У своїй заяві Селлафілд також відмовився коментувати свою нездатність повідомити регуляторам, натомість зосередившись на покращеннях, яких, за його словами, було зроблено за останні роки.

Тіньовий держсекретар Лейбористської партії з енергетичної безпеки та чистого нуля Ед Мілібенд сказав, що це «дуже тривожний звіт про одну з наших найбільш чутливих частин енергетичної інфраструктури».

«Це висуває звинувачення, до яких уряд має поставитися з найбільшою серйозністю», – сказав він.

«Уряд зобов’язаний сказати, коли він вперше дізнався про ці звинувачення, які заходи вжив він і регулятор, і надати гарантії щодо захисту нашої національної безпеки».

Проблема незахищених серверів у Селлафілді отримала прізвисько Волдеморт на честь лиходія з Гаррі Поттера, за словами урядовця, знайомого з розслідуванням ONR та збоями IT на сайті, оскільки це було дуже чутливим і небезпечним. Це стосувалося дуже конфіденційних даних, якими могли скористатися вороги Британії. Серверна мережа Sellafield була охарактеризована чиновником як «фундаментально незахищена».

Масштаб проблеми було виявлено лише тоді, коли співробітники зовнішнього сайту виявили, що вони можуть отримати доступ до серверів Селлафілда, і повідомили про це в ONR, за словами інсайдера в сторожовому центрі.

Інші проблеми стосуються того, що зовнішні підрядники можуть підключати карти пам’яті до системи без нагляду.

Під час одного надзвичайно незручного інциденту, який стався в липні минулого року, дані для входу та паролі для безпечних IT-систем були випадково передані на національному телебаченні BBC One у серіалі про природу Countryfile після того, як знімальні групи були запрошені на безпечний сайт для матеріалу про сільські громади та атомну промисловість.

ONR підготувало повідомлення про судове переслідування Селлафілда з питань кібербезпеки – форму примусового заходу, яке воно може вжити, лише якщо вважає, що є «достатньо доказів для забезпечення реалістичної перспективи засудження».

Згідно зі звітом від 2012 року, з яким ознайомилася Guardian, про кіберпроблеми знали високопоставлені особи на ядерному майданчику принаймні десять років, у якому попереджалося про «критичні вразливості безпеки», які необхідно терміново усунути.

Було встановлено, що ресурсів безпеки на той час було «недостатньо для контролю внутрішньої загрози [з боку персоналу] … не кажучи вже про реагування на значне зростання зовнішньої загрози».

Понад десять років потому співробітники Селлафілда, регулятори та джерела в розвідувальному співтоваристві вважають, що системи на величезному звалищі ядерних відходів все ще не відповідають призначенню. Вони також вважають, що вище керівництво намагалося навмисно приховати масштаб проблем, пов'язаних із проблемами кібербезпеки на сайті, від представників служби безпеки, яким в останні роки доручено перевіряти вразливість Великобританії до атак. Це є предметом потенційного судового переслідування.

Співробітники служби безпеки також стурбовані тим, що ONR не поспішає ділитися своєю розвідкою про кіберпровали в Селлафілді, оскільки вони вказують на те, що його власний контроль був неефективним протягом більше десяти років.

В останньому річному звіті ONR зазначено, що «потрібні покращення» Sellafield та інших сайтів, щоб усунути ризики кібербезпеки. Він також підтвердив, що цей сайт перебував під «значно підвищеною увагою» через цю діяльність.

ONR заявило, що виявило «недоліки» в кібербезпеці під час своїх інспекцій і зазначило, що в результаті вжило «примусових заходів».

Такі масштаби занепокоєння кібербезпекою, деякі чиновники вважають, що цілі нові системи повинні бути терміново побудовані в центрі управління надзвичайними ситуаціями Селлафілда неподалік – окремому безпечному об'єкті.

Серед дуже конфіденційних документів, які зберігаються в Селлафілді, є посібники з надзвичайних ситуацій, плани, які ведуть людей через надзвичайні ядерні протоколи та те, що робити під час іноземного нападу на Великобританію.

Ці документи включають деякі знання, отримані під час різноманітних важливих операцій, включаючи навчання Reassure у 2005 році та регулярні навчання Оскар, які мали на меті перевірити здатність Великобританії впоратися з ядерною катастрофою в Камбрії.

ONR було настільки стурбоване тим фактом, що сторонні сайти могли отримати доступ до серверів Селлафілда, і очевидним прикриттям персоналом, що

опитувало команди з обережністю. Правління Селлафілда провело розслідування проблеми в 2013 році, і ONR попередив, що буде потрібно більше прозорості в IT-безпеці.

За словами представників служби безпеки, кібератаки та кібершпигунство з боку Росії та Китаю є одними з найбільших загроз для Великобританії. Останній Національний реєстр ризиків, офіційний документ, який описує основні небезпеки, з якими може зіткнутися Великобританія, включає кібератаку на цивільну ядерну інфраструктуру.

Останніми роками зловмисники з ворожих держав атакували союзників у спільноті обміну розвідданими «П'ять очей». У червні цього року США зазнали атаки через програмне забезпечення для передачі файлів.

Британське кіберпідрозділ GCHQ, яке має офіси в центрі Лондона та є частиною внутрішньої розвідувальної мережі зі штаб-квартирою в Челтенхемі в графстві Глостершир, попередило про підвищений ризик кібератак на критично важливу національну інфраструктуру з Росії та Китаю.

Зростаюча стурбованість уряду щодо участі Китаю в критично важливій національній інфраструктурі Великобританії призвела до того, що китайська державна енергетична компанія CGN була виключена з ядерного проекту Sizewell C у Саффолку, а продукти Huawei були вилучені з серця телекомунікаційної мережі в останні роки.

Це перекреслило заклинання тісних англо-китайських відносин, кульмінацією яких став тодішній прем'єр-міністр Девід Кемерон, який вітав «золоту еру» між країнами та пив пиво з китайським прем'єр-міністром Сі Цзіньпіном у пабі в Бакінгемширі в 2015 році.

Уряд Ріші Сунака підтримав розширення ядерної промисловості країни після енергетичної кризи, продовживши там, де зупинився його попередник Борис Джонсон. На початку цього року тодішній міністр енергетики Грант Шаппс заснував організацію Great British Nuclear, призначену для створення нових атомних електростанцій. Покоління нових ядерних проектів зрештою вимагатиме розширення діяльності Великобританії з виведення з експлуатації.

Виведення з експлуатації атомних станцій, велика частка яких здійснюється в Селлафілді, є одним із найбільших витрат річного бюджету британського уряду. Робота сайту коштує приблизно 2,5 мільярда фунтів стерлінгів на рік. Виведення з експлуатації є настільки великим, довгостроковим законопроектом, що він був розглянутий як «фіскальний ризик» для економічного здоров'я Великобританії органом контролю за витратами, Управлінням з бюджетної відповідальності. За оцінками, управління ядерною енергетикою та збройовою промисловістю Великобританії може коштувати 263 мільярди фунтів стерлінгів.

Ця цифра різко змінюється залежно від того, як розраховується майбутній грошовий потік, і OBR попереджає, що довгострокові витрати Sellafield можуть коливатися від мінус 50% до плюс 300%.

Представник Sellafield сказав: «Ми дуже серйозно ставимося до кібербезпеки в Sellafield. Усі наші системи та сервери мають кілька рівнів захисту.

«Критичні мережі, які дозволяють нам працювати безпечно, ізольовані від нашої загальної IT-мережі, тобто атака на нашу IT-систему не проникне в них.

«За останні 10 років ми еволюціонували, щоб відповідати викликам сучасного світу, включаючи більшу увагу до кібербезпеки.

«Ми тісно співпрацюємо з нашим регулятором. У результаті прогресу, якого ми досягли, ми маємо узгоджений шлях відмови від «суттєво посиленого» регулювання».

Представник ONR сказав: «Sellafield Ltd наразі не відповідає високим стандартам, які ми вимагаємо щодо кібербезпеки, тому ми приділили їм значно посилену увагу.

«Деякі конкретні питання є предметом поточних розслідувань, тому ми не можемо наразі коментувати».

До публікації Sellafield і ONR відмовилися відповідати на низку конкретних запитань або сказати, чи були мережі Sellafield скомпрометовані групами, пов’язаними з Росією та Китаєм. Після публікації вони заявили, що у них немає записів, які б припускали, що мережі Селлафілда були успішно атаковані державними діячами, як це описав Guardian.

Представник Департаменту енергетичної безпеки та Net Zero сказав: «Ми очікуємо найвищих стандартів безпеки та безпеки, оскільки колишні ядерні об'єкти демонтуються, і регулятор чітко заявляє, що громадська безпека в Селлафілді не загрожує.

«Багато піднятих проблем є історичними, і регулятор деякий час працював із Sellafield, щоб забезпечити впровадження необхідних покращень. Ми очікуємо регулярних оновлень про те, як це просувається». ***(Anna Isaac, Alex Lawson. Sellafield nuclear site hacked by groups linked to Russia and China // Guardian News & Media Limited or its affiliated companies (https://www.theguardian.com/business/2023/dec/04/sellafield-nuclear-site-hacked-groups-russia-china). 04.12.2023).***

***

«За останні 50 років поля битв були відзначені повітрям, землею та морем. Однак сьогодні традиційне поле битви розширюється, коли космос і кібербезпека стають четвертим і п'ятим полем битв відповідно.

Атака російських хакерів на компанію супутникового зв'язку Viasat увечері перед тим, як країна вторглася в Україну, є яскравим прикладом появи обох фронтів битви. Світ змінюється, і сучасна війна продовжуватиме включати як кібернетичні, так і фізичні елементи. Галузь кібербезпеки зобов'язана сповістити про цю зміну та обговорити її наслідки з радами директорів, керівниками CISO та іншим керівництвом компаній, а також запропонувати вказівки щодо того, як підготуватися до цієї нової реальності.

Підготовка кіберслужби швидкого реагування

Подібно до того, як військові герої нашої країни нескінченно тренуються до фізичної війни, нам потрібно підготувати перших спеціалістів із кібербезпеки для створення та підтримки стійкості під час кібервійни. Хоча посібник, безсумнівно, змінюватиметься залежно від ландшафту загроз, що розвивається, є кілька перевірених і надійних основ, які залишаться основою потужних програм кібербезпеки та стійкості.

1. Надайте пріоритет людському фактору.

Хоча внутрішні загрози завжди були ризиком, генеративний штучний інтелект збільшив ризик ненавмисних загроз, зробивши фішингові та інші атаки соціальної інженерії правдоподібнішими, ніж будь-коли. Якщо кіберзлочинець обманом змусить співробітника надати облікові дані свого облікового запису або натиснути зловмисне посилання, він може проникнути в корпоративні мережі, щоб викрасти IP-адресу та фінансові дані, вимкнути системи або завдати шкоди бізнесу (або навіть економіці чи нашому способу життя).

Люди є нашою першою лінією захисту та вістрям стійкості підприємства. Таким чином, нам потрібно подвоїти рівень обізнаності та навчання з кібербезпеки. Відмова від тривалих щорічних тренінгів за допомогою PowerPoint на користь частого, короткого та привабливого вмісту може сприяти резонансу повідомлень і залишати кібербезпеку в центрі уваги працівників. Основні напрямки навчання мають включати усвідомлення загроз, кібербезпечну поведінку та процеси звітування у разі виявлення підозрілої активності.

Найголовніше, якщо ви хочете, щоб співробітники серйозно ставилися до кібербезпеки, вам потрібно навчити їх тому, як їхні дії можуть вплинути на безпеку організації, і побудувати корпоративну культуру, яка надає пріоритет кібербезпеці від зали засідань до пошти.

2. Створіть стійкість підприємства.

Стійкість вимагає проактивного підходу до кібербезпеки. Сумна реальність полягає в тому, що питання вже не в тому, чи нападуть на вас, а в тому, коли. Якщо ми чекатимемо з діями, поки не станеться інцидент, наслідки можуть бути катастрофічними.

Щоб розробити ефективний план стійкості, який дозволить вам швидко відновлюватися після будь-якої втрати даних, усі бізнес-департаменти повинні об’єднатися, щоб визначити критичні активи, включаючи системи, дані та програми, а також бізнес-процеси, на які вони покладаються, і потім визначити пріоритети. їх захист на основі бізнес-ризиків, які вони становлять.

Наприклад, деякі системи, що містять критично важливі бізнес-дані, можливо, потрібно буде повернути в режим онлайн перед певними програмами. Після того, як ви визначили та визначили пріоритети активів вашої компанії, ви можете почати оцінювати кожен у порядку важливості, щоб виявити та усунути прогалини в безпеці.

Можливість швидко й точно реагувати на кіберзагрози для кращої підтримки безперервності бізнесу та забезпечення оптимального відновлення також вимагає:

• Освоєння основ безпеки, таких як впровадження шифрування, багатофакторної автентифікації, програм керування виправленнями тощо.

• Розробка та відпрацювання плану реагування на інцидент, щоб кожен знав про свої обов’язки, якщо станеться інцидент, і міг швидко відреагувати, щоб обмежити шкоду.

3. Створюйте коаліції на благо.

Змінюються не тільки традиційні поля битв; опоненти також. Зловмисники більше не є людьми, які зламують у своїх підвалах. Зараз переважна більшість — це національні держави та організовані злочинні групи. Якщо є коаліційна гра проти хороших, ми повинні формувати коаліції проти поганих, щоб мати шанс на перемогу.

З точки зору галузі, це означає посилення співпраці між державним і приватним секторами для обміну інформацією про загрози та найкращими методами захисту від атак. Для окремих організацій це означає усвідомлення того, що вам не потрібно самостійно брати участь у боротьбі з кібербезпекою. Створення екосистеми надійних партнерів, які можуть консультувати, розгортати та діяти від вашого імені, допоможе вам створити міцний захист, який витримає навіть найдосконаліших супротивників.

Нестандартне мислення, щоб виграти кібервійну

Організації вже давно використовують реактивний підхід до кібербезпеки, де вони купують новий продукт для кожної нової загрози, яка з’являється. Однак таке мислення, орієнтоване на вхідні дані, ненавмисно створило додаткові складності та плутанину, збільшуючи ризик, а не зменшуючи його.

Оскільки кібербезпека стала п’ятим полем битви, нам потрібно зробити нашу ставку на землю та замінити цей застарілий підхід проактивною стратегією, яка зосереджена на людях, процесах, технологіях і партнерстві. Це єдиний спосіб зменшити системний ризик і підвищити стійкість підприємства. І це єдиний спосіб забезпечити велич на сьогоднішньому полі кібербою». ***(Kevin Lynch. Cybersecurity: The Fifth Battlefield // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/12/05/cybersecurity-the-fifth-battlefield/?utm_source=flipboard&utm_content=untangledcj%2Fmagazine%2FMSP1337+Cybersecurity+News&sh=98c59cf22755). 05.12.2023).***

***

«Відповідно до висновків урядового Агентства з кібербезпеки та безпеки інфраструктури (CISA), іранські хакери, очевидно, стоять за нещодавніми атаками на водні заводи США.

CISA опублікувала спільну консультацію з ФБР, АНБ, Агентством з охорони навколишнього середовища (EPA) та Ізраїльським національним кіберуправлінням (INCD), відзначаючи, що хакер (або група) під псевдонімом «CyberAv3ngers» націлений на програмовану логіку Unitronics контролери (PLC), кінцеві точки, які зазвичай використовуються компаніями у секторі систем водопостачання та водовідведення (WWS).

Ці пристрої також іноді використовуються в енергетиці, виробництві харчових продуктів і напоїв, а також у сфері охорони здоров’я, додали в консультації.

Рекомендовано пом’якшення

Ймовірно, CyberAv3ngers належать до Корпусу вартових ісламської революції (IRGC) Ірану та вирішили націлитися на ПЛК, оскільки їх виготовила ізраїльська компанія.

«Принаймні з 22 листопада 2023 року ці кібератори, афілійовані з IRGC, продовжували компрометувати облікові дані за замовчуванням у пристроях Unitronics», — йдеться в спільній консультації. «Кібератори, афілійовані з IRGC,

залишили зображення зіпсації, на якому написано: «Вас зламали, геть Ізраїль». Кожне обладнання, «вироблене в Ізраїлі», є законною ціллю CyberAv3ngers». Жертви охоплюють кілька штатів США».

Поки що це були лише кампанії зі псування, і немає жодних повідомлень про програм-вимагачів. встановлення

CISA повідомила, що всі постраждалі кінцеві точки були «відкриті для Інтернету з паролями за замовчуванням і за замовчуванням перебувають на порті TCP 20256». Надалі CISA рекомендує всім компаніям, які займаються критичною інфраструктурою, змінити всі паролі за замовчуванням на пристроях Unitronics і переконатися, що вони відключені від широкого Інтернету. Також корисно додати багатофакторну автентифікацію (MFA), а також налаштувати та підтримувати резервні копії.

Інші країни також використовують PLC того ж виробника. Infosecurity повідомляє, що Національний центр кібербезпеки Великої Британії (NCSC) нещодавно опублікував оновлене попередження про потенційний ризик, але додав, що ризик, швидше за все, «мінімальний, обмежений невеликими постачальниками» і, ймовірно, не порушить водопостачання країни». ***(Sead Fadilpašić. US government confirms Iran is behind cyberattacks on water companies // Future US, Inc. (https://www.techradar.com/pro/security/us-government-confirms-iran-is-behind-cyberattacks-on-water-companies?utm_source=flipboard&utm_content=larrybricker5%2Fmagazine%2FTO+READ+LATER+WHILE+DRIVING). 05.12.2023).***

***

«Згідно зі звітом Australian Cybersecurity Magazine, під час нещодавньої кібератаки кіберзлочинна група Hunters International націлилася на Austal USA, американську дочірню компанію австралійської суднобудівної фірми Austal, відомої своїми контрактами з ВМС США.

Цю інформацію було виявлено в щоденному оновленні атаки від HackNotice, постачальника аналізу загроз, 3 грудня 2023 року.

Austal USA, що базується в Мобілі, штат Алабама, бере участь у важливих військово-морських проектах, включаючи програму створення бойових кораблів Littoral і програму будівництва атомних підводних човнів типу Virginia.

Компанія також робить кроки вперед у секторі автономного будівництва човнів.

Однак час поточної атаки має вирішальне значення, оскільки підрозділ Austal у США, ключовий джерело прибутку для материнської компанії, зараз продається.

Hunters International, яка тепер замінює недіючу групу програм-вимагачів Hive, працює як група Ransomware-as-a-Service (RaaS) і погрожувала опублікувати 43 зразки файлів, що містять 87,2 МБ даних, відповідно до їх темного веб-сайту.

Значні наслідки

Атака на Austal USA має значні наслідки, особливо враховуючи попередній досвід компанії з атаками програм-вимагачів п’ять років тому.

Повідомляється, що під час цього інциденту жодної конфіденційної інформації не було викрадено.

Витік конфіденційних даних може мати значні наслідки як для Austal, так і для ВМС США.

Атака підкреслює важливість суворих заходів кібербезпеки, особливо в секторах, що стосуються національної безпеки.

Федеральна система правил закупівель Міністерства оборони США вимагає від підрядників повідомляти про будь-які кібератаки протягом 72 годин, підкреслюючи критичний характер цих загроз». ***(Ransomware attack compromises US subsidiary of Australian shipbuilder Austal // Fusion Media Limited (https://au.investing.com/news/stock-market-news/ransomware-attack-compromises-us-subsidiary-of-australian-shipbuilder-austal-3055203?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 05.12.2023).***

***

«Зусилля Міжнародного Комітету Червоного Хреста (МКЧХ) щодо встановлення правил ведення бойових дій із учасниками кібервійни заслуговують на міжнародне схвалення, навіть якщо їх дотримання буде обмеженим. Нещодавно МКЧХ опублікував набір правил для цивільних хакерів, які беруть участь у конфліктах, щоб прояснити межу між цивільними та комбатантами, оскільки кіберпростір може бути розмитим місцем для роботи — особливо під час війни.

Триваючий конфлікт між Росією та Україною, зокрема, спричинив безпрецедентну кількість цивільних хакерів, які опинилися в центрі війни, використовуючи свої навички для розпалювання атак на банки, виробничі потужності, лікарні та залізниці, намагаючись вплинути на війну. в ту чи іншу сторону. Кібер-пильність не є новою концепцією, але великий масштаб цих новонароджених патріотичних кібер-«банд» дав підстави МКЧХ вжити заходів з надією, що хакери з обох сторін дотримуються цих правил.

Що потрібно і чого не можна робити для Хактивістів

Вісім правил МКЧХ для «хактивістів» такі:

Не спрямовуйте кібератаки на цивільні об'єкти.

Не використовуйте зловмисне програмне забезпечення чи інші інструменти чи методи, які поширюються автоматично та завдають шкоди військовим і цивільним об’єктам без розбору.

Плануючи кібератаку на військовий об’єкт, зробіть усе можливе, щоб уникнути або мінімізувати вплив вашої операції на цивільних осіб.

Не проводите жодних кібероперацій проти медичних та гуманітарних закладів.

Не проводите жодних кібератак на об’єкти, необхідні для виживання населення або які можуть вивільнити небезпечні сили.

Не погрожуйте насильством, щоб посіяти терор серед цивільного населення.

Не підбурюйте до порушень міжнародного гуманітарного права.

Дотримуйтеся цих правил, навіть якщо ворог цього не робить.

Ці правила з’явилися в той час, коли групам або навіть окремим особам ніколи не було так просто брати участь у нападах і виконувати свою роль у їхній справі. Чим легше будь-кому, хто має зло, здійснити кібератаку, тим менш обмежувальними будуть ці правила і тим менше їх дотримуватимуться. Багато груп осіб без громадянства, залучених до російсько-українського конфлікту, не зв’язані діючими національними чи міжнародними законами. Дійсно, кілька груп, наприклад проросійська група Killnet, уже повідомили, що не дотримуватимуться правил ICRS.

Незважаючи на те, що ці правила, швидше за все, не будуть прийняті хакерськими групами, які зараз діють у російсько-українському конфлікті, слід похвалити МКЧХ за розробку та публікацію цих правил. Встановлення норм має вирішальне значення для притягнення таких груп до відповідальності за потенційні військові злочини, загибель і руйнування цивільного населення та інші шкідливі допоміжні наслідки.

Передбачається, що ці правила відповідають міжнародному гуманітарному праву, набору правил, спрямованих на обмеження наслідків збройних конфліктів, і, якщо їх порушують, становлять військові злочини. Норми МГП для збройних конфліктів мають вирішальне значення для захисту громадян у військових зонах під час війни, але часто анонімний і відсторонений характер кіберпростору означає, що буде набагато, набагато важче контролювати ці нові норми МГП, орієнтовані на кібернетичність.

Правило № 3, наприклад, є абсолютно критичним для пом’якшення шкоди цивільним особам під час конфлікту. Але цивільні хакери, які працюють від імені військової цілі, можуть абсолютно не знати про ненавмисне руйнування, яке вони спричинять своїми атаками. При підготовці будь-якого виду кібератаки інтелект, який має актор, потрапляючи в цільове середовище, рідко досягає 100%, навіть якщо він є професіоналом. Наприклад, якщо намір полягає в тому, щоб вплинути на один компонент банку, але зловмисник не усвідомлює, що сусідня лікарня покладається на ту саму електричну мережу, ситуація може дуже швидко загостритися. А коли це малокваліфікований зловмисник, який мало звертає увагу

або не розуміє, що може зробити потужний інструмент, прорахунки стають надзвичайно легкими.

Побічний збиток

Також цілком імовірно, що приватний сектор візьме на себе основний тягар цього супутнього збитку. Наприклад, NotPetya — цілеспрямована атака на українську інфраструктуру — розгорнулася у 2017 році, паралізувавши заводи по всьому світу та завдавши транспортній компанії Maersk 300 мільйонів доларів. Інша причина для занепокоєння полягає в тому, що комерціалізація кіберзлочинності дозволила менш просунутим суб'єктам орендувати найсучасніше зловмисне програмне забезпечення та швидко й легко запускати кампанії. Наприклад, атака Colonial Pipeline, ймовірно, була організована філією, яка заплатила за зловмисне програмне забезпечення DarkSide. Це значно ускладнює моніторинг того, хто є мішенню, і навіть розробники, ймовірно, не знають напевно, як і де використовуватиметься їх шкідливе програмне забезпечення.

МКЧХ надсилає ці правила хакерським групам з обох сторін конфлікту та закликає всі держави — не лише Росію та Україну — «приділити належну увагу ризику заподіяння шкоди цивільним особам, якщо заохочувати або вимагати їх участі у військових кібероперація̈х». Створення параметрів для цивільних хакерів, які зараз беруть участь у конфліктах, сподіваємося, призведе до міжнародно прийнятих і обов'язкових правил у майбутньому. Якщо за допомогою цих правил можна досягти навіть певного рівня стримування, це допоможе уникнути непотрібної шкоди та шкоди в майбутніх конфліктах». ***(Adam Marrè. Establishing New Rules for Cyber Warfare // Informa PLC (https://www.darkreading.com/cyberattacks-data-breaches/establishing-new-rules-cyber-warfare?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 04.12.2023).***

***

«Дослідники кібербезпеки помітили значне зростання російських фішингових кампаній, націлених на державні установи та інші організації на Заході.

У новому дослідницькому звіті Proofpoint повідомила, що виявила, що APT28, також AKA Fancy Bear, розповсюджує більшу кількість шкідливих електронних листів по всій Європі та Північній Америці.

Кампанія почалася в березні 2023 року та призвела до десятків тисяч фішингових електронних листів, надісланих організаціям в урядовому, аерокосмічному, освітньому, фінансовому, виробничому та технологічному секторах.

Outlook і WinRAR

Розвідка США передає Fancy Bear у пряме підпорядкування Головного розвідувального управління (ГРУ) російського Генштабу.

Ці електронні листи містять або шкідливі файли, або посилання, і намагаються використати численні вразливості, які спільнота кібербезпеки виявила та виправила кілька місяців тому. Це означає, що Fancy Bear стежить за організаціями, які не надто старанні, коли йдеться про їхні системи та кінцеві точки.

Proofpoint виділяє дві вразливості — CVE-2023-23397, яка є недоліком підвищення привілеїв, виявленим у Microsoft Outlook, і CVE-2023-38831, недоліком віддаленого виконання коду, нещодавно виявленим у WinRAR. У той час як перший дозволяє ATP28 використовувати файли TNEF і захоплювати хеш пароля NTLM цільової програми, останній дозволяє виконувати «довільний код, коли користувач намагається переглянути нешкідливий файл у ZIP-архіві».

Хоча мета кампанії є дискусійною, швидше за все, це збір розвідувальних даних. Це може бути особливо шкідливим, якщо кампанія буде успішною в державному, аерокосмічному та технологічному секторах…». ***(Sead Fadilpašić. This huge Russian phishing campaign is hitting targets across the world // Future US, Inc. (https://www.techradar.com/pro/security/this-huge-russian-phishing-campaign-is-hitting-targets-across-the-***

world?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 06.12.2023).

***

«Велика Британія звинувачує Службу безпеки Росії, ФСБ, у постійній кампанії кіберзлому, націленої на політиків та інших осіб у громадському житті.

Уряд заявив, що одна група викрала дані за допомогою кібератак, які пізніше були оприлюднені, включаючи матеріали, пов'язані з виборами 2019 року.

Росія неодноразово заперечувала свою причетність до такої діяльності.

Міністр закордонних справ Девід Кемерон назвав дії групи «повністю неприйнятними».

«Незважаючи на їхні неодноразові зусилля, вони зазнали невдачі. Ми продовжуватимемо співпрацювати з нашими союзниками, щоб викрити російську таємну кіберактивність і притягнути Росію до відповідальності за її дії», - сказав колишній прем'єр-міністр.

Міністр закордонних справ Лео Дочерті повідомив у четвер у Палаті громад, що російського посла викликали, а проти двох осіб застосовано санкції. Один із них – чинний офіцер ФСБ.

Російський посол був недоступний після того, як його викликали в середу, але натомість офіційні особи зустрілися із заступником глави місії російського посольства та висловили глибоку стурбованість Великої Британії щодо ймовірних кібератак.

Групу звинувачують у здійсненні сотень цілеспрямованих хакерських атак проти політиків, державних службовців, аналітичних центрів, журналістів, науковців та інших осіб у суспільному житті. Вони в основному були націлені на приватні електронні листи окремих осіб після ретельного дослідження та створення фальшивих облікових записів, які видавали себе за їхніх довірених контактів.

Серед жертв був депутат, який у лютому повідомив BBC, що його електронні листи викрали.

Федеральна служба безпеки (ФСБ) є правонаступницею КДБ, яка діяла протягом холодної війни.

Президент Росії Володимир Путін був директором ФСБ протягом 1990-х років.

Вважається, що група, пов’язана з ФСБ, а саме її частина, відома як «Центр 18», займається нападами на Велику Британію, викрадаючи інформацію в політичних і громадських діячів принаймні з 2015 року.

Зазначається, що група залишається активною.

Також очікується, що США оголосить про заходи проти групи.

«Росія націлена на демократичний процес у Великобританії», - заявили західні офіційні особи.

Проте кампанію було визнано невдалою щодо втручання в демократичний процес.

Публічне звинувачення в четвер спрямоване на те, щоб перешкодити роботі групи та підвищити обізнаність напередодні великих виборів у всьому світі наступного року.

«Ця група зібрала величезну кількість даних», - заявили західні офіційні особи. «Ця інформація використовується для підриву Заходу різними способами».

Велика Британія вже звинувачувала Росію у втручанні у вибори 2019 року після крадіжки документів про торгівлю між США та Великою Британією у депутата-консерватора Ліама Фокса, які потім були оприлюднені.

Але коли це звинувачення було висунуто в 2020 році, конкретна група, яка стоїть за цією атакою, не була названа, і тепер її пов’язують із більш широкою діяльністю тієї ж групи, пов’язаної з ФСБ.

Ті, на кого орієнтована організація, походять з усього політичного спектру.

Депутат від SNP Стюарт Макдональд розповів BBC цього лютого, що група, яка, ймовірно, була пов’язана з російською розвідкою, викрала його електронні листи, видаючи себе за одного з його співробітників. Він опублікував інформацію, щоб запобігти витоку будь-яких електронних листів. Вони не з'явилися.

Виступаючи в Палаті громад у четвер, Брендан О'Хара від SNP, речник партії у закордонних справах, сказав, що дії Росії є частиною «постійної моделі поведінки», і запитав, чи уряд «розглядав можливість зробити навчання з кібербезпеки обов'язковим для всіх». депутати та їх апарат».

Представник лейбористів Девід Леммі сказав, що демократія «будується на довірі» і запитав, чи уряд «впевнений», що всі масштаби нападу були розкриті.

Вважається, що сама група, пов’язана з ФСБ, зосереджена на зломі даних разом з іншими, залученими до їх поширення через різні канали та посилення свого впливу.

Серед інших цілей – мозковий центр Institute for Statecraft і його засновник Кріс Доннеллі, чиї дані злилися в Інтернет, а також колишній глава MI6 сер Річард Дірлав.

Західні офіційні особи заявили, що група була залучена до «отримання розвідданих» шляхом злому облікових записів електронної пошти та крадіжки даних. У деяких випадках він потім передавав інформацію іншим, щоб оприлюднити її.

Звинувачення Великої Британії, за якими будуть подальші кроки з боку США, покликане перешкодити діяльності групи ФСБ шляхом їх викриття.

Вважається, що США та Великій Британії знадобилося кілька місяців, щоб з достатньою впевненістю встановити, що Центр 18 ФСБ несе відповідальність, і скоординувати публічні оголошення про цю діяльність.

Попередня порада Національного центру кібербезпеки, підрозділу GCHQ, попереджала в січні про загрозу того, що електронні листи стануть мішенню як з боку Росії, так і з Ірану, і подальші попередження, в тому числі для високопоставлених осіб, видаються пізніше в четвер.

Проінформовано всіх, про кого відомо, що він був зламаний.

Чиновники хочуть підвищити обізнаність про небезпеку, оскільки Великобританія прямує до виборів, ймовірно, наступного року. Вибори в США, які відбудуться наступного листопада, також можуть стати мішенню хакерів.

У 2016 році іншу частину російської розвідки звинуватили у крадіжці та оприлюдненні електронних листів, що належали кампанії Гілларі Клінтон, і цей крок дехто вважав важливим у напруженій боротьбі.

Хакерська група відома під різними назвами, зокрема Star Blizzard, Cold River і Seaborgium.

Вважається, що протягом останніх років група ФСБ викрала велику кількість даних, і лише частина з них була оприлюднена.

Відповідаючи на запитання, чи можуть вони оприлюднити більше даних, які вони зібрали, західні чиновники сказали: «Немає доказів цього наміру. Є така можливість. Вони зібрали багато інформації». ***(Gordon Corera. Russia hacking: 'FSB in years-long cyber attacks on UK', says government // BBC (https://www.bbc.com/news/uk-politics-67647548?utm_source=flipboard&utm_content=other). 07.12.2023).***

***

«Російська хакерська група, пов'язана з Кремлем, розв'язала глобальну атаку. Вони використовують те, що виглядає як посилання на невинні веб-сайти, щоб викрасти інформацію.

Ці хакери з Star Blizzard, яка раніше діяла як SEABORGIUM, також відомі як Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie.

Небезпечна група націлена на всіх, хто може мати інформацію, яку вони можуть використовувати. Вони навіть переслідують уряд США.

Наразі Star Blizzard атакувала людей, пов'язаних із науковцями, обороною, урядовими організаціями тощо як у США, так і у Великій Британії. За даними Агентства з кібербезпеки та безпеки інфраструктури США, група також націлена на членів НАТО та країни поблизу Китаю…

За даними CISA, хакери Star Blizzard використовуватимуть соціальні мережі та мережеві платформи, щоб переслідувати своїх жертв. Вони знадобляться час, щоб по-справжньому пізнати свою ціль.

Потім вони створять підроблені облікові записи електронної пошти, такі як Outlook, Gmail та інші, а також профілі в соціальних мережах, щоб видати себе за ваших близьких контактів або експертів. Хакери навіть зайдуть так далеко, що створять шкідливі веб-сайти, які здаються законними, щоб обдурити вас. І CISA каже, що були випадки, коли зловмисники створювали підроблені запрошення на заходи, щоб заманити своїх жертв.

Пастка хакерів Star Blizzard

Звідти вони дотягнуться до вас і почнуть втягувати вас у свою пастку. Зазвичай вони шукають спільні інтереси, щоб почати розмову. Потім хакери надішлють зловмисне посилання, видаючи себе за Google Drive, OneDrive або інше посилання, за яким вам потрібно було б увійти на платформу. За даними Microsoft, деякі з поширених URL-адрес, які використовують хакери Star Blizzard, виглядають так (з міркувань безпеки точну URL-адресу було змінено):

https://drive.google.com/file/d/XXXXXXXXXXXXXX/view?usp=sharing

https://onedrive.live.com/?authkey=%XXXXXXXXXXXXXXXXXXXXXXXXXXXXX%XXXX&cid=8XXXXXXXXX9B7

https://www.dropbox.com/s/XXXXXXXXXXXXX/Star_Blizzard_Report.pdf?dl=0

Ці URL-адреси можуть виглядати законними, але насправді вони створені, щоб змусити вас ввести облікові дані або завантажити шкідливі файли. Ви ніколи не повинні натискати посилання, які ви отримуєте з невідомого або підозрілого джерела.

Якщо ви це зробите, хакери зможуть викрасти вашу інформацію, щойно ви її введете, завантажите або натиснете шкідливий файл чи посилання. Коли ви це зробите, вони отримають повний доступ до вашого облікового запису. Після цього ваша інформація є їхньою власністю.

Як захистити себе від хакерів Star Blizzard

Будьте обережні, натискаючи посилання в електронних листах або повідомленнях із невідомих або підозрілих джерел, особливо в соціальних мережах і мережевих платформах, оскільки хакери Star Blizzard саме так люблять

переслідувати своїх жертв. Вони можуть привести вас до шкідливих веб-сайтів, які можуть викрасти вашу інформацію або заразити ваш пристрій шкідливим програмним забезпеченням.

Перевірте особу відправника, перш ніж відкривати будь-які вкладення або завантажувати файли. Ви можете зробити це, перевіривши їх електронну адресу, профіль у соціальних мережах або іншу присутність в Інтернеті. Якщо ви не впевнені, ви можете зв'язатися з ними через інший канал, щоб підтвердити.

Використовуйте надійні й унікальні паролі для своїх онлайн-акаунтів і регулярно їх змінюйте. Обов'язково використовуйте окремі паролі для облікових записів електронної пошти та намагайтеся уникати повторного використання тих самих паролів знову і знову. Використання одного пароля на кількох платформах завжди зробить вас більш уразливими, тому що якщо один обліковий запис буде зламано, вони будуть зламані. Ви також можете використовувати менеджер паролів, щоб зберігати та створювати надійні паролі. Таким чином ви можете запобігти доступу кіберзлочинців, таких як хакери Star Blizzard, до ваших облікових записів, якщо вони скомпрометують один із них.

Увімкніть двофакторну автентифікацію (2FA) для своїх онлайн-акаунтів, коли це можливо. Це додає додатковий рівень безпеки, оскільки для входу потрібен код або пристрій. Таким чином, навіть якщо російська хакерська група отримає ваш пароль, вони не зможуть отримати доступ до вашого облікового запису без другого чинника.

Оновлюйте програмне забезпечення та пристрої за допомогою останніх виправлень безпеки та оновлень. Це може допомогти вам виправити будь-які вразливості чи помилки, якими можуть скористатися хакери Star Blizzard.

Встановіть хороше антивірусне програмне забезпечення на всіх своїх пристроях. Найкращий спосіб захистити себе від злому ваших даних — встановити антивірусний захист на всіх своїх пристроях. Хороша антивірусна програма, яка активно працює на ваших пристроях, попередить вас про будь-яке зловмисне програмне забезпечення у вашій системі, застереже від натискання будь-яких шкідливих посилань у фішингових електронних листах і, зрештою, захистить вас

від злому хакерами Star Blizzard…» ***(Kurt Knutsson. Russian cybergroup Star Blizzard unleashes global spear-phishing attack // FOX News Network, LLC. (https://www.foxnews.com/tech/russian-cyber-group-star-blizzard-unleashes-global-spear-phishing-attack?utm_source=flipboard&utm_content=FoxNews%2Fmagazine%2FLatest%20News). 15.12.2023).***

***

«Щоб протистояти зростаючим кіберзагрозам Північної Кореї та запуску космічних супутників-шпигунів, США, Південна Корея та Японія сформували єдиний фронт, активізуючи свої скоординовані зусилля проти діяльності Пхеньяна.

Після зобов'язань, взятих на початку цього року на саміті, організованому президентом Байденом, три країни пообіцяли скоординувати дії для боротьби з економічним примусом і мерзенною кібердіяльністю, організованою Корейською Народно-Демократичною Республікою (КНДР).

Японія, Південна Корея, США об'єднали зусилля

Reuters повідомляє, що радник Білого дому з національної безпеки Джейк Салліван оголосив про нові ініціативи, які випливають із зустрічі радників з національної безпеки трьох країн у Сеулі.

Салліван наголосив на основних напрямках цих ініціатив, виявляючи кіберзлочинність, відмивання грошей у криптовалюті та спірні випробування балістичних ракет і космічні випробування, проведені Північною Кореєю, і все це всупереч резолюціям Організації Об'єднаних Націй.

«Ми також запустили нові тристоронні ініціативи для протидії загрозам, які створює КНДР, від її кіберзлочинності та відмивання грошей у криптовалюті до безрозсудних випробувань у космосі та балістичних ракет», — зазначив Салліван.

Ці зусилля є не просто риторикою, а охоплюють відчутне зобов'язання, про що свідчать поточні плани домовленості про обмін інформацією в режимі

реального часу про запуски ракет Північної Кореї, посилюючи оборонну співпрацю між країнами-союзниками.

Погрози з боку Північної Кореї

Незважаючи на те, що Північна Корея заявляє про своє право захищати себе шляхом освоєння космосу, США заперечують ці заяви, посилаючись на порушення міжнародних норм і резолюцій.

AP News повідомляє, що підвищене занепокоєння пов'язане з потенційною торгівлею зброєю між Північною Кореєю та Росією, що викликає тривогу через передачу боєприпасів, які допомагають Росії в поточному конфлікті в Україні.

Салліван, виступаючи після тристоронньої зустрічі, наголосив на серйозності дій Північної Кореї, що вказує на колективне занепокоєння серед трьох країн.

Однак деталі щодо обсягів і типів озброєнь, які нібито постачаються до Росії, залишаються нерозкритими. Тим не менш, Салліван підкреслив одностайність серед союзників щодо тривожного характеру поставок зброї, підкресливши серйозну стурбованість альянсу.

У ході цих дискусій з'явилися менш критичні, але важливі подробиці, зокрема плани Північної Кореї розгорнути додаткові супутники-шпигуни, її критика подвійних стандартів у запусках супутників і її заперечення звинувачень щодо кібератак або розповсюдження зброї.

Під час дискусій також згадувалися припущення про те, що Північна Корея потенційно постачає зброю групам бойовиків, і про наслідки відмови країни від попередніх угод.

Незважаючи на ці заплутані діалоги та спільні занепокоєння, очевидно, що Сполучені Штати, Південна Корея та Японія перебувають у складній павутині геополітичних викликів, породжених розвитком кіберпотенціалу Північної Кореї та її амбітними вилазками в космос.

Оскільки напруженість на Корейському півострові залишається високою, цей єдиний фронт демонструє непохитну відданість цих країн протидії багатогранним загрозам Пхеньяна». ***(John Lopez. US, South Korea, Japan Unite Efforts Against North Korea's Cyber Threats, Space Launches // TECHTIMES***

(https://www.techtimes.com/articles/299573/20231209/south-korea-japan-us-unite-efforts-against-north-koreas-cyber-threats.htm?utm_source=flipboard&utm_content=other). 09.12.2023).

***

«Агентство з кібербезпеки США CISA попередило, що невідомі хакери зламали сервери федерального урядового агентства, скориставшись відомою раніше вразливістю програмного забезпечення, яке більше не отримує оновлень, тобто агентство не могло б виправити його, навіть якби хотіло.

У вівторок CISA оприлюднила консультацію, в якій описується дві окремі кібератаки на неназване федеральне державне агентство. Хакери атакували агентство в червні та липні, націлившись на загальнодоступні сервери, на яких працювало застаріле або вичерпане програмне забезпечення Adobe ColdFusion, яке використовується для створення веб-додатків.

Термін експлуатації програмного забезпечення означає, що розробник публічно оголосив, що воно більше не підтримуватиметься та не отримуватиме подальших оновлень програмного забезпечення чи безпеки. Запуск вичерпаного програмного забезпечення за визначенням є ризикованим, оскільки його неможливо виправити, наражаючи організацію, яка запускає програмне забезпечення, на кібератаки.

У CISA заявили, що немає жодних доказів того, що зловмисники підклали шкідливе програмне забезпечення або зробили щось більше, ніж переглядали мережу зламаного агентства.

«Аналіз показує, що зловмисна діяльність, здійснена загрозливими суб’єктами, була розвідувальною спробою відобразити ширшу мережу», але CISA визнала, що не може підтвердити, чи були дані викрадені з мережі агентства.

Речник CISA Антоніо Соліз відмовився від коментарів, коли TechCrunch запитав більше інформації про те, хто, на думку агентства, є хакерами, відповідальними за атаку на агентство.

У повідомленні CISA заявило, що не знає, чи дві кібератаки були здійснені одними і тими ж хакерами.

Під час обох кібератак Microsoft Defender for Endpoint, власне антивірусне програмне забезпечення Windows, сповістило агентство про потенційне використання вразливості Adobe ColdFusion і «перевело» дії хакерів на карантин.

У березні CISA наказав усім федеральним агентствам виправити одну з відомих уразливостей в Adobe ColdFusion, які були використані в цих атаках, CVE-2023-26360». ***(Lorenzo Franceschi-Bicchierai. CISA says US government agency was hacked thanks to 'end of life' software // Yahoo (https://techcrunch.com/2023/12/06/cisa-says-us-government-agency-was-hacked-thanks-to-end-of-life-software/?utm_source=flipboard&utm_content=AWC%2Fmagazine%2FOur+Electronic+%26+Digital+Lives.). 06.12.2023).***

***

«Підтримувана Іраном група кібершпигунства активно атакує телекомунікаційні компанії в Північній і Східній Африці.

За даними дослідників із безпеки Symantec, останні кібератаки передової постійної загрози (APT), яку вона називає Seedworm (також відомої як MuddyWater, APT34, Crambus, Helix Kitten або OilRig), спрямовані на організації телекомунікаційного сектора в Єгипті, Судані та Танзанії. Зокрема, одна організація телекомунікаційного сектору — раніше проникла Seedworm у 2023 році, але досі не названа — несе основний тягар останніх нападів.

Гра Seedworm's Power (Shell).

Перші докази зловмисної активності надійшли від виконання коду PowerShell для підключення до системи керування (C2) під назвою MuddyC2Go, інфраструктури, яку дослідники раніше пов'язували з Seedworm.

«Зловмисники також використовують інструмент віддаленого доступу SimpleHelp і Venom Proxy, які раніше були пов'язані з діяльністю Seedworm, а також використовують спеціальний інструмент клавіатурного журналу та інші

загальнодоступні інструменти та інструменти, що живуть за межами землі», – повідомили дослідники Symantec. в аналізі кібератак від 19 грудня.

Життя поза межами землі відноситься до практики використання готових технологій і власних програм операційної системи для приховування зловмисної активності. Використовуючи законні додатки зловживанням, зловмисники уникають створення незвичайного трафіку або активності в скомпрометованій мережі, тим самим зменшуючи ризик їх виявлення.

Dark Reading звернувся до Symantec, щоб отримати коментарі щодо деталей останньої серії атак Seedworm, а також пропозиції щодо можливих контрзаходів.

Насіння сумніву

Seedworm працює протягом шести років з 2017 року і раніше був пов'язаний з Міністерством розвідки та безпеки Ірану (MOIS). Група зазвичай покладається на фішингові електронні листи, що містять архіви або посилання на архіви, які містять різні законні інструменти віддаленого адміністрування, включаючи утиліти віддаленого доступу SimpleHelp і AnyDesk.

Якщо передбачувана ціль відкриває файл в архіві, вона встановлює інструмент віддаленого адміністрування, який дозволяє зловмиснику запускати додаткові інструменти та шкідливі програми. Нещодавно група почала розміщувати шкідливе програмне забезпечення в захищених паролем архівах RAR, намагаючись уникнути виявлення продуктами безпеки електронної пошти в цільових організаціях, згідно з нещодавньою публікацією в блозі дослідницької компанії Deep Instinct.

Найновіші шкідливі файли, які передає група, містять вбудований сценарій PowerShell, який автоматично підключається до MuddyC2Go. Такий підхід позбавляє зловмисників необхідності ручного виконання сценаріїв.

Дослідники Symantec виявили, що Seedworm зазвичай націлений на державні та приватні організації в різних секторах, включаючи телекомунікації, місцеве самоврядування, оборону, нафту та природний газ. Цілями групи є здебільшого сусіди Ірану на Близькому Сході, включаючи Туреччину, Ізраїль, Ірак, Об'єднані Арабські Емірати та Пакистан.

Іранська кіберторгівля

Іранські групи кібершпигунства відомі тим, що встановлюють фальшиві особи в LinkedIn та інших місцях, щоб переконати цілі відкрити шкідливі посилання або вкладення, а не покладатися на невиправлені вразливості для злому цільових організацій.

Іран почав інвестувати значні кошти у свою програму кібероперацій після виявлення сумнозвісної. зброї кібершпигунства Stuxnet у 2010 році. Зловмисне програмне забезпечення Stuxnet заразило системи диспетчерського контролю та збору даних (SCADA) на ядерних об'єктах Ірану, зокрема його центрифуги для збагачення урану, і саботувало їх функціонування. Дослідники безпеки приписують зловмисне програмне забезпечення спільній операції розвідок США та Ізраїлю.

Іранський Корпус вартових ісламської революції (КВІР) з тих пір був пов'язаний з руйнівними та руйнівними атаками, такими як атаки зловмисного програмного забезпечення Shamoon wiper на нафтогазові компанії в Саудівській Аравії та Катарі. Навпаки, MOIS є цивільною розвідувальною службою, яка в основному зосереджена на таємному отриманні розвідданих. Seedworm було названо підпорядкованим елементом або підрозділом у складі MOIS Ірану». ***(John Leyden. Iranian 'Seedworm' Cyber Spies Target African Telcos & ISPs // Informa PLC (https://www.darkreading.com/cyberattacks-data-breaches/iranian-seedworm-cyber-spies-target-african-telcos-isps?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 20.12.2023).***

***

Формування на функціонування кібервійськ

«Згідно з даними Adroit Market Research, до 2029 року ринок військової кібербезпеки досягне значних 7,2 мільярдів доларів США, збільшуючись із середньорічним темпом зростання (CAGR) на 11% з 2021 року.

Військова кібербезпека, також відома як військова кібербезпека або військова кіберзахист, була розгорнута для захисту цифрових активів, комунікаційних мереж та IT-інфраструктури військових організацій і оборонних відомств. Основною метою цих процесів є захист життєво важливих військових даних для забезпечення безперервного виконання військових дій. Це включає захист військових мереж від зловмисних загроз і атак, а також забезпечення конфіденційності, точності та доступності критично важливих військових даних.

Ці системи також включають процедури для створення та використання тактик виявлення, реагування та пом'якшення кіберінцидентів. Ці захисні заходи часто вимагають координації дій швидкого реагування та співпраці з групами кіберзахисту. Невід'ємною частиною цих методів захисту є надання військовому персоналу доступу до захищених і зашифрованих мереж передачі голосу та даних, а також захист критичної військової інфраструктури від онлайн-загроз, які можуть перервати військові операції.

Інвестиції у військові системи кібербезпеки були зумовлені все більш складною природою кіберзагроз. Ці загрози включають спонсоровані державою кібератаки, хактивізм та операції, які проводять кіберзлочинці. У результаті цифрової трансформації, яка розширила потенційну поверхню атак, військові організації змушені інвестувати в рішення кібербезпеки, які відповідають суворим критеріям кібербезпеки, встановлених урядами та оборонними відомствами. Ця потреба була задоволена шляхом стратегічного розподілу більших оборонних бюджетів у ряді країн для боротьби з цими новими загрозами безпеці.

Було помічено збільшення інвестицій як у наступальну, так і в оборонну кіберспроможність завдяки дедалі більшому визнанню невід'ємної ролі кібервійни в сучасному конфлікті. Цьому також сприяє співпраця між оборонними відомствами та комерційними фірмами з кібербезпеки, які прагнуть використати новаторські технології та досвід. Ця співпраця призвела до покращення можливостей виявлення та реагування військових рішень кібербезпеки за допомогою передових технологій, таких як штучний інтелект (AI), машинне навчання та розвідка загроз.

У нинішньому кліматі триваючої геополітичної напруженості та конфліктів кібербезпека набула першочергового значення для багатьох країн. Таким чином, ці обставини посилили увагу до кіберспроможностей, як оборонних, так і наступальних. Інвестиції в заходи кібербезпеки тепер захищають пов’язані з обороною технології та програмне забезпечення. Зараз головним пріоритетом є захист життєво важливих військових інфраструктур від кібератак. У результаті випереджувальні заходи щодо підвищення загальної стійкості військового кіберзахисту прискорили розширення ринку.

Історично поняття «забезпечення інформації» набуло популярності, підкреслюючи цінність збереження конфіденційності, точності та доступності військових даних. Зусилля для цього були зроблені у співпраці з такими агентствами, як NSA (Агентство національної безпеки). На початку 2000-х військові організації активно запроваджували докладні протоколи кібербезпеки для захисту своїх мереж.

У відповідь на складні загрози, створені національними державами та кваліфікованими кіберзлочинними організаціями, виникла необхідність розвитку передових наступальних і оборонних кіберспроможностей. У відповідь уряди та військові організації створили стандарти кібербезпеки та нормативно-правову базу для застосування в обороні та національній безпеці. Відповідно до цього, дотримання правил стало головною увагою. Зараз військові організації координують заходи кіберзахисту та обмінюються інформацією про загрози з комерційним сектором і своїми міжнародними партнерами». ***(Tom Raynel. Military cyber security market to reach $7.2 billion by 2029 // TechDay (https://securitybrief.co.nz/story/military-cyber-security-market-to-reach-7-2-billion-by-2029). 01.12.2023).***

***

«Національне кіберуправління Ізраїлю (INCD) оголосило минулого тижня, що уряд схвалив надзвичайні правила для посилення здатності країни захищатися від широкомасштабних кібератак. З початку війни з ХАМАС у Газі INCD виявив приблизно 40 спроб кібератак на компанії та цифрові служби зберігання даних, які обслуговують численні ізраїльські підприємства.

Метою цих правил є мінімізація потенційного побічного збитку для економіки під час надзвичайних ситуацій, спричинених цими кібератаками.

Через характер послуг, що пропонуються службами зберігання даних і цифровими службами, вони надають зловмисникам шлюз для проникнення та зламу підключених об'єктів або збереженої інформації, потенційно впливаючи на кількох клієнтів одночасно.

Обсяг збитків може поширюватися на такі критично важливі установи, як лікарні, транспортні компанії та державні установи, які відіграють важливу роль у звичайній роботі, особливо під час надзвичайних ситуацій.

Хвиля кібератак обрушилася на Ізраїль на тлі війни з ХАМАС

Протягом війни з ХАМАСом спостерігалося зростання кількості шкідливих кібератак, спрямованих проти компаній цього типу. Щоб захистити громадськість і забезпечити безперебійне функціонування ізраїльської економіки, виникла потреба в терміновому впровадженні надзвичайних правил для виявлення, стримування та мінімізації впливу таких атак.

У разі серйозної кібератаки, яка становить загрозу державі або основним службам, або INCD, Shin Bet (Агентство безпеки Ізраїлю) або Міністерство оборони - залежно від типу компанії, що постраждала, матиме повноваження надавати вказівки службі зберігання даних провайдерів і цифрових послуг про те, як впоратися з ситуацією. Ці інструкції будуть надані лише в тому випадку, якщо постачальники послуг зберігання та цифрові служби не зможуть належним чином протистояти кібератаці.

Крім того, правила передбачають, що перед видачею інструкцій необхідно ретельно розглянути потенційний вплив на аспекти конфіденційності та економічні

наслідки впровадження інструкцій. Державні органи також звітуватимуть генеральному прокурору та Комітету Кнесету у закордонних справах і обороні кожні два тижні щодо.

Затверджені надзвичайні положення набирають чинності негайно та діятимуть протягом місяця». ***(YINON BEN SHUSHAN. Israel cyber directorate, Shin Bet given power to fight cyberattacks // Jpost Inc. (https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-775856?utm_source=flipboard&utm_content=KitArrowsmith%2Fmagazine%2F%F0%9F%87%B5%F0%9F%87%B8MIDDLE+EAST%F0%9F%87%B1%F0%9F%87%A7%26%F0%9F%87%AA%F0%9F%87%ACISRAEL%F0%9F%87%AE%F0%9F%87%B1). 03.12.2023).***

***

«Веб-сайт прес-секретаря ЦАХАЛу зазнав атаки пропалестинських хакерів у середу ввечері, причому хакери замінили домашню сторінку сайту загрозою Ізраїлю.

«Ваша нахабність і несправедливість по відношенню до нашого народу в Газі зашкодять вам лише через терор, вбивства та війну, чи то на суші, чи в повітрі, чи в електронному вигляді», — написали хакери, які підписали повідомлення як «Анонімний Джо» та назвали себе йорданцями.

«Це не що інше, як відповідь на ваші брудні дії та варварство та вбивство наших уразливих людей у Газі», — додали хакери. «Це тільки початок, і звідси ми говоримо вам, що ми приймемо тільки звільнення нашої землі, Палестини, від річки до моря. Навіть якщо наша війна з вами триватиме вічність, ви не знайдете від нас нічого, крім вбивство і терор».

Ціллю хакерів є Ізраїль під час війни

Серія кібератак була спрямована на Ізраїль після початку війни між Ізраїлем і ХАМАС у жовтні.

Раніше цього місяця група хакерів заявила, що викрала понад 500 гігабайт даних, у тому числі сотні тисяч медичних записів IDF, під час кібератаки на медичний центр Ziv.

Останніми тижнями Національне кіберуправління Ізраїлю (INCD) оголосило, що уряд схвалив надзвичайні правила для підвищення здатності країни захищатися від широкомасштабних кібератак.

З початку війни з ХАМАС у Газі INCD виявив приблизно 40 спроб кібератак на компанії та цифрові служби зберігання даних, які обслуговують численні ізраїльські підприємства». ***(IDF website attacked by pro-Palestinian hackers // JERUSALEM POST STAFF (https://www.jpost.com/breaking-news/article-777898?utm_source=flipboard&utm_content=jeanineheming%2Fmagazine%2FHistory). 13.12.2023).***

***

«Хакери, пов'язані з урядом Ізраїлю, в понеділок взяли на себе відповідальність за кібератаку, яка закрила АЗС по всьому Ірану.

«Ця кібератака є відповіддю на агресію Ісламської Республіки та її проксі в регіоні», — заявила група Gonjeshke Darande, що перською мовою означає «Хижий горобець») у дописі на X.

За словами міністра нафти країни, цифрові атаки, які почалися рано вранці в понеділок, спочатку вразили приблизно 70% заправних станцій Ірану. У наступному оновленні він сказав, що 56% станцій залишилися офлайн.

Кілька ЗМІ повідомили, що Predatory Sparrow є частиною елітного військового кіберкорпусу Ізраїлю, який неодноразово здійснював руйнівні кібератаки на іранські установи в рамках тривалого конфлікту між двома країнами.

Злом іранських автозаправних станцій стався в той час, як Ізраїль продовжує свою наземну атаку в секторі Газа на ХАМАС, який, на думку офіційних осіб США та Ізраїлю, отримує фінансування від Ірану. Збої також збіглися з візитом до Ізраїлю вищих військових чиновників президента Джо Байдена, які закликають

уряд ізраїльського прем'єр-міністра Біньяміна Нетаньяху деескалувати свої операції в Газі, щоб уникнути ширшої війни на Близькому Сході.

Ізраїль може використовувати Predatory Sparrow, щоб покарати Іран за допомогу ХАМАС. За кілька днів після нападу бойовиків на Ізраїль 7 жовтня угруповання відновилося після майже річної перерви та натякнуло, що відновить свою діяльність.

У дописі в Telegram хакери заявили, що їх атака на автозаправні станції Ірану «була проведена контрольованим способом, одночасно вживаючи заходів для обмеження потенційної шкоди екстреним службам». Угруповання заявило, що попереджало іранські екстрені служби перед початком атаки та навмисно залишило деякі заправні станції в робочому стані, «незважаючи на наш доступ і можливість повністю перервати їх роботу».

Predatory Sparrow має репутацію хакерів, які завдають серйозної фізичної шкоди, що є рідкістю у світі кібероперацій. У липні 2022 року група опублікувала записи з камер спостереження вибуху на іранському металургійному заводі, який, за її словами, став результатом одного з кількох цифрових вторгнень, здійснених у металургійній промисловості Ірану минулого місяця.

У своїй публікації в Telegram у понеділок група попередила верховного лідера Ірану Алі Хаменеї, що «гра з вогнем має ціну». ***(Eric Geller. 'Playing With Fire Has a Price': Israeli Hackers Say They Disabled Most of Iran's Gas Stations // JAF Communications Inc. (https://themessenger.com/tech/israel-iran-gas-stations-cyberattack-war-hamas?utm_source=flipboard&utm_content=TheMessenger%2Fmagazine%2FThe+Messenger+Latest). 18.12.2023).***

***

Кібербезпека закладів охорони здоров'я

«Хакери погрожували оприлюднити особисту медичну інформацію, включаючи рентгенівські знімки, листи консультантів, клінічні довідки та

інформацію про патологію, що належить членам британської королівської родини, якщо їм не буде виплачено викуп у біткойнах у розмірі 300 000 фунтів стерлінгів (380 000 доларів США).

Як повідомляє Daily Mail, банда «Rhysida», названа на честь виду отруйних багатоніжок, погрожувала оприлюднити інформацію, викрадену з лікарні короля Едуарда VII у Лондоні, якщо не отримає 10 біткойнів до вівторка.

«Вашій увазі представлені унікальні файли! Дані королівської родини! Велика кількість даних пацієнтів і співробітників. Розпродаж одним лотом!!», – написала банда в темній мережі. Він також опублікував зображення документів на продаж…

Лікарня використовується королівською сім'єю понад 100 років і має список відомих пацієнтів, включаючи принца Філіпа в 2021 році, Кейт, принцесу Уельську в 2012 році, і королеву Єлизавету II.

GCHQ, британське агентство з розвідки, безпеки та кібернетики, заявляє, що розслідує напад і «взаємодіє з лікарнею короля Едуарда VII, щоб зрозуміти наслідки». Однак деякі вважають, що викуп цілком можливо буде сплачено.

Колишній британський полковник Філіп Інгрем сказав Daily Mail: «Враховуючи дуже чутливу природу пацієнтів, на госпіталь буде чинитися певний тиск, щоб спробувати зупинити оприлюднення цих даних.

«І тому я очікую, що вони дослідять можливість сплати викупу».

Але, додає він, немає жодних гарантій, що дані будуть повернуті та навіть можуть бути продані іншим злочинним угрупованням…» ***(Hackers want $380K in bitcoin for Royal Family's stolen medical records // Protos (https://protos.com/hackers-want-380k-in-bitcoin-for-royal-family-stolen-medical-records/). 04.12.2023).***

***

«Галузь охорони здоров'я є найбільш жертвою витоку даних. Поєднання інформації про здоров'я, фінансової інформації та досліджень і розробок зробило інформацію про охорону здоров'я більш цінною в темній мережі, ніж інформацію, викрадену з банківських і фінансових установ.

Тенденції

Міністерство охорони здоров'я та соціальних служб США (HHS) вимагає, щоб повідомлялося про порушення, які стосуються понад 500 пацієнтів, і звідти вони публічно публікуються в базі даних. З тих пір як HHS відслідковує ці порушення в 2009 році, відбулося помітне зрушення в основних причинах порушень. З 2009 по 2015 рік у повідомленнях про порушення домінували втрата та викрадення записів. Запровадження електронних медичних записів підскочило майже до 100% лише за чотири роки в лікарнях у 2010-2014 роках. Пам'ятаю, як у 2009 році я була медсестрою у великій міській лікарні. Ми використовували паперові діаграми, записи про прийом ліків (MAR) і систему на базі DOS (де ви не могли використовувати мишу), щоб документувати оцінки, нотатки та плани догляду одночасно. Перехід на повністю електронну систему ведення медичних записів (EHR) у моїй лікарні був здійснений у 2011 році. Хоча це було полегшенням не мати відсутніх сторінок, скріплених степлером на звороті вашого паперового MAR, не кажучи вже про радощі тлумачення почерку поспішного лікарів – з того часу це спричинило інші проблеми.

Перехід до цифрового ведення записів і широке використання шифрування даних стали ключовими для зменшення фізичних втрат і крадіжок, але спричинили інші ризики. З 2018-2022 років тренд перемістився на хакерство та IT-інциденти. HHS повідомила про збільшення на 93% великих зломів і на 278% про збільшення великих зломів за участю програм-вимагачів.

Очікується, що тривалі тенденції в охороні здоров'я, включаючи дистанційне обслуговування пацієнтів і моніторинг використання телемедицини та інтелектуальних пристроїв, збережуться до 2024 року. Поверхня атаки для хакерів продовжує розширюватися, а сектор охорони здоров'я покладається на EHR, хмарні сервіси, платформи телемедицини. і мобільні програми. Крім того, продовжує зростати використання керованих і розміщених постачальників послуг. Сторонні постачальники та хмарні платформи є привабливими для постачальників медичних послуг та організацій, оскільки вони зменшують їхні операційні витрати, підвищують ефективність і надають доступ до спеціалізованих послуг та

інструментів. Перш за все, це дозволяє їм зосередитися на основних компетенціях, як-от надання допомоги. Однак саме ця залежність від сторонніх постачальників створює нові проблеми, зокрема забезпечення безпеки та конфіденційності даних, керування їхніми контрактами та моніторинг продуктивності та відповідності постачальників. Це також означає, що лікарням і постачальникам заборонено самостійно вирішувати проблеми. Тим часом догляд може припинитися.

Фінансовий підсумок

Чи знаєте ви, що усунення витоку даних коштує в середньому 4,45 мільйона доларів? Це приблизно 165 доларів за рекорд, і в усіх галузях. Але вже 13-й рік поспіль порушення системи охорони здоров'я є найдорожчими, і тепер їх усунення становить у середньому 10,93 мільйона доларів. Це більш ніж удвічі більше середнього. Більшість витрат пов'язана з доступністю та надійністю технологій і систем охорони здоров'я, але існують витрати, пов'язані з повідомленням пацієнтів і штрафами, які стягує HHS. Більше половини медичних установ перекладають витрати на порушення на споживачів (тобто пацієнтів). Однак довіра пацієнтів і репутація організації також можуть постраждати: 80% пацієнтів кажуть, що змінили б постачальника послуг, якби їхні дані були скомпрометовані, а 50% уникали б постачальника, який зазнав кібератаки.

Що може зробити окремий постачальник? Приклад

Найпоширеніші атаки здійснюються через фішинг. Дослідження підтверджують, що знеструмлені співробітники більш схильні до спроб фішингу.

Один із моїх друзів-провайдерів розповів мені, наскільки гарним став фішинг. Під час роботи їй зателефонували з Управління по боротьбі з наркотиками та повідомили, що її облікові дані, можливо, було зламано, і щоб перевірити інформацію. Виявилося, це зовсім не DEA: це була спроба фішингу. Ми дивувалися цьому. У них був номер її мобільного телефону, місце її роботи та її NPI. Вони навіть підробили DEA щодо ідентифікатора абонента. Шахраї стають все більш витонченими після появи Nigerian Prince Scams.

Ще більш тривожним є те, що найбільше часу потрібно для виявлення та локалізації вкрадених або скомпрометованих облікових даних. У середньому для вирішення потрібно близько року (328 днів).

Винос:

Для лікарень і організацій перевірте свої застарілі системи на наявність сучасніших і безпечніших.

Щодо постачальників, уряд чи агентство не запитуватимуть вашу особисту інформацію по телефону. Якщо вони законні та дзвонять вам, вони вже мають це.

Для провайдерів і адміністраторів,

Нехай вашу угоду про ділове партнерство перевірить юрист, який обізнаний у цій сфері.

Дізнайтеся середню вартість середньостатистичного порушення кібербезпеки, подумайте про те, щоб включити її або придбати свій поліс, щоб допомогти покрити відповідні юридичні збори та звітність про сповіщення». ***(Andrea Chase. Trends in Health Care and the Intersection of Cybersecurity // Spencer Fane LLP (https://www.spencerfane.com/insight/trends-in-health-care-and-the-intersection-of-cybersecurity/). 19.12.2023).***

***

«Небезпека кіберзлочинності та порушень безпеки нависла над галуззю охорони здоров'я, як повільна буря.

Станом на середину грудня Управління з громадянських прав (OCR) Департаменту охорони здоров'я та соціальних служб (HHS) отримало 541 повідомлення про витік даних понад 500 осіб протягом 2023 року. Серед них були випадки, які скомпрометували інформацію мільйонів, або навіть десятки мільйонів осіб, як це було у випадку з гучним порушенням цього літа в HCA Healthcare.

Деякі атаки змушували постачальників медичних послуг коригувати свої робочі процеси або переривати послуги через блокування їхніх комп'ютерних систем. Наприклад, шістнадцять лікарень Prospect Medical Holdings зазнали атаки в серпні, яка призвела до того, що деякі локації перейшли на паперові записи або

призупинили кілька планових і амбулаторних процедур. Ardent Health Services пережила атаку програм-вимагачів на День подяки, яка зрештою призвела до того, що система з 30 лікарень завчасно закрила та призупинила доступ усіх користувачів до своїх IT-додатків, що призвело до призупинення ненадзвичайних процедур.

«Очевидно, що це ескалація, і що тактика змінюється», — сказав Fierce Healthcare Майк Гамільтон, керівник інформаційної безпеки фірми Critical Insight, що надає кібербезпеку як послугу.

Окрім загрози життю пацієнтів, ці інциденти можуть мати тривалий вплив на фінансовий стан організації, що надає послуги.

Відповідно до липневого звіту IBM та Ponemon Institute, у 2022 році організації охорони здоров'я втратили в середньому 10,1 мільйона доларів США на інцидент від порушень кібербезпеки, що на 9,4% більше, ніж у 2021 році, і значно перевищує те, що змушені витрачати інші сектори економіки. Насправді сільська лікарня штату Іллінойс, яка закрила свої двері влітку, пояснила своє закриття частково багатотижневим інцидентом з програмами-вимагачами, від якого вона зазнала два роки тому, що стало першим в історії випадком, коли закриття лікарні було явно пов'язане з кібератакою.

Крім того, ці інциденти піддають організаціям судові позови з боку тих, чиї дані були скомпрометовані. Вищезазначений витік даних HCA приніс системі щонайменше чотири колективні позови лише за тиждень після його розкриття (хоча в цьому випадку величезна комерційна мережа незабаром після цього повідомила інвесторам, що заявки не повинні мати «матеріалу). вплив» на його бізнес).

На цьому тлі не дивно, що керівники провайдерів прагнуть зміцнити свої позиції. Звіт про опитування, опублікований минулого місяця консалтинговою компанією Guidehouse, показує, що 85% організацій респондентів планують збільшити свої цифрові та IT-бюджети на 2024 рік, причому кібербезпека вказана як головний інвестиційний пріоритет.

Ерік Пупо, директор департаменту комерційних IT-консультацій у галузі охорони здоров'я в Guidehouse, сказав, що значна частина інвестиційних рішень є реакцією на «зовнішнє загрозливе середовище — [багато лідерів] прагнуть інвестувати в кібербезпеку зсередини І ззовні, а не зокрема, аналізуючи, де рентабельність інвестицій у кібербезпеку допомагає підвищити рівень кібербезпеки».

Від нормативного середовища, що розвивається, до зміни кутів атаки, експерти з кібербезпеки кажуть, що керівникам лікарень і систем охорони здоров'я, які сподіваються захистити свої організації, варто подумати про багато речей, вступаючи в новий рік.

Хто в перехресті прицілу?

Експерти кажуть, що минулий рік показав, що кіберзлочинці більш ніж готові вдарити. Оскільки видатні, забезпечені ресурсами заклади витратили останні кілька років на будівництво своїх стін, менші постачальники залишаються як нижчий плод.

«Існує помітне зростання кількості атак на менших регіональних постачальників медичних послуг, яким, можливо, знадобляться надійні заходи кібербезпеки», — сказала Ані Чаудхурі, співзасновник і генеральний директор фірми з безпеки даних Dasera. «Ці організації часто зберігають дуже конфіденційні дані, що робить їх привабливими цілями для хакерів».

За словами Гамільтона, постачальники послуг із низьким ринком послуг, такі як спеціалізовані клініки чи медичні центри візуалізації, також стають все більшою мішенню для зловмисників.

З іншого боку, він сказав, що також було більше уваги приділено «виходу на вершину організації, яка має багато філіалів, де верхівка організації обробляє записи для дюжини чи більше лікарень, і це стає єдиним пунктом магазин.» Цей тип стратегії сприяв більшому масштабу зареєстрованих порушень цього року порівняно з минулими.

Атаки на сторонніх бізнес-партнерів постачальників медичних послуг і ширший ланцюжок поставок також різко почастішали протягом останніх кількох

місяців. Наприклад, майже дві третини респондентів одного нещодавнього опитування IT-спеціалістів у сфері охорони здоров'я сказали, що їхня організація стикалася з атаками на ланцюг поставок протягом останніх двох років, а частка тих, хто сказав, що це остаточно порушило обслуговування пацієнтів, зросла на 70% порівняно з попереднім періодом. опитування за рік.

«Забезпечення того, щоб сторонні постачальники дотримувалися надійних стандартів кібербезпеки, більше не є заняттям, яке є приємним або встановленим прапорцем; Це фундаментальний обов'язок захищати конфіденційні дані пацієнтів, підтримувати безперервність роботи та захищати від наростаючої хвилі кіберзагроз», – сказав Fierce Healthcare Майк Парізі, керівник відділу залучення клієнтів у фірмі з дотримання вимог кібербезпеки Schellman. «Лікарні повинні активно співпрацювати з постачальниками, щоб запровадити суворі протоколи кібербезпеки, проводити регулярні аудити та розвивати культуру постійного вдосконалення».

Окрім наполягання на договірних положеннях щодо безпеки даних, Чаудхурі виступав за регулярні спільні кібернавчання та обмін розвідданими про загрози між лікарнями та їхніми партнерами.

«Прозорість і відкрите спілкування з діловими партнерами щодо потенційних вразливостей і загроз є життєво важливими», — сказав він.

Вектори атаки

Декілька експертів заявили, що кібератакники частіше використовують уразливості програмного забезпечення як свою точку входу.

«Грунтуючись на аналізі нашого звіту про порушення даних, фішинг як кращий початковий вектор доступу поступився місцем використанню вразливостей», — сказав Гамільтон. «Отже, увага зосереджена на швидкому виправленні ваших вразливостей, отриманні ваших оновлень — зараз гонка, коли постачальник випускає виправлення».

«Фундаментальна гігієна безпеки» з підключеними пристроями повинна бути однією з головних областей кібербезпеки для керівництва охорони здоров'я, сказав Сону Шанкар, директор зі стратегії компанії Phosphorus, що займається

розширеною безпекою в Інтернеті речей, Fierce Healthcare. Оскільки застарілий підхід до кібербезпеки надавав пріоритет моніторингу та контролю мережевого трафіку, зараз «дуже часто», коли використовувані медичні пристрої все ще працюють із паролями за замовчуванням, попередив він.

«Немає великої обізнаності про те, що це проблема», - сказав Шанкар. «Першим кроком тут було б отримати справжню точну інвентаризацію всіх пов'язаних речей у лікарняному середовищі, у клінічному середовищі, які потенційно можуть бути використані для різноманітних цілей кіберзлочинців».

З іншого боку, «з боку [зловмисників] зростає усвідомлення того, що з традиційними IT-пристроями, такими як ноутбуки Windows, у вас є передові рішення, наприклад CrowdStrike, які можна розгорнути на цих робочих станціях Windows. Але ви не можете зробити це для великої кількості підключених пристроїв, які є у вашому середовищі; ви просто не можете розгорнути в них агента кінцевої точки», — сказав він.

Хоча атаки, орієнтовані на пристрій, є «імовірною» тактикою для майбутніх атак, Чаудхурі не готовий применшувати загрозу фішингу. Він передбачає, що цілеспрямовані спроби використання людських помилок можуть почастішати наступного року – і, як і інші стратегії, можуть бути навіть підкріплені новими технологіями.

«Сектор охорони здоров'я повинен підготуватися до посилення кібератак на основі штучного інтелекту, які є більш досконалими та адаптивними, ніж традиційні загрози», – сказав він. «Ці атаки включають високоперсоналізовані фішингові електронні листи, автоматизоване використання вразливостей IT-системи та адаптивне шкідливе програмне забезпечення, яке ухиляється від виявлення. Крім того, атаки, керовані ШІ, можуть імітувати звичайну поведінку мережі, минаючи системи виявлення аномалій».

Враховуючи скрутне фінансове становище багатьох систем охорони здоров'я та зростання кількості суб'єктів загрози, особливо тих, хто підтримується іноземними державами, ворожими до США, експерти сказали, що лікарні мають думати про те, «коли», а не «якщо».

«Багаторівневі» стратегії безпеки, які включають сегментацію мережі та виявлення загроз у реальному часі, є «життєво важливими» для обмеження шкоди, сказав Чаудхурі.

Джейк Ауранд, керівник групи контррозвідки в охоронній фірмі Binary Defense, зазначив, що простого плану реагування на інциденти недостатньо.

«Компанії повинні запускати реалістичне моделювання атаки, щоб переконатися, що всі, хто буде залучений, знають, що робити, що дозволяє швидко реагувати на інцидент замість того, щоб люди не розуміли своєї ролі в цьому процесі», — сказав він.

Коли кіберінцидент все ж таки стався, «відкритість і чесність з пацієнтами також можуть мати велике значення», – продовжив Ауранд. «Чим раніше їх можна повідомити про інцидент, тим швидше вони зможуть спробувати захистити себе та бути напоготові для атак, націлених на них, таких як фішингові електронні листи, шантаж і шахрайство з рахунками страхування».

Посилення федерального та державного регулювання

М’яч уже перекочується на нових галузевих вимогах щодо безпеки даних охорони здоров’я.

Алаап Шах, член юридичної фірми Epstein Becker Green (не кажучи про жодну юридичну особу), сказав Fierce Healthcare, що ключові заходи щодо політики та нормативно-правового забезпечення «імовірно з’являться» в результаті нещодавніх зусиль держави щодо посилення безпеки.

Зокрема, він вказав на правила Каліфорнійського Закону про захист прав споживачів щодо проведення оцінки ризиків; правила, запропоновані Нью-Йорком минулого місяця, які вимагають певних рівнів кібербезпеки лікарень; і Закон Вашингтона про моє здоров’я та мої дані, який був підписаний у квітні.

Додаткові розробки також будуть надходити від федеральних органів, від HHS та OCR відповідно до HIPAA та Федеральної торгової комісії відповідно до Правил сповіщення про порушення здоров’я, сказав Шах. Крім того, Агентство з кібербезпеки та безпеки інфраструктури (CISA) і Національний інститут стандартів

і технологій продовжуватимуть виконувати свої повноваження щодо обміну інформацією про загрози та іншої технічної допомоги.

Наразі HHS опублікувала концептуальний документ, у якому викладено плани щодо зміцнення позицій галузі охорони здоров'я в галузі кібербезпеки. Департамент заявив, що планує запровадити комбінацію добровільних цілей кібербезпеки; попередні інвестиції та стимули; і нові вимоги до кібербезпеки в рамках Medicare, Medicaid і HIPAA, які, якщо Конгрес підтримає, можуть супроводжуватися порушеннями платежів і більшими цивільними грошовими штрафами.

Дорожню карту швидко розкритикувала Американська асоціація лікарень, яка описала обов'язкові вимоги кібербезпеки та фінансові штрафи як «контрпродуктивний» захід у важкій боротьбі лікарень із зловмисниками.

Така відповідь не є несподіванкою для Гамільтона, який передбачив, що встановлення нових вимог «насправді не принесе нічого доброго» для фінансово «хисткого» сектору охорони здоров'я (якщо вони не прийдуть рука об руку з грантовими грантами).

Читаючи чайне листя, Гамільтон сказав, що більш імовірно, що майбутні регулятивні та політичні зусилля будуть зосереджені на стійкості, а не на превентивному контролі. Він вказав на кампанію CISA «Shields Ready», де «замість того, щоб намагатися запобігти поганому результату, ми тепер вважаємо це передбачуваною подією, а мета полягає в тому, щоб вийти з килимка після того, як ви приймете удар перед рахунком 10».

Що стосується діяльності на рівні штату, Гамільтон зазначив, що запропоновані правила «майже ідентичні» тим, які пріоритетними вважаються федеральні агентства. Різниця, за його словами, полягає в тому, що ідеологічно стабільніша держава менше ризикує серйозно переглядати політику кожні чотири роки.

«Якщо дисфункція федерального уряду така, що кожного разу, коли відбуваються нові вибори, регулятивний вітер буде дути в іншу сторону, штати почнуть це приймати, щоб вони могли стабільно працювати», — сказав він.

З іншого боку, Гамільтон сказав, що державні закони, пов’язані з конфіденційністю, навряд чи стануть довгостроковим фактором для галузі. Він вказав на обтяжливу «лоскутну» статуту звітності про порушення даних, яка вийшла з усіх 50 штатів, коли федеральні законодавці не зробили жодного кроку. Навіть «непрацюючий Конгрес» хотів би прийняти національні закони про конфіденційність і уникнути повторення цієї помилки, сказав він.

Що стосується того, що буде включено в ці статути конфіденційності, Гамільтон сказав, що можливо, що Конгрес спробує «зняти певний тиск» з боку сектору охорони здоров’я, який часто викликає судові спори.

Зокрема, він сказав, що такі національні закони можуть переважати приватному праву на позов, дозволяючи негайні колективні позови після порушення протоколу, що захищений, включене в закони багатьох штатів. «Замість групового позову, який відбувається негайно лише через те, що мій запис було вкрадено, вам [потрібно було б] довести, що з цим записом було скоєно шахрайство», — сказав він.

Згідно з кампанією Shields Ready та іншими нещодавніми вказівками HHS і Комісії з цінних паперів і бірж, у майбутньому федеральна регулятивна увага, здається, зосереджена на управлінні, участі виконавчої влади та недбалості, передбачив Гамільтон. За його словами, претензії останніх «будуть ставати все більш і більш поширеними» як механізм примусу, який, швидше за все, створить позитивні зміни, ніж нові правила, що вимагають превентивних заходів.

«Нездатність звернути увагу на передбачуваний ризик є недбалістю, і цей стандарт передбачуваності фактично втілений у правовій доктрині», — сказав він. «Ми побачимо більше прикладів [застосування], коли лікарні не дотримувалися порад, наданих їм у [Практиці кібербезпеки в галузі охорони здоров’я] та деяких інших вказівках HHS щодо управління. Вони хочуть, щоб керівники були залучені до управління ризиками. Вони повинні залишити свої відбитки пальців на цих рішеннях, а не просто засунути голову в пісок і не хвилюватися про це, і якщо вони цього не зроблять, це буде недбалість».

Але чи призведе цей підхід до забезпечення виконання більшої відповідальності керівників до меншої кількості інцидентів кібербезпеки?

Гамільтон визнав, що навіть за наявності комітету з управління ризиками, який заслуховуватиме та розглядатиме рекомендації їхніх груп IT та безпеки, керівництво охорони здоров'я все одно матиме право зважувати витрати та приймати ризики кібербезпеки для своєї організації.

Швидше, він і лобі лікарні дійшли згоди щодо того, що ще потрібно для зміни поведінки в галузі.

«Знову ж таки, це якщо вони можуть собі це дозволити, чи не так? Це продовжує залишатися проблемою в секторі охорони здоров'я», – сказав він». ***(Dave Muoio. 2024 Outlook: The cybersecurity trends health system leaders need to know // Questex LLC (https://www.fiercehealthcare.com/providers/2024-outlook-cybersecurity-trends-health-system-leaders-need-know). 21.12.2023).***

***

Захист персональних даних та соціальні мережі

«Користувачі Booking.com висловлювали свій гнів через те, що компанія не змогла перешкодити їм стати жертвами кіберзлочинців.

Протягом принаймні року шахраям вдавалося проникнути в його додаток і обманом виманити у користувачів сотні фунтів.

Десятки людей зв'язалися з BBC, щоб повідомити, що вони втратили гроші, одна з яких сказала, що її «підвела» туристична фірма.

Booking.com заявив, що впроваджує нові функції безпеки, але «не вирішує».

Сама компанія, яка є одним із найбільших веб-сайтів для готелів і відпочинку у світі, не була зламана.

Натомість зловмисники обманом проникли на портали адміністрування окремих готелів, які користуються послугою.

Це дозволяє їм надсилати повідомлення з офіційного додатка та обманювати клієнтів, щоб вони платили їм, а не готелям.

Цей вид шахрайства відбувається вже більше року, але останнім часом, здається, його інтенсивність зросла, оскільки хакери почали використовувати темну мережу, щоб знайти нових жертв.

44-річна Колін Марплз із Дербішир Дейлз втратила 147 фунтів стерлінгів, бронюючи відпустку в Єгипті на 50-річчя свого чоловіка в березні.

Після обміну повідомленнями з тим, що вона вважала готелем у Каїрі через додаток Booking.com, їй надіслали запит на оплату. Насправді це було від шахраїв.

«Я натиснула на нього, не підозрюючи, що це шахрайство, враховуючи, що це було в тому самому поточному чаті в додатку», — сказала вона BBC.

Вона не змогла повернути гроші з веб-сайту чи свого банку.

«Це невелика сума грошей для Booking.com, але це значна сума грошей у повсякденному житті.

«Booking.com має обов'язок перед своїми клієнтами, і вони зазнали невдачі в цій справі. Я все ще борюся, щоб отримати свої гроші».

Інший британський клієнт, який побажав залишитися анонімним, розповів BBC, що втратив 1200 фунтів стерлінгів після того, як його обдурили через додаток.

Він також бореться за повернення коштів і сказав, що відчуває себе «надзвичайно розчарованим».

«Я вважаю, що як клієнт, який вирішив використовувати офіційну платформу, створену компанією, ви можете розраховувати на рівень безпеки та довіри в цій системі».

Тим часом 64-річний Ян Робінсон із Камбрії розповів, як хакери двічі намагалися ошукати його за 122 фунти стерлінгів, а потім за 283 фунти стерлінгів у двох непов'язаних готелях у різних містах, коли він бронював поїздку до Великобританії.

«На щастя, я зателефонував безпосередньо до готелів і таким чином уникнув того, щоб мене спіймали, але коли я повідомив про це Booking.com, вони не зацікавилися», — сказав він.

Представник Booking.com сказав, що немає «срібної кулі, щоб викорінити все шахрайство в Інтернеті», але команда безпеки компанії постійно відстежує та зупиняє нові загрози.

«Ми впроваджуємо нові заходи для забезпечення безпеки облікових записів як наших клієнтів, так і партнерів, включаючи нові функції безпеки для блокування або блокування неактивних облікових записів адміністраторів партнерів, де ми бачили шахрайську діяльність, коли шахраї отримують неавторизований доступ до Бронювання готелю. рахунок».

Компанія заявила, що також відстежує підозрілу активність у своєму додатку та вимикає загальні посилання, якщо чати здаються нелегітимними». ***(Booking.com users angry at firm's response to hacks // BBC (https://www.bbc.co.uk/news/technology-67591310?utm_source=flipboard&utm_content=BBCNews%2Fmagazine%2FBusiness). 04.12.2023).***

***

«…У 2023 році кілька серйозних витоків даних вплинули на мільйони людей і організацій у всьому світі. Ось деякі з найзначніших витоків, які сталися цього року.

X (Twitter)

(4 січня 2023 р.)

Twitter вже кілька років звинувачують у витоку даних. Подібний випадок на сайті був і цього року. Лише за 2 долари можна придбати базу даних темного вебу з електронними адресами приблизно 200 мільйонів користувачів.

Порушення було пов’язано з недоліком програмного інтерфейсу (API) X, який дозволив зловмисникам використовувати систему, отримуючи адреси електронної пошти, пов’язані з обліковими записами X з червня 2021 року по січень 2022 року. Дані все ще передаються особам, які загрожують, навіть після того, як У січні 2022 року усунуто вразливість, яка спричинила злом.

Reddit

(5 лютого 2023 р.)

Reddit став жертвою фішингової атаки 5 лютого 2023 року, що призвело до витоку даних, що призвело до використання скомпрометованих облікових даних для доступу до внутрішніх документів, вихідного коду, даних співробітників і обмеженої інформації про рекламодавців компанії.

Порушення було виявлено в певних внутрішніх системах, і Reddit запевнив користувачів, що їхні первинні робочі системи, які зберігають більшість даних користувачів, залишаються в безпеці. Reddit вжив швидких заходів для усунення порушення, захистивши свої системи та сповістивши постраждалих осіб.

ChatGPT

(24 березня 2023 р.)

ChatGPT багато чого здобув у сфері штучного інтелекту завдяки своїй сучасній системі чат-ботів. Цього року також було представлено багато нових оновлень API для користувачів, зокрема GPT 4 Turbo, GPT 4 Vision і GPT 4 Plus, а також нові функції, як-от розпізнавання голосу. Проте збій у бібліотеці з відкритим вихідним кодом ChatGPT призвів до ненавмисного розкриття даних клієнтів, зокрема часткових даних кредитної картки та заголовків чатів.

OpenAI негайно вирішив проблему, перевівши ChatGPT в автономний режим. Протягом уразливого періоду користувачі могли переглядати певні особисті дані інших, як-от імена, адреси електронної пошти, платіжні адреси та часткову інформацію про кредитні картки. Однак OpenAI запевнив користувачів, що повні номери кредитних карт залишалися в безпеці протягом усього інциденту.

MSI

(6 квітня 2023 р.)

Популярний постачальник комп’ютерів MSI став жертвою атаки програм-вимагачів, яка призвела до фінансових втрат, і стверджував, що викрала 1,5 ТБ даних із систем MSI, включаючи конфіденційну інформацію, таку як вихідний код, закриті ключі та мікропрограмне забезпечення. Вони вимагали викуп у розмірі 4

мільйонів доларів, погрожуючи оприлюднити викрадені дані, якщо їхні вимоги не будуть виконані.

T-mobile

(1 травня 2023 р.)

До витоку даних у січні, який торкнувся 38 мільйонів клієнтів, T-Mobile знову зазнав подібної загрози, яка торкнулася 800 клієнтів, спричинена несанкціонованим доступом до облікових записів, захищених PIN-кодом, і зловмисники змогли викрасти контактні дані клієнтів, ідентифікаційні картки та номери соціального страхування. Компанія зіткнулася із загрозами також у 2021 та 2022 роках.

T-Mobile повідомив своїх постраждалих клієнтів про порушення, а також вжив заходів для захисту своїх систем, щоб запобігти майбутнім порушенням. Компанія також запропонувала постраждалим клієнтам безкоштовні послуги захисту від крадіжки особистих даних.

MOVEit

(червень 2023)

Один із значних витоків даних, який стався у 2023 році, інструмент передачі файлів MOVEit, вплинув на 200 організацій у всьому світі, що призвело до розкриття особистої інформації до 17,5 мільйонів осіб.

Уразливість, ідентифікована як CVE-2023-34362, уможливила неавторизований доступ до серверів MOVEit, порушуючи конфіденційні дані у версіях 11.2–12.5 MOVEit Transfer і MOVEit Cloud. Організаціям довелося інвестувати кошти у відновлення даних і виправлення, щоб відновити свої системи та захистити від подальших порушень.

ROBLOX

(липень 2023)

Компанія зазнала трагічного зламу, який розкрив особисту інформацію майже 4000 розробників Roblox. Витік даних, який включав номери телефонів, адреси електронної пошти та дати народження, був отриманий від учасників конференцій розробників Roblox, що відбулися між 2017 і 2020 роками.

Зловмисники отримали доступ до систем Roblox у 2021 році, що призвело до несанкціонованого отримання даних відвідувачів конференції розробників..

Duolingo

(серпень 2023)

Близько 2,6 мільйона користувачів Duolingo постраждали від витоку даних, який стався в серпні, розкривши особисту інформацію на форумах зловмисників темної мережі. Інцидент викликав занепокоєння щодо розголошення імен, адрес електронної пошти, номерів телефонів, профілів у соціальних мережах і вибраних користувачами мов.

Це було пов’язано з уразливістю в інтерфейсі прикладного програмування (API) Duolingo, що дозволяє зловмисникам використовувати систему та отримувати доступ до профілів користувачів, скомпрометувавши розкриті дані. Проблему було вирішено, попросивши користувачів бути уважними щодо майбутніх фішингових атак і порекомендувавши двофакторну автентифікацію для їхніх облікових записів.

SONY

(вересень 2023)

Sony зазнала атаки з боку групи програм-вимагачів, що призвело до викрадення понад 6000 файлів, включаючи журнали збірки та файли Java, які можна використовувати для розробки експлойтів для систем Sony. Зловмисники погрожували продати вкрадені дані на аукціоні, якщо не задовольнять їхні вимоги про викуп. Хоча деталі початку злому невідомі, виявилося, що зловмисники використовували дірку в безпеці Sony». ***(Sandhra Jayan. The Biggest Data Breaches of 2023 // Analytics India Magazine Pvt Ltd & AIM Media House LLC (https://analyticsindiamag.com/the-biggest-data-breaches-in-2023/?utm_source=flipboard&utm_content=onelife007%2Fmagazine%2FYou%27d+Love+It%21). 04.12.2023).***

***

«Xfinity від Comcast виявила порушення безпеки, яке вплинуло на понад 36 мільйонів клієнтів. Порушення сталося між 16 і 19 жовтня цього року, але для повної історії нам потрібно трохи повернутися назад.

10 жовтня постачальник хмарних послуг Citrix оголосив про вразливість, що впливає на програмне забезпечення, яке використовує Xfinity та «тисячі інших компаній» по всьому світу.

Минуло ще майже два тижні – 23 жовтня – перш ніж Citrix поділиться додатковими вказівками щодо пом'якшення. Xfinity заявила, що негайно виправила та пом'якшила вразливість у своїх системах, але 25 жовтня під час звичайних навчань з кібербезпеки вони виявили несанкціонований доступ до своєї системи, який мав місце тижнем раніше з використанням уразливості.

В окремій заявці до Maine AG Comcast стверджує, що порушення вплинуло на 35 879 455 осіб.

Розслідування Xfinity показало, що інформація про клієнтів, включаючи імена користувачів, хешовані паролі, офіційні імена, контактну інформацію, останні чотири номери соціального страхування, дати народження та/або таємні запитання та відповіді, була скомпрометована. Компанія заявила, що все ще вивчає це питання, тому, можливо, були скомпрометовані додаткові дані.

Xfinity вимагає від клієнтів скинути паролі облікових записів і наполегливо рекомендує ввімкнути двофакторну автентифікацію. Провайдер також радить не використовувати паролі в кількох облікових записах і службах; якщо ви використовували свій пароль Xfinity деінде, обов'язково змініть його.

Примітно, що компанія не згадала про будь-які безкоштовні послуги кредитного моніторингу, які пропонуються постраждалим клієнтам. Такі пропозиції є звичайними для гучних вторгнень у дані, хоча, оскільки ця не включала дані кредитної картки, можливо, тому Xfinity не пропонує її.

Comcast не чужий інцидент з безпекою. Ще в 2018 році було виявлено, що сайт Comcast, який використовувався для активації маршрутизаторів Xfinity, передавав особисті дані, включаючи домашні адреси, назви мереж Wi-Fi і паролі.

Тим, у кого є додаткові запитання, радимо переглянути звіт Xfinity про витік даних або звернутися безпосередньо до компанії». ***(Shawn Knight. Xfinity data breach impacts over 35 million customers // TechSpot, Inc. (https://www.techspot.com/news/101270-xfinity-data-breach-impacted-358-million-customers.html?utm_source=flipboard&utm_content=TechSpot%2Fmagazine%2FTechSpot). 19.12.2023).***

***

Кібербезпека та хмарні технології

«Сучасні технології постійно розвиваються, щоб задовольнити потреби та запити ділового світу, який вимагає ефективності, співпраці та безпеки в будь-який час. У той час як програмне забезпечення як послуга (SaaS) відіграє вирішальну роль у виробництві роботи та можливостях спільної роботи, переваги хмарних обчислень ще більше покращили досвід користувачів. Однак хмара, як наслідок, поставила перед організаціями багато нових викликів безпеці. У результаті організації зобов'язані приділяти пріоритет захисту найбільш конфіденційної інформації в хмарному домені від безлічі загроз безпеці, але це не без труднощів.

Відсутність чітко визначених меж ускладнює безпеку хмарних програм. Тенденція гібридної роботи та багатохмарних середовищ порушила це, усунувши весь нагляд і контроль, які раніше мали команди безпеки, коли люди працювали з одного місця. Природно, що традиційні інструменти безпеки, які використовувалися історично, зараз фактично застаріли та не можуть впоратися з цими новими викликами.

У спробах вирішити цю проблему в цілому деякі організації вирішили використовувати Cloud Access Security Broker (CASB), щоб зменшити ризики безпеки хмари. Хоча це, безумовно, доцільно, організації повинні розуміти, що вибір правильного CASB для свого середовища є не менш важливим завданням. В

ідеалі організації повинні дотримуватися рекомендованих передових практик, щоб гарантувати захист даних у програмах SaaS.

Вказівка №1: зрозумійте хмарну екосистему

За останні роки хмарний ландшафт різко змінився і постійно розвивається. Десять років тому компанії використовували лише невелику кількість хмарних програм. Сьогодні сучасні підприємства використовують сотні хмарних додатків, що потребує продукту CASB, який міг би забезпечити дотримання правил у мережі. Однак для ефективного захисту від хмарних загроз організаціям важливо приділити час, щоб зрозуміти ландшафт свого хмарного середовища. Хоча програми SaaS зазвичай перебувають у центрі уваги, не менш важливо визначити, як рішення для зберігання даних, такі як Amazon Web Services і Google використовуються Cloud Platform. З цієї причини рішення CASB має мати можливості, які включають захист цих сховищ.

Цикл новин регулярно наповнюється порушеннями даних або витоками з хмарних додатків і сховищ даних через неправильну конфігурацію. Таким чином, CASB також повинен мати можливості для виявлення та виправлення цих неправильних конфігурацій, щоб відповідати стандартам безпеки організації.

Вказівка №2: чи є у вас розширена видимість?

Є багато шляхів, якими кіберзлочинці можуть погрожувати конфіденційним даним, особливо тому, що вони не обмежуються лише програмами SaaS. У сучасну епоху віддаленої та гібридної роботи зловмисники намагатимуться використовувати різні некеровані пристрої та програми, які використовуються співробітниками, партнерами та підрядниками для доступу до корпоративних даних.

Вибираючи рішення CASB для організації, переконайтеся, що воно може виявляти обмін даними в несанкціонованих хмарних програмах, некерованих пристроях і платформах електронної пошти. Усі три цінні для сприяння гібридній роботі та співпраці, але вони також представляють одні з найбільших ризиків для безпеки даних. Зрештою, рішення CASB має надати організації чітку видимість

користувачів, програм і пристроїв, а також того, як вони взаємодіють з даними в мережі.

Вказівка №3: використовуйте адаптивний доступ

Як золоте правило, хмарна безпека ніколи не повинна перешкоджати продуктивності, натомість вона має діяти як стимул. При дослідженні традиційних рішень для керування доступом часто траплялося, що рішення порушували захист конфіденційних даних, щоб забезпечити безперебійний доступ. Як правило, доступ надається користувачеві, який має відповідні облікові дані та не розглядатиме, чи обліковий запис зламано, чи існує небезпека внутрішніх загроз. Цей метод дуже ризикований, і його слід уникати будь-якою ціною. Натомість організації повинні розгорнути рішення CASB, яке може інтелектуально визначати, кому потрібен доступ, оскільки це встановить баланс між безпекою та продуктивністю. Крім того, дотримання адаптивного підходу нульової довіри до контролю доступу надаватиме доступ на основі кількох факторів, включаючи безпеку пристроїв і аналітику поведінки користувачів і об’єктів (UEBA). Цей розширений рівень безпеки доступу постійно оцінюватиме рівні ризику, перш ніж визначити, чи потрібно надавати доступ.

Рекомендація № 4: Проактивний захист даних

Уявлення про безпеку хмарних додатків все ще дуже реактивні, і, на жаль, більшість організацій роблять безпеку пріоритетом лише після інциденту. Дані є найважливішим активом, яким володіє бізнес, тому їх захист від хмарних загроз безпеки має залишатися головним пріоритетом. Без даних підприємства не можуть працювати ефективно, а також не можуть надавати необхідні послуги своїм клієнтам, тому їх часто називають джерелом життя. Тому організації повинні застосовувати проактивний підхід до захисту конфіденційних даних у CASB за допомогою запобігання втраті даних (DLP). За допомогою цього інструменту CASB може застосовувати політики, які гарантують дотримання стандартів безпеки даних без впливу на рівень продуктивності робочої сили. Крім того, використання підходу, орієнтованого на дані, може включати певні заходи безпеки даних, такі як редагування або маскування конфіденційної інформації у файлі, водяні знаки

документів або вимкнення завантажень – що є прогресивнішим, ніж автоматична відмова в доступі до документів. Крім того, для команд безпеки життєво важливо мати можливість захистити конфіденційні дані, оскільки вони поширюються на некеровані програми та пристрої. Управління цифровими правами підприємства (EDRM) можна використовувати для автоматичного шифрування даних, коли вони передаються за межі компанії, забезпечуючи захист конфіденційної інформації навіть поза вашим контролем.

У міру того, як темпи впровадження хмарних технологій у діловому світі зростають, загрози хмарним технологіям і конфіденційній інформації, яка міститься в них, ставатимуть все більш поширеними. Враховуючи численні правила безпеки та конфіденційності даних, які застосовуються, організації та групи безпеки мають обов'язок і відповідальність за забезпечення належного захисту даних. Невиконання цього буде вважатися актом недбалості, який карається великими штрафами та пенею. З огляду на те, що сучасні дані є цифровими та переміщуються без обмежень, свого часу організації зайняли проактивну позицію та розгорнули безпеку, яка переміщується разом із ними. Інвестиції в відповідне рішення CASB є кроком у правильному напрямку. Він допоможе організаціям забезпечити захист даних, одночасно зменшуючи витрати, підвищити продуктивність, забезпечити відповідність нормативним вимогам, забезпечити видимість і гнучкість і зменшити ризик несанкціонованого використання або доступу». ***(Sundaram Lakshmanan. Enhancing SaaS app security: Best practices for cloud protection // Future US, Inc. (https://www.techradar.com/pro/enhancing-saas-app-security-best-practices-for-cloud-protection?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 15.12.2023).***

***

«…Члени Європейського Союзу ввечері в четвер погодили новий закон про кібербезпеку для захисту так званого Інтернету речей (IoT). Закон про захист від кібернетичного впливу (CRA) — це спроба Європи зупинити незахищені цифрові пристрої, які все частіше захоплюють будинки та робочі місця, від створення кіберзагроз.

Це наріжний камінь ширшої стратегії ЄС щодо реагування на безліч загроз, з якими стикаються європейські уряди, промисловість і громадяни — часто від кіберзлочинців і підтримуваних державою хакерських груп з Росії, Китаю та інших іноземних держав.

Ідея закону про безпеку IoT виникла, коли Європа зіткнулася з рекордною кількістю розподілених атак на відмову в обслуговуванні (DDoS) у 2016 році, коли підключені до IoT пристрої, такі як камери, були викрадені хакерами та перетворені на великі системи «ботнету», такі як Mirai. ботнет і надсилав інтернет-трафік на веб-сайти та сервери, роблячи їх недоступними для користувачів.

Ботнети показали, що багато пристроїв, підключених до Інтернету, надто легко піддавалися підробці, дозволяючи зловмисникам заволодіти камерами безпеки або скомпрометувати підключену до Інтернету іграшку.

Для багатьох галузей — особливо тих, що не належать до «критичної інфраструктури» — кібербезпека також досі в основному нерегульована та надана ринку. Це призвело до того, що всі, від державних служб до приватних компаній, стикаються зі все більш агресивними спробами отримати доступ до їхніх систем через уразливості або шляхом злому постачальників.

Європейський кіберзакон IoT намагається вирішити цю проблему, накладаючи суворі вимоги на будь-кого, хто продає цифрові продукти в усьому блоці.

Продукти з маркуванням CE повинні відповідати мінімальному рівню перевірок кібербезпеки, включаючи забезпечення доступності оновлень безпеки,

перевірку кібербезпеки ланцюгів постачання та кращий обмін інформацією про вразливості з органами кібербезпеки.

Ось що вам потрібно знати про закон.

Компанії повинні позначати вразливі місця

Згідно з правилами, компанії повинні повідомляти владі про збої у своїх програмних і апаратних системах протягом 24 годин і надавати більш розширені звіти протягом 72 годин, щоб прискорити обмін попередженнями про ризики та атаки.

Суперечливо те, що їм навіть доведеться повідомити владі про вразливості, якими активно користуються хакери. Про ці зареєстровані вразливості буде надано як національним органам влади, так і Агентству кібербезпеки Європейського Союзу (ENISA).

Це викликало занепокоєння, що Європа створить величезну базу даних з активними лазівками — скарбницю для хакерів, яка, якщо її зламати, може призвести до збільшення кількості атак.

Ви довше отримуватимете оновлення безпеки

Групи споживачів були захоплені CRA, який вимагав від виробників надавати оновлення безпеки протягом очікуваного терміну служби продукту.

Учасники переговорів стверджували, що підтримувати продукти потрібно щонайменше п’ять років — якщо тільки очікуваний термін служби пристрою не буде коротшим. Це означає, що споживачі можуть бути впевнені, що телефони, холодильники, фотоапарати та інші пристрої продовжуватимуть отримувати оновлення безпеки протягом пристойного часу.

Закон зосереджується на підключених пристроях у низці секторів, включаючи «критичні» сфери, такі як фінанси, аерокосмічна сфера, транспорт, енергетика та інші; вони також стикаються з жорсткими вимогами щодо кібербезпеки відповідно до Директиви ЄС NIS2.

Підприємствам загрожують штрафи, коли вони помиляються

Компанії можуть бути оштрафовані на суму до 15 мільйонів євро або 2,5 відсотка свого річного доходу (залежно від того, що більше), якщо вони не

забезпечать кібербезпеку свого продукту шляхом проведення оцінки своїх продуктів і звітування про вразливості.

Штрафи в розмірі до 10 мільйонів євро або 2 відсотків доходу компанії застосовуватимуться, якщо імпортери або дистриб'ютори не гарантують, що продукт має маркування CE.

Китай може зіткнутися з новими обмеженнями

Новий закон дозволяє національним регуляторам враховувати «нетехнічні фактори ризику» при визначенні значущості ризику кібербезпеки.

«Залежність від високоризикованих постачальників продуктів з цифровими елементами може становити стратегічний ризик, який необхідно розглянути на рівні Союзу, особливо коли продукти з цифровими елементами призначені для використання основними суб'єктами», — йдеться в тексті.

Такі терміни, як «постачальники високого ризику», повторюють законодавство ЄС про 5G Security Toolbox, яке призвело до національних обмежень на використання китайського телекомунікаційного обладнання від фірм Huawei і ZTE.

Новий закон про Інтернет речей може призвести до більш цілеспрямованих заходів, що обмежують використання продуктів, виготовлених у Китаї та інших країнах і правових системах, яким не довіряють європейські країни-члени.

Знадобляться роки, щоб стати реальністю

Текст має бути офіційно підписаний на пленарному засіданні Європейського парламенту та національними урядами в Раді ЄС.

У промисловості та урядів буде три роки, щоб адаптуватися до нових вимог, тобто вони почнуть діяти лише на початку 2027 року.

Щодо деяких правил, таких як повідомлення про вразливості, ЄС хоче, щоб фірми дотримувалися їх до середини 2026 року». ***(Laurens Cerulus and Antoaneta Roussi. Europe's internet of things cyber law, explained // POLITICO (https://www.politico.eu/article/europe-internet-of-things-cyber-law-explained/?utm_source=flipboard&utm_content=rhudaur%2Fmagazine%2FCybersecurity+Today). 01.12.2023).***

***

«Коли йдеться про кібербезпеку для розумних міст, які значною мірою використовують інформаційні та комунікаційні технології для підвищення ефективності роботи, обміну інформацією та покращення якості життя своїх громадян, ставки високі.

Оскільки розумні міста все більше покладаються на взаємопов'язані системи та пристрої, поверхня для атак і, отже, вразливість таких основних компонентів, як енергетична інфраструктура, стає критичною. Одна цілеспрямована атака може вимкнути опалення взимку, перервати доставку чистої води або спричинити вибух магістралей природного газу.

У кібербезпеці один розмір не підходить для всіх. Наприклад, захист транспортного рівня (TLS) є незамінним для електронної комерції, тоді як віртуальні приватні мережі (VPN) мають вирішальне значення для підключених підприємств. Однак навіть підключене підприємство (яке ми зазвичай вважаємо досить складною архітектурою) порівняно з розумним містом є відносно простою системою.

Захист критичної інфраструктури в розумних містах вимагає вирішення більш різноманітних компонентів, починаючи від енергетики до чистої води та навіть систем реагування на надзвичайні ситуації. А отже, це потребує більш масштабного, фундаментального та глибшого підходу.

У цій статті розглядатимуться унікальні проблеми захисту критичної інфраструктури в розумних містах і обговорюватимуться найефективніші стратегії для досягнення надійного захисту.

Унікальні виклики безпеки критичної інфраструктури розумного міста

Розумні міста покладаються на багато взаємопов'язаних систем і пристроїв для надання послуг своїм громадянам. У результаті вони стикаються з унікальними проблемами, коли справа доходить до безпеки критичної інфраструктури.

• Взаємозалежність: взаємопов'язаний характер інфраструктури розумного міста означає, що одна вразливість може мати далекосяжні наслідки з каскадними ефектами для кількох систем. Наприклад, Ready.gov зазначає, що втрата

електроенергії може порушити транспорт, водопостачання, зв’язок і системи грошових переказів. Це, у свою чергу, може призвести до закриття магазинів, а також до псування їжі та забруднення води. Що ще гірше, медичне обслуговування може бути перервано, а в деяких районах може статися сплеск насильницької злочинності.

• Складність: величезна кількість компонентів, пристроїв і систем, задіяних в інфраструктурі розумного міста, ускладнює реалізацію комплексних заходів безпеки. Єдине розумне місто буде використовувати розгалужену архітектуру Інтернету речей (IoT) з потенційно сотнями тисяч датчиків та інших пристроїв, які збирають і передають дані в режимі реального часу для управління транспортом, енергією та різними іншими аспектами основних функцій міста.

Крім того, він значною мірою покладається на штучний інтелект (ШІ), серед іншого, для прогнозного обслуговування критично важливих систем. Блокчейн також може відігравати ключову роль у збереженні записів, тоді як геопросторові технології часто виконують важливу функцію в управлінні навколишнім середовищем.

• Різноманітні зацікавлені сторони: інфраструктура «розумного міста» передбачає участь багатьох зацікавлених сторін, у тому числі державних і приватних організацій, які мають різний досвід і ресурси в галузі кібербезпеки. Це означає, що більше людей потребують доступу до різних систем, що збільшує ймовірність того, що зловмисник увійде.

• Загрози, що розвиваються: кіберзагрози, націлені на критичну інфраструктуру, постійно розвиваються, вимагаючи від зацікавлених сторін розумного міста бути в курсі останніх тенденцій і технологій. У той час як більшість кібератак на окремих осіб або корпорації можуть мати вузькі цілі, атаки на інфраструктуру міста можуть мати набагато більші амбіції, такі як створення економічного хаосу або руйнування критично важливих служб. Крім того, ці атаки, які можуть фінансуватися державою, можуть бути більш складними та динамічними, ніж стандартні кіберзагрози.

Розробка безпеки для критичної інфраструктури розумного міста

Враховуючи унікальні виклики безпеки критичної інфраструктури в розумних містах, індивідуальний підхід до кібербезпеки є важливим. Наведені нижче стратегії можуть допомогти захистити такі важливі компоненти, як енергетична інфраструктура.

• Прийняття архітектури нульової довіри (ZTA): ZTA забезпечує міцну основу для захисту критичної інфраструктури, припускаючи, що жодному користувачу, пристрою чи системі не можна довіряти. У системі, до якої в будь-який момент часу можуть отримати доступ тисячі людей із багатьох організацій, ризик того, що хтось із поганими намірами проникне у вашу систему, є високим. Перевірка та автентифікація кожного запиту на доступ гарантує, що жоден користувач ніколи не матиме повних ключів до королівства.

• Впровадження механізмів безпеки на основі оцінки ризиків. Маючи справу з такою складною системою, як розумне місто, важливо дотримуватися методичного підходу до впровадження заходів безпеки. Оскільки ви не можете усунути кожну потенційну вразливість на першому проході, дуже важливо визначити, які області становлять найбільшу небезпеку, і захистити їх першими. Фреймворки, такі як NIST Cybersecurity Framework або серія ISO/IEC 27000, забезпечують структурований підхід до управління ризиками, дозволяючи організаціям визначати пріоритетність ресурсів і впроваджувати відповідні заходи безпеки.

• Використання сегментації мережі та мікросегментації: для розумного міста найгірший сценарій передбачає вхід зловмисника в систему та вільний перехід від однієї програми до іншої, потенційно вимикаючи кілька служб та компонентів інфраструктури. Організації можуть ізолювати потенційні загрози та обмежити їх бічний рух у системі, розділивши мережу на менші сегменти. Завдяки такому підходу, навіть якщо зловмисник все-таки проникне в систему, пошкодження може бути обмежено в одному сегменті мережі.

Крім того, коли йдеться про захист складної системи, подумайте про потік інформації, пов’язаної з безпекою. Подумайте, як ви озброюєте своїх ключових

людей правильною інформацією та надаєте їм можливість координувати свої зусилля з іншими ключовими гравцями. Ви можете зробити це:

• Інвестиції в безперервний моніторинг і розвідку про загрози: моніторинг мережевого трафіку, продуктивності системи та поведінки користувачів у режимі реального часу є критично важливим компонентом виявлення потенційних загроз і реагування на них. Канали розвідки про загрози можуть надати цінну інформацію про нові тенденції та вектори атак.

• Заохочення співпраці та обміну інформацією: враховуючи різноманітність зацікавлених сторін, залучених до інфраструктури розумного міста, сприяння культурі співпраці та обміну інформацією має вирішальне значення для забезпечення єдиного підходу до кібербезпеки.

• Пріоритет навчання: нарешті, добре навчена робоча сила є важливою для підтримки безпеки критичної інфраструктури. Інвестиції в навчальні програми та забезпечення постійного навчання можуть гарантувати, що зацікавлені сторони «розумного міста» готові протистояти кіберзагрозам, що розвиваються.

Висновок

У світі все більш витончених атак на дедалі складнішу архітектуру настав час адаптувати наші заходи кібербезпеки до унікальних потреб розумних міст. Це вимагає індивідуального підходу та усвідомлення того, що традиційних рішень, таких як TLS і VPN, може бути недостатньо в цьому складному ландшафті. Застосовуючи стратегії, про які йдеться в цій статті, зацікавлені сторони можуть створити надійний захист для основної інфраструктури». ***(Julian Durand. Customizing Cybersecurity For Critical Infrastructure: Finding The Perfect Fit For Smart Cities // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/12/05/customizing-cybersecurity-for-critical-infrastructure-finding-the-perfect-fit-for-smart-cities/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff&sh=6fe8ffa76df7). 05.12.2023).***

***

«Інструменти штучного інтелекту більш уразливі, ніж вважалося раніше, до цілеспрямованих атак, які фактично змушують системи ШІ приймати неправильні рішення, показує дослідження.

Йдеться про так звані «змагальні атаки», під час яких хтось маніпулює даними, що надходять у систему ШІ, щоб заплутати їх. Наприклад, хтось може знати, що розміщення певного типу наклейки в певному місці на знаку зупинки може фактично зробити знак зупинки невидимим для системи ШІ. Або хакер може встановити код на рентгенівському апараті, який змінює дані зображення таким чином, що змушує систему ШІ робити неточні діагнози.

«Здебільшого ви можете вносити всілякі зміни в знак «стоп», і штучний інтелект, навчений розпізнавати знаки «стоп», все одно знатиме, що це знак «стоп», — говорить Тіанфу Ву, співавтор статті про нову роботу. і ад'юнкт-професор електротехніки та комп'ютерної інженерії в Університеті штату Північна Кароліна. «Однак, якщо штучний інтелект має вразливість, і зловмисник знає про вразливість, зловмисник може скористатися вразливістю та спричинити аварію».

Нове дослідження, проведене Ву та його співробітниками, зосереджено на визначенні того, наскільки поширеними є такі вразливі місця в глибоких нейронних мережах ШІ. Вони виявили, що вразливі місця набагато більш поширені, ніж вважалося раніше.

«Більше того, ми виявили, що зловмисники можуть скористатися цими вразливими місцями, щоб змусити штучний інтелект інтерпретувати дані так, як вони хочуть», — говорить Ву. «Використовуючи приклад зі знаком «стоп», ви можете змусити систему штучного інтелекту вважати, що знак «стоп» — це поштова скринька, або знак обмеження швидкості, або зелене світло тощо, просто використовуючи дещо інші наклейки — або будь-яку іншу вразливість.

«Це надзвичайно важливо, тому що якщо система штучного інтелекту не стійка проти таких атак, ви не захочете використовувати систему для практичного використання, особливо для програм, які можуть вплинути на життя людей».

Щоб перевірити вразливість глибоких нейронних мереж до цих агресивних атак, дослідники розробили частину програмного забезпечення під назвою

QuadAttacK. Програмне забезпечення можна використовувати для тестування будь-якої глибокої нейронної мережі на вразливі місця.

«По суті, якщо у вас є навчена система штучного інтелекту, і ви тестуєте її з чистими даними, система штучного інтелекту поводитиметься, як передбачувано. QuadAttacK спостерігає за цими операціями та дізнається, як ШІ приймає рішення, пов'язані з даними. Це дозволяє QuadAttacK визначити, як можна маніпулювати даними, щоб обдурити ШІ. Потім QuadAttacK починає надсилати оброблені дані в систему ШІ, щоб побачити, як ШІ реагує. Якщо QuadAttacK виявив уразливість, він може швидко змусити штучний інтелект бачити все, що QuadAttacK хоче бачити».

Під час перевірки концепції дослідники використовували QuadAttacK для тестування чотирьох глибоких нейронних мереж: двох згорткових нейронних мереж (ResNet-50 і DenseNet-121) і двох трансформаторів зору (ViT-B і DEiT-S). Ці чотири мережі були обрані тому, що вони широко використовуються в системах ШІ по всьому світу.

«Ми були здивовані, виявивши, що всі ці чотири мережі дуже вразливі до агресивних атак», — каже Ву. «Ми були особливо здивовані тим, якою мірою ми змогли налаштувати атаки, щоб мережі бачили те, що ми хотіли, щоб вони бачили»…

«Тепер, коли ми можемо краще ідентифікувати ці вразливості, наступним кроком є пошук способів мінімізації цих вразливостей», — говорить Ву. «У нас уже є деякі потенційні рішення, але результати цієї роботи ще очікуються»…» ***(Matt Shipman-NC State. surprisingly vulnerable to targeted attacks // Futurity (https://www.futurity.org/ai-vulnerable-targeted-attacks-3005912-2/?utm_source=rss&utm_medium=rss&utm_campaign=ai-vulnerable-targeted-attacks-3005912-2). 07.12.2023).***

***

«Штучний інтелект (AI) і машинне навчання (ML) не є новими темами в кібербезпеці. Протягом останніх двох десятиліть вони використовувалися як взаємозамінні.

До цього часу штучний інтелект і машинне навчання використовувалися переважно в продуктах виявлення загроз, таких як виявлення кінцевих точок і реагування на них, аналітика поведінки користувачів і об'єктів, а також інформація про безпеку та управління подіями, як механізм для виявлення шаблонів, які вказують на потенційну зловмисну поведінку.

У зв'язку зі стрімким поширенням генеративного штучного інтелекту в громадській обізнаності у 2023 році з'явилися абсолютно нові міркування про те, як ШІ можна використовувати для вирішення проблем кібербезпеки, а також про нові загрози кібербезпеці, які він може створити. Ці міркування включають такі тактики, як застосування штучного інтелекту для кращого розуміння середовища, яке захищають організації, на додаток до загроз, націлених на них, а також для оптимізації співпраці та інших процесів під час щоденних операцій безпеки, розширення та розширення можливостей постачальників кібербезпеки або захисників.

Крім того, з новими продуктами, включаючи ChatGPT від Open AI, кожна організація повинна думати про те, як безпечно та безпечно впровадити та інтегрувати AI у корпоративні середовища та продукти, які їх захищають.

Хоча багато постачальників кібербезпеки стверджують, що використовують кібербезпеку у своїх послугах, мало хто може чітко сформулювати, як вони застосовують її для вирішення нових проблем і як вони впроваджують її безпечно та відповідально.

Нижче наведено деякі міркування, про які слід пам'ятати, оцінюючи постачальників кібербезпеки, які стверджують, що використовують ШІ у своїх продуктах і послугах.

Застосування ШІ до проблеми запобігання, а не виявлення

Не можна захистити те, чого не розумієш. Однією з найбільших переваг, яку має захисник перед нападником, є той факт, що він може знати своє оточення краще, ніж атакуючий. На жаль, через складність сучасних IT (не кажучи вже про IoT та OT) реалізувати цю перевагу набагато важче, ніж будь-кому з нас хотілося б. Ця проблема загострюється, коли організації вирішують передати елементи своїх

операцій безпеки постачальникам керованих послуг безпеки (MSSP) і постачальникам керованого виявлення та реагування (MDR).

Хоча штучний інтелект і машинне навчання традиційно використовувалися для моделювання минулої поведінки зловмисників для виявлення майбутніх загроз, тепер у нас є можливість застосувати штучний інтелект до проблеми кращого розуміння нашого середовища, поверхонь атак і навіть поведінки захисників, щоб ми могли ліквідувати прогалини та запобігати загрозам. на першому місці.

Приклади цього:

• Використання штучного інтелекту для визначення потенційно критичних активів, особливо якщо ці активи неправильно каталогізовано в базі даних керування конфігурацією чи іншому сховищі активів.

• Використання штучного інтелекту для побудови моделей для розрахунку ймовірності того, що сповіщення є доброякісним позитивним проти справжнього позитивного.

• Створення інструментів штучного інтелекту, які моделюють поведінку захисника, щоб визначити можливості для вдосконалення, включаючи процеси, які дозріли для автоматизації.

Оцінюючи постачальників кібербезпеки, які стверджують, що мають досвід роботи зі штучним інтелектом, обов’язково запитайте їх, як вони використовують штучний інтелект, щоб не лише виявляти загрози, але й запобігати їм і покращувати вашу загальну безпеку.

Використання ШІ для сприяння співпраці SecOps

Це не було б розмовою про штучний інтелект, якби ми не розглянули можливості великих мовних моделей (LLM) для трансформації того, як команди спілкуються та співпрацюють у щоденних операціях безпеки. Доступ до потрібної інформації в потрібний час є важливим для ефективних операцій безпеки. Традиційно це було проблемою для організацій, які використовують MSSP та постачальників MDR, оскільки, хоча інформація надається команді безпеки клієнта через веб-портали чи системи продажу квитків, немає хорошого механізму для

того, щоб поставити людині додаткові запитання та отримати зворотний зв’язок в реальному часі.

LLM пропонують відповідь на цей виклик, надавши чат-ботам можливість генерувати розуміння питань природної мови, на які раніше ніхто, крім людини, не міг відповісти. У поєднанні з моделями, розробленими для формування розуміння самого середовища, штучний інтелект може відповідати не лише на загальні запитання, а й на дуже локалізовані запитання щодо певного середовища. Наприклад, загальний LLM може відповісти на запитання: «Як моя організація може заощадити гроші на витратах на прийом даних?» шляхом повернення відповіді з блогу передових практик щодо найкращих практик прийому даних. Але LLM із моделлю того, які дані отримує організація та як ці дані зберігаються, дасть конкретні дієві рекомендації щодо того, як змінити їх прийом або зберігання, щоб заощадити гроші компанії.

Удосконалення чат-ботів за допомогою LLM – це лише один із застосувань цієї технології. LLMs можна використовувати для оптимізації всіх видів комунікації під час щоденних операцій безпеки, включаючи узагальнення інцидентів, результати пошуків загроз, рекомендації та покращення стану безпеки тощо. Сьогодні створення цих типів підсумків і письмової документації — це здебільшого ручний процес, який виконують оператори служби безпеки, що займає не лише значний час, але й може спричиняти помилки. Штучний інтелект може повністю автоматизувати більшу частину цієї роботи, генеруючи підсумки за лічені секунди, які потім можуть перевірити та перевірити оператори безпеки.

Оцінюючи постачальників засобів кібербезпеки, які стверджують, що мають чат-бота на основі штучного інтелекту, запитайте їх, як вони локалізують або пристосовують результати штучного інтелекту до вашої організації. Також запитайте їх, як ще вони використовують штучний інтелект для оптимізації співпраці та спілкування в своїх продуктах або послугах

Сучасна безпека має використовувати штучний інтелект, щоб зробити людський інтелект ефективнішим

З мого досвіду, великий відсоток цих постачальників використовує машинне навчання для виявлення моделей поведінки, які вказують на атаки, що призводить до надсилання шквалу сповіщень до команд безпеки, не визначаючи пріоритетів і не реагуючи на них. Коли у вашій команді вже недостатньо персоналу, ресурсів і перевантажено, отримувати перелік загроз не допоможе. Вашій організації потрібні захисники кібербезпеки, які допоможуть вам зосередити зусилля. Це означає, що вони повинні вміти відрізнити справжні загрози від шуму та визначити пріоритети, а також допомогти вам визначити вразливі місця, які можуть мати негативний вплив на вашу організацію, якщо їх не усунути; ми називаємо цей випадок переконанням.

Організаціям слід використовувати штучний інтелект, щоб ефективніше відрізняти справжні позитивні сповіщення від помилкових і доброякісних. Це пришвидшує час для вирішення інцидентів і зменшує ескалацію клієнтів, що призводить до того, що ваші команди витрачають менше часу.

Зарядіть своїх захисників

У світі, де кіберзлочинці все частіше використовують ШІ для загрози вашій безпеці, важливо зробити ШІ ключовим компонентом вашої стратегії безпеки. Іншими словами, використовуйте AI для боротьби з AI.

Багато елітних хакерів розглядають ШІ не як загрозу, а як інструмент, який розширює їхні здібності, покращуючи творчі навички вирішення проблем і надаючи їм конкурентну перевагу.

Але якщо штучний інтелект посилює можливості зловмисників, він має потенціал зробити те саме для захисників. Співпрацюйте з захисниками, які можуть скористатися цією можливістю та активно використовувати ШІ проти реальних загроз. Перш ніж підписувати контракт із постачальником, поясніть йому, як він використовуватиме ШІ, щоб забезпечити цінність вашої організації. Якими конкретними способами вони застосовують штучний інтелект для підвищення ефективності безпеки та захисту? Як вони розвинуть знання про ваше середовище та стануть розширенням вашої команди? Які минулі результати вони досягли для клієнтів, наприклад, заощадили робочі години для команд операційного центру

безпеки або скоротили середній час відповіді? І як вони гарантують, що їхній штучний інтелект реалізований безпечно?

Поєднання штучного інтелекту та людського досвіду

ШІ сам по собі не є ідеальним засобом для забезпечення керованої безпеки. Щоб бути ефективним, точним і відповідним, його потрібно поєднувати з досвідом людини. Я часто чую від клієнтів, які мають обґрунтовані занепокоєння щодо помилок ШІ. Їх головне запитання: якщо ви робите все автоматично за допомогою ШІ, що робити, якщо ШІ помиляється?

Цілеспрямоване постійне тримання реальної людини в курсі подій дозволяє експертам-людям перевіряти факти рішень, керованих штучним інтелектом, і точно налаштовувати моделі штучного інтелекту, щоб вони не робили ту саму помилку двічі. Ця співпраця гарантує, що ШІ є цінним інструментом для захисників, а не заміною людського судження.

ШІ готовий зробити революцію в кібербезпеці. Включення штучного інтелекту в стратегію кібербезпеки організації — це не просто варіант, а ключ до побудови міцної позиції кібербезпеки». ***(Geoff Haydon. Leveraging The True Potential Of AI In Cybersecurity // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/12/08/leveraging-the-true-potential-of-ai-in-cybersecurity/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA&sh=2d9c1a9d4597). 08.12.2023).***

***

«Широке поширення Інтернету речей (IoT) і хмарних обчислень стало очевидним у цьому світі технологій, що постійно розвивається. Кожен використовує потенціал цих трансформаційних технологій для покращення повсякденної діяльності.

Давайте поглянемо на переваги та труднощі, пов’язані з широким впровадженням Інтернету речей і хмарних обчислень, розкриваючи уявлення про динаміку сучасного цифрового зв’язку.

Розквіт IoT

IoT змінив спосіб взаємодії світу. Він плавно інтегрувався майже в усі аспекти нашого повсякденного життя, від розумних будинків і переносних пристроїв до автономних транспортних засобів і промислових датчиків. Однак це також проклало шлях для кіберзагроз. З’явилося більше можливостей для загроз через кількість взаємопов’язаних пристроїв, що робить традиційні заходи некомпетентними.

Кібербезпека почала зосереджуватися на шифруванні даних, безпеці на рівні пристрою та надійних механізмах автентифікації для вирішення проблем безпеки. Зараз виробники підкреслюють, що безпека включена в план пристроїв IoT з самого початку. Це включає виконання безпечних процесів завантаження, регулярне оновлення мікропрограми, а також покращення відстеження та підзвітності за допомогою унікальних пристроїв.

Універсальність хмарних обчислень

З появою хмарних обчислень бізнес-операції змінилися з традиційної локальної інфраструктури на масштабовані та гнучкі хмарні рішення. За даними Statista, у 2022 році світовий ринок публічних хмарних обчислень становив 478 мільярдів доларів, а у 2024 році він досягне 679 мільярдів доларів. Це колосальний приріст на 201 мільярд доларів за 2 роки.

Хоча хмарні обчислення приносять очевидні переваги, такі як доступність і економія коштів, вони також мають проблеми з кібербезпекою. Хмарні сервіси централізовані за своєю природою; це означає, що порушення може виявити величезну кількість конфіденційних даних. Щоб протистояти цим загрозам, передові заходи кібербезпеки зосереджені на шифруванні даних, багатофакторній автентифікації та надійному контролі доступу.

Зараз постачальники хмарних послуг інвестують значні кошти в передові засоби безпеки, такі як моніторинг у реальному часі, розвідка про загрози та

автоматизовані системи реагування на інциденти. Модель спільної відповідальності наголошує на співпраці між хмарними провайдерами та їхніми клієнтами, що стало основою кібербезпеки для забезпечення комплексної безпеки.

Злиття IoT і хмарних обчислень

Злиття IoT і Cloud Computing створило взаємні відносини, які збільшують як ризики, так і переваги. Хмара забезпечує необхідну інфраструктуру для зберігання, обробки та аналізу величезної кількості даних, створених пристроями IoT. Незважаючи на це, це з'єднання також створює складний ландшафт безпеки.

Зрештою, кібербезпека спрямована на створення узгодженого та безпечного потоку даних, тому вона еволюціонувала, щоб забезпечити наскрізний захист, який включає захист каналів зв'язку між пристроями та хмарою.

На користь екосистеми Інтернету речей і хмарних обчислень рішення з кібербезпеки застосовують покращене керування ідентифікацією та доступом і використовують штучний інтелект для виявлення аномалій і прогнозування аналізу загроз.

Виклики в мінливому ландшафті

Незважаючи на розвиток кібербезпеки, існують труднощі в мінливому ландшафті IoT і хмарних обчислень.

Кожне з різних пристроїв IoT має власні специфікації та протоколи безпеки, що є серйозною проблемою. У практиці безпеки в галузі стандартизація життєво важлива для забезпечення єдиної та надійної системи безпеки.

Постійно мінливий характер кіберзагроз є ще одним викликом. Зі зміною технологій змінюються і методи, які використовують кіберзлочинці; вони продовжують знаходити нові способи порушити безпеку. Cybersecurity Ventures заявляє, що глобальні витрати на кіберзлочинність зростатимуть на 15 відсотків щорічно протягом наступних п'яти років, з 3 трильйонів доларів у 2015 році до 10,5 трильйонів доларів у порівнянні з минулим роком до 2025 року.

Заходи кібербезпеки потребують постійного моніторингу, регулярних оновлень і спільних зусиль експертів з кібербезпеки, виробників пристроїв і

постачальників мережевої безпеки, щоб залишатися динамічними та універсальними перед зростаючими загрозами.

Людський фактор

Людський фактор є важливою складовою кібербезпеки. Хоча основна увага приділяється технологічним рішенням, користувачі також повинні знати про ризики та найкращі методи підтримки безпечного цифрового середовища.

Атаки програм-вимагачів, внутрішні загрози та фішингові атаки викликають серйозне занепокоєння. Статистика фішингових електронних листів показує, що 1,2 відсотка всіх надісланих електронних листів є шкідливими, що означає 3,4 мільярда фішингових електронних листів щодня.

Освітні та просвітницькі програми дуже важливі. Людей слід навчити розпізнавати ці загрози та повідомляти про них, відвідувати форуми та заходи з кібербезпеки, а також бути в курсі безпечних онлайн-практик, зокрема використання надійних паролів або менеджерів паролів.

Крім того, організації повинні проводити регулярні тренінги та дотримуватися суворої політики кібербезпеки, щоб інформувати співробітників про останні кіберзагрози та запобіжні заходи. За даними Cybersecurity Ventures, у 2023 році глобальні витрати на навчання співробітників з питань безпеки зросли з приблизно 5,6 мільярда доларів США та, за прогнозами, перевищать 10 мільярдів доларів США до 2027 року – це цілих 15 відсотків щорічного збільшення.

Майбутнє кібербезпеки

Оскільки світ щодня покладається на цифрові мережі, існує потреба зміцнювати та вдосконалювати кібербезпеку. У звіті Marsh US Cyber Purchasing Trends зазначено, що протягом першого кварталу 2023 року ціни на страхування кібербезпеки в США зросли на 11 відсотків порівняно з 28 відсотками у 2022 році, і вартість все ще зростає.

Майбутнє кібербезпеки буде сформовано такими технологіями, як штучний інтелект (ШІ), який відіграє важливу роль у виявленні загроз і їх рішеннях, квантові обчислення, які можуть створити нові проблеми та рішення для дешифрування, а також мережі 5G.

Хоча поширення мереж 5G призведе до швидшої швидкості та підключення, це також може поступитися місцем кіберзагрозам. Таким чином, щоб випередити атаки, необхідно створити правильну основу мереж 5G для життєво важливих систем і послуг.

Висновок

Еволюція кібербезпеки — це безперервний процес і вона постійно змінюється. З появою та злиттям таких технологій, як IoT і Cloud Computing, ризики кіберзагроз зросли, а кіберзлочинці щодня знаходять нові способи порушувати безпеку.

Управління цими проблемами вимагає командної роботи та розгорнутої стратегії безпеки. Ця стратегія має бути спрямована на покращення зв'язку цифрової екосистеми та забезпечення безпеки цифрового майбутнього. Це також має включати освіту, регулярний моніторинг, поєднання всіх новітніх технологій і створення обізнаності про кібербезпеку». ***(Faith Adeyinka. The Evolution of Cybersecurity in the Age of IoT and Cloud Computing // ReadWrite, INC (https://readwrite.com/the-evolution-of-cybersecurity-in-the-age-of-iot-and-cloud-computing/?utm_source=flipboard&utm_content=ReadWrite%2Fmagazine%2FAll+Stories). 08.12.2023).***

***

«Новий звіт, опублікований сьогодні компанією з кібербезпеки Abnormal Security Corp., попереджає про зростання кількості атак на електронну пошту, згенерованих штучним інтелектом, і зростання загрози з боку кіберзлочинців, які продовжують використовувати штучний інтелект у своєму щоденному використанні.

Згідно зі звітом, доступність генеративних технологій штучного інтелекту, таких як ChatGPT, призвела до їх неправильного використання для створення передових кіберзагроз. Інструменти штучного інтелекту дозволяють зловмисникам швидко створювати унікальний і складний контент, що ускладнює виявлення цих загроз традиційним програмним забезпеченням безпеки.

Зловмисники почали використовувати генеративний ШІ для покращення тактики соціальної інженерії. Приклади включають використання інтерфейсу програмування додатків ChatGPT для реалістичних фішингових електронних листів і створення шкідливих платформ штучного інтелекту, таких як WormGPT і FraudGPT, які не мають етичних огорож.

У звіті обговорюється кілька випадків атак, створених штучним інтелектом, виявлених Abnormal, таких як спроби доставки зловмисного програмного забезпечення під виглядом страхових компаній, видавання себе за облікові дані Netflix для фішингу та шахрайство з рахунками-фактурами шляхом видавання себе за бренд косметики. Атаки використовують складну мову та не мають звичайних ознак фішингу, таких як граматичні помилки, що робить їх більш переконливими для потенційних жертв.

Майк Бріттон, головний спеціаліст з інформаційної безпеки, Майк Бріттон, зазначає, що традиційні рішення безпеки електронної пошти важко ідентифікують ці атаки, згенеровані штучним інтелектом, оскільки вони текстові, походять від легальних служб електронної пошти та значною мірою покладаються на соціальну інженерію. Відсутність загальних ознак, таких як друкарські чи граматичні помилки, ускладнює людям розпізнати їх як атаки.

Шкідливі електронні листи «раніше потрапляють у скриньку вхідних повідомлень співробітників, де вони змушені приймати рішення про те, чи варто їх залучати, а завдяки штучному інтелекту, який повністю усуває граматичні помилки та описки, які історично були ознаками атаки, люди мають набагато більше шансів стати жертвами, ніж будь-коли», - зазначає Бріттон.

У звіті стверджується, що для боротьби з цими загрозами компаніям необхідно впроваджувати засоби кібербезпеки на базі ШІ, рішення, які виходять за рамки традиційних методів. Це включає розуміння особистості та поведінки людей в організації, контекстне спілкування та вміст електронних листів, що забезпечує більш ефективний захист від атак, створених ШІ. «Для керівників служби безпеки це тривожний дзвінок для того, щоб визначити пріоритетність заходів кібербезпеки для захисту від цих загроз, поки не пізно», — додає Бріттон». ***(Duncan Riley. New***

report warns of a rise in AI-generated email fraud and phishing attacks // SiliconANGLE Media Inc. (https://siliconangle.com/2023/12/19/new-report-warns-rise-ai-generated-email-fraud-phishing-attacks/?utm_source=flipboard&utm_content=SiliconANGLE%2Fmagazine%2FSiliconANGLE). 19.12.2023).

***

«Хакерська група під назвою Anonymous Sudan бере на себе відповідальність за деякі збої в ChatGPT, які сталися в останні місяці.

Згідно з його веб-сайтом, бот не працював приблизно на 40 хвилин у середу, що стало другим серйозним збоєм після того, як він не працював більше ніж на 90 хвилин 8 листопада. ChatGPT також мав інші проблеми, включаючи періодичні збої та підвищений рівень помилок протягом цього часу.

OpenAI не вказав причину нещодавнього великого збою, але Anonymous Sudan взяв на себе заслугу, заявивши на своєму каналі на платформі обміну повідомленнями Telegram у середу, що він «продовжуватиме націлюватися на ChatGPT, доки прихильник геноциду, Тал Брода не буде звільнений і ChatGPT не припинить дегуманізувати погляди палестинців».

Тел Брода, керівник дослідницької платформи OpenAI, не відповів на запит Business Insider про коментарі.

Але група каже, що її кібератаки на OpenAI виходять за рамки її сприйняття особистих поглядів Броди.

У дописі Telegram, в якому взяли на себе відповідальність за збій ChatGPT 8 листопада, Anonymous Sudan заявив, що націлився на OpenAI і ChatGPT через співпрацю компанії з тим, що вони назвали «державою окупації» Ізраїлю, і відносини генерального директора Сема Альтмана з країною. Anonymous Sudan також заявив, що ChatGPT упереджено ставиться до палестинців та Ізраїлю, і що Ізраїль може використовувати ШІ для розробки зброї, яка може «ще більше пригнічувати» палестинців.

OpenAI не відповів на запит щодо коментарів щодо останньої атаки, але раніше CNBC посилався на думку компанії, що збій 8 листопада був спричинений цілеспрямованою атакою. Anonymous Sudan покладається на технологію розподіленої відмови в обслуговуванні, яка переповнює цільову службу синтетично згенерованим трафіком. Репортер Axios Сем Сабін написав, що група «навряд чи порушує внутрішні мережі OpenAI».

Американські компанії: можливо, варто перевірити Telegram

Незважаючи на те, що Anonymous Sudan запустила хвилю атак по всьому світу в останні місяці, незрозуміло, чи є її мотивація боротися з ісламофобією, націлюватися на те, що вона вважає проізраїльськими організаціями, чи щось зовсім інше.

Угруповання взяло на себе відповідальність за серію атак у Європі, які, очевидно, були «відплатою за сприйману антиісламську діяльність», повідомляє сайт новин про кібербезпеку Dark Reading.

Але деякі експерти з кібербезпеки стверджують, що група спеціально зосереджена на Судані, де 90% населення країни вважають себе мусульманами, згідно зі звітом Державного департаменту США щодо Судану.

«З моменту створення свого офіційного каналу Telegram 18 січня 2023 року Anonymous Sudan регулярно публікують свої наміри атакувати тих, хто націлений на Судан», — сказав Аарон Хемблтон, директор Близького Сходу та Африки компанії кібербезпеки SecurityHQ, у дописі на веб-сайті компанії.

Однак існує третя можливість, яка полягає в тому, що Anonymous Sudan пов’язана з проросійською хакерською групою під назвою Killnet, яка відома своїми DDoS-атаками. За даними Axios, це одна з кількох хакерських груп, спрямованих на ізраїльські організації під час війни країни в Газі. Killnet також погрожував перевантажити систему онлайн-голосування Євробачення, надсилаючи їй мільярди запитів під час конкурсу 2022 року.

Вирішальним моментом для американських компаній є те, що група, у своїй публікації в Telegram, яка бере на себе відповідальність за нещодавній збій в OpenAI, заявила, що буде спрямована на «будь-яку американську компанію».

Anonymous Sudan також приписав Telegram відповідальність за атаку на відеогру «Rocket League» американської компанії Epic Games наступного дня після збою OpenAI. BBC повідомило, що група також знищила X приблизно на дві години в серпні, зазначивши тоді в Telegram: «Зробіть так, щоб наше повідомлення дійшло до Ілона Маска: «Відкрийте Starlink в Судані». ***(Lakshmi Varanasi. Hackers behind recent ChatGPT outage say they'll target the AI bot until it stops 'dehumanizing' Palestinians // Insider Inc. (https://www.businessinsider.com/hackers-behind-chatgpt-outage-bot-must-stop-dehumanizing-palestinians-2023-12?utm_source=flipboard&utm_content=user%2FBusinessInsider). 16.12.2023).***

***

«Відповідно до нещодавнього звіту MarketsandMarkets™, світовий ринок штучного інтелекту в сфері кібербезпеки готовий до експоненційного зростання з прогнозованим зростанням з 22,4 мільярдів доларів США у 2023 році до вражаючих 60,6 мільярдів доларів США до 2028 року.

Прогноз вказує на надійний зведений річний темп зростання (CAGR) на рівні 21,9% протягом зазначеного періоду, що підкреслює зростаюче значення технологій штучного інтелекту в зміцненні заходів кібербезпеки.

Ключові моменти:

Поведінкова аналітика та виявлення загроз: майбутнє штучного інтелекту в кібербезпеці полягає в поведінковій аналітиці та складному виявленні загроз. Алгоритми машинного навчання (ML), особливо в поведінковій біометрії, стають вирішальними для проактивного захисту від загроз. Динамічний характер кіберзагроз вимагає передових рішень ШІ для ефективного захисту.

Ринкові чинники та тенденції: сплеск кібератак на технологічні компанії, оборонні та державні установи підштовхнув попит на рішення ШІ. У звіті підкреслюється життєво важлива роль штучного інтелекту, зокрема в обробці природної мови (NLP) і ML, у підвищенні кібербезпеки. Банківський сектор, який стикається зі зростаючими проблемами конфіденційності, підкреслює важливість кібербезпеки на основі ШІ.

Фактори зростання ринку. Очікується, що ринок штучного інтелекту на ринку кібербезпеки буде розширюватися завдяки підвищенню попиту з боку малих і середніх підприємств (МСП). Впровадження рішень кібербезпеки на основі штучного інтелекту додатково стимулюється зростанням використання підключених пристроїв, тенденцією Bring Your Own Device (BYOD) і глобальним зростанням використання Інтернету.

Домінування в сегменті програмного забезпечення: очікується, що сегмент програмного забезпечення займатиме найбільшу частку ринку протягом прогнозованого періоду. Суворіші правила та правила щодо конфіденційності даних сприяють зростанню попиту на рішення кібербезпеки на основі штучного інтелекту, що борються з проблемами, пов'язаними з розвитком кіберзагроз.

Керовані послуги на підйомі: очікується, що керовані послуги демонструватимуть найвищий CAGR протягом прогнозованого періоду. Алгоритми ШІ в керованих службах покращують виявлення загроз у реальному часі, автоматизують реагування на інциденти та оптимізують розподіл ресурсів за допомогою автоматизації ШІ.

Провідне зростання в Азіатсько-Тихоокеанському регіоні: за оцінками, в Азіатсько-Тихоокеанському регіоні буде найвищий CAGR протягом прогнозованого періоду. Такі фактори, як зростання чисельності населення, урядова політика та впровадження нових технологій, таких як машинне навчання, IoT та аналітика великих даних, сприяють зростанню кібербезпеки ШІ в регіоні.

Відомі співпраці та розробки:

NVIDIA та Oracle об'єднали зусилля, щоб перенести прискорені обчислення та ШІ в хмарну інфраструктуру Oracle (OCI), пропонуючи клієнтам розширені рішення для бізнес-завдань.

Компанія Samsung Electronics Co., Ltd випустила LPDDR5X DRAM з високою швидкістю обробки, що обслуговує різноманітні програми, включаючи смартфони, ПК, високопродуктивні обчислювальні системи, сервери та автомобілі.

Check Point Software Technologies Ltd співпрацювала з Intel, щоб легко інтегрувати засоби кібербезпеки в пристрої IoT, підвищуючи безпеку без впливу на продуктивність продукту.

Оскільки глобальний ландшафт стикається зі змінними та складними кіберзагрозами, ШІ на ринку кібербезпеки відіграє ключову роль у зміцненні оборонної інфраструктури. Прогнозований ріст підкреслює зростаючу залежність від рішень на основі штучного інтелекту для вирішення динаміки кібервійни, яка постійно змінюється». ***(AI Cybersecurity Market Surges: Expected to Reach $60.6 Billion by 2028 // BOL News (https://www.bolnews.com/technology/2023/12/ai-cybersecurity-market-surges-expected-to-reach-60-6-billion-by-%202028/). 21.12.2023).***

***

Кіберзлочинність та кібертероризм

«Ландшафт кібербезпеки знаходиться на порозі суттєвої трансформації, спричиненої швидким прогресом генеративного ШІ (GenAI) і великих мовних моделей (LLM). Компанія Trend Micro Incorporated, лідер у сфері глобальних рішень для кібербезпеки, випустила суворе попередження про потенційний вплив цих технологій на природу та складність кіберзагроз.

Удосконалена тактика фішингу та соціальної інженерії

Однією з найбільш тривожних тенденцій є еволюція тактики фішингу. Ерік Скіннер, віце-президент із ринкової стратегії Trend Micro, зазначає, що вдосконалені магістри права, які володіють різними мовами, готові усунути поширені ознаки фішингу, такі як граматичні помилки чи незвичне форматування. Ця розробка значно ускладнює виявлення, вимагаючи від компаній виходити за межі традиційного навчання фішингу та застосовувати сучасні засоби безпеки. Очікується, що ці передові системи перевищать людські можливості у виявленні та нейтралізації таких загроз.

Руйнівна роль GenAI і GAN

Звіт також проливає світло на взаємодію між GenAI і Generative Adversarial Networks (GANs), передбачаючи значні зміни на ринку фішингу до 2024 року. За прогнозами, ця комбінація сприятиме економічно ефективному створенню гіперреалістичного аудіо- та відеовмісту, до складних сценаріїв компрометації бізнес-електронної пошти (BEC), віртуального викрадення та інших складних шахрайств. Легка доступність і підвищена якість цих технологій можуть значно збільшити арсенал кіберзлочинців.

Вразливість моделей ШІ та хмарної безпеки

Інша критична сфера, яка викликає занепокоєння, — це вразливість самих моделей ШІ. Спеціалізовані хмарні моделі машинного навчання, особливо ті, що навчаються на цілеспрямованих наборах даних, стають все більш привабливими цілями для загроз. Ці моделі вразливі до атак з отруєнням даних, які можуть варіюватися від викрадання конфіденційних даних до порушення зв’язаних систем, зокрема транспортних засобів. Доступність цих атак, деякі з яких коштують менше 100 доларів США, посилює терміновість усунення цих вразливостей.

Крім того, гострою проблемою є зростання кількості атак хмарних черв’яків, націлених на вразливості та неправильні конфігурації. Автоматизація, задіяна в цих атаках, робить їх особливо небезпечними, оскільки вони можуть швидко вразити кілька контейнерів, облікових записів і служб. Це підкреслює необхідність надійних механізмів захисту та ретельних перевірок безпеки в хмарних середовищах.

Регуляторні наслідки та реакція промисловості

Ландшафт загроз, що розвивається, може спонукати до більш рішучої відповіді регуляторних органів, причому сектор кібербезпеки потенційно стане лідером у розробці політики та правил щодо ШІ. За словами Грега Янга, віце-президента з кібербезпеки Trend Micro, галузь, ймовірно, випереджатиме зусилля уряду, рухаючись до саморегулювання на основі вибору.

Статті, надані Trend Micro, є важливим тривожним сигналом для спільноти кібербезпеки. Оскільки технології GenAI і LLM продовжують розвиватися, вони

приносять із собою нові виклики, які вимагають проактивних та інноваційних рішень. Потреба в передових заходах безпеки в поєднанні з розумінням еволюції природи кіберзагроз ніколи не була такою критичною. З наближенням 2024 року випередження цих подій і підготовка до їх наслідків стануть ключовими для захисту від складних кіберзагроз майбутнього». ***(Brenda Kanana. The Rising Tide of GenAI in Cybersecurity: Trends and Threats in 2024 // Cryptopolitan (https://www.cryptopolitan.com/the-rising-tide-of-genai-in-cybersecurity/?utm_source=flipboard&utm_content=Cryptopolitan%2Fmagazine%2FLatest+Crypto+and+Blockchain+News). 06.12.2023).***

***

«Округ Даллас став жертвою кіберзлочинності, яка коштувала платникам податків округу 2,4 мільйона доларів.

У вівторок за зачиненими дверима комісії округу Даллас були проінформовані про потенційний шахрайський платіж, який було здійснено після того, як службовець округу отримав фальшиве повідомлення електронної пошти, яке видавало себе за одного з партнерів округу.

Команда CBS News Texas I-Team дізналася, що електронний лист схоже на те, що він надійшов від одного з постачальників округу з проханням оплатити. Насправді це був фішинговий електронний лист, який зрештою переконав службовця округу переказати понад 2 мільйони доларів.

Згідно із заявою адміністратора округу Даллас Дарріла Мартіна, округу стало відомо про інцидент 17 листопада та передало всі докази ФБР.

Закон штату вимагає від усіх державних службовців проходити навчання з питань кібербезпеки. У цьому тренінгу описано, як виявляти фішингові електронні листи.

«Їх навчають, що (кіберзлочинці) можуть змінювати ім’я у своїй електронній адресі та на що їм слід звернути увагу», — сказав експерт із кібербезпеки Бен Сінглтон. Компанія Сінглтона Net Genius в Арлінгтоні є державним сертифікованим провайдером навчання з кібербезпеки.

«Я не думаю, що одержувач цього електронного листа в Далласі не пройшов такого навчання. Вони б знали, на що звернути увагу», — сказав Сінглтон.

Команда I-Team запитала в чиновників округу, чи ті, хто отримав шахрайську електронну пошту, пройшли навчання, передбачене штатом. Станом на вечір вівторка округ не відповів на запитання.

У жовтні хакери отримали доступ до мережі округу Даллас і викрали дані. Організація кіберзлочинців Play погрожувала опублікувати дані в темній мережі.

Округ Даллас каже, що цей останній інцидент не пов'язаний з жовтневою кібератакою». ***(Dallas County scammed out of $2.4M by cyber criminals // CBS Broadcasting Inc. (https://www.cbsnews.com/texas/news/dallas-county-scammed-out-of-2-4m-by-cyber-criminals/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 05.12.2023).***

***

«Поліція Південної Кореї розслідує, чи північнокорейська хакерська група, звинувачена в крадіжці даних з 14 організацій, отримала інформацію про оборонні технології, включаючи зенітний лазер, повідомив у середу представник міської поліції Сеула.

Розслідування, яке проводиться спільно з Федеральним бюро розслідувань США (ФБР), намагається визначити обсяг даних, отриманих групою, відомою як Андаріель, Чон Джін Хо, який очолює групу в Сеулі. Управління столичної поліції розслідує справу, повідомили Reuters.

У 2019 році Міністерство фінансів США включило Andariel до списку хакерських груп, спонсорованих державою Північної Кореї, зосереджених на проведенні зловмисних кібероперацій проти іноземних компаній, державних установ і оборонної промисловості.

Цього тижня місцеві ЗМІ повідомили, що кеш даних містить ключові секрети оборони Південної Кореї.

Згідно з попередньою заявою поліції, серед об’єктів нападу були південнокорейські оборонні фірми, дослідницькі інститути та фармацевтичні компанії. Хакери забрали близько 250 файлів або 1,2 терабайта інформації та даних.

Поліція повідомила, що до проксі-сервера, створеного групою, в районі столиці Північної Кореї Пхеньяні 83 рази зверталися з грудня по березень минулого року.

Сервер використовувався для доступу до веб-сайтів фірм і установ, причому група скористалася південнокорейською службою хостингу, яка орендує сервери невстановленим клієнтам.

Група також виманила біткоїни на 470 мільйонів вон (357 866 доларів США) у трьох південнокорейських та іноземних компаній під час атак програм-вимагачів, повідомила поліція.

Північнокорейських хакерів звинувачують у кібератаках, які принесли мільйони доларів, хоча раніше Пхеньян заперечував свою причетність до кіберзлочинів.

Поліція повідомила, що проти жінки-іноземки проводилося розслідування у зв’язку з атаками програм-вимагачів після того, як частина біткойнів була переведена через її банківський рахунок і знята в банку в Китаї. Вона заперечує будь-які правопорушення». ***(North Korea Hackers May Have Stolen Data on Laser Weapon –Police // U.S. News & World Report L.P. (https://www.usnews.com/news/world/articles/2023-12-06/north-korea-hackers-may-have-stolen-data-on-laser-weapon-police?utm_source=flipboard&utm_content=seanjkernan%2Fmagazine%2FUS+News). 06.12.2023).***

***

«Звіт Cisco Talos Year in Review, опублікований у вівторок, висвітлює нові тенденції в ландшафті загроз кібербезпеці. Ми зосередимося на трьох розглянутих темах: кіберзлочинна екосистема програм-вимагачів, атаки на

мережеву інфраструктуру та зловмисне програмне забезпечення для завантаження товарів.

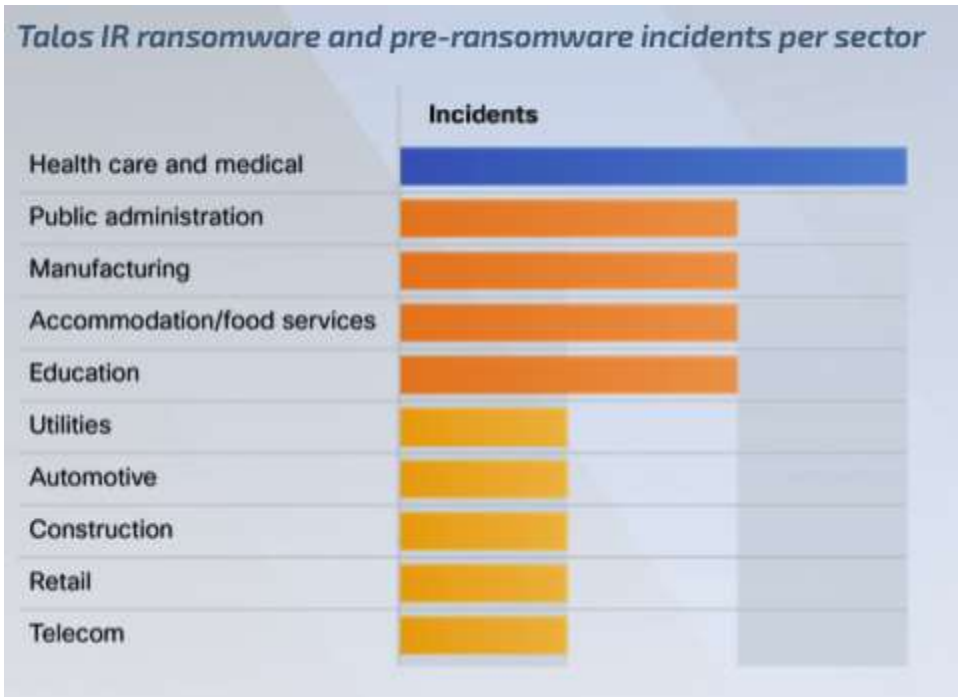
Більше учасників програм-вимагачів перейшли на вимагання, а не на шифрування, тоді як завантажувачі товарів стали більш прихованими та високоефективними, хоча у 2023 році відбулися нові серйозні покращення безпеки, наприклад Microsoft Office відключив макроси за замовчуванням. Мережеві пристрої все більше зазнають впливу кіберзлочинців і спонсорованих державою дійових осіб.

Екосистема кіберзлочинців програм-вимагачів змінилася

Найбільш націлена галузь

З точки зору програм-вимагачів, за спостереженнями Cisco Talos у 2023 році, найбільш цільовою галуззю є охорона здоров'я та сектор громадського здоров'я, що не дивно, оскільки організації в цьому секторі часто страждають від недофінансування бюджетів на кібербезпеку та низької толерантності до простоїв (мал. А). Крім того, ці організації є цікавими цілями, оскільки вони володіють захищеною інформацією про здоров'я.

Малюнок А



Інциденти з програмами-вимагачами/програмами-вимагачами, які передували програмному забезпеченню-вимагачу, на сектор, за спостереженнями Cisco Talos.

Деякі групи програм-вимагачів змінилися

Найактивнішою групою програм-вимагачів другий рік поспіль стала LockBit (25,3% від загальної кількості публікацій на сайтах витоку даних), за нею йдуть ALPHV (10,7%) і Clop (8,2%).

Однак у 2023 році деякі групи програм-вимагачів продовжували змінюватися; ці структури часто об'єднували або ребрендингували, намагаючись заплутати правоохоронні органи та дослідників, які їх відстежують. Кіберзлочинці, активні в цій галузі, часто працюють одночасно на кілька служб-вимагачів як послуг.

Численні витоки вихідного коду програм-вимагачів і конструкторів також вплинули на ландшафт загроз програм-вимагачів, оскільки вони дозволили більшій кількості людей (навіть тих, хто має невеликі технічні знання) почати власні операції.

Zero-days експлуатуються з безпрецедентною швидкістю

Високотехнічні гравці використовують уразливості нульового дня з безпрецедентною швидкістю. Група програм-вимагачів Clop, зокрема, змогла використати численні вразливості нульового дня, зокрема вразливості в платформі GoAnywhere MFT, MOVEit і PaperCut.

Cisco Talos заявляє, що «неодноразові спроби Клопа використати вразливості нульового дня є дуже незвичайними для групи програм-вимагачів, враховуючи ресурси, необхідні для розробки таких можливостей», але все ще не впевнені, що вони розробляють експлойти самостійно. Відповідаючи на питання про це в електронному інтерв'ю, представник Cisco сказав TechRepublic: «Через туманність у відносинах, які складають екосистему програм-вимагачів, може бути важко точно розібрати, який персонал/організації відповідають за які дії. Через це ми не маємо прямого уявлення про те, як Cl0p отримав 0days, і не помітили жодних ознак того, що вони їх придбали. Незалежно від того, розробили вони їх самостійно чи придбали, використання свідчить про те, що Cl0p має достатньо ресурсів, або інженерних талантів, або фінансів і зв'язків, які дозволять їм отримати від третьої сторони».

Більше афілійованих компаній використовують модель вимагання крадіжки даних

Ще одна визначна зміна в ландшафті загроз програм-вимагачів полягає в тому, що більше філій тепер переходять на модель вимагання крадіжки даних, а не на звичайну модель шифрування. У цих атаках кіберзлочинці не розгортають програми-вимагачі; замість цього вони викрадають конфіденційну інформацію організацій, перш ніж попросити викуп.

Покращення можливостей виявлення програм-вимагачів за допомогою програмного забезпечення Endpoint Detection and Response і Extended Detection and Response може бути однією з причин для зміни тактики та припинення розгортання програм-вимагачів у цільових системах. Cisco Talos також підозрює, що агресивні дії американських і міжнародних правоохоронних органів проти учасників програм-вимагачів можуть бути ще однією причиною цієї зміни.

Зросла кількість атак на мережеву інфраструктуру

Cisco Talos помітила збільшення атак на мережеві пристрої у 2023 році, зокрема атак, які здійснюються групами, що базуються в Китаї та Росії, які прагнуть досягти шпигунських цілей і сприяють прихованим операціям проти вторинних цілей. Дослідники спостерігали за такою активністю з боку інших кіберзлочинців, включаючи брокерів початкового доступу та учасників програм-вимагачів.

Слабкий захист мережевих пристроїв

Незважаючи на те, що мережеві пристрої є ключовими компонентами IT-інфраструктури будь-якої організації, вони нечасто перевіряються з точки зору безпеки та часто погано виправлені, що робить їх цікавою мішенню для кіберзлочинців. Проте ці пристрої часто працюють на нестандартних операційних системах, що ускладнює їх використання кіберзлочинцями, але також не контролюється стандартними рішеннями безпеки.

Типовий компрометація таких пристроїв починається з того, що зловмисники використовують невиправлені вразливості, слабкі або стандартні облікові дані або незахищену конфігурацію пристрою.

Представник Cisco сказав TechRepublic, що «постійне переважання облікових даних за замовчуванням частково можна пояснити великою кількістю постачальників і продуктів у поєднанні з відсутністю єдиних стандартів/найкращих практик. Відмова від облікових даних за замовчуванням, безсумнівно, допоможе покращити ситуацію. Важливо зазначити, що слабкі облікові дані також можуть бути використані, якщо актор може застосувати грубу силу або пароль, і що брокери доступу все одно досягають успіху в отриманні облікових даних і продажу їх у темній мережі. Це означає, що навіть якщо організації не використовують облікові дані за замовчуванням, важливо, щоб вони створювали унікальні та складні паролі, використовували MFA, де це можливо, і також наголошували на додаткових заходах безпеки, таких як сегментація та планування ІК».

Цільові пристрої мали високу оцінку серйозності

За даними Cisco Talos, усі вразливості, які впливали на мережеві пристрої у 2023 році, мали високий рівень серйозності, тобто ці пристрої можна було легко використати та потенційно могли завдати значного впливу на роботу.

Після зламу ці пристрої дозволяють зловмисникам захоплювати конфіденційну мережеву інформацію, полегшуючи подальший доступ до цільових мереж. Зловмисники також можуть встановити зловмисне програмне забезпечення на пристрої, щоб створити початкову точку опори в цільовій інфраструктурі без необхідності будь-якої автентифікації або перенаправити мережевий трафік на сервери, контрольовані актором. Нарешті, пристрої також часто використовуються зловмисниками як проксі-сервери анонімізації для проведення атак на інші цілі.

Зловмисне програмне забезпечення завантажувача товарів розвивалося

Зловмисне програмне забезпечення для завантаження товарів, таке як Qakbot, Ursnif, Emotet, Trickbot і IcedID, існує вже багато років. Спочатку вони були банківськими троянами, які шукали крадіжку даних кредитної картки на заражених комп’ютерах.

Наприкінці 2023 року з’явилися нові варіанти IcedID і Ursnif із разючою відмінністю від їхніх старих версій: їх можливості банківського трояна було видалено, а функції дроппера було покращено. Нові зразки IcedID використовували

брокери початкового доступу, відомі тим, що зазвичай продають доступ до мережі групам програм-вимагачів. Останні варіанти Ursnif використовували Королівська група програм-вимагачів.

Qakbot також розвивався, розгортаючи нові функції, які ідеально підходять для допомоги групам програм-вимагачів.

Ця еволюція від банківського трояна до завантажувача є привабливою для кіберзлочинців, які хочуть бути більш непомітними; видалення функції банківського трояна робить шкідливе програмне забезпечення менш помітним.

Вектор зараження для Qakbot, IcedID і Ursnif розвивався, оскільки нові заходи безпеки Microsoft для продуктів Office вплинули на ландшафт загроз зловмисного програмного забезпечення, змушуючи кіберзлочинців знаходити нові способи використовувати макроси непоміченими або повністю уникати їх використання (мал. В).

Малюнок В

Зміни в тактиці, методах і процедурах завантажувача товарів у відповідь на зміни функцій безпеки.

Порівняно з попередніми роками, зловмисники використовували інші методи для розповсюдження свого шкідливого програмного забезпечення та зараження пристроїв, як-от використання JavaScript, PowerShell, документів OneNote або файлів HTA. Вони також використовували платформу Google Ads для розгортання шкідливих програм, таких як Ursnif, IcedID або Trickbot, повністю уникаючи макросів.

Деякі інші суб’єкти загрози, які розгортають Emotet, IcedID і Ursnif, спостерігали за використанням старіших методів із макросами, ймовірно, через те,

що рівень успіху в невиправлених застарілих корпоративних системах все ще високий.

Як захистити свій бізнес від цих загроз кібербезпеці

Ландшафт загроз розвивається відповідно до потреб кіберзлочинців, і ваша команда безпеки має переконатися, що її стратегії пом'якшення відповідають тенденціям. Ось кілька порад щодо захисту вашого бізнесу від цих кіберзагроз. Крім того, усі операційні системи та програмне забезпечення мають бути оновленими та виправленими, щоб уникнути поширених вразливостей.

програми-вимагачі

Слід ретельно перевірити механізми контролю доступу в усіх корпоративних середовищах, а для зберігання конфіденційних даних слід застосовувати сегментацію даних, оскільки суб'єкти програм-вимагачів дедалі частіше намагаються викрасти конфіденційні дані, а не зашифрувати їх.

Мережеві пристрої

Мережеві пристрої мають бути оновлені та виправлені. Паролі за умовчанням, якщо такі є, потрібно змінити на надійні. Усі конфігураційні файли пристроїв слід ретельно проаналізувати та налаштувати, щоб уникнути зловмисного використання. Якщо можливо, на цих пристроях має бути розгорнуто багатофакторну автентифікацію. Крім того, слід відстежувати вхідні та вихідні зв'язки з пристроїв, щоб виявити зловмисний зв'язок.

Вантажники товарні

Основні сімейства товарних завантажувачів відмовилися від можливостей банківських троянів, щоб стати легшими та прихованими, навіть без використання макросів — часто для полегшення операцій програм-вимагачів. Організаціям слід навчити своїх співробітників обережно працювати з іншими типами файлів, як-от файли PDF або архіви ZIP, які можуть містити шкідливі файли». ***(Cedric Pernet. Cisco Talos Report: New Trends in Ransomware, Network Infrastructure Attacks, Commodity Loader Malware // TechnologyAdvice (https://www.techrepublic.com/article/cisco-talos-year-end-***

report/?utm_source=flipboard&utm_content=TechRepublic%2Fmagazine%2FLatest+News). 06.12.2023).

***

«Дослідники кібербезпеки з BlackBerry виявили нову кампанію кібершпигунства, спрямовану проти американських організацій аерокосмічної промисловості.

Метою кампанії, здається, є крадіжка даних і кібершпигунство, хоча кінцева гра учасників загрози залишається загадкою. Дослідники стверджують, що група, швидше за все, нова, тому вони назвали її AeroBlade.

Ця група влаштувала атаки в два етапи: перший був скоріше розвідувальним ходом, а другий – фактичне викрадення даних за допомогою зловмисного програмного забезпечення.

Продаж даних онлайн

Атака починається з фішингового електронного листа, який містить ретельно створений шкідливий файл DOCX. Цей файл, якщо його відкрити, завантажує файл DOTM із віддаленого розташування. Якщо ви не знайомі з розширенням DOTM, це шаблон документа для Microsoft Word. Потім цей файл може виконувати макрос, який створює зворотну оболонку на цільовій кінцевій точці. Ця оболонка підключиться до сервера C2 і чекатиме подальших інструкцій.

«Після того, як жертва відкриває файл і запускає його, вручну клацнувши сповіщення «Увімкнути вміст», документ [відредаговано].dotm дискретно завантажує новий файл у систему та відкриває його», — йдеться у звіті BlackBerry. «Щойно завантажений документ читається, що змушує жертву повірити, що файл, який спочатку отримав електронною поштою, є законним».

Перший крок, який, як було помічено, мав місце у вересні минулого року, перераховує всі каталоги на скомпрометованій кінцевій точці, надаючи зловмисникам карту королівства та таким чином спрощуючи пошук цінних даних. Другий етап, який відбувся в липні цього року, завершився крадіжкою даних.

Походження Aeroblade або кінцева гра залишаються загадкою. Хоча кампанії кібершпигунства можуть бути дуже руйнівними, це також може бути роботою цілком незалежного, орієнтованого на прибуток загрозливого суб'єкта, який пізніше спробує продати викрадені дані в темній мережі тому, хто запропонує найвищу ціну». ***(Sead Fadilpašić. US aerospace companies are facing dangerous new cyberattacks // Future US, Inc. (https://www.techradar.com/pro/security/us-aerospace-companies-are-facing-dangerous-new-cyberattacks?utm_source=flipboard&utm_content=other). 05.12.2023).***

***

«…Сплеск кібератак — це не просто швидкоплинне занепокоєння; це нокаутуючий удар по непідготовленим системам. Згідно зі звітом Hiscox Cyber Readiness Report, більше половини з 5000+ компаній, опитаних у 2023 році, вже відчули цей удар, зіткнувшись з одним або кількома кіберінцидентами цього року.

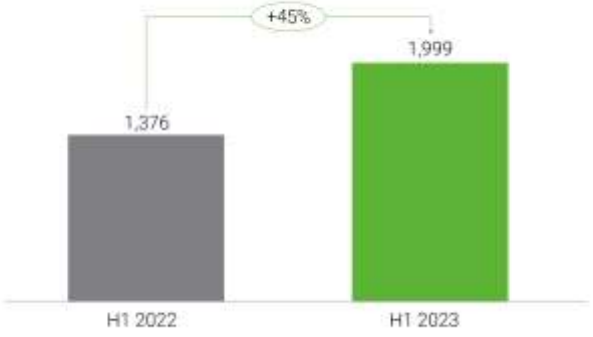
Такі резонансні зломи в таких критичних галузях, як аерокосмічна та оборонна промисловість, підкреслюють жахливу реальність: кіберзагрози розвиваються швидше, ніж багато хто може адаптуватися, що робить їх значним фінансовим і операційним ризиком для транснаціональних корпорацій. Це тенденція, яка вимагає термінової уваги та надійної стратегії захисту. Компанії зараз шукають способи посилити захист своєї кібербезпеки, щоб не просто передбачити удар, але й ефективно йому протистояти.

Як це відбувається

Атаки програм-вимагачів тепер є звичним явищем, і компанії повідомляють про зростання кількості інцидентів приблизно на 45% порівняно з роком. США є осередком таких атак. Ця ескалація відбувається, оскільки групи, які колись вважалися елементами-ізгоями, які прагнуть зробити політичну позицію чи просто спричинити хаос, переростають у професійні організації, залучаючи справжніх менеджерів облікових записів, щоб допомогти натхненникам керувати списком пропозицій програм-вимагачів, які можуть полегшити злочинну діяльність.

FIGURE 1: **RANSOMWARE-AS-A-SERVICE VICTIM COUNTS, H2 2022- H1 2023**

The numbers of active RaaS and extortion groups and victim organizations of successful ransomware attacks



Sources: RaaS and extortion groups' leak sites

FIGURE 2: **RANSOMWARE-AS-A-SERVICE COUNTS BY COUNTRY, H1 2023**

Sources: RaaS and extortion groups' leak sites and Trend's OSINT research

Ця тенденція не викликає сміху. Візьмемо випадок з Boeing: на початку жовтня американський аерокосмічний гігант став жертвою банди кіберзлочинців LockBit. Повідомляється, що хакери вкрали ~45 ГБ конфіденційних даних у Boeing, значна частина яких потрапила в мережу. Атака також на кілька тижнів призвела до блокування частини веб-сайту Boeing Global Services.

Скандинавська авіакомпанія (SAS) тим часом зазнала нещастя атаки бумерангом. Перший був у лютому, наступний – у травні. Так звані хактивісти запустили розподілену атаку на відмову в обслуговуванні (DDoS), паралізувавши веб-сайт SAS і розкривши деяку інформацію про клієнтів в Інтернеті.

В іншому нещодавньому інциденті мішенню став постачальник SpaceX Maximum Industries, у результаті чого частини схем двигуна Raptor V2 потрапили в Інтернет. SpaceX була кінцевою метою цієї атаки, оскільки зловмисники висунули свої вимоги щодо викупу безпосередньо до засновника SpaceX Ілона Маска.

Чому це має значення?

Boeing, SAS і SpaceX не знали про кіберзагрози. Кожна компанія важлива для національних інтересів, геополітичної стабільності та глобальної економіки. Проте, зрештою, кожен був уразливим, незалежно від планів, які вони мали.

Успішні кібератаки завдають шкоди корпоративній репутації, підривають довіру громадськості та заохочують злочинців до подальших нападів на відомі компанії. Ці інциденти мають реальні наслідки: компрометація конфіденційних даних, уможливлення фінансового шахрайства, порушення потоків доходів і – у випадку SpaceX – послаблення безпеки космічного ланцюжка створення вартості.

Як наслідок, зростає усвідомлення зростаючої залежності економіки та національної безпеки США від аерокосмічної, авіаційної та оборонної промисловості як критичної інфраструктури. Різні установи вживають заходів, наприклад:

Федеральне управління авіації (FAA) дотримується суворих стандартів кібербезпеки для оновлень системи.

Космічне командування США прагне співпрацювати з некомерційним Центром обміну та аналізу космічної інформації (Space ISAC), щоб стати більш активним проти загроз як приватним, так і державним організаціям.

Агентство з кібербезпеки та безпеки інфраструктури (CISA) окреслило 16 критично важливих компонентів інфраструктури, включаючи оборонно-промислову базу, державні об’єкти та інформаційні технології, для всіх яких характерна спільна ознака нападів такого типу. Зараз розглядається пропозиція назвати космічну галузь 17-м «сектором критичної інфраструктури».

Вжиття заходів

Комп’ютери, телефони та планшети – як особисті, так і робочі – пропонують численні точки доступу до систем компанії. Кожна з цих точок доступу, створена для максимального підвищення продуктивності співробітників, створює ще одну потенційну слабкість у кіберзахисті компанії.

Політика кібербезпеки організацій повинна розвиватися, оскільки атаки стають все більш витонченими та зухвалими. Це вимагає послідовного аналізу та

моніторингу подій у всьому світі в різних галузях промисловості та державних організаціях. Це також підвищує терміновість впровадження надійних багаторівневих стратегій захисту, від швидкого встановлення виправлень і аналізу платформ до примусового перезавантаження пристроїв для оновлення, а також постійного навчання користувачів шляхом регулярного навчання та спеціального тестування.

Кібербезпека залишатиметься проблемою для всіх компаній, оскільки вони змушені захищатися від поточних загроз, одночасно захищаючи своє майбутнє від небезпек, що швидко розвиваються. Чим гнучкішою є організація, тим краще вона буде підготовлена.

AlixPartners пропонує спеціалізовані рішення з кібербезпеки, адаптовані до аерокосмічної та оборонної промисловості, включаючи швидку діагностику, можливості QuickStrike®, оцінку ризиків безпеки продукту, галузеві перевірки нормативно-правових актів і відповідності, стратегію та дизайн безпеки та конфіденційності, комплексне тестування на проникнення та багато іншого для підвищення організаційної ефективності. стійкість до кіберзагроз.

В епоху, коли кіберзагрози є всюдисущими, посилення заходів кібербезпеки є не лише корпоративною відповідальністю. Це критично важливий аспект національної безпеки та цілісності промисловості. У AlixPartners ми прагнемо співпрацювати з організаціями в аерокосмічному та оборонному секторах, щоб зміцнити їхній захист, забезпечити безпеку їх операцій і зберегти довіру до їхніх організацій». ***(Eric Bernardini, David Wireman, Beth Musumeci, Megha Kalsi, Dean Weber and Lindsey Gyngell. Plan vs. reality: Strengthening defenses in the cyber arena // AlixPartners LLP (https://insights.alixpartners.com/post/102iu5k/plan-vs-reality-strengthening-defenses-in-the-cyber-arena). 01.12.2023).***

***

«Латинська Америка зараз є гарячою точкою кібератак. Експерти припускають, що в Латинській Америці відбувається 1600 кібератак на секунду, підкреслюючи, що кібератаки є однією з найшвидше зростаючих

проблем безпеки в регіоні. У Латинській Америці кібербезпека є питанням культури, політики та бізнесу. Латиноамериканські уряди, директори, політики — усі продовжують вирішувати проблеми кібербезпеки та конфіденційності в регіоні, але вони все ще відстають від Великобританії, ЄС та Сполучених Штатів. Багато країн регіону розробляють свої закони про захист даних, щоб привести їх у відповідність із GDPR. Однак у регіоні все ще бракує гармонізації стандартів, оскільки кожна країна регулюється по-різному. Регіон наполегливо працює над тим, щоб інформувати своїх громадян і організації про сучасні ситуації, забезпечуючи більшу кіберобізнаність. Створення стратегічної можливості для кібер (пере)страховиків надавати (пере)страхове покриття, щоб захистити організації від нових зобов'язань, з якими вони стикаються.

Зростання кіберзагроз

Збільшене використання нових технологій у регіоні має приховану ціну: кіберуразливість. Після пандемії Covid-19 стався сплеск кількості організацій та окремих людей, які перенесли своє життя в Інтернет, із збільшенням інновацій у таких сферах, як фінансові технології та електронна комерція в Латинській Америці. Однак багато нових технологій і систем, що впроваджуються, не відповідають необхідним інвестиціям у кібербезпеку. Через рівень початкових витрат більші корпоративні компанії встановлюють багатофакторну автентифікацію, але це рідко можна побачити на рівні SME/PYME. Статистика спроб кібератак показує, що для більшості малих і середніх підприємств/підприємств PYME компаніям бракує базових заходів безпеки на мобільних телефонах своїх співробітників, з чого починається багато кібератак. Для одних це проблема довіри до нових технологій, а для інших – недостатня обізнаність. Необхідно проводити більше навчання, оскільки зловмисники користуються недоліком знань користувачів, щоб отримати облікові дані, які потім використовуються для здійснення кібератак.

Які типи кібератак відбуваються і де? Коротше кажучи, все ті ж кібератаки, які спостерігаються в усьому світі. Хоча не всі атаки в Латинській Америці є виключно фінансовими. Латинська Америка пережила справедливу частку

соціальних заворушень, і це також відображається в її кібератаках. Останніми роками в регіоні зазнали нападів на багато урядових установ і органів, що послужило тривожним дзвінком для організацій по всій Латинській Америці:

Аргентина: у 2021 році дані про все населення Аргентини з'явилися на продаж у дарк-мережі після зламу Національного реєстру персон. Дані, які були оприлюднені, включали домашні адреси, номери соціального страхування, ідентифікаційні номери та офіційні посвідчення особи з фотографією. На той час населення Аргентини становило 45 мільйонів чоловік.

Бразилія: у 2020 році Вищий суд Бразилії зазнав атаки програм-вимагачів, коли його системи були офлайн понад два тижні, а потім його Міністерство охорони здоров'я у 2021 році, де дані мільйонів громадян про вакцинацію проти Covid-19 були видалені.

Колумбія: у Колумбії стався витік даних громадян Медельїна, коли її державна енергетична компанія стала мішенню групи BlackCat у 2022 році.

Мексика: у Мексиці хакери також витягли з її банківської системи близько 20 мільйонів доларів. У 2022 році група загрозливих осіб, яка називає себе Guacamaya (іспанське слово для ара), зламала міністерство оборони Мексики, яке містило інформацію про здоров'я президента.

Коста-Ріка: Коста-Ріка оголосила «надзвичайний стан» через серію атак програм-вимагачів невдовзі після обрання президента Родріго Чавеса. Тепер Конті стверджує, що вони почали атаку та тиснули на громадян Коста-Ріки, щоб вони тиснули на їхній уряд, щоб вони заплатили викуп у 20 мільйонів доларів. Уряд відмовився платити викуп, а сайт Конті про здирництво вказує, що він опублікував 50% даних уряду Коста-Ріки.

Чилі: у 2023 році чилійські військові зазнали атаки програми-вимагача Rhysida, у результаті якої зловмисники оприлюднили 360 000 документів, викрадених з уряду.

Організації Латинської Америки також стають цілями, незалежно від розміру. Фактично, він не застрахований від кібератак ланцюга поставок, оскільки вони стають все більш поширеними. У жовтні 2023 року в Чилі телекомунікаційна

компанія GTD була вражена бандою програм-вимагачів Роршаха, яка постраждала від 3500 компаній.

Дослідження 2023 року показало, що BlackCat, Vice Society, Lazarus APT і LockBit 2.0/3.0 були групами, які найбільше націлювалися на Латинську Америку. Існує також теорія, згідно з якою деякі менш відомі групи загроз використовують Латинську Америку як випробувальний полігон перед розширенням своїх операцій. Це стало очевидним, коли ARCrypter націлився на чилійський уряд, а потім розширив свою діяльність по всьому світу. З наближенням до 2024 року ми прогнозуємо, що ландшафт кіберзагроз зросте, і країни також зіткнуться з більшою кількістю інцидентів компрометації бізнес-електронної пошти разом із більш складними фішинговими кампаніями. Програми-вимагачі залишатимуться проблемою, але інші типи інцидентів також збільшаться.

Багатьом організаціям потрібна допомога у підготовці надійного плану реагування на кіберінциденти, який є ключовим для пом’якшення будь-якої форми кібератак. Зрозуміло, що все ще потрібна додаткова освіта, навіть незважаючи на те, що рівень обізнаності в регіоні різко зріс, але було б корисно побачити більше ініціатив щодо розвідки та обміну інформацією в регіоні.

Вимоги щодо відповідності захисту даних

Кібератаки та/або інциденти є глобальною проблемою. У країнах, які запровадили закони про захист даних, організації віддають перевагу запровадженню заходів кібербезпеки через контроль, з яким вони можуть зіткнутися з боку регулятора, якщо вони цього не зроблять. Хоча Латинська Америка може відставати у своєму законодавстві про захист даних, існує низка законів, які були прийняті в різних країнах, щоб відповідати зусиллям і нормам у Великобританії та ЄС. Країни, які мають чинне законодавство про захист даних, це Аргентина, Бразилія, Колумбія, Коста-Ріка, Еквадор, Мексика, Перу та Уругвай. Інші країни розробляють закони про захист даних або адаптують свої існуючі закони про захист даних на основі GDPR.

Країни Латинської Америки, здається, схиляються до моделі «повідомлення органу влади» про випадки даних, але не всі так роблять. Насправді деякі країни

взагалі не вимагають сповіщення або не мають спеціального органу із захисту даних. Деякі країни Латинської Америки, такі як Мексика та Перу, мають закони, які вимагають сповіщення суб'єктів даних, але не органів влади. У Чилі, наприклад, немає регулятора захисту даних, і лише спеціальні установи для регульованих ринків зобов'язані повідомляти про порушення, наприклад фінансові установи. Колумбія схожа на Бразилію тим, що вимагається сповіщення влади, причому Бразилія є однією з перших країн у регіоні, яка накладає значні штрафи.

Можливості кіберринку

Зростаюча частота та складність кібератак у Латинській Америці створює попит на (пере)страхове покриття для захисту організацій будь-якого розміру від зобов'язань, що виникають внаслідок кіберінцидентів.

До пандемії Covid-19 на Лондонському ринку існувала невизначеність з боку андеррайтерів, але нещодавно ми побачили різку зміну підходу з поверненням апетиту, хоча все ще є набагато більше можливостей для зростання. Латинська Америка — це величезний ринок з організаціями різного розміру. Зважаючи на те, що останнім часом так багато урядових установ стали жертвами кібератак, усвідомлення кіберзагроз у регіоні зростає. Багато організацій різко підвищили свою зрілість у сфері кібербезпеки та, у свою чергу, так само шукають відповідне кіберстрахове покриття.

Ключові висновки

Інтерес до кібербезпеки зростає в Латинській Америці, але потрібна додаткова освіта.

Країни Латинської Америки розробляють закони про конфіденційність і захист даних відповідно до норм ЄС.

Кібератаки, особливо атаки програм-вимагачів, є серйозною проблемою в регіоні.

Поінформованість про кібератаки та загрози зростає, оскільки організації збільшують свої інвестиції в кібербезпеку.

Поширення кіберстрахування зростає, але є місце для зростання». ***(Astrid Hardy and Nicolas Le Blanc. Securing Tomorrow: Why Latin America should top***

Global Cyber Insurers' Lists // DAC Beachcroft (https://www.dacbeachcroft.com/en/articles/2023/december/securing-tomorrow-why-latin-america-should-top-global-cyber-insurers-lists/). 06.12.2023).

***

«У нещодавньому попередженні команда безпеки Microsoft пролила світло на тривожну тенденцію у світі кіберзлочинності.

Злочинці все частіше використовують систему OAuth, яка зазвичай використовується веб-сайтами для перевірки ідентичності користувачів, отримання несанкціонованого доступу до систем і здійснення різних форм кібератак, включаючи незаконний майнінг криптовалюти.

Використання додатків OAuth кіберзлочинцями представляє багатогранну проблему для організацій. Зловмисники розпочинають свої кампанії, компрометуючи облікові записи користувачів, часто за допомогою фішингових атак або атак з використанням пароля.

Їх головними цілями є облікові записи, у яких відсутні надійні механізми автентифікації, що робить їх уразливими до атак із підбиранням облікових даних. Коли ці облікові записи зламано, кіберзлочинці закріплюються в системі.

Однією з нечесних дій, які слідують, є розгортання віртуальних машин (ВМ) для майнінгу криптовалюти. Це не тільки перекачує обчислювальні ресурси, але також може мати значний вплив на енергоспоживання організації та загальну продуктивність.

Окрім майнінгу криптовалют, зловмисники встановлюють стійкість у системі після інцидентів компрометації бізнес-електронної пошти (BEC) і використовують ресурси організації для розсилки спаму. Цей багатоаспектний підхід підкреслює серйозність загрози, яку становлять ці кіберзлочинці.

Майкрософт докладає зусиль щодо відстеження та виявлення

Корпорація Майкрософт активно відстежує ці шкідливі дії та вжила заходів для покращення виявлення шкідливих програм OAuth. Такі інструменти, як

Microsoft Defender for Cloud Apps, були розгорнуті для швидкого виявлення та нейтралізації загроз.

Одним із ключових заходів є запобігання скомпрометованим обліковим записам доступу до критичних ресурсів, що має ключове значення для запобігання спробам зловмисників підвищити свої привілеї та здійснити зловмисні дії.

Зменшення ризиків: рекомендації Microsoft

Комплексний аналіз цих атак, проведений корпорацією Майкрософт, дав важливі рекомендації для організацій щодо посилення безпеки та захисту від використання OAuth:

Запровадження багатофакторної автентифікації (MFA): значна кількість скомпрометованих облікових записів не мала MFA, що робило їх вразливими до атак. Увімкнення MFA значно знижує ризик несанкціонованого доступу, вимагаючи від користувачів надавати кілька форм підтвердження.

Використовуйте політики умовного доступу та безперервну оцінку доступу: ці вдосконалені заходи безпеки дозволяють оцінювати ризики в реальному часі та відкликати доступ у разі виявлення підозрілих дій. Організації можуть швидко реагувати на потенційні загрози, запобігаючи подальшій шкоді.

Використовуйте параметри безпеки за замовчуванням у Azure Active Directory (Azure AD). Особливо корисно для організацій із безкоштовним рівнем ліцензування Azure AD. Стандартні параметри безпеки пропонують попередньо налаштовані параметри, такі як MFA та захист для привілейованих дій. Ці параметри за замовчуванням забезпечують надійну основу безпеки.

Регулярно перевіряйте програми та дозволи. Організаціям рекомендується переглядати програми та дозволи, надані в їхніх системах. Дотримання принципу найменших привілеїв гарантує, що надається лише необхідний доступ, зменшуючи поверхню атаки». ***(Benson Mawira. Cybercriminals exploit OAuth system to hijack user accounts and fuel cybercrime // Cryptopolitan (https://www.cryptopolitan.com/cybercriminals-exploit-oauth-system/?utm_source=flipboard&utm_content=Cryptopolitan%2Fmagazine%2FLatest+Crypto+and+Blockchain+News). 13.12.2023).***

***

«Здається, злом служби передачі файлів MOVEit був однією з найбільших кібератак 2023 року, незважаючи на те, що це був рік, коли з'явилася низка нових небезпечних тенденцій і тактик.

У новому звіті ESET проаналізовано найбільш значні кіберінциденти другої половини 2023 року, зазначивши, що те, що зробило злом MOVEit унікальним, окрім його широкого впливу, це те, що програми-вимагачі Cl0p, банда, яка стоїть за атакою, фактично не розгорнула.

Він також злив викрадені дані з організацій-жертв на загальнодоступний веб-сайт, ще один випадок нової тактики, яку використовують кіберзлочинці. Це наслідувала сумнозвісна банда програм-вимагачів ALPHV/BlackCat, яка також була поширеною цього року.

Нові тенденції

У своєму звіті ESET зазначає, що через величезний масштаб злому MOVEit Cl0p, ймовірно, доклав занадто багато зусиль для шифрування кожної захопленої жертви. ESET наводить дані Emsisoft, які оцінюють, що через шість місяців кількість постраждалих організацій перевищить 2600.

Жертвами були різні державні установи, школи та заклади охорони здоров'я, а також такі великі компанії, як Sony і PricewaterhouseCoopers (PwC).

Ще однією новою тенденцією цього року стало зростання кількості атак із застосуванням ШІ, що не дивно, враховуючи бум, який ця технологія пережила після публічного випуску ChatGPT у листопаді 2022 року.

Багато кампаній були націлені на користувачів таких інструментів штучного інтелекту, як ChatGPT, а також на створення підроблених доменів, які за своїм формулюванням нагадують «ChatGPT». До таких доменів належать веб-програми, які використовують ключі OpenAI API у небезпечний спосіб, що загрожує конфіденційності даних користувача.

Також цього року штурмом став викрадач Lumma, який був дуже успішним у крадіжці криптовалютних гаманців. Лише воно спричинило зростання кількості крадіжок криптовалюти на 68% цього року, що становить 80% випадків виявлення

в цьому секторі. Lumma Зловмисне програмне забезпечення також викрадає облікові дані та іншу інформацію, при цьому загальна кількість виявлень Lumma зросла втричі між першим і другим півріччям 2023 року.

І постійна загроза Magecart, яка турбує роздрібних торговців з 2015 року, все ще залишається сильною - фактично цього року вона зростає. Він впроваджує код на незахищені веб-сайти, щоб викрасти інформацію користувачів, наприклад дані їхніх кредитних карток. Кількість виявлень з 2021 по 2023 рік зросла на 343%.

Їржі Кропач, директор із виявлення загроз в ESET, робить висновок, що «ці події свідчать про те, що ландшафт кібербезпеки постійно розвивається, коли суб'єкти загроз використовують широкий спектр тактик». З розвитком штучного інтелекту та постійною зміною тактики загрозливих суб'єктів схоже, що наступного року атаки лише погіршаться». ***(Lewis Maddison. The MOVEit breach may well have been the biggest cyberattack of the year // Future US, Inc. (https://www.techradar.com/pro/security/the-moveit-breach-may-well-have-been-the-biggest-cyberattack-of-the-year?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 13.12.2023).***

***

«…Кіберзлочинність має багато проявів, але деякі з ключових ризиків, з якими стикається бізнес:

Витоки даних – це одна з найпоширеніших форм кіберзагроз, яка виникає, коли шахраї отримують доступ до конфіденційної інформації (часто даних клієнтів) і продають її в темній мережі з метою отримання прибутку або використовують цю інформацію для викрадення особистих даних ваших клієнтів або співробітників і заподіяти їм шкоду, використовуючи свій високий кредитний рейтинг для отримання товарів шахрайським шляхом.

Атаки програм-вимагачів – це тип шкідливого програмного забезпечення, яке шифрує дані компанії, роблячи їх недоступними, доки не буде сплачено викуп.

Фішинг і соціальна інженерія – це коли працівника обманом змушують або натиснути посилання, яке надає шахраю доступ до IT-систем компанії, або шахраї використовують соціальну інженерію для досягнення тієї ж мети.

Шкідливе програмне забезпечення та віруси – це випадки, коли шахрайська частина програмного забезпечення (вірус) проникає в системи компанії, що призводить до збоїв у роботі, втрати даних і потенційно несанкціонованого доступу.

Інсайдерські загрози – не всі загрози є зовнішніми, і співробітники можуть мати зловмисні наміри та використовувати свій доступ для викрадення або витоку конфіденційної інформації.

DDoS-атаки – це «розподілена атака на відмову в обслуговуванні», і вона перевантажить сервери компанії, зробивши її онлайн-сервіси недоступними для користувачів, що може призвести до втрати прибутку, шкоди репутації компанії та втрати довіри з боку клієнтів.

Компрометація електронної пошти – це випадки, коли електронну пошту компанії зламано, і шахрай видає себе за керівника компанії та обманом змушує працівників здійснювати грошові перекази або ділитися конфіденційною інформацією. Це також відоме як «шахрайство генерального директора».

Це не вичерпний список, і існує низка різних видів шахрайства та кіберзагроз, які тримають бізнес у стані настрою…

Згідно з опитуванням про порушення кібербезпеки 2021 року, проведеним урядом Великої Британії, у 2020 році два з п’яти британських підприємств зазнали кібератак. Останні дані показують, що у Великобританії найбільше жертв кіберзлочинів на мільйон користувачів Інтернету – 4783 у 2022 рік – на 40% більше, ніж у 2020 році. Також вважається, що через стигматизацію жертви кібератаки ця кількість насправді може бути більшою, оскільки про це часто не повідомляється.

У 2020 році відбулося різке зростання кіберзлочинності через пандемію, і це показало, що підприємства були погано готові до цифрової війни, яку прискорив

COVID. За останні три роки компанії вживають заходів і докладають більше зусиль, щоб захистити себе від кіберзлочинності.

Хоча всі підприємства піддаються ризику, є певні галузі, які стають об’єктами нападу частіше через те, що вони, швидше за все, зберігають персональні дані про клієнтів, і це:

Фінанси та страхування;

Охорона здоров'я, соціальна робота та соціальна допомога; і

Якщо ви працюєте в одній із цих галузей, особливо важливо вжити заходів для захисту вашої компанії від будь-яких потенційних загроз.

Приклад небезпеки можна побачити в нашій власній галузі, коли юридична фірма піддається кібератаці, що завдає клієнту значних збитків.

Чому боротьба з шахрайством і кіберзлочинністю має сенс для бізнесу

Шахрайство та кіберзлочинність становлять 41% усіх злочинів у Великій Британії і, навпаки, поліцейські ресурси, спрямовані на економічні злочини, складають приблизно 1%. Якщо ваша компанія стала жертвою кіберзлочинної атаки, можливі наслідки варіюються від фінансових втрат, шкоди репутації та втрати довіри клієнтів.

Важливо, щоб підприємства активно захищали себе від шахрайства. Роблячи це, ви можете допомогти зменшити ризик шахрайства та працювати з упевненістю та впевненістю, тим самим вселяючи довіру до вашого бізнесу у ваших клієнтів.

Які кроки вжити, щоб захистити свій бізнес від кіберзлочинності

Боротьба з кіберзлочинністю є складним завданням, оскільки це постійні зміни. Крім того, на жаль, не існує універсальної процедури, яку може застосувати бізнес. Куди ви спрямуєте свої зусилля, залежатиме від профілю ризику вашого бізнесу, однак ось 5 швидких порад, які допоможуть вашому бізнесу випередити загрозу кіберзлочинності.

Надійні заходи безпеки – це в основному означає забезпечення безпеки ваших IT-систем або принаймні достатньої непроникності, щоб шахрай міг перейти до іншої м’якшої мішені. Способи забезпечення надійних заходів безпеки:

Встановлення останніх оновлень на комп'ютери та пристрої. Кіберзлочинці часто використовують відомі вразливості програмного забезпечення, і шляхом регулярного оновлення операційних систем і програм ці вразливості усуваються.

Переконайтеся, що у вас є брандмауери. Брандмауери діють як бар’єр між внутрішніми мережами та Інтернетом, контролюючи вхідний і вихідний трафік.

Майте хороше антивірусне програмне забезпечення. Антивірусне програмне забезпечення призначене для захисту, запобігання та видалення різних типів шкідливих програм, таких як трояни, програми-вимагачі, рекламні програми тощо. Він сканує в режимі реального часу, щоб виявити шкідливі коди та помістити їх у карантин, перш ніж вони можуть завдати шкоди.

Забезпечення надійного контролю доступу. Багатофакторна автентифікація гарантує, що користувачам необхідно надати кілька форм ідентифікації, перш ніж отримати доступ до даних або систем. Це також працює навпаки, оскільки компанії повинні обмежувати привілеї користувачів, щоб лише окремі люди мали доступ до конфіденційної інформації та систем, необхідних для виконання своїх ролей.

Навчання та навчання співробітників. На жаль, людські помилки є значним фактором кіберзлочинності. Проведення регулярних тренінгів для співробітників щодо загроз і найкращих практик підвищить обізнаність і, сподіваємось, дозволить їм виявляти такі загрози, як фішингові електронні листи.

Регулярне резервне копіювання даних – виконуйте регулярне резервне копіювання даних, щоб у разі кіберінциденту або атаки програм-вимагачів можна було відновити критичну інформацію. Ці резервні копії мають зберігатися поза сайтом і бути зашифрованими для забезпечення безпеки.

План реагування на інциденти – розробіть комплексний план реагування на інциденти, у якому описано кроки, яких необхідно вжити у випадку кіберінциденту. Цей план має включати протоколи виявлення, стримування, викорінення, відновлення та уроки, отримані після атаки. На жаль, часто компанії вводять протоколи лише після атаки.

Управління ризиками третіх сторін – якщо ваш бізнес співпрацює з іншими постачальниками (що дуже ймовірно в наш сучасний час), тоді це процес, за

допомогою якого ви визначаєте, оцінюєте та зменшуєте ризики, пов’язані з цими відносинами. Дії, які необхідно вжити, можуть полягати в тому, щоб оцінити їхні практики кібербезпеки та переконатися, що вони відповідають вашим стандартам безпеки, і потенційно вимагати від них підписання угод щодо дотримання заходів безпеки та негайного повідомлення про будь-які інциденти.

До яких загроз шахрайства відкриті ланцюги поставок?

Є багато способів, якими ланцюг поставок може опинитися під загрозою шахрайства. Деякі з найпоширеніших:

Шахрайство з рахунками-фактурами: тут створюються підроблені рахунки-фактури або змінюються законні рахунки-фактури, щоб стягнути завищену плату за товари чи послуги чи перевести кошти за начебто справжні товари/послуги на рахунок шахрая. Це зона ризику, яка зазвичай пов’язана з кіберзлочинністю.

Заміна продукту: це коли відбувається заміна продуктів, які використовуються в ланцюжку постачання, на неякісні або підроблені матеріали. Вони часто мають низьку якість і можуть призвести до несправності всього продукту, що спричинить проблеми з контролем якості та невдоволення клієнтів.

Відкати та хабарництво: це відбувається, коли особи в ланцюжку постачання отримують хабарі або відкати від постачальників в обмін на надання переваги їхнім продуктам або послугам, часто за рахунок найкращих інтересів компанії-жертви. Компанії також повинні знати про Закон про хабарництво 2010 року, який (серед інших правопорушень) зазначає, що комерційна організація може бути винною у скоєнні злочину, якщо вона не запобігає підкупу осіб, пов’язаних з нею.

Маніпулювання даними: шахраї можуть маніпулювати даними ланцюга постачання, такими як рівень запасів, показники виробництва або дані про продажі, щоб ввести в оману зацікавлених сторін і створити неправдиву фінансову звітність. Прикладом тому є скандал навколо Patisserie Valerie.

Привиди співробітників і постачальників: тут шахраї створюють фіктивних співробітників або постачальників для проведення шахрайських платежів і перенаправлення коштів.

Змова та співпраця: тут кілька співробітників змовляються разом, щоб обійти та/або скасувати певні бізнес-протоколи та транзакції для здійснення шахрайства. Це часто може включати зовнішніх третіх сторін.

Порушення санкцій: бувають випадки, коли вводяться економічні санкції, які обмежують потік активів до певних країн або з них. Імпортуючи товари з цих країн, підприємства можуть порушити ці санкції, що може завдати значної шкоди репутації (а також грошовій). Існує багато способів порушення санкцій, і це часто набуває форми приховування походження товарів. Прикладами цього є навмисне відключення системи стеження за судном або створення складної та заплутаної мережі компаній, щоб уникнути виявлення.

Шахрайство з контрактом і введення в оману: це випадки, коли існує спотворення інформації щодо ціноутворення, здатності виконати проект на основі досвіду чи ресурсів або інших аспектів контракту ланцюга поставок, що може призвести до збитків для однієї зі сторін.

Висновок

Кіберзлочинність – це сфера, яка постійно розвивається. Кіберзлочинці адаптуються та використовують уразливості, що ускладнює боротьбу. Однак, переконавшись, що ви вживаєте заходів для захисту свого бізнесу, ви можете бути на крок попереду кіберзлочинців і зробити себе незавидною мішенню…» ***(Rebecca Craig. How To Be A Cybercrime Buster // Tenet Compliance & Litigation Limited (https://tenetlaw.co.uk/articles/how-to-be-a-cybercrime-buster/). 15.12.2023).***

***

«Щороку приблизно в грудні експерти NordVPN намагаються спрогнозувати ризики кібербезпеки, які чекають на нас у наступному році. Цього року вони вирішили піти іншим шляхом і заглянути на найбільший темний веб-форум, щоб дізнатися, які теми найбільше обговорювали, і заснувати свої прогнози на своїх висновках.

«Щороку ми намагаємося передбачити складні атаки від досвідчених хакерів, які здебільшого націлені на бізнес або впливових людей», — говорить Маріюс

Брієдіс, технічний директор NordVPN. «Цьогорічний підхід допоміг нам зрозуміти, що звичайні користувачі Інтернету часто піддаються атакам хакерів-любителів, які все ще розвивають свою майстерність. Вони також можуть завдати великої шкоди своїм нічого не підозрюючим жертвам, і користувачів потрібно поінформувати про їхні плани».

Нижче ви знайдете п’ять найкращих прогнозів, зроблених експертами з кібербезпеки NordVPN на основі того, про що говорять хакери в Інтернеті.

У тренді темної мережі

Найбільш коментовані гілки на форумі включали теми про витік оголених людей з OnlyFans, Instagram та інших платформ для обміну контентом. Теми про витік оголених людей отримали майже 1850 коментарів і увійшли до топ-20 найбільш коментованих тем на форумі.

«Це означає, що в наступному році ми побачимо ще більше атак, де будуть витікати фотографії оголених людей. Іншим шляхом, яким можуть скористатися злочинці, є використання штучного інтелекту або технологій deepfake для створення підроблених оголених зображень, щоб обдурити своїх покупців», — говорить Маріюс Брієдіс.

Щоб уникнути витоку фотографій в Інтернеті, Варменховен рекомендує утримуватися від надсилання фотографій через соціальні мережі та використовувати зашифровані хмарні рішення для обміну фотографіями.

Штучний інтелект допоможе хакерам

Зламані облікові записи ChatGPT і навчальні посібники з використання ШІ для атак дуже популярні серед хакерів. Це не тільки означає, що користувачі штучного інтелекту знаходяться на радарі, але й хакери вчаться використовувати штучний інтелект, щоб збільшити продуктивність своєї роботи та зробити свою роботу легшою, швидшою та ефективнішою.

«Використання інструментів штучного інтелекту сприятиме автоматизації значної частини фішингових атак, і очікується, що частота таких атак у майбутньому зросте, створюючи значні загрози кібербезпеці», — говорить Брієдіс.

Він також зазначає, що користувачі, які не впевнені, що можуть ідентифікувати фішингові електронні листи, можуть використовувати розширення браузера, створені для цієї мети.

Кількість хакерів-любителів зростатиме

Кожне десяте повідомлення на форумі було про те, як навчитися виконувати якусь атаку. Серед найбільш коментованих тем були: «Як dox», «Список корисних ресурсів для пентестерів і хакерів», «Як зламати WhatsApp вашого друга, надіславши одне чорнило», «Як легко миттєво зламати облікові записи TikTok», «Курс злому WiFi» та ін.

Це означає, що хакери діляться своїми знаннями, і ми можемо очікувати, що кількість хакерів-любителів зросте разом із кількістю атак, які вони здійснюють. Тож користувачі повинні ще серйозніше ставитися до своєї освіти з кібербезпеки та тримати себе в курсі останніх атак.

Дані клієнтів будуть продаватися як гарячі пиріжки

Дослідники виявили, що близько 55% дискусій стосуються витоку даних клієнтів, таких як облікові дані в соціальних мережах, водійські права, адреси, електронні адреси та інша особиста інформація. Це означає, що хакери все ще шукають вразливі особисті дані, і жоден користувач не застрахований від злому.

Варменховен каже, що найпростіша річ, яку користувачі можуть зробити, щоб захистити свої онлайн-дані, — це використовувати MFA (багатофакторну автентифікацію), де це можливо.

Біометрична автентифікація не буде відповіддю

Багато платформ, які піклуються про безпеку своїх користувачів, тепер надають можливість біометричної автентифікації. Однак дослідження показало, що хакери вже навчилися обходити деякі методи біометричної автентифікації, такі як перевірка селфі, яку використовують деякі криптоплатформи. Тема про те, як обійти перевірку селфі, зібрала понад 200 коментарів.

«Біометрична автентифікація, безсумнівно, стане частиною автентифікації в майбутньому, але лише якщо вона буде багатофакторною», — каже Маріюс Брієдіс. «Отже, ми можемо не тільки передбачити, що біометрична автентифікація

виявиться ненадійною, але й що з'являться більш багатошарові способи захисту онлайн-акаунтів.

Однією з останніх розробок у цій сфері стала технологія ключів доступу. Ключ доступу — це пара пов'язаних ключів: відкритого та закритого. Відкритий і закритий ключі не працюють один без одного, тому вони марні для хакерів. Крім того, ключ доступу на вашому гаджеті (приватний ключ) неможливий без біометричної ідентифікації (власника пристрою) або PIN-коду, що додає додатковий захист». ***(Hackers predict: The biggest cybersecurity worries in 2024 // Annex Business Media (https://www.ept.ca/2023/12/hackers-predict-the-biggest-cybersecurity-worries-in-2024/). 24.12.2023).***

***

«Команда Google Cloud нещодавно розповіла про найпомітніші загрози кібербезпеці 2023 року — багатогранне здирництво та використання нульового дня — і передбачила більше атак нульового дня у 2024 році під час двох публічних віртуальних сесій. Крім того, Google передбачає, що і зловмисники, і захисники продовжуватимуть використовувати генеративний ШІ. Однак генеративний штучний інтелект, ймовірно, не створюватиме власне шкідливе програмне забезпечення у 2024 році.

Дві найпомітніші загрози кібербезпеці 2023 року

Двома найпомітнішими загрозами кібербезпеці 2023 року, за словами Люка Макнамари з Google Cloud, головного аналітика довіри та безпеки, були багатогранне здирництво (також відоме як подвійне здирництво) та експлуатація нульового дня.

Багатогранна експлуатація

Багатогранна експлуатація включає програмне забезпечення-вимагач і крадіжку даних, хоча кількість атак програм-вимагачів, відстежених Google Cloud, зменшилася в 2023 році. Найпоширенішими сімействами програм-вимагачів, які використовуються в багатогранних атаках експлуатації, були LockBit, Clop і ALPHV.

Більшість атак програм-вимагачів спочатку відбувалися через вкрадені облікові дані. Атаки грубої сили та фішинг були наступними за поширеністю початковими векторами зараження програм-вимагачів.

За словами Макнамари, зловмисники все частіше виставляють викрадені облікові дані на сайти витоку даних. «У цьому минулому кварталі (3 квартал 2023 року) ми спостерігали найбільшу кількість публікацій на сайтах DLS з тих пір, як ми почали відстежувати це у 2020 році», — сказав Макнамара.

Багато зловмисників агностикують галузь, але «з кварталу за кварталом виробництво зазнає особливого удару та непропорційного впливу», — сказав Макнамара. «Тут ми спостерігаємо велику активність з точки зору обсягу».

Експлуатація нульового дня

Експлуатація нульового дня визначається Google Cloud як уразливості без відомих виправлень, якими активно користуються зловмисники. У 2023 році Google Cloud Security відстежила 89 таких атак, перевищивши попередній максимум 2021 року.

Багато загроз нульового дня є афілійованими або спонсорованими національними державами. Другою найпоширенішою мотивацією серед суб'єктів загроз, які використовують загрози нульового дня, є отримання грошей.

Прогноз кібербезпеки Google Cloud на 2024 рік

Ендрю Копченскі, головний аналітик аналізу загроз у комунікаційному центрі Google Mandiant, під час своєї презентації про кіберзагрози у 2024 році розповів про суб'єктів загрози національних держав, атаки нульового дня, переміщення між хмарними середовищами та крадіжки облікових даних. Зокрема, Китай і Росія зосереджуються на атаки нульового дня, сказав він.

«Ми повністю очікуємо, що у 2024 році побачимо набагато більше використання «нульового дня» не лише зловмисниками, які фінансуються національною державою, але й кіберзлочинцями», — сказав Копченскі. «Нуль днів — це один із найкращих методів, щоб зловмисники залишалися непоміченими, коли вони проникли в мережу».

Організатори загроз, спонсоровані Китаєм

Спонсоровані Китаєм актори зосередилися на розвитку можливостей пошуку та використання нульових днів і ботнетів, щоб залишатися непоміченими, сказав Копченскі. Google Cloud очікує, що зусилля Китаю щодо боротьби з кіберзагрозами будуть зосереджені на сферах високих технологій, таких як розробка чіпів.

Спонсорований Росією шпигунство

За його словами, російське шпигунство, зосереджене на Україні, було проблемою. Google Cloud виявив, що Росія також проводила кампанії за межами України, але вони здебільшого зосереджені на отриманні стратегічної інформації про Україну, сказав Копченський. Спонсоровані Росією зловмисники використовують атаки «живуть за рахунок землі», які не потребують шкідливого програмного забезпечення; натомість вони зловживають рідними можливостями, і їхній трафік виглядає як рідний трафік. Google Cloud очікує більше атак з боку підтримуваних Росією акторів у 2024 році, здебільшого зосереджених на жертвах в Україні або пов’язаних з Україною.

Організатори загроз, спонсоровані Північною Кореєю

Google Cloud також уважно придивився до національних державних акторів, пов’язаних із Північною Кореєю.

«Вони розробили погані можливості для запуску атак на ланцюг поставок програмного забезпечення», — сказав Копченскі.

Північна Корея була першою відомою національною державою, яка використала «каскадні» атаки на ланцюг поставок програмного забезпечення, які взаємодіяли одна з одною. Багато з цих атак стосуються крадіжки криптовалюти або компаній, які здійснюють операції з криптовалютою. Google Cloud очікує, що у 2024 році кількість атак, пов’язаних із Північною Кореєю, поширюється.

Крадіжка облікових даних і вимагання

Ще одна тривога 2024 року – здирництво. «Крадіжка облікових даних — це назва гри... яка стала найрадикальнішим і найпопулярнішим заходом, який використовують багато зловмисників», — сказав Копченскі.

«У 2024 році ми очікуємо, що ми зосередимося на сайтах витоку даних, особливо з боку здирників», — сказав він.

Переміщення між хмарними середовищами

У 2024 році зловмисники можуть використовувати тактику, методи та процедури, які дозволять їм подорожувати різними хмарними середовищами, ймовірно, через збільшення використання хмарних і гібридних середовищ.

Як генеративний ШІ вплине та вплине на кібербезпеку у 2023 та 2024 роках

Зловмисники можуть використовувати генеративний штучний інтелект для створення тексту, голосових повідомлень і зображень, і Google Cloud очікує, що це стане більш поширеним явищем.

«Штучний інтелект надає можливість певним типам зловмисників, переважно в рамках кампаній з дезінформації. Ми дуже стурбовані наступним роком впливом дезінформації, яка була посилена штучним інтелектом, особливо коли мова йде про вибори 2024 року», — сказав Копченскі.

У 2023 році генеративний ШІ використовувався зловмисниками та захисниками. У 2024 році штучний інтелект може бути використаний для збільшення масштабу атак, наприклад, шляхом впровадження штучного інтелекту в кол-центри, які ведуть переговори про програми-вимагачі.

Генеративний ШІ, можливо, зможе створювати зловмисне програмне забезпечення в якийсь момент у майбутньому, але Копчуенський сказав, що не очікує, що це станеться лише у 2024 році. Він рекомендує фахівцям з кібербезпеки «залишатися на землі» і не втрачати сну, коли мова йде про генеративний ШІ. За його словами, багато з його загроз є «гіпотетичними».

«Уже є багато галасу та дезінформації про те, що ШІ може, а що ні. …Штучний інтелект не є надзвичайною революцією з точки зору наявних загроз», – сказав він». ***(Megan Crouse. Google Cloud's Cybersecurity Predictions of 2024 and Look Back at 2023 // TechnologyAdvice (https://www.techrepublic.com/article/google-cloud-security-talks-2023/). 21.12.2023).***

***

«Минулого року Україна посіла 24 місце в Національному індексі кібербезпеки (NCSI). Він оцінює рівень кіберзахисту країни за різними критеріями і показує її готовність боротися з кіберзагрозами. Чудовий результат, з урахуванням того, що ми випередили Австрію, Норвегію та Ірландію.

Рейтинг NCSI постійно оновлюється, і станом на кінець листопада 2023 року ми опинилися вже на третьому місці. Україна значно поліпшила свої показники, наприклад, рівень воєнного кіберзахисту (military cyber defence). У нас працюють дуже круті профі.

Зрозуміло, що розвиток цієї галузі відбувається у відповідь на збільшення кількості кіберінцидентів. На жаль, «відбити» всі кібератаки неможливо (нагадує якийсь пекельний бадмінтон). І часом відбувається жесть на кшталт проблем зі зв'язком чи банкінгом. Але це квіточки порівняно з тим, як усе могло б бути без кіберзахисту. Сьогодні розповімо про найвідоміші кібератаки в історії. Хочемо ще раз підсвітити важливість того, що роблять фахівці з кібербезпеки.

Перший кіберзлочин: як усе починалося

Перший кіберзлочин скоїв Роберт Морріс в 1988 році. Аспірант Корнелльського університету від нудьги створив і запустив у мережу ARPANET, попередницю інтернету, хробака. Йому було цікаво, наскільки далеко той поширюється. Але експеримент вийшов з-під контролю, і Morris worm спричинив серйозні проблеми.

Тоді ARPANET налічувала близько 60 000 комп'ютерів. Хробак встиг заразити 6000 із них. Він захоплював ресурси пам'яті та уповільнював роботу багатьох наукових і військових установ у США. Збитки за різними оцінками склали до $100 млн. Погодься, вражаючі результати.

Попри відсутність злого наміру, Морріса засудили до трьох років умовно і оштрафували на $10 000. Його кібератака показала, що навіть прості програми можуть завдати шкоди комп'ютерним мережам. Ця подія стала поштовхом до розвитку кібербезпеки.

Зараз Роберт Морріс веде звичайне життя і працює професором у MIT. Тепер поговоримо про наймасштабніші кіберінциденти. Порівняно з ними Morris worm – безневинний жарт.

Найгучніші кіберзлочини в історії

З плином часу кіберзлочинці стають дедалі небезпечнішими та хитрішими. При цьому жертвою може стати хто завгодно: від звичайних людей до компаній і державних організацій. Ось список кіберзлочинів, які приголомшили світ:

Програма-вимагач WannaCry. Атака почалася в травні 2017 року і вразила понад 200 000 комп'ютерів у 150 країнах. WannaCry шифрував дані користувачів і вимагав за них викуп у Bitcoin. Це спричинило збої в роботі шкіл, систем зв'язку, банкоматів і лікарень. Зламало частину медичного та промислового обладнання, що призвело до серйозних наслідків для здоров'я та безпеки людей. WannaCry – один із найбільш руйнівних здирників. На щастя, спеціаліст із кібербезпеки Маркус Гатчінс випадково помітив, що вірус перед зараженням надсилає запит до неіснуючого доменного імені. Після його реєстрації «епідемія» припинилася.

NotPetya. Ця потужна кібератака почалася з України, але швидко поширилася світом, зачепивши понад 100 країн. NotPetya був задуманий як шкідливе ПЗ, що маскується під здирницьке. Він «бив» по бізнесу і намагався завдати максимальної шкоди. NotPetya шифрував дані, псував жорсткі диски і розправлявся з внутрішніми мережами менше ніж за хвилину. Відновити інформацію в більшості випадків було неможливо. В Україні від нього постраждали аеропорти, банки, госпіталі, термінали, поштові та енергетичні компанії. У світі під удар потрапили логістичні, харчові, фармацевтичні та будівельні гіганти (наприклад, Maersk, Merck і FedEx). Фінансові збитки оцінюють у $10 млрд.

Ботнет Mirai. Він став причиною масштабної DDoS-атаки проти провайдера доменних імен Dyn, який надавав послуги великим компаніям на кшталт Netflix, Twitter, PayPal, Pinterest, Airbnb, Spotify і Reddit. Кібератака тимчасово відключила безліч сервісів і сайтів. Спочатку Mirai придумали гравці в Minecraft, щоб заробити грошей. У 2016 році вони опублікували вихідний код, що дало змогу іншим хакерам його використовувати. У результаті Mirai заразив понад 600 000 пристроїв

IoT. Саме з їхньою допомогою проводили DDoS-атаки. Випадок із Mirai показав вразливість інтернету речей. Ці девайси часто мають слабкі паролі і стають легкою мішенню для кіберзлочинців.

Атака на Sony. У 2014 році група хакерів Guardians of Peace (GOP) вкрала величезну кількість інформації з мережі Sony Pictures. Включно з електронними листами, особистими даними співробітників і фільмами, які ще не вийшли в прокат. Їх виклали на платформах для обміну файлами. Також GOP погрожували терактами в кінотеатрах, які показували стрічку «Інтерв'ю» – комедію з місцем дії в Північній Кореї. Саме з цією країною і пов'язують діяльність кіберзлочинців. Внаслідок кібератаки Sony зазнала великих грошових і репутаційних втрат.

Stuxnet. Один із найскладніших і найруйнівніших комп'ютерних хробаків в історії. Його розробили для атаки на іранські ядерні об'єкти. У 2010 році він зламав 20% центрифуг для збагачення урану і відкинув ядерну програму країни на кілька років назад.

Це всього лише п'ять прикладів відомих кіберзлочинів, які показують, наскільки важливо дбати про кібербезпеку і постійно вдосконалювати методи захисту. Тепер ти знаєш, чим небезпечні кібератаки і до яких наслідків вони можуть призвести.

Чи варто вивчати кібербезпеку у 2024 році

За даними деяких експертів, глобальні збитки від кіберзлочинів за 2023 рік сягають $8,7 трлн. В Україні кількість кібератак теж значно збільшилася (ти й сам помітив). Найчастіше вони спрямовані на фінансові, освітні, державні, телекомунікаційні та громадські організації. А ще на критичну інфраструктуру (хто б сумнівався). Розумієш, з чим доводиться працювати фахівцям із кібербезпеки? Особливо з огляду на те, що за атаками часто стоять не поодинокі хакери, а цілі групи і серйозні ресурси.

У відповідь на ситуацію, що склалася, у сфері кібербезпеки з'являтиметься дедалі більше вакансій. Тенденція актуальна не тільки для України, а й для інших країн…» ***(Кібербезпека: найгучніші кібератаки в історії // GoIT***

(https://goit.global/ua/articles/kiberbezpeka-nayhuchnishi-kiberataky-v-istorii/). 21.12.2023).

***

Вірусне та інше шкідливе програмне забезпечення

«…Кембриджський словник описує зловмисне програмне забезпечення як «комп'ютерне програмне забезпечення, яке призначене для пошкодження роботи комп'ютера». Однак сьогодні це вже не обмежується лише комп'ютерами, оскільки ви також можете знайти зловмисне програмне забезпечення на своєму Android або iPhone.

У 2023 році Astra стверджує, що щодня виявляється 560 000 нових прикладів зловмисного програмного забезпечення, і вже відомо про існування понад мільярда шкідливих програм. Лише в першій половині 2022 року понад 236 мільйонів атак програм-вимагачів спричинили середню вартість 4,54 мільйона доларів США за інцидент.

Хоча зловмисне програмне забезпечення, очевидно, може створити проблеми для великих корпорацій, воно також може завдати шкоди звичайним людям. Фактично наявність шкідливого програмного забезпечення на вашому комп'ютері може призвести до втрати грошей, засобів до існування та навіть особистої безпеки. За даними AAG, щонайменше 15,45% користувачів Інтернету у світі зазнали принаймні одну атаку класу зловмисного програмного забезпечення у 2021 році. Знаючи це, дуже ймовірно, що більшість користувачів зіткнеться зі зловмисним програмним забезпеченням у певний момент під час роботи в Інтернеті, але є деякі ознаки ознаки, щоб визначити, чи ваш пристрій зламано.

Млява продуктивність

Залежно від того, яке зараження або вірусні програми наявні, зловмисне програмне забезпечення може проявлятися одним із способів уповільнення комп'ютера. Однак, хоча такі речі, як повільний запуск або завершення роботи, затримка запуску програм або незрозумілі збої програми, майже завжди є ознаками

того, що щось не так, важливо знати, що може бути багато інших причин, чому ваш ПК працює повільно.

Отже, перш ніж вважати, що проблемою є зловмисне програмне забезпечення, ви можете спробувати зробити щось, щоб ізолювати проблему; як-от дефрагментація жорсткого диска, видалення непотрібних програм і виконання інших порад, щоб ваша Windows знову працювала як нова. Для користувачів Mac деякі з поширених причин, через які ваш Mac може працювати повільно, полягають у тому, що у вас відкрито занадто багато енергоємних програм, у вас немає місця на диску або вам потрібно оновити macOS до новішої версії.

Коли ви вичерпаєте всі інші варіанти, ви можете обвести назад і спостерігати, чи ваш комп'ютер з Windows або Mac все ще не працює оптимально. Загалом, якщо ви помітили, що ваш новий ПК чи MacBook уже демонструє ознаки сповільнення після кількох місяців регулярного використання, є ймовірність, що на нього може вплинути зловмисне програмне забезпечення.

Незвичайна мережева активність

Завдяки вдосконаленню процесів виявлення загроз, які запускаються щороку, розробники зловмисного програмного забезпечення також знаходять більш просунуті способи створення програмного забезпечення, яке може уникнути виявлення. За даними компанії з кібербезпеки Proofpoint, є кілька незвичайних мережевих дій, які можуть вказувати на те, що ваш пристрій скомпрометовано зловмисним програмним забезпеченням.

Наприклад, хакери іноді можуть запускати програмне забезпечення для збору та надсилання даних на контрольовані ними сервери в непіковий час, щоб уникнути виявлення. У деяких випадках він посилається на трафік із підозрілими IP-адресами, що може призвести до дивних географічних місць.

Окрім цього, Utilities One також попереджає, що зловмисне програмне забезпечення може призвести до надмірних витрат на передачу даних. Порівнюючи зловмисне програмне забезпечення з цифровими шкідниками, воно стверджує, що зловмисне програмне забезпечення може виконувати серію дій, які споживають дані без вашої згоди. У деяких випадках зловмисне програмне забезпечення може

передавати мультимедійні файли на вашому пристрої, постійно синхронізувати дані у фоновому режимі, захоплювати ваше з'єднання для відвідування рекламних сайтів або навіть ставати частиною більшої мережі заражених пристроїв, які використовуються для переповнення веб-сайтів трафіком та іншим підлі методи.

Щоб перевірити використання мережі, LMG Security пропонує встановити безкоштовні інструменти моніторингу мережі для вашого комп'ютера, такі як Wireshark і Argus. За допомогою них ви зможете захоплювати та аналізувати пакети та записи потоків, які можуть виявити вашу мережеву активність. Крім того, ви можете використовувати інструменти аналізу Wi-Fi, щоб діагностувати проблеми з Інтернетом, оскільки в деяких випадках можуть бути звичайні причини, чому ваш Інтернет повільний, як-от неправильне розташування маршрутизатора.

Несподівані спливаючі вікна та реклама

Google Chrome визначає розширення як щось, що «може вносити зміни у ваші налаштування Chrome, що покращує ваш досвід перегляду та полегшує використання розширення». Серед цих змін Google називає можливість налаштовувати налаштування для вашої домашньої сторінки, сторінки нової вкладки, пошукової системи або стартової сторінки.

Хоча ці розширення можуть здаватися нешкідливими, лише у 2020 році майже 3 мільйони людей були заражені зловмисним програмним забезпеченням із сторонніх розширень браузера. У деяких випадках зловмисне програмне забезпечення може бути вбудовано в розширення, а в інших випадках це може бути наслідком того, що розробники пропускають критичні проблеми безпеки.

За словами дослідників Avast, виявлено, що зловмисне програмне забезпечення приховано щонайменше у 28 розширеннях для деяких із найпопулярніших платформ в Інтернеті, таких як Facebook, Instagram і Vimeo. У своєму прес-релізі Avast поділився інформацією про те, як користувачі повідомили, що ці розширення можуть маніпулювати їхньою роботою в Інтернеті за допомогою шкідливого коду в розширенні на основі Javascript. Кожного разу, коли користувач натискав посилання, він надсилав інформацію на контрольний сервер зловмисника

за зламаною URL-адресою, перш ніж відправляти його на веб-сайт, який він насправді хотів би відвідати.

У деяких випадках кіберзлочинці також видають себе за законні програми безпеки, щоб обманом змусити вас натиснути їхні посилання. У 2023 році хакери створили спливаюче вікно з повідомленням про те, що «ваш пристрій заражено вірусом» або «термін дії захисту від вірусів закінчився», схоже на бренд антивіруса McAfee. Використовуючи бренди справжніх охоронних компаній, хакери обманом змусили користувачів встановити клоновану програму на їхні пристрої.

Зміни в налаштуваннях системи

Хоча певно є налаштування ПК з Windows, які вам, імовірно, слід змінити, неприємно, коли це робить хтось інший без вашої згоди. Насправді хакери використовують зловмисне програмне забезпечення, щоб діяти як бекдор, щоб проникнути у ваш комп’ютер. Серед багатьох налаштувань, які хакери намагатимуться змінити за допомогою зловмисного програмного забезпечення, CyberTriage стверджує, що вони, ймовірно, включатимуть відключення програмного забезпечення для виявлення, щоб запобігти знаходженню, увімкнення віддаленого доступу або відключення резервного копіювання, щоб запобігти відновленню.

У більш запущених випадках хакери також змінять рівні аудиту, щоб зменшити кількість журналів і активно вимкнути облікові записи, щоб запобігти доступу спеціалістів з кібербезпеки до системи. CyberTriage також ділиться тим, що зловмисне програмне забезпечення може встановлювати зловмисні кореневі сертифікати шифрування, які можуть змусити вашу операційну систему подумати, що зловмисне програмне забезпечення має законний дозвіл на запуск. Завдяки цьому зловмисники можуть видати себе за вас чи іншого адміністратора та спричинити хаос на вашому комп’ютері.

Збільшене використання ЦП

У деяких випадках надзвичайно високе використання ЦП може свідчити про зараження шкідливим програмним забезпеченням. Коли ви не використовуєте програмне забезпечення або не завантажуєте веб-сторінки, Lifewire стверджує, що

нормальне використання ЦП або «центрального процесора» має становити приблизно від 1% до 5%. Однак різні типи зловмисного програмного забезпечення можуть використовувати ваш недостатньо завантажений ЦП без вашої згоди різними способами, зокрема для майнінгу криптовалюти.

За даними Check Point Software, зловмисне програмне забезпечення для майнінгу криптовалют заражає комп'ютер і використовує його для пошуку блоків криптовалюти. визначає цю практику, яка називається «видобутком за кермом», Malwarebytes як «частина коду JavaScript вбудована у веб-сторінку для виконання майнінгу криптовалюти на комп'ютерах користувачів, які відвідують цю сторінку».

У 2018 році тисячі веб-сайтів були скомпрометовані за допомогою програмного забезпечення для майнінгу криптовалют, включаючи веб-сайти уряду США та Великобританії через сторонній плагін, розроблений Texthelp для допомоги користувачам із вадами зору під назвою «Browsealoud». Для цього типу зловмисного програмного забезпечення нічого не підозрюючі відвідувачі цих законних веб-сайтів відчули раптовий сплеск використання ЦП, коли їхні веб-переглядачі були відкриті.

Щоб перевірити використання ЦП на наявність будь-якої незвичної діяльності в Windows, одночасно натисніть Ctrl+Shift+Esc. У лівому стовпці виберіть Продуктивність > ЦП. Для користувачів Mac ви можете переглянути монітор активності GPU, перейшовши до монітора активності. Для цього запустіть Spotlight і знайдіть «Монітор активності». Потім на панелі меню виберіть «Вікно» > «Історія ЦП». Обидва покажуть, який відсоток енергії використовує ваш браузер, який має бути менше 10%.

Незрозумілі файли або програми

У 2021 році кіберзлочинці використовували сповіщення на екрані, щоб обманом змусити користувачів Android встановити шпигунське програмне забезпечення зі стороннього магазину на їхні мобільні телефони. Маскуючись під легітимне оновлення системи, дослідники безпеки Zimperium стверджували, що після встановлення розширеного шкідливого програмного забезпечення Android

воно може отримати доступ до таких даних, як ваші повідомлення, вміст буфера обміну та навіть записувати аудіо та дзвінки.

Відомо навіть, що хакери користуються людьми, які хочуть завантажити операційні системи Windows. У 2022 році компанія HP, присвячена дослідженню загроз, опублікувала звіт про зловмисне програмне забезпечення під назвою «RedLine Stealer», яке поширювалося хакерами у вигляді підробленого інсталятора Windows 11. Користуючись підробленим веб-сайтом, HP згадує, що він переконав користувачів завантажити файл під назвою «Windos11InstallationAssistant.zip», стиснутий розмір якого становив лише 1,5 МБ.

Після того, як люди, які нічого не підозрюють, запустили програму, HP стверджує, що зловмисне програмне забезпечення продовжило завантаження та встановлення корисного навантаження, яке здатне збирати кілька точок даних; включаючи дані кредитної картки, паролі та ключі до їхніх криптовалютних гаманців.

Якщо на вашому комп'ютері раптово з'явилося нове програмне забезпечення, яке ви не пам'ятаєте встановлювати, варто спробувати з'ясувати, коли і як це сталося. Якщо ви помітили, що воно з’явилося після того, як ви завантажили програму з неофіційного веб-сайту, ви можете діяти так, ніби ви вже заразилися зловмисним програмним забезпеченням, і не вводити конфіденційну інформацію на своєму пристрої, доки проблему не буде вирішено». ***(Quina Baterna. 6 Signs Your Computer Could Be Infected With Malware // Static Media (https://www.slashgear.com/1460292/signs-computer-infected-malware/). 04.12.2023).***

***

«Згідно з тривожним викриттям платформи боротьби з шахрайством Arkose Labs, близько 73% інтернет-трафіку веб-сайтів і додатків, проаналізованого в період з січня по вересень 2023 року, пов’язано з ботами, які займаються зловмисними діями. Це відкриття викликає дискусії про значну втрату цінних ресурсів, спричинену такими мерзенними діями.

У третьому кварталі 2023 року спостерігалося домінування п’яти основних категорій шкідливих дій ботів, включаючи захоплення облікових записів, сканування, створення підроблених облікових записів, керування обліковими записами та зловживання в продуктах. Це подібно до другого кварталу, за помітним винятком зловживань у продукті, які втручалися під час тестування карток.

Серед категорій шахрайство з SMS-дзвінками зазнало найвищого квартального зростання, яке зросло на приголомшливі 2141% у третьому кварталі порівняно з попереднім 2. Не менш заслуговує на увагу 160% збільшення кількості атак на кол-центри підтримки клієнтів за той самий період. Збір даних, який мав найбільший сплеск з першого по другий квартал 2023 року на 432%, підкреслює динамічний характер цих шкідливих дій.

Arkose Labs повідомила про зростання атак інтелектуальних ботів на 291% з першого кварталу до другого. Цей сплеск пов’язаний з використанням складних методів, включаючи машинне навчання та ШІ, які дозволяють цим роботам імітувати людську поведінку з підвищеною адаптивністю. У випадках, коли штучний інтелект і технології не справляються, кіберзлочинці вдаються до керованих людьми шахрайських ферм для здійснення своїх атак. Шахрайські операції переважно виявляються в Бразилії, Індії, Росії, В’єтнамі та на Філіппінах.

Зростаюча тенденція до атак шкідливих ботів свідчить про те, що кіберзлочинці вважають такий спосіб роботи дуже прибутковим. Очікується, що інтеграція ефективного ШІ погіршить ситуацію, викликаючи занепокоєння щодо ефективності поточних механізмів захисту. Кілька місяців тому ми повідомляли, що Microsoft Bing Chat рекомендує рекламу зловмисного програмного забезпечення, яке спрямовує користувачів на шкідливі веб-сайти замість того, щоб фільтрувати їх.

Хоча поширеність шкідливих ботів викликає занепокоєння, важливо визнати існування корисних ботів, які роблять позитивний внесок в онлайн-екосистему. Багато з них виконують такі корисні функції, як індексація веб-сайтів для пошукових систем, виконання базових завдань обслуговування клієнтів і керування

соціальними мережами». ***(Kunal Khullar. Malicious bots make up 73% of internet traffic, report says // Digital Trends Media Group (https://www.digitaltrends.com/computing/over-70-percent-internet-malicious-activity/?utm_source=flipboard&utm_content=DigitalTrends%2Fmagazine%2FDigital+Trends%3A+Tech+for+the+Way+We+Live). 01.12.2023).***

***

«Дослідники безпеки виявили нову мультиплатформенну загрозу зловмисного програмного забезпечення під назвою NKAbuse, яка використовує небачену раніше тактику для викрадення своїх жертв.

У своєму звіті Глобальна група реагування на надзвичайні ситуації Kaspersky каже, що зловмисне програмне забезпечення використовує технологію NKN – протокол підключення до однорангової мережі та екосистему на базі блокчейну, яка отримала свою назву від абревіатури «New Kind of Network».

Зловмисне програмне забезпечення також використовує Go, мову програмування, яка набирає популярності у світі шкідливого програмного забезпечення та кібератак.

Kaspersky припускає, що NKAbuse наразі націлений на робочі столи Linux. Однак, оскільки він може інфікувати системи MISP і ARM, він також може становити загрозу для пристроїв IoT.

NKAbuse використовує 60 000 офіційних вузлів NKN, щоб здійснювати лавинні атаки та підключатися до серверів C2.

За словами Касперського, NKAbuse містить великий арсенал DDoS-атак, але він також містить численні функції, які перетворюють його на потужний бекдор або троян віддаленого доступу (RAT).

Аналітики додали: «Використання в ньому технології блокчейн забезпечує як надійність, так і анонімність, що вказує на потенціал для цього ботнету, який буде постійно розширюватися з часом, мабуть, позбавлений ідентифікованого центрального контролера».

Наразі було помічено, що NKAbuse заражає пристрої в Колумбії, Мексиці та В'єтнамі через доставку особою, яка використовує вразливість, оскільки вважається, що немає функції саморозповсюдження.

Російська команда також зібрала докази того, що атака використовує стару вразливість (CVE-2017-5638), націленою на фінансову компанію.

Вплив NKAbuse на жертв може включати різноманітні ускладнення, включаючи компрометацію та/або крадіжку даних, віддалене адміністрування та контроль, збереження й маніпуляції системою, а також DDoS-атаки.

Використання технології блокчейн також свідчить про те, що NKAbuse може мати потенціал для розширення з часом, розкриваючи потенціал інтеграції ботнету». ***(Craig Hale. Blockchain systems hijacked for DDoS attacks by seemingly all-new malware tactics // Future US, Inc. (https://www.techradar.com/pro/security/blockchain-systems-hijacked-for-ddos-attacks-by-seemingly-all-new-malware-tactics?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 15.12.2023).***

***

«Експерти попереджають, що користувачів Windows і macOS атакують JaskaGO, рідкісний екземпляр кросплатформного шкідливого програмного забезпечення, здатного до викрадання даних, розгортання шкідливого програмного забезпечення на другому етапі тощо.

За даними AT&T Alien Labs, які виявили загрозу, JaskaGO написаний на мові програмування Go та оснащений «широким набором команд із свого сервера командування та керування (C&C)».

Хоча способи доставки відрізняються, дослідники кажуть, що для користувачів Apple JaskaGo імітує інсталятори CapCut і AnyConnect, зокрема.

Відстеження буфера обміну для криптовалютних платежів

Після встановлення зловмисне програмне забезпечення спочатку виконає тести, щоб перевірити, чи працює воно в пісочниці. Якщо він виявляє, що його

відкривають у середовищі віртуальної машини, він виконуватиме безглузді завдання, щоб уникнути позначення зловмисного. Якщо, з іншого боку, він вважає середовище законною ціллю, він захопить системні дані та спробує підключитися до свого C2.

Зловмисне програмне забезпечення здатне до різноманітних дій, включаючи виконання команд оболонки, перерахування запущених процесів і завантаження додаткових шкідливих програм. Він також може відстежувати буфер обміну для адрес гаманців криптовалюти.

Зазвичай користувачі криптовалюти здійснюють транзакції, копіюючи та вставляючи адресу одержувача (оскільки це довгий рядок, здавалося б, випадкових символів, які майже неможливо запам’ятати) у програму чи службу. Відстежуючи буфер обміну, зловмисне програмне забезпечення може ввести адресу зловмисника, змусивши жертву вставити неправильний рядок і відправити кошти на контрольований зловмисником гаманець.

«У macOS JaskaGO використовує багатоетапний процес для встановлення стійкості в системі», — сказав TheHackerNews дослідник безпеки Офер Каспі.

На даний момент дослідники AT&T Alien Labs не знають, як JaskaGo доставляється більшості користувачів, і чи задіяно якийсь фішинг або соціальну інженерію. На даний момент вони також не можуть оцінити кількість заражених пристроїв.

«JaskaGO сприяє зростанню тенденції розробки зловмисного програмного забезпечення з використанням мови програмування Go», — додав Каспі. «Go, також відомий як Golang, відомий своєю простотою, ефективністю та крос-платформенними можливостями. Його простота використання зробила його привабливим вибором для авторів шкідливих програм, які прагнуть створювати різноманітні та складні загрози». ***(Sead Fadilpašić. Windows and macOS targeted by new Go-based malware // Future US, Inc. (https://www.techradar.com/pro/security/windows-and-macos-targeted-by-new-go-based-***

malware?utm_source=flipboard&utm_content=pcesari%2Fmagazine%2FMobile+Tech+Weekly). 20.12.2023).

***

Програми-вимагачі

«Кіберзлочинці, відомі як Twisted Spider (AKA Storm-0216), використовували служби Storm-1044, які інфікували цільові кінцеві точки за допомогою трояна початкового доступу під назвою DanaBot. Потім Twisted Spider використовував би цей доступ для розгортання програми-вимагача CACTUS.

У повідомленні в Twitter дослідники безпеки Microsoft повідомили, що Storm-0216 відомий тим, що використовує інфраструктуру QakBot для зараження, але оскільки правоохоронні органи припинили цю операцію минулого літа, група була змушена перейти на іншу платформу.

«Схоже, що поточна кампанія Danabot, яку вперше спостерігали в листопаді, використовує приватну версію шкідливого програмного забезпечення для крадіжки інформації замість пропозиції шкідливого програмного забезпечення як послуги», — пояснили в компанії. Як було додано, DanaBot запропонував своїм партнерам практичну роботу з клавіатурою.

Само шифрування

Після того, як група Storm-1044 викраде необхідні облікові дані для входу, вони будуть переміщатися по всій мережі та через кінцеві точки через спроби входу RDP. Після встановлення початкового доступу група передала його Twisted Spider, який потім заразив кінцеві точки програмою-вимагачем CACTUS.

Здається, CACTUS швидко стає вибором для багатьох операторів програм-вимагачів. Минулого тижня дослідники з Arctic Wolf попередили, що хакери використали три вразливості в аналітичному рішенні Qlik Sense, щоб розгорнути цей конкретний варіант і викрасти конфіденційні дані компанії.

У травні дослідники Kroll виявили, що програмне забезпечення-вимагач має унікальний метод ухилення від захисту кібербезпеки: «CACTUS фактично шифрує себе, ускладнюючи його виявлення та допомагаючи йому уникнути антивірусних програм і інструментів моніторингу мережі», — Лорі Яконо, заступник керуючого директора з кіберризиків компанії Кролл, сказав Bleeping Computer.

Cactus — відносно новий учасник програми-вимагача, вперше його помітили в березні цього року. Він має звичайний спосіб дії, крадіжку конфіденційних даних і систем шифрування, щоб пізніше вимагати платіж у криптовалюті в обмін на ключ дешифрування та збереження конфіденційності даних». ***(Sead Fadilpašić. Watch out, there's a new malvertising scheme spreading dangerous ransomware // Future US, Inc. (https://www.techradar.com/pro/security/watch-out-theres-a-new-malvertising-scheme-spreading-dangerous-ransomware?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 04.12.2023).***

***

«Міністерство охорони здоров'я та соціальних служб США («HHS») Управління з громадянських прав («OCR») уклало своє перше врегулювання потенційних порушень Закону про перенесення та підзвітність медичного страхування («HIPAA»), що виникли внаслідок атаки програм-вимагачів, сигналізуючи OCR продовжує приділяти увагу безпеці даних.

31 жовтня 2023 року OCR оголосив про першу у своєму роді угоду щодо програм-вимагачів із Doctors' Management Services («DMS»), компанією з управління практикою, яка діє як діловий партнер кількох охоплених організацій, за ймовірні порушення HIPAA.

Що сталося

У квітні 2019 року OCR розпочав розслідування звіту про порушення від DMS, у якому зазначено, що приблизно 206 695 осіб постраждали від атаки програм-вимагачів. Хоча перший несанкціонований доступ до його мережі відбувся 1 квітня 2017 року, DMS не виявив це вторгнення до 24 грудня 2018 року,

після того як програми-вимагачі вже зашифрували його файли. На основі свого розслідування OCR стверджував, що DMS не:

Провести точний і ретельний аналіз ризиків, щоб оцінити потенційні ризики та вразливі місця, пов'язані з обробкою електронної захищеної інформації про здоров'я («ePHI») в організації;

Впровадити процедури для регулярного перегляду записів про діяльність інформаційної системи, таких як журнали аудиту, звіти про доступ і звіти про відстеження інцидентів безпеки; і

Впроваджувати та підтримувати відповідні політики та процедури для дотримання правил безпеки HIPAA.

Угода про дозвіл

Угода про врегулювання вимагає, щоб DMS сплатила 100 000 доларів США та запровадила трирічний план коригувальних дій, згідно з яким DMS має, серед іншого:

Оновити аналіз ризиків за умови схвалення HHS;

Розробити повний перелік усіх своїх середовищ, які містять або зберігають ePHI;

Оновити план управління ризиками для всього підприємства;

Переглядати свої письмові політики та процедури, як це вказано в аналізі ризиків і затверджено HHS;

Забезпечити навчання робочої сили HIPAA; і

Надайте HHS щорічні звіти про навчання з підсумковим дотриманням.

Велика картина

Уклавши цю першу у своєму роді угоду про вирішення проблеми, OCR сигналізує про свою готовність притягнути до відповідальності жертв атак програм-вимагачів, якщо OCR визнає, що невідповідність організації є фактором, що сприяє атаці. Подібним чином федеральні агентства все частіше перевіряють організації на наявність порушень, пов'язаних із медичною інформацією. Лише цього року Федеральна торгова комісія вжила свої перші примусові заходи щодо порушення Правил сповіщення про порушення здоров'я, а HHS опублікував звіт, у

якому зазначено, що кібербезпека залишається головним пріоритетом. Ділові партнери, охоплені юридичні особи та інші підприємства повинні продовжувати ретельно впроваджувати відповідні засоби контролю для захисту інформації про здоров'я». ***(Alexis S. Gilroy, Lisa M. Ropple, Claire E. Castles, Jennifer C. Everett, Kristen Pollock McDonald and Mauricio F. Paez. HHS Enters Into First-Ever Ransomware Resolution Agreement and Corrective Action Plan // Jones Day (https://www.jonesday.com/en/insights/2023/12/hhs-enters-into-firstever-ransomware-resolution-agreement-and-corrective-action-plan). 12.2023).***

***

«Міністерство юстиції США (DOJ) повідомляє, що ФБР створило інструмент дешифрування, який допоміг йому повернути дані понад 500 жертв програм-вимагачів у рамках багатонаціональних заходів правоохоронних органів. У ньому також написано, що бюро вилучило «кілька веб-сайтів», якими керує банда програм-вимагачів ALPHV / Blackcat.

Однак Bleeping Computer повідомляє, що сьогодні вдень ALPHV / Blackcat стверджували, що відновили контроль над своїм сайтом і що ФБР мало ключі дешифрування лише для приблизно 400 компаній, залишивши понад 3000 жертв, чиї дані залишаються зашифрованими. Повідомляється, що банда також заявила, що більше не обмежує афілійованим особам, які використовують програмне забезпечення-вимагач, атакувати критичну інфраструктуру, включаючи лікарні та атомні електростанції.

За даними Міністерства юстиції, «за останні 18 місяців ALPHV/Blackcat став другим найпоширенішим варіантом програми-вимагача як послуги у світі на основі сотень мільйонів доларів викупу, сплаченого жертвами по всьому світу. » У цій моделі банда відповідає за створення та оновлення програм-вимагачів, а філії знаходять цілі та здійснюють атаки, а потім ділять прибуток.

Влітку банда також заявила про злом Reddit, вимагаючи 4,5 мільйона доларів за повернення даних, а також за крадіжку даних від видавця ігор Namco Bandai. Ближче до кінця літа банда взяла на себе відповідальність за закриття кількох

казино та готелів MGM Resorts у Лас-Вегасі, штат Невада». ***(Wes Davis. Ransomware gang 'unseizes' its site and issues new threats after FBI takedown // Vox Media, LLC (https://www.theverge.com/2023/12/19/24008093/alphv-blackcat-ransomware-gang-site-seized-fbi-doj). 20.12.2023).***

***

«12 грудня Rhysida, група програм-вимагачів, оголосила, що взяла 1,67 терабайт даних — понад 1,3 мільйона файлів — із Sony Insomniac Games і запросила 2 мільйони доларів. Тепер минув тижневий термін для Insomniac Games, щоб заплатити Rhysida, і група виконала свою погрозу оприлюднити викрадену інформацію, повідомляє Cyber Daily.

Дані включають внутрішні документи відділу кадрів, скріншоти розмов співробітників у Slack тощо, але головна увага приділяється відеогрі Wolverine, яка ще не була випущена. Опубліковані файли містять деталі про дизайн рівнів, персонажів і справжні скріншоти з гри. Існує також підписана видавнича угода між Sony та Marvel, яка викладає три майбутні ігри про Людей Ікс, першою з яких є Росомаха, а дві інші досі не називаються. Однак у ньому деталізується, що Sony, яка планує витратити 120 мільйонів доларів на гру, має випустити Wolverine до 1 вересня 2025 року, а інші — до кінця 2029 та 2033 років відповідно.

Rhysida стверджує, що групі знадобилося лише 20-25 хвилин, щоб отримати адміністратора домену, і що гроші були їхньою єдиною мотивацією. «Ми знали, що розробники, які створюють подібні ігри, будуть легкою мішенню», — сказав Cyber Daily представник Rhysida. «Sony почала розслідування, але краще було б на задньому дворі».

Примітно, що початкове повідомлення Rhysida про викуп дозволяло будь-кому робити ставки на дані, а не лише Insomniac Games, і, здається, частину з них було куплено. Група програм-вимагачів заявила, що всі непродані дані були опубліковані, але лише 98 відсотків викраденої інформації є загальнодоступними. Rhysida обумовила, що будь-які придбані дані не можна перепродувати, але хто знає, чи будуть нові власники дотримуватися цього правила.

Rhysida була спрямована лише на Insomniac Games у Sony, але в травні окрема атака отримала доступ до особистих даних 6800 поточних і колишніх співробітників. Атака, яку взяла на себе група програм-вимагачів CLOP, стала загальновідомою в жовтні». ***(Sarah Fielding. Hackers release footage from upcoming Wolverine game and 1.3 million other stolen files // Yahoo (https://www.engadget.com/insomniac-games-hackers-leak-13-million-files-after-demanding-2-million-ransom-102134429.html?guccounter=1&guce_referrer=aHR0cHM6Ly9uZXdzLmdvb2dsZS5jb20v&guce_referrer_sig=AQAAAD9hTdt30BfEOgYSmUobo1VtzWXzth6zbVZUvWuErW5b5nalmAm_Y2sipSo4UmtCKcBJ2fg14vXLOvofhWv6969kpmB10vlmV_yJcMeBvkdXm8RpfFMrEVhhSN24zfc0dTXN7Q2_AFRRwrtx43wcqALXIXo_tQAvlYFqARStLAjA). 19.12.2023).***

***

«Вимагач Play, який з'явився приблизно півтора роки тому, на сьогоднішній день зробив жертвами близько 300 осіб, деякі з яких є організаціями критичної інфраструктури, йдеться в новій спільній заяві, опублікованій ФБР, CISA та Австралійським центром кібербезпеки Австралійського директорату зв'язку (Australian Signals Directorate's Australian Cyber Security Centre).

«З червня 2022 року група програм-вимагачів Play (також відома як Playcrypt) вплинула на широкий спектр підприємств і критичну інфраструктуру в Північній Америці, Південній Америці та Європі», — йдеться в повідомленні. «Станом на жовтень 2023 року ФБР було відомо про приблизно 300 постраждалих об’єктів, які ймовірно використовувалися програмами-вимагачами».

Незважаючи на те, що програми-вимагачі Play роблять те ж саме, що й інші оператори – крадуть і шифрують конфіденційні дані, у них є кілька унікальних функцій, повідомляє BleepingComputer. Наприклад, він спілкуватиметься зі своїми жертвами не через Tor, а скоріше електронною поштою. Крім того, він використовує спеціальний інструмент копіювання VSS, який допомагає

захоплювати файли, знайдені в тіньових томах, навіть якщо вони використовуються програмами під час шифрування.

Збереження безпеки

Серед відомих жертв — місто Окленд у Каліфорнії, місто Антверпен у Бельгії та гігант хмарних обчислень Rackspace.

Спільна консультація також закликає організації захищати свої кінцеві точки, дотримуючись найкращих практик безпеки. До них належать підтримка всього програмного та апаратного забезпечення в актуальному стані та забезпечення якнайшвидшого застосування всіх термінових виправлень безпеки, які зазвичай усувають відомі та зловживані вразливості.

Крім того, компанії закликають підтримувати свої паролі свіжими та надійними, а також розгортати багатофакторну автентифікацію (MFA), де це можливо.

Нарешті, компаніям рекомендується навчати своїх співробітників про небезпеку фішингу та соціальної інженерії. Зрештою, більшість кібератак починається з, здавалося б, нешкідливого електронного листа або миттєвого повідомлення в одній із найпопулярніших мереж сьогодні (LinkedIn, X та інші), які доставляють зловмисне програмне забезпечення, яке надає зловмисникам доступ до системи». ***(Sead Fadilpašić. FBI reveals Play ransomware has hit hundreds of businesses, including critical firms // Future US, Inc. (https://www.techradar.com/pro/security/fbi-reveals-play-ransomware-has-hit-hundreds-of-businesses-including-critical-firms?utm_source=flipboard&utm_content=other). 19.12.2023).***

***

«Згідно зі звітом Verizon про розслідування витоку даних (DBIR 2023), атаки на комунальні підприємства та сектор видобутку сировини зростають. Програми-вимагачі є основною загрозою. Інформаційна безпека залишається постійною проблемою для компаній

Комунальні послуги та видобувний сектор сировини стали важливими для національних економік, особливо через зростання витрат, пов’язаних зі зміною клімату та міжнародною напруженістю.

Зважаючи на їхню важливість, не дивно, що ці сектори стають дедалі більшою мішенню для кіберзлочинців. Вони розглядають компанії в цьому секторі як потенційно прибутковий бізнес, враховуючи їхню готовність платити значні суми, щоб уникнути договірних збитків або мільйонних штрафів через перебої в наданні послуг, спричинені кіберзломами.

Рівень безпеки все ще низький

В останні роки компанії присвятили себе покращенню своєї кібербезпеки шляхом впровадження передових рішень, створення планів реагування на атаки та навчання співробітників.

Однак, незважаючи на зусилля, дані вказують на те, що шлях до задовільного рівня безпеки ще далекий.

Нещодавні докази підтверджують це Звіт про розслідування витоку даних (DBIR 2023) від Verizon, який висвітлює проблеми ланцюжка поставок у сфері кібербезпеки.

Програми-вимагачі – основна загроза

Основною загрозою у сфері кібербезпеки є програмне забезпечення-вимагач, тип шкідливого програмного забезпечення, призначеного для блокування доступу до системи або даних, вимагаючи оплати для відновлення доступу або видачі ключа дешифрування.

Згідно з DBIR 2023, програми-вимагачі залишаються однією з основних форм атак у секторі, на них припадає 32% порушень, що значно перевищує загальний середній показник, який становить близько 24%.

Понад 80% порушень походять від системних вторгнень, атак веб-додатків і різноманітних помилок, у той час як порушення, спричинені соціальною інженерією, зменшуються.

До скомпрометованої інформації в основному входять особисті дані (50%), потім дані компанії (33%).

Виклик для компаній

Дані показують, що цей сектор залишається однією з улюблених цілей для кіберзлочинців, які розуміють його стратегічне значення на глобальному рівні. Завдання для компаній полягає в тому, щоб постійно оновлювати свої плани безпеки, щоб протистояти дедалі складнішим і небезпечнішим атакам.

Лише завдяки безперервній відданості запобіганню кіберзагрозам і управлінню ними компанії в секторі зможуть підтримувати безпеку своєї діяльності та сприяти глобальній економічній стабільності». ***(Matthew Lirosi. Cybersecurity: utilities and the extractive sector are increasingly attractive targets for cybercriminals // FIRST online (https://www.firstonline.info/en/cybersecurity-utilities-and-the-extractive-sector-are-increasingly-attractive-targets-for-cybercriminals/). 22.12.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Інтерпол, міжнародна поліцейська організація, заарештувала майже 3500 осіб, імовірно причетних до кіберзлочинності, у ході широкомасштабної операції, оголошеної у вівторок. Повідомляється, що було арештовано активи в 34 країнах на суму 300 мільйонів доларів. Операція Haechi IV заблокувала понад 80 000 підозрілих банківських рахунків і попередила урядовців про нові види шахрайства з використанням ШІ та підроблених NFT.

«Вилучення 300 мільйонів доларів США є приголомшливою сумою та чітко ілюструє стимули сьогоднішнього вибухового зростання транснаціональної організованої злочинності», – сказав Стівен Кавана, виконавчий директор поліцейських служб Інтерполу. «Це величезне накопичення незаконних багатств є серйозною загрозою глобальній безпеці та послаблює економічну стабільність націй у всьому світі».

Останнім часом у новинах домінували зловмисні хакерські атаки, оскільки за даними операції Інтерполу цього року кількість арештів зросла на 200%. За даними Wall Street Journal у вівторок, Comcast зазнала витоку даних, що вплинуло на 36 мільйонів облікових записів, потенційно скомпрометувавши кожен обліковий запис Xfinity. У вівторок банда програм-вимагачів Rhysida також викрила майбутню відеогру Marvel від PlayStation разом із сканами паспортів розробників ігор. А лише минулого місяця 23andMe втратив біодані 6,9 мільйонів клієнтів через хакерську атаку. У той час, коли злом даних стає все гіршим, приємно чути, що кіберзлочинців у світі стало на 3500 менше.

За даними агентства, більшість арештів були пов'язані з інвестиційним шахрайством, компрометацією бізнес-електронної пошти та шахрайством в електронній комерції. Проте Haechi IV попередив країни-учасниці про дві нові тактики, які використовують кіберзлочинці. Інтерпол виявив, що створений штучним інтелектом контент кілька разів використовувався для шахрайства з видаванням себе за іншу особу, сексуального онлайн-шантажу та інвестиційного шахрайства по всій території Сполученого Королівства. Технологія клонування голосу часто використовувалася, щоб видати себе за людей, знайомих жертвам.

Продаж NFT був ще однією тактикою шахрайства, яку ідентифікував Інтерпол, широко поширеною в Кореї, у якій жертвам обіцяли високу віддачу від їхніх інвестицій. Однак ці обманні криптопроекти часто залишають після початкових інвестицій. Обидва ці шахрайства використовують нові технології, які використовують обмежене розуміння людей цього питання. Кавана каже, що зростання арештів на 200% свідчить про «постійну проблему кіберзлочинності, що нагадує нам бути пильними та продовжувати вдосконалювати нашу тактику боротьби з онлайн-шахрайством». ***(Maxwell Zeff. INTERPOL Arrests 3,500 Suspects in Sweeping Cybercrime Operation // gizmodo (https://gizmodo.com/interpol-arrest-3-500-cybercrime-operation-300-million-1851113003). 19.12.2023).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Експерти попереджають, що тисячі репозиторіїв модулів Go на GitHub уразливі до атаки, відомої як викрадення репозиторію або повторне захоплення.

У цій атаці хакер зловживає тим фактом, що розробник змінив назву свого облікового запису або взагалі його видалив. Вони зловживають ним, створюючи обліковий запис і однойменний репозиторій, а потім додаючи до нього шкідливий код. Отже, це дозволяє їм влаштовувати нищівні атаки на ланцюг поставок, оскільки розробники можуть інтегрувати цей код, не знаючи, що це зловмисний імітатор.

Згідно з новим звітом дослідників кібербезпеки з VulnCheck, існує понад 9000 сховищ, уразливих до повторного захоплення через зміну імені користувача GitHub, і 6000 сховищ уразливих через видалення облікового запису. Разом вони містять принаймні 800 000 версій модулів Go.

Залишаючись пильним

Аналізуючи попередження, The Hacker News сказав, що модулі, написані на Go, «особливо сприйнятливі» до повторного захоплення, оскільки вони децентралізовані та публікуються на платформах контролю версій, таких як GitHub або BitBucket.

«Тоді будь-хто може вказати дзеркалу модуля Go і pkg.go.dev кешувати деталі модуля», — сказав виданню Джейкоб Бейнс, головний технічний директор VulnCheck. «Зловмисник може зареєструвати щойно невикористане ім’я користувача, скопіювати репозиторій модулів і опублікувати новий модуль на proxy.golang.org і go.pkg.dev».

GitHub вже намагався вирішити цю проблему за допомогою функції під назвою «відмова від простору імен популярного репозиторія». Це не дозволяє

користувачам створювати сховища з іменами вилучених просторів імен, які були клоновані більше 100 разів у минулому. Однак VulnCheck стверджує, що ця функція не дуже корисна, оскільки модулі Go кешуються дзеркалом модулів, а це означає, що популярні модулі Go можуть мати менше ніж 100 клонів і, отже, все ще чутливі до повторного захоплення.

«На жаль, пом'якшення всіх цих повторних захоплень — це те, що доведеться взяти на себе Go або GitHub», — сказав Бейнс. «Стороння сторона не може обґрунтовано зареєструвати 15 000 облікових записів GitHub. До того часу розробникам Go важливо знати про модулі, які вони використовують, і про стан сховища, з якого походять модулі». ***(Sead Fadilpašić. Thousands of Go module repositories on GitHub are vulnerable to attack // Future US, Inc. (https://www.techradar.com/pro/security/thousands-of-go-module-repositories-on-github-are-vulnerable-to-attack?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 06.12.2023).***

****

«Недоліки підвищення привілеїв є найпоширенішою вразливістю, якою користуються корпоративні інсайдери під час здійснення несанкціонованих дій у мережах із зловмисною метою або шляхом завантаження ризикованих інструментів у небезпечний спосіб.

Звіт Crowdstrike, заснований на даних, зібраних у період з січня 2021 року по квітень 2023 року, показує, що внутрішні загрози зростають і що використання недоліків ескалації привілеїв є значним компонентом несанкціонованої діяльності.

Згідно зі звітом, 55% інсайдерських загроз, зареєстрованих компанією, покладаються на експлойти підвищення привілеїв, а решта 45% мимоволі створюють ризики, завантажуючи або зловживаючи образливими інструментами.

Інсайдери-шахраї зазвичай обертаються проти свого роботодавця через те, що їм надали фінансові стимули, на зло чи через розбіжності з їхніми керівниками.

CrowdStrike також класифікує інциденти як інсайдерські загрози, якщо вони не є зловмисними атаками на компанію, наприклад використання експлойтів для встановлення програмного забезпечення або проведення тестування безпеки.

Однак у цих випадках, хоча вони не використовуються для атаки на компанію, вони зазвичай використовуються в ризикований спосіб, потенційно запроваджуючи загрози або зловмисне програмне забезпечення в мережу, якими зловмисники можуть зловживати.

Crowdstrike виявив, що атаки, розпочаті з цільових організацій, коштують у середньому 648 000 доларів США за шкідливі інциденти та 485 000 доларів США за нешкідливі інциденти. Ці цифри можуть бути ще вищими у 2023 році.

Окрім значних фінансових витрат від внутрішніх загроз, Crowdstrike підкреслює непрямі наслідки шкоди бренду та репутації.

Типова інсайдерська атака

Crowdstrike пояснює, що використання вразливостей ескалації привілеїв для отримання адміністративних привілеїв має вирішальне значення для багатьох інсайдерських атак, оскільки в більшості випадків шахраї-інсайдери починають із низькорівневого доступу до свого мережевого середовища.

Більш високі привілеї дозволяють зловмисникам виконувати такі дії, як завантаження та встановлення неавторизованого програмного забезпечення, стирання журналів або навіть діагностування проблем на комп’ютері за допомогою інструментів, які потребують прав адміністратора.

Згідно зі спостереженнями CrowdStrike, найбільше використовуваних недоліків для локальної ескалації привілеїв зловмисниками є наступні:

CVE-2017-0213 : недолік Windows дозволяє підвищувати привілеї через використання інфраструктури COM.

CVE-2022-0847 (DirtyPipe) : недолік керування операціями каналу ядра Linux.

CVE-2021-4034 (PwnKit) : недолік Linux, що впливає на системну службу Polkit.

CVE-2019-13272 : уразливість Linux, пов’язана з неправильним використанням привілеїв користувачів у процесах ядра.

CVE-2015-1701 : помилка Windows, пов’язана з драйвером режиму ядра «win32k.sys» для несанкціонованого виконання коду.

CVE-2014-4113 : також націлено на «win32k.sys», але передбачає інший метод використання.

Вищевказані недоліки вже перераховані в каталозі відомих використаних уразливостей CISA (KEV), оскільки вони історично використовувалися в атаках зловмисниками.

Навіть якщо в системі було виправлено ці недоліки, інсайдери можуть отримати підвищені привілеї іншими способами, як-от помилки викрадення DLL у програмах, які працюють із підвищеними привілеями, незахищені дозволи файлової системи чи конфігурації служб або атаки Bring Your Own Vulnerable Driver (BYOVD).

Crowdstrike бачив численні випадки використання CVE-2017-0213, що вплинуло на роздрібну компанію в Європі, де співробітник завантажив експлойт через WhatsApp, щоб встановити uTorrent і грати в ігри. Ще один випадок стосується звільненого працівника медіа-компанії в США

Експлуатацію PwnKit спостерігав співробітник австралійської технологічної компанії, який намагався отримати права адміністратора для вирішення проблем з комп’ютером.

Приклад використання CVE-2015-1701 стосується співробітника американської технічної фірми, який намагався обійти існуючі засоби керування, щоб встановити неавторизовану віртуальну машину Java.

Хоча майже всі ці випадки внутрішньої загрози не вважаються зловмисними атаками, вони створюють ризик, змінюючи спосіб роботи пристрою або потенційно запускаючи шкідливі чи небезпечні програми в мережі.

Внутрішні помилки створюють ризик

Майже половина інсайдерських інцидентів, зафіксованих Crowdstrike, стосуються ненавмисних нещасних випадків, як-от тестування експлойтів, що виходить з-під контролю, використання образливих інструментів безпеки без належних заходів захисту та завантаження неперевіреного коду.

Наприклад, CrowdStrike каже, що деякі інциденти були спричинені професіоналами з безпеки, які тестували експлойти та набори експлойтів безпосередньо на робочій станції, а не через віртуальну машину, яка сегментована від решти мережі.

Аналітики повідомляють, що більшість подібних випадків стосується таких інструментів, як Metasploit Framework і ElevateKit, а вразливості, які найчастіше з'являються в результаті необережних дій, такі:

CVE-2021-42013 : уразливість проходження шляху на HTTP-сервері Apache 2.4.49 і 2.4.50.

CVE-2021-4034 (PwnKit) : Поза межами вразливості в системній службі Polkit.

CVE-2020-0601 : уразливість підробки в Windows CryptoAPI.

CVE-2016-3309 : Проблема з підвищенням привілеїв у ядрі Windows.

CVE-2022-21999 : уразливість щодо підвищення привілеїв у спулері друку Windows.

Впровадження цих недоліків у корпоративні мережі може збільшити загальний ризик безпеки, надаючи суб'єктам загрози, які вже мають точку опори в мережі, додаткові вектори для використання.

Однак, що ще важливіше, нерідко зловмисники створюють підроблені експлойти для підтвердження концепції або інструменти безпеки, які встановлюють шкідливе програмне забезпечення на пристрої.

Наприклад, у травні зловмисники поширювали фальшиві експлойти для підтвердження концепції Windows, які заражали пристрої бекдором Cobalt Strike.

Під час іншої атаки Rapid7 виявив, що зловмисники поширювали підроблені PoC для експлойтів нульового дня, які встановлювали зловмисне програмне забезпечення Windows і Linux.

В обох сценаріях встановлення підробленого експлойта на робочу станцію дозволить отримати початковий доступ до корпоративної мережі, що може призвести до кібершпигунства, крадіжки даних або атак програм-вимагачів». ***(Bill Toulas. Privilege elevation exploits used in over 50% of insider attacks // Bleeping***

Computer® LLC (https://www.bleepingcomputer.com/news/security/privilege-elevation-exploits-used-in-over-50-percent-of-insider-attacks/?utm_source=flipboard&utm_content=kuryakin%2Fmagazine%2FIn+Search+Of+The+Truth). 08.12.2023).

***

«Приховане багатофункціональне зловмисне програмне забезпечення Linux, яке заражало телекомунікаційні компанії, залишалося майже непоміченим протягом двох років, поки в четвер дослідники вперше не задокументували його.

Дослідники з охоронної фірми Group-IB назвали троян віддаленого доступу «Krasue» на честь нічного духа, зображеного у фольклорі Південно-Східної Азії, «що плаває в повітрі, без тулуба, лише її кишки звисають з-під підборіддя». Дослідники обрали таку назву, оскільки наявні на сьогоднішній день дані показують, що він майже виключно націлений на жертв у Таїланді та «становить серйозний ризик для критично важливих систем і конфіденційних даних, оскільки він здатний надати зловмисникам віддалений доступ до цільової мережі.

За словами дослідників:

Krasue — це троян для віддаленого доступу до Linux, який працює з 20 років і націлений переважно на організації в Таїланді.

Group-IB може підтвердити, що телекомунікаційні компанії були ціллю Krasue.

Зловмисне програмне забезпечення містить кілька вбудованих руткітів для підтримки різних версій ядра Linux.

Руткіт Krasue взято з відкритих джерел (3 руткіти Linux Kernel Module з відкритим кодом), як і у випадку з багатьма руткітами Linux.

Руткіт може підхопити системний виклик kill(), пов’язані з мережею функції та операції зі списком файлів, щоб приховати свою діяльність і уникнути виявлення.

Примітно, що Krasue використовує повідомлення RTSP (протокол потокової передачі в реальному часі), щоб служити замаскованим «живим пінгом», тактика, яку рідко можна побачити в дикій природі.

Це зловмисне програмне забезпечення для Linux, припускають дослідники Group-IB, розгортається на пізніших етапах ланцюжка атак, щоб зберегти доступ до хосту-жертви.

Імовірно, Krasue буде розгорнуто як частина ботнету або продано брокерами початкового доступу іншим кіберзлочинцям.

Дослідники Group-IB вважають, що Krasue створив той самий автор, що й троян XorDdos Linux, задокументований Microsoft у публікації в блозі від березня 2022 року, або кимось, хто мав доступ до вихідного коду останнього.

На етапі ініціалізації руткіт приховує свою присутність. Потім він перехоплює системний виклик kill(), функції, пов’язані з мережею, і операції зі списком файлів, тим самим приховуючи свою діяльність і уникаючи виявлення.

Дослідники поки що не змогли точно визначити, як встановлюється Krasue. Можливі вектори зараження включають використання вразливості, атаки з крадіжкою облікових даних або вгадуванням або мимовільне встановлення як троян, схований у файлі встановлення, або оновлення, видане за законне програмне забезпечення.

У Krasu є три руткіт-пакети з відкритим кодом:

Diamorphine

Suterusu

Rooty

Руткіти — це різновид зловмисного програмного забезпечення, яке приховує каталоги, файли, процеси та інші докази своєї присутності в операційній системі, у якій його встановлено. Перехоплюючи законні процеси Linux, зловмисне програмне забезпечення може призупинити їх у вибраних точках і вставити функції, які приховують його присутність. Зокрема, він приховує файли та каталоги, що починаються з імен «auwd» і «vmware_helper» у списках каталогів, а також приховує порти 52695 і 52699, через які відбувається зв’язок із серверами,

контрольованими зловмисниками. Перехоплення системного виклику kill() також дозволяє трояну пережити команди Linux, які намагаються перервати програму та завершити її роботу…

Окрім функцій руткіта, у Krasue є інсталяційний файл, який захищено всередині UPX, так званий пакувальник, який забезпечує криптографічну оболонку навколо основного виконуваного файлу, що може перешкоджати виявленню антивірусним програмним забезпеченням. Повідомлення Group-IB надає індикатори компрометації та цифрові характеристики для виявлення заражених систем». ***(Dan Goodin. Stealthy Linux rootkit found in the wild after going undetected for 2 years // Condé Nast (https://arstechnica.com/security/2023/12/stealthy-linux-rootkit-found-in-the-wild-after-going-undetected-for-2-years/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 08.12.2023).***

***

«Приблизно на початку 1995 року невідома особа встановила програму для аналізу паролів у магістральній мережі Гельсінського технологічного університету Фінляндії (нині відомого як Університет Аалто). Потрапивши на місце, це спеціальне обладнання таємно вдихнуло тисячі імен користувачів і паролів, перш ніж було нарешті виявлено. Деякі з документів належали працівникам компанії, якою керував Тату Юленен, який також був дослідником баз даних в університеті.

Ця подія виявилася визначальною не лише для компанії Юленен, а й для всього світу. До цього моменту такі люди, як Ylönen, підключалися до мереж за допомогою інструментів, які реалізовували такі протоколи, як Telnet, rlogin, rcp і rsh. Усі ці передані паролі (і всі інші дані) у вигляді відкритого тексту, забезпечуючи нескінченний потік цінної інформації для сніферів. вирішив розробити протокол Secure Shell Protocol (SSH). Йленен, який на той час мало знав про впровадження надійної криптографії в коді, на початку 1995 року, приблизно через три місяці після виявлення сніфера паролів,

Будучи одним із перших мережевих інструментів для маршрутизації трафіку через неприступний тунель, укріплений все ще езотеричною функцією, відомою як «шифрування відкритим ключем», SSH швидко набув популярності в усьому світі. Окрім безпрецедентних гарантій безпеки, SSH легко встановлювати на широкий спектр операційних систем, у тому числі на безліч тих, які забезпечували роботу пристроїв, які використовували адміністратори, і серверів, до яких ці пристрої підключалися віддалено. SSH також підтримував перенаправлення X11, що дозволяло користувачам запускати графічні програми на віддаленому сервері.

У 1996 році Ylönen представив SSH Інженерній групі Інтернету, і він швидко став майже повсюдним інструментом для віддаленого підключення комп'ютерів. Сьогодні важко переоцінити важливість протоколу, який лежить в основі безпеки додатків, що використовуються в мільйонах організацій, включаючи хмарні середовища, важливі для Google, Amazon, Facebook та інших великих компаній.

Оголошення

«У той час атаки з перехопленням пароля були дуже поширеними, про нові інциденти повідомлялося майже щотижня, і, мабуть, це була найбільша проблема безпеки в Інтернеті на той час», — написав Юленен в онлайн-інтерв'ю. «Я справді мав на меті, щоб SSH став використовуватися якомога ширше. Це було критично необхідно для захисту мереж і обчислювальних систем, і це здебільшого вирішило проблему перехоплення паролів».

Тепер, майже через 30 років, дослідники розробили атаку, яка потенційно може підірвати, якщо не скасувати, криптографічний захист SSH, який мережевий світ сприймає як належне.

Зустрічайте Terrapin

Новий хак під назвою Terrapin працює лише тоді, коли зловмисник має активного супротивника в середині зв'язку між адміністраторами та мережею, до якої вони віддалено підключаються. Також відомий як атака «людина посередині» або MitM, це відбувається, коли зловмисник, таємно розташований між двома сторонами, перехоплює комунікації та припускає особу як одержувача, так і відправника. Це забезпечує можливість як перехоплювати, так і змінювати

комунікації. Хоча зловмиснику може бути важко досягти такої позиції, це один із сценаріїв, від якого SSH, як вважають, має імунітет.

Щоб Terrapin був життєздатним, з'єднання, якому він заважає, також має бути захищене «ChaCha20-Poly1305» або «CBC with Encrypt-then-MAC», обидва з яких є режимами шифрування, доданими до протоколу SSH (у 2013 та 2012 роках, відповідно). Сканування, проведене дослідниками, виявило, що 77 відсотків SSH-серверів, доступних до Інтернету, підтримують принаймні один із вразливих режимів шифрування, а 57 відсотків із них вказують вразливий режим шифрування як кращий вибір.

За своєю суттю Terrapin працює, змінюючи або пошкоджуючи інформацію, що передається в потоці даних SSH під час рукостискання — самого раннього етапу з'єднання, коли дві сторони узгоджують параметри шифрування, які вони використовуватимуть для встановлення безпечного з'єднання. Атака спрямована на BPP, скорочення від Binary Packet Protocol, який розроблено для того, щоб супротивники з активною позицією не могли додавати або скидати повідомлення, якими обмінюються під час рукостискання. Terrapin покладається на скорочення префіксів, клас атаки, який видаляє певні повідомлення на самому початку потоку даних…

Під час рукостискання BPP відстежує кількість повідомлень, якими обмінюються клієнт (зазвичай керований віддаленим адміністратором) і демон SSH (серверна програма, яка полегшує підключення до мережі). У статті, опублікованій у понеділок, у координації з розкриттям близько трьох десятків програм SSH, на які впливає Terrapin, дослідники включили два зображення нижче. Перший показує хід звичайного рукостискання; другий ілюструє потік рукостискання, змінений Terrapin…

У своєму поточному втіленні Terrapin містить три вразливості:

CVE-2023-48795

CVE-2023-46445

CVE-2023-46446

CVE-2023-48795 — це загальна помилка протоколу SSH, яка допускає атаку скорочення префіксів. CVE-2023-46445 і CVE-2023-46446, тим часом, знаходяться в додатку під назвою AsyncSSH, який реалізує протокол SSH. Хоча останні два недоліки реалізації не впливають безпосередньо на протокол SSH, їх можна використовувати лише в поєднанні з Terrapin, і як такі демонструють несприятливі наслідки, які можуть бути результатом Terrapin. (Уразливості AsyncSSH виправлено у версії 2.14.1.)

Оцінка ризику

Оцінити повну серйозність недоліку протоколу, який робить Terrapin можливим, важко на цій ранній стадії, оскільки це залежить від ряду змінних, які змінюються від мережі до мережі, і в які дослідники не втягнуті.

На даний момент дослідники винайшли два способи використання атаки скорочення префіксів. Один із способів знижує версії деяких розширень OpenSSH та інших програм SSH, які можуть використовувати для захисту з'єднань. Наприклад, зниження версії розширення може вимкнути контрзахід, доступний у жовтневому випуску OpenSSH версії 9.5. Розширення запобігає синхронізації натискань клавіш, класу атак, які можуть точно передбачити введені слова шляхом вимірювання часу між натисканнями клавіш. Terrapin також може перевизначати старіший параметр розширення, який визначає використання криптографічної хеш-функції SHA2. У результаті замість цього SSH використовуватиме слабший SHA1.

Інший спосіб, за допомогою якого Terrapin дозволяє використовувати раніше невідомі вразливості, згадувався раніше щодо AsyncSSH, реалізації SSH для Python із приблизно 60 000 завантажень на день. Одну з уразливостей, CVE-2023-46445, можна використати для заміни інформаційного повідомлення розширення, надісланого сервером, дозволяючи зловмиснику контролювати його вміст. Це трохи серйозніше, ніж просто скинути повідомлення (як у загальній атаці). Експлойти спрацьовують, коли клієнт, який використовує AsyncSSH, підключається до сервера за допомогою будь-якого типу програмного забезпечення SSH, а обидва передають повідомлення «EXTINFO», як зазначено в протоколі SSH…

Terrapin дозволяє використовувати CVE-2023-46446, коли клієнт, який використовує будь-яку програму SSH, підключається до сервера, на якому працює AsyncSSH. Експлойти дозволяють зловмиснику контролювати віддалений кінець сеансу клієнта SSH шляхом введення або видалення пакетів або емуляції встановленої оболонки.

«У гіршому випадку сервер AsyncSSH запускає оболонку для автентифікованого користувача після з'єднання, перемикаючи користувача на автентифікованого», — йдеться в консультації для CVE-2023-46446. «У цьому випадку зловмисник може заздалегідь підготувати модифіковану оболонку для виконання ідеальних фішингових атак і стати MitM на прикладному рівні. Якщо ім'я автентифікованого користувача не використовується після автентифікації, ця вразливість не впливає на безпеку з'єднання».

За відсутності Terrapin спроба використати будь-яку з уразливостей AsyncSSH призведе до помилки, яка призведе до збою з'єднання до того, як буде встановлено безпечний канал. Цей запобіжний захід видаляється в результаті скорочення префікса, який перебудовує порядкові номери, щоб дозволити введення повідомлення в першу чергу.

Усічення можливе через те, як SSH забезпечує цілісність рукостискання підключення. Щоб запобігти впровадженню чи видаленню будь-яких повідомлень під час цієї важливої фази, BPP присвоює кожному порядковий номер. І клієнт, і сервер підтримують різні лічильники, які починаються з нуля та збільшуються кожного разу, коли надсилається або отримується двійковий пакет. Як зазначено на діаграмі вище цифрами, виділеними жирним шрифтом, кількість повідомлень, надісланих клієнтом (позначених Snd у стовпці клієнта), має дорівнювати кількості повідомлень, отриманих сервером (позначених Rcv у стовпці сервера). Подібним чином, кількість серверних Snd має дорівнювати кількості клієнтських Rcv.

У SSH порядкові номери можна лише збільшувати. Навпаки, протоколи, такі як TLS, IPsec і IKE, скидають порядкові номери до нуля після встановлення зашифрованого сеансу, уникаючи маніпулювання порядковими номерами

зловмисною стороною в безпечному каналі. Натомість порядкові номери SSH монотонно збільшуються та не залежать від стану шифрування.

Наслідки маніпулювання порядковими номерами SSH під час рукостискання зберігаються після встановлення безпечного каналу. Це запобігає збою з'єднань SSH, навіть якщо лічильники порядкових номерів маніпулювали. У статті дослідники пояснюють:

Атака має два етапи:

Зловмисник використовує техніку RcvIncrease, щоб збільшити C.Rcv на одиницю, наприклад, шляхом введення повідомлення IGNORE клієнту перед NEWKEYS.

Зловмисник видаляє перше повідомлення SC1, надіслане сервером.

Спочатку ми проаналізуємо цю атаку з огляду на автентифікацію рукостискання та порядкові номери. Оскільки обмін ключами не захищає стенограму рукостискання від вставлення повідомлень IGNORE, автентифікація рукостискання не порушується. Перед першим кроком ми маємо C.Rcv = C.Snd. Після першого кроку ми маємо C.Rcv = S.Snd + 1, але під час рукостискання ця маніпуляція не виявляється. Після другого кроку ми маємо C.Rcv = S.Snd, і порядкові номери знову синхронізовані.

Залишається показати, що зловмисник може видалити повідомлення з каналу, для чого потрібно знати його довжину, і що його видалення не впливає на результати перевірки MAC-адреси та дешифрування для наступних повідомлень. Цей аналіз залежить від режиму шифрування...

(NS, NC) - Атака скорочення префікса. Під час однієї атаки зловмисник зазвичай може видалити довільну кількість початкових повідомлень NS, надісланих із сервера, та початкових повідомлень NC, надісланих від клієнта. Це просто: замість того, щоб вставляти одне повідомлення IGNORE клієнту перед NEWKEYS, зловмисник вставляє NS таких повідомлень клієнту та NC серверу. Отже, замість того, щоб видалити перше повідомлення з сервера, зловмисник видаляє початкові повідомлення NS з сервера та початкові повідомлення NC з клієнта.

Зауважте, що наведена вище атака одним повідомленням є конкретним випадком атаки скорочення (1,0)-префікса.

Дослідники відзначають, що вони не перші люди, які описують атаку з усіканням префіксів на мережевий протокол шляхом маніпулювання порядковими номерами. У 2015 році дослідник Седрік Фурне передбачив подібну атаку на чернетку майбутньої версії 1.3 TLS. Техніка Фурне збільшила порядкові номери шляхом фрагментації повідомлень, а не введення їх, як це робить Terrapin. (Terrapin вводить повідомлення IGNORE, щоб асиметрично збільшити порядковий номер на одній стороні зв'язку.) Атаку Fournet вважали теоретичною, оскільки маніпуляція в цьому випадку могла призвести до збою рукостискань TLS. Тим не менш, можливість успішного використання спонукала інженерів слідувати пораді Fournet і повернутися до практики 1.2 скидання порядкових номерів рівня запису до 0 щоразу, коли встановлювалися нові ключі.

У відповідь на рекомендації, надані дослідниками перед публікацією статті в понеділок, розробники програмного забезпечення SSH, включаючи майже всюдисущий OpenSSH, оновили свої реалізації для підтримки додаткового суворого обміну ключами. Він забезпечує скидання порядкового номера, а також запобігає здатності зловмисника вводити пакети під час початкового незашифрованого рукостискання. Щоб виправлення набуло чинності, клієнт і сервер повинні підтримувати цю зворотну сумісність змін.

Terrapin працює проти будь-якої реалізації SSH, яка підтримує та налаштована для надання chacha20-poly1305@openssh.comалгоритм шифрування або будь-який алгоритм шифрування з суфіксом -cbc у поєднанні з будь-яким алгоритмом MAC із суфіксом -etm@openssh.com. Зображення нижче порівнюють різні потоки атак, необхідні для націлювання на кожен алгоритм». ***(Marcus Brinkmann and Jörg Schwenk. SSH protects the world's most sensitive networks. It just got a lot weaker // Condé Nast (https://arstechnica.com/security/2023/12/hackers-can-break-ssh-channel-integrity-using-novel-data-corruption-attack/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 19.12.2023).***

***

«Експерти попереджають, що хмарна платформа Microsoft Azure містить уразливість безпеки високого рівня, через яку організації-жертви можуть несвідомо запускати зловмисне програмне забезпечення на своїх кінцевих точках.

Дослідники з Vectra окреслили проблему в нещодавній публікації в блозі, зазначивши, що вразливість полягає в Azure Logs, інструменті, який, як не дивно, використовується для відстеження зловмисної активності в хмарному середовищі (серед іншого). Хоча журнали схожі на те, що адміністратор Azure лише читав би, а не редагував, є деякі дані, які користувач може контролювати, як-от ідентифікатори користувачів, адреси електронної пошти, теми повідомлень тощо.

Дослідники стверджують, що, вводячи шкідливі дані в журнали, програми, які їх обробляють, можуть обманом змусити запустити зловмисне програмне забезпечення.

«Наприклад, у формі реєстрації облікового запису можна надіслати підроблену адресу електронної пошти, яка містить корисне навантаження XSS (міжсайтовий сценарій), — йдеться в дослідженні. «І адміністратор програми, який відкриває цей журнал у браузері, може стати жертвою XSS-атаки».

Але є ще один спосіб завантажувати зловмисне програмне забезпечення на пристрої людей – ін’єкція CSV. Оскільки журнали Azure можна завантажити як файл CSV (значення, розділені комами), файл може містити формулу Excel, яку програма виконує під час відкриття файлу. Деякі формули, як ви здогадалися, можуть бути зловмисними, змушуючи виконувати команди ОС та інші експлойти. «Це може бути небезпечним не лише тому, що можна запускати довільні команди, а й тому, що користувачі зазвичай не знають про це, думаючи, що файли CSV — це лише звичайні текстові файли, які не можуть завдати жодної шкоди», — йдеться у звіті.

Дослідники прийшли до висновку, що ці вразливості можуть бути виконані без автентифікації, припускаючи, що зловмисникам не потрібно мати обліковий запис у хмарному середовищі.

Хороша новина полягає в тому, що вразливість не працює на повністю виправлених екземплярах Excel, тому переконайтеся, що ваш оновлений». ***(Sead Fadilpašić. Researchers uncover major security issue in Microsoft Azure - here's what we know // Future US, Inc. (https://www.techradar.com/pro/security/researchers-uncover-major-security-issue-in-microsoft-azure-heres-what-we-know?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 19.12.2023).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Цифровий ландшафт, який постійно розширюється та розвивається, спричинив зростання кількості вразливостей безпеки. Щоб вирішити цю проблему, було представлено новий проект із відкритим вихідним кодом під назвою Vulnerability Impact Scoring System (VISS). VISS розроблено для посилення заходів безпеки, надаючи унікальний інструмент оцінки, який вимірює вплив вразливостей з точки зору захисника. Цей інноваційний підхід фокусується на фактичному впливі потенційних загроз, а не на їх теоретичному існуванні.

З березня 2023 року Zoom, провідна платформа для відеоконференцій, використовує VISS для оцінки виплат винагород у рамках своєї програми Bug Bounty. Ця програма заохочує дослідників безпеки та користувачів продукту виявляти та оприлюднювати вразливі місця, надаючи їм правовий захист. Включення VISS у цю програму допомогло Zoom визначати пріоритети вразливостей, які найімовірніше вплинуть на них, що дозволило ефективніше використовувати ресурси.

Система оцінки впливу вразливостей аналізує вразливості на основі 13 аспектів впливу. Ці аспекти поділяються на три групи: платформа, інфраструктура та дані. Отриманий бал у діапазоні від 0 до 100 відображає серйозність впливу в конкретному середовищі. Ця система підрахунку балів забезпечує об’єктивну

оцінку потенційної шкоди, яку може завдати вразливість, що дозволяє організаціям відповідно визначати пріоритети своїх заходів реагування.

Оцінка впливу вразливості ZOOM VISS

VISS було протестовано під час HackerOne H1-4420 хакерської події у Лондоні в 2023 році. Захід продемонстрував ефективність VISS у покращенні розподілу ресурсів і зосередженні на усуненні вразливостей критичного та високого рівня. Впровадження VISS призвело до зміни подання звітів про вразливості до цих категорій вищого рівня серйозності, зі значним скороченням спостережень у поданнях звітів середнього ступеня серйозності.

Цей зсув до націлювання на вразливості вищого ступеня серйозності є свідченням ефективності VISS. Забезпечуючи чітке об'єктивне вимірювання потенційного впливу вразливості, VISS дозволяє організаціям зосередити свої ресурси там, де вони найбільше потрібні. Це, у свою чергу, веде до більш надійного та безпечного цифрового середовища.

VISS — це не просто інструмент для окремих організацій, а глобальна місія з посилення заходів безпеки. Забезпечуючи комплексне й об'єктивне вимірювання впливу вразливості, VISS прагне розширити можливості груп реагування на інциденти та безпеки по всьому світу. Природа проекту з відкритим вихідним кодом запрошує долучитися до його розвитку, сприяючи спільному підходу до покращення цифрової безпеки.

Розробка та впровадження системи оцінки впливу вразливостей є значним кроком вперед у сфері цифрової безпеки. Зосереджуючись на фактичному впливі вразливостей, VISS пропонує більш реалістичний і ефективний підхід до управління цифровими загрозами. Успішне використання системи в програмі Zoom Bug Bounty Program і заході HackerOne H1-4420, присвяченому хакерству в реальному часі, підкреслює її потенціал змінити те, як організації реагують на вразливі місця в безпеці.

Проект VISS відкритий для дослідження та внеску за ліцензією GPL 3.0 за адресою https://github.com/zoom/viss. Цей проект із відкритим вихідним кодом є свідченням духу співпраці цифрової спільноти, запрошуючи всіх долучитися до

постійного розвитку та вдосконалення цього інноваційного інструменту безпеки. З продовженням розвитку та впровадження VISS майбутнє цифрової безпеки виглядає багатообіцяючим». ***(Julian Horsey. ZOOM VISS vulnerability impact scoring system announced // Geeky Gadgets (https://www.geeky-gadgets.com/zoom-viss-vulnerability-impact-scoring/?utm_source=flipboard&utm_content=GeekyGadgets%2Fmagazine%2FGeeky+Gadgets). 19.12.2023).***

***

«Telecom Italia (TIM) (TLIT.MI) у четвер випустила новий розроблений нею мікрочіп, призначений для підвищення кібербезпеки в таких сферах, як мобільні пристрої, хмарна інфраструктура та системи захисту.

Оголошення було зроблено під час заходу в Римі, на якому були присутні міністр промисловості Італії Адольфо Урсо та виконавчий директор TIM П'єтро Лабріола.

Мікрочіп «являє собою новий інструмент для зміцнення технологічної автономії та суверенітету в рамках національних і європейських стратегій кібербезпеки», забезпечуючи повністю зашифрований зв'язок, йдеться в заяві TIM.

Він також спрямований на захист критичної інфраструктури, такої як залізничні колії, електромережі, водопровідні мережі та дамби, від загроз кібербезпеці, додала компанія.

Захищений чіп був повністю розроблений підрозділом TIM Telsy, який розробляє послуги кібербезпеки та надає технологію зашифрованого зв'язку таким клієнтам, як державна адміністрація, і виготовлений через європейський ланцюг поставок.

Країни Європейського Союзу та законодавці ЄС минулого місяця погодили правила захисту ноутбуків, мобільних додатків і розумних домашніх пристроїв, підключених до Інтернету, від кіберзагроз після серії таких атак і вимог викупу в останні роки». ***(Telecom Italia launches microchip to boost cybersecurity services //***

Reuters (https://www.reuters.com/business/media-telecom/telecom-italia-launches-microchip-boost-cybersecurity-services-2023-12-14/). 14.12.2023).

***

«У середовищі цифрових технологій, що постійно розвивається, потреба в надійних заходах кібербезпеки стала більш критичною, ніж будь-коли. Оскільки як компанії, так і окремі особи все більше покладаються на взаємопов'язані мережі та цифрові платформи, уразливість до кіберзагроз зросла. У відповідь на цей зростаючий виклик технологія блокчейн стала потужним інструментом для зміцнення захисту кібербезпеки. У цьому всебічному огляді розглядаються багатогранні способи, за допомогою яких блокчейн сприяє підвищенню кібербезпеки.

Розуміння основ блокчейну:

Перш ніж ми заглибимося в його роль у кібербезпеці, давайте коротко дослідимо основи блокчейна. За своєю суттю блокчейн — це децентралізована та розподілена технологія реєстру, яка забезпечує безпечний і прозорий запис транзакцій у мережі комп'ютерів. Кожен блок у ланцюжку містить криптографічний хеш попереднього блоку, створюючи безпечний і захищений від втручання ланцюжок інформації.

Незмінність і прозорість:

Стовпи кібербезпеки:

Однією з ключових сильних сторін блокчейна є його незмінність. Як тільки блок додається до ланцюжка, змінити інформацію в ньому стає практично неможливо. Ця характеристика робить блокчейн потужним інструментом для захисту конфіденційних даних, оскільки він усуває ризик неавторизованих змін.

Крім того, прозорість, притаманна блокчейну, сприяє його ефективності в підвищенні кібербезпеки. Усі учасники мережі блокчейн мають доступ до однієї й тієї самої інформації в режимі реального часу, створюючи прозору екосистему, де будь-які спроби зловмисної діяльності можуть бути швидко виявлені та усунені. Ця

прозорість особливо важлива в контексті кібербезпеки, де швидке реагування має першочергове значення.

Децентралізація:

Перевизначення парадигм безпеки:

Традиційні моделі кібербезпеки часто покладаються на централізовані органи влади для захисту даних і систем. Однак цей централізований підхід чутливий до окремих точок збою, що робить його привабливою мішенню для кіберзлочинців. З іншого боку, блокчейн працює в децентралізованій мережі, розподіляючи контроль і повноваження між кількома вузлами.

Ця децентралізація не тільки зменшує ризик виникнення єдиної точки відмови, але й додає додатковий рівень безпеки. У децентралізованій блокчейн-мережі зловмисникові потрібно буде скомпрометувати більшість вузлів одночасно, щоб скомпрометувати систему. Ця розподілена архітектура значно підвищує планку для кібер-зловмисників, роблячи блокчейн грізним союзником у боротьбі з кіберзагрозами.

Розумні контракти:

Самовиконуваний код для покращеної безпеки:

Розумні контракти, ключова функція технології блокчейн, є самовиконуваними контрактами з умовами угоди, записаними безпосередньо в коді. Ці контракти автоматизують і забезпечують виконання договірних положень, усуваючи потребу в посередниках. У сфері кібербезпеки смарт-контракти відіграють трансформаційну роль у посиленні заходів безпеки.

Автоматизуючи певні протоколи безпеки та відповіді, смарт-контракти зменшують можливість людської помилки, що є поширеним слабким місцем у традиційних налаштуваннях кібербезпеки. Крім того, самовиконуваний характер смарт-контрактів гарантує послідовне застосування попередньо визначених заходів безпеки, створюючи більш стійкий захист від кіберзагроз.

Керування ідентифікацією:

Блокчейн-революція:

Крадіжка особистих даних і несанкціонований доступ є вічними проблемами в сфері кібербезпеки. Blockchain пропонує революційне рішення цих проблем завдяки надійним можливостям керування ідентифікацією. Традиційні системи керування ідентифікацією часто зберігають конфіденційну інформацію в централізованих базах даних, що робить їх привабливими цілями для хакерів.

Навпаки, керування ідентифікацією на основі блокчейну працює за децентралізованою моделлю, де кожен користувач зберігає контроль над своєю власною ідентифікаційною інформацією. Це не тільки покращує конфіденційність, але й зменшує ризик великомасштабного витоку даних. Крім того, використання криптографічних ключів у системах ідентифікації на основі блокчейну додає додатковий рівень захисту, що значно ускладнює для кіберзлочинців скомпрометувати ідентифікаційні дані користувачів.

Блокчейн у безпеці ланцюга поставок:

Оскільки підприємства все більше залежать від складних мереж ланцюгів поставок, ризики кібербезпеки, пов’язані з цими взаємопов’язаними системами, зростають. Технологія блокчейн надає революційне рішення для підвищення безпеки ланцюга поставок. Реєструючи кожну транзакцію та рух товарів у незмінній книзі, блокчейн забезпечує прозорість і відстежуваність у всьому ланцюжку постачання.

Ця прозорість є важливою для виявлення та пом’якшення потенційних загроз безпеці, таких як підроблені продукти, підробка або несанкціонований доступ. Завдяки блокчейну зацікавлені сторони можуть відстежувати походження кожного продукту, створюючи безпечний і перевірений ланцюжок зберігання, який зміцнює кібербезпеку в ланцюжку постачання.

Виклики та перспективи на майбутнє:

Хоча блокчейн має величезні перспективи для зміцнення кібербезпеки, важливо визнати проблеми, які супроводжують його впровадження.

Масштабованість, функціональна сумісність і регуляторні проблеми є одними з перешкод, які необхідно вирішити для широкого впровадження.

Заглядаючи вперед, майбутнє блокчейну в кібербезпеці виглядає багатообіцяючим. Такі інновації, як блокчейни, орієнтовані на конфіденційність, і покращені алгоритми консенсусу спрямовані на усунення існуючих обмежень, що робить блокчейн ще більш потужним інструментом у поточній боротьбі з кіберзагрозами.

висновок:

Роль блокчейну в підвищенні кібербезпеки є багатогранною та трансформаційною. Від основоположних принципів незмінності та прозорості до практичного застосування розумних контрактів і децентралізованого керування ідентифікацією, блокчейн змінює ландшафт кібербезпеки. Оскільки компанії та окремі особи продовжують орієнтуватися в складнощах цифрової епохи, застосування технології блокчейн є не просто можливістю, а стратегічним імперативом у зміцненні захисту від нових кіберзагроз. Подорож до більш безпечного цифрового майбутнього тісно пов’язана з інноваційними та стійкими можливостями технології блокчейн». ***(The Role of Blockchain in Enhancing Cybersecurity: A Comprehensive Overview // TechBullion (https://techbullion.com/the-role-of-blockchain-in-enhancing-cybersecurity-a-comprehensive-overview/). 24.12.2023).***

***

«Проблеми кібербезпеки, які намагаються вирішити стартапи, часто випереджають основні. Вони можуть рухатися швидше, ніж більшість відомих компаній, щоб заповнити прогалини або виникнути потреби. Стартапи часто можуть впроваджувати інновації швидше, оскільки їх не обмежує встановлена база.

Недоліком, звичайно, є те, що стартапам часто бракує ресурсів і зрілості. Для компанії ризиковано взяти на себе зобов’язання щодо продукту або платформи стартапу, і це вимагає іншого типу відносин між клієнтом і постачальником. Однак

винагорода може бути величезною, якщо це дає компанії конкурентну перевагу або зменшує навантаження на ресурси безпеки.

Постачальники, наведені нижче, представляють деякі з найцікавіших стартапів (тут визначаються як компанії, засновані або вийшли з стелс-режиму протягом останніх двох років). Якщо ви берете участь у стартапі, який виходить із стелсу, повідомте регіонального виконавчого редактора CSO Ендрю Флінна за адресою aflynn@foundryco.com, щоб ми розглянули питання про включення до цього списку.

Aembit

Aembit створює хмарну ідентифікаційну платформу, яка дозволяє командам DevOps і безпеки виявляти, керувати, запроваджувати та перевіряти доступ між об’єднаними робочими навантаженнями. Компанія допомагає організаціям застосовувати структуру безпеки з нульовою довірою для доступу до робочого навантаження, подібно до існуючих рішень для доступу робочої сили, надаючи плавний і безпечний доступ від робочих навантажень до послуг, від яких компанії залежать, наприклад API, баз даних і хмарних ресурсів. Aembit запущений у 2023 році.

Akto

Заснована в 2021 році, Akto зосереджується на безпеці API. Компанія стверджує, що її платформа, яка працює локально або в хмарі, виявляє та тестує внутрішні, зовнішні та сторонні API. Потім він швидко знаходить вразливі місця під час виконання. Він підтримує ключові джерела даних API, такі як AWS, Google Cloud і Kubernetes. Платформу можна розгорнути приблизно за хвилину, повідомляє Akto.

Axiado

Axiado розробляє довірені процесори блоків управління/обчислення (TCU), які пропонують технології безпеки на основі апаратного забезпечення та на основі ШІ. Компанія стверджує, що її напівпровідники забезпечують превентивне виявлення загроз у підході до безпеки платформи, керованому штучним інтелектом, від програм-вимагачів, ланцюжків поставок, побічних каналів та інших

кібератак на хмарні центри обробки даних, мережі 5G та інші дезагреговані обчислювальні мережі.

Backslash Security

Backslash Security, хмарне рішення безпеки додатків для корпоративних команд AppSec, забезпечує уніфіковану безпеку та бізнес-контекст для ризиків у хмарному коді, а також автоматизоване моделювання загроз, визначення пріоритетності ризиків у коді та спрощене виправлення для програм і команд. Платформа компанії націлена на високоризикові кодові комбінації, які називаються «токсичними кодовими потоками» у хмарних програмах.

Binarly

Binarly — це розширена автоматизована платформа безпеки ланцюга постачання мікропрограм, яка використовує методи машинного навчання як для відомих, так і для невідомих уразливостей, неправильних конфігурацій і зловмисного коду в мікропрограмних і апаратних компонентах. Платформа робить найтемніші частини стека безпеки видимими, доступними та захисними. Поєднуючи предметний досвід із новітнім штучним інтелектом, він дає змогу захисникам захищати пристрої від невідомих і нових загроз як у мікропрограмному, так і в апаратному забезпеченні, надаючи оперативним центрам безпеки та групам реагування на інциденти можливість кількісно оцінювати, підтримувати та захищати базові елементи корпоративної інфраструктури. Binarly була заснована в 2021 році.

BoostSecurity

BoostSecurity пропонує платформу автоматизації DevSecOps, яка, як стверджується, може допомогти виявити та усунути вразливості, дозволяючи DevOps працювати у своєму власному темпі. Це також полегшує створення та керування політиками в коді, хмарі та потоках CI/CD. Єдина площина керування забезпечує видимість ризиків ланцюга постачання програмного забезпечення. BoostSecurity вийшов із стелс-режиму у 2022 році.

BreachQuest

Платформа реагування на інциденти Priori від BreachQuest обіцяє швидко збирати та аналізувати дані про події безпеки, щоб виявляти та стримувати атаки, а також пришвидшувати відновлення. Пріорі постійно відстежує системи на наявність зловмисної активності. Коли відбувається злом, він негайно надсилає сповіщення з інформацією про те, які кінцеві точки було зламано. Компанію було засновано у 2021 році. На момент написання цієї статті у листопаді 2022 року BreachQuest не випустила Priori.

Camelot Secure

що займається виявленням і пом’якшенням загроз, Компанія Camelot Secure, пропонує «наступальний підхід» до кібербезпеки, пропонуючи оцінку вразливості, оцінку ризиків, об’єднання в команду, пошук кіберзагроз і аналіз даних про кіберзагрози з використанням штучного інтелекту та машинного навчання. У компанії працюють експерти з військових, розвідувального співтовариства та приватного сектору.

Ceritas

Ceritas надає аналіз вразливості номенклатури матеріалів (HBOM) і передачу даних цифрової номенклатури матеріалів (DBOM). Платформа визначає всі відомі зв’язки вразливостей і використовує штучний інтелект (ШІ), щоб допомогти компаніям знизити ризики шляхом моніторингу обладнання, яке зараз використовується, і проведення належної перевірки закупівель. Компанія запущена в 2022 році.

Circle Security

Компанія з кібербезпеки Circle Security розробила спеціальну платформу для захисту від загроз, керованих обліковими даними, і хмарних атак. Завдяки децентралізованій архітектурі, Circle доступний як власний сервіс для пристрою, мобільний додаток, рішення на основі браузера та через API, орієнтований на розробника, за словами фірми. Децентралізована платформа Circle забезпечує безпечний доступ до хмарних даних і додатків, одночасно захищаючи дані під час

входу в систему та протягом усього шляху користувача, незалежно від того, куди вони переміщуються, йдеться в прес-релізі компанії.

CommandK

Заснована в 2022 році компанія CommandK пропонує рішення для керування наскрізним життєвим циклом конфіденційних даних у віртуальній приватній хмарі компанії. Його платформа спрямована на забезпечення нульової залежності від розробника в управлінні конфіденційними даними, дозволяючи командам безпеки досягти високого рівня безпеки, дозволяючи розробникам зосередитися на розробці функцій. CommandK розгортається як кероване рішення у віртуальній приватній хмарі компанії, гарантуючи, що конфіденційні дані залишаються в мережі компанії.

Confidencial

Каліфорнійська компанія Confidencial розробляє рішення для безпечного обміну конфіденційною інформацією в неструктурованих документах. Компанія стверджує, що «створила продукт, який відповідає потребам окремих осіб і компаній, які шукають кращий спосіб обміну документами, що містять конфіденційну клієнтську або корпоративну інформацію». Основні функції платформи включають інтеграцію в звичайні настільні програми, повне шифрування документів або вибіркове шифрування, а також надійну панель аналітики та звітності. Виробнича версія платформи включає відстеження індивідуальних і групових документів, шифрування папок, пошук і шифрування PDF-файлів і шифрування зображень.

Conveyor

Conveyor, заснований у 2021 році, пропонує спосіб спростити заповнення анкет безпеки клієнтів. Це онлайн-сервіс, де постачальники можуть завантажувати відповідні документи безпеки та відповіді на поширені запитання на платформі довіри клієнтів Conveyor. Потім клієнти можуть отримати доступ до цього вмісту через Vendor Trust Platform компанії, яка закрита та вимагає угоди про нерозголошення для доступу, або клієнти можуть порівняти рівень безпеки кількох постачальників.

Cranium

Компанія Cranium, яка займається програмним забезпеченням безпеки та довіри, пропонує програмну платформу Cranium Enterprise, спрямовану на допомогу організаціям у картографуванні, моніторингу та управлінні середовищами AI/ML проти загроз, не перериваючи процес навчання, тестування та розгортання своїх моделей AI. 15 червня компанія випустила картку Cranium AI Card, яка дозволяє організаціям збирати та ділитися інформацією про надійність і відповідність своїх моделей штучного інтелекту як клієнтам, так і регуляторним органам, а також отримувати доступ до безпеки систем штучного інтелекту своїх постачальників.

Cyclops

Cyclops, що базується в Тель-Авіві, створює контекстну пошукову платформу кібербезпеки. Заснована в 2020 році ветеранами кібербезпеки Ераном Зільберманом (генеральний директор), Елай Гета (технічний директор) і Біран Франко (CPO), Cyclops пропонує пошукову систему на основі генеративного штучного інтелекту, щоб відповідати на важливі та своєчасні запитання про стан безпеки організації та забезпечувати проактивну роботу захист від кіберзагроз і усунення вразливостей.

Dapple

Dapple Security пропонує можливість безпечного входу в системи без зберігання конфіденційних ідентифікаційних даних. Оскільки немає необхідності зберігати конфіденційні дані користувача, Dapple Security запобігає фішингу та пов’язаним з ним атакам, які покладаються на викрадені облікові дані, зберігаючи конфіденційність користувачів і значно зменшуючи площу атаки на дані. Компанія Dapple була заснована в 2022 році.

Descope

Descope — це платформа автентифікації та керування користувачами для автентифікації без пароля. Він пропонує розробникам інструменти для легкого додавання до програм можливостей автентифікації, керування користувачами та авторизації. Платформа захищає від атак ботів на сторінки входу, шахрайства з захопленням облікових записів і крадіжки сеансів, виявляючи ризиковані сигнали

користувачів для проведення посиленої автентифікації. Компанію засновано у 2022 році.

Discern Security

Discern Security визначає себе як «центр аналізу політики», який використовує можливості штучного інтелекту для моніторингу та оптимізації елементів керування безпекою в ряді інструментів кібербезпеки. Він спрямований на використання штучного інтелекту для створення динамічної взаємопов'язаної платформи для конфігурації безпеки та керування політикою. Компанія була заснована в 2023 році.

DoControl

Платформа DoControl надає автоматизовані інструменти самообслуговування для моніторингу доступу до даних, оркестровки та виправлення додатків SaaS. Він має здатність ідентифікувати конфіденційну інформацію та запобігати її виходу з хмарної інсталяції організації. DoControl — це безагентна платформа, керована подіями. Компанія була заснована в 2020 році.

Dope.security

Представляючи себе «єдиним у світі безпечним веб-шлюзом fly-direct (SWG)», dope.security забезпечує безпеку безпосередньо на кінцевій точці замість маршрутизації трафіку через зупинкові центри обробки даних. Цей процес «підвищує продуктивність до 4 разів, гарантує, що розшифровані дані ніколи не залишать пристрій, і підвищує надійність шляхом усунення зовнішніх залежностей.

Eureka Security

Eureka Security — це хмарна платформа для керування безпекою даних, яка допомагає командам із безпеки зрозуміти, де й якого типу дані, дізнатися, хто й що може до них отримати доступ, а також постійно підтримувати їх у безпеці. Платформа на базі Saas була запущена в січні 2022 року з фінансуванням у 8 мільйонів доларів.

Gem Security

Gem Security, заснована в травні 2022 року, пропонує платформу хмарного виявлення та реагування (CDR) із централізованим підходом до реагування на

хмарні загрози. Платформа застосовує методологію «припустити порушення» з видимістю операцій у режимі реального часу. Рішення забезпечує цілісний підхід для команд SecOps для боротьби з рідними хмарними загрозами, забезпечуючи хмарний контекст через єдину платформу, інтегровану в існуючі робочі процеси SecOps (SIEM/SOAR, IAM, CSPM, системи продажу квитків тощо). лютий 2023 р.

Gutsy

Gutsy застосовує аналіз процесів до кібербезпеки, надаючи автоматичне, кероване даними розуміння того, як команди, інструменти та процеси організації працюють разом і які результати вони забезпечують. За словами компанії, платформа надає керівникам безпеки дані та розуміння, щоб ставити складні запитання та приймати правильні рішення. Він містить три модулі, що охоплюють процеси керування ідентифікацією, реагування на інциденти та керування вразливістю, інтегруючись із широким спектром інструментів від хмарних провайдерів до систем управління персоналом, інструментів керування вразливістю, систем продажу квитків, платформ EDR тощо.

Hadrian

Hadrian — це стартап із кібербезпеки, керований хакерами, що базується в Лондоні та Амстердамі та пропонує атакуючу платформу безпеки на основі подій у моделі SaaS. У компанії кажуть, що її «автономна технологія визначає реальні загрози та визначає пріоритети, де потрібні дії, пов’язуючи термінові завдання з існуючими інструментами та процесами робочого процесу, щоб важливі речі були оброблені першими». Використовуючи хмарну технологію та модулі ML, Hadrian проактивно та постійно сканує та тестує IT-інфраструктури компаній, щоб надавати швидку та точну цілісну інформацію.

Harmonic Security

Компанія Harmonic Security, заснована в 2023 році, забезпечує видимість впровадження ШІ на підприємстві. Платформа виконує оцінку ризиків для всіх програм штучного інтелекту, щоб виявити служби штучного інтелекту з високим рівнем ризику, які можуть призвести до інцидентів відповідності, безпеки чи конфіденційності. Це дозволяє організаціям за потреби контролювати доступ до

додатків штучного інтелекту, включаючи вибіркове блокування завантаження конфіденційного вмісту, не потребуючи правил чи точних збігів.

Hush

Hush пропонує послуги цифрової конфіденційності на основі ШІ для окремих осіб і сімей, але також має продукт корпоративного рівня для захисту конфіденційності працівників. Після того, як підприємства розгорнуть службу Hush, їхні співробітники зможуть керувати власними профілями Hush. Це дозволяє їм відстежувати проблеми конфіденційності та повідомляти про них, а також усувати проблеми, які ставлять під загрозу конфіденційність. Hush також робить «захисника конфіденційності» доступним по телефону або онлайн. Компанію засновано у 2021 році.

Inside-Out Defense

Запущена в 2023 році Inside-Out Defense стверджує, що є «першою платформою в індустрії кібербезпеки, яка розв'язує зловживання привілеями». Пропозиція компанії забезпечує цільовий доступ, виявлення в реальному часі та вбудоване виправлення через платформу SaaS. «Платформа дає змогу визначати розбіжності між відомою та невідомою поведінкою зловживань, тим самим припиняючи зловживання привілеями в реальному часі в масштабі», — кажуть у компанії.

Interpres Security

Вийшовши з режиму стелс у грудні 2022 року, Interpres Security пропонує платформу, яка дозволяє організаціям краще керувати своєю «поверхнею захисту». Він покаже, що їх поточний набір інструментів безпеки може виявити та захистити від них. Платформа також допомагає виявляти прогалини та неефективність кіберзахисту, дозволяючи командам безпеки використовувати підхід, що керується даними, для покращення стану безпеки.

Kodem

Kodem стверджує, що є «першою у світі платформою для створення динамічного програмного забезпечення». Пропозиція компанії використовує час виконання програми для виявлення ризиків програми, створюючи контекст

програми на основі того, що відбувається під час виконання, а не лише в статичному коді. За словами компанії, «дослідивши проблему шуму, помилкових спрацьовувань і неефективного виправлення, ми виявили, що єдиний спосіб усунути помилкові спрацьовування та ефективно визначити пріоритети виправлення — це спостерігати за додатками під час виконання. Аналізуючи їх під час роботи, можна точно знати, які компоненти використовуються, як дані переміщуються між ними та яка частина програми дійсно вразлива».

Lasso Security

Lasso надає спеціальний набір інструментів для виявлення, моніторингу та захисту використання великих мовних моделей (LLM). Платформа виявляє використання тіньового штучного інтелекту та визначає, які інструменти та моделі використовуються в мережі організації. Він реєструє зовнішню та внутрішню взаємодію користувачів із інструментами на основі LLM, виявляє ризиковані дані та блокує зловмисні спроби з боку загрозливих суб'єктів або внутрішніх користувачів. Компанія була заснована в 2023 році.

LeakSignal

LeakSignal — це платформа для видимості даних і керування станом для мікросервісів, яка пропонує безперервну видимість витоків даних і ризиків. Він забезпечує видимість даних рівня 4-7 і захист для мікросервісних середовищ, дозволяючи групам безпеки взяти під контроль і встановити обмеження на доступ до конфіденційних даних за допомогою технології для аналізу та ідентифікації потенційного викрадання даних, зміцнення сітчастих мереж. Його було засновано у 2021 році.

Mobb

Автоматичний засіб усунення вразливостей Mobb використовує технологію на базі штучного інтелекту для автоматизації усунення вразливостей, щоб значно зменшити відставання в системі безпеки та звільнити розробників зосередитися на інноваціях. Mobb отримує результати SAST з різних інструментів сканування та автоматично виправляє код, інформуючи розробників під час процесу, щоб вселити довіру та забезпечити точність. Mobb використовує результати багатьох рішень

SAST. Компанія каже, що «її автоматичне виправлення коду працює за допомогою штучного інтелекту та базується на найкращих практиках безпеки та інформації розробників, які вносять виправлення».

Naxo Labs

Naxo Labs була заснована в 2022 році групою відомих експертів і колишніх спецагентів ФБР для надання послуг криміналістики та розслідування. Компанія працює над справами, пов'язаними з кіберзлочинами, як-от внутрішні погрози чи крадіжка інтелектуальної власності, і збирає факти для передачі до правоохоронних органів або для судового розгляду. Naxo також здатний виконувати аналіз блокчейну та криптовалюти, а також відновлювати дані.

Nudge Security

Nudge Security пропонує рішення, спрямоване на керування безпекою програмного забезпечення як послуги (SaaS) для розподілених робочих сил. Його платформа дозволяє виявляти хмарні активи SaaS, створені без необхідності змін мережі, агентів кінцевих точок або розширень браузера. Компанія стверджує, що забезпечує видимість усієї поверхні атаки SaaS, включаючи керовані та некеровані облікові записи, з'єднання OAuth і ресурси. Він також сповіщає про створення нових облікових записів SaaS. Nudge засновано у 2022 році.

Oligo Security

Заснована у 2022 році компанія Oligo пропонує платформу безпеки з відкритим вихідним кодом, яка виявляє та запобігає таким атакам, як Log4Shell, відстежуючи зловмисну активність на рівні бібліотеки. Компанія стверджує, що її моніторинг під час виконання бібліотек з відкритим кодом зосереджується лише на актуальних уразливостях. Платформа працює з більшістю сучасних мов розробки, таких як Python, Go, Java і Node, і з усіма постачальниками хмарних послуг, такими як GCP, Azure і AWS.

Onyxia

Onyxia пропонує свою платформу керування кібербезпекою, яка надає прогнозну інформацію, забезпечує оцінку безпеки та порівняльний аналіз у

реальному часі, повну видимість стеку безпеки та спрощену звітність дошки. Компанію засновано у 2022 році.

Opus Security

У вересні 2022 року було запущено платформу організації хмарної безпеки та виправлення помилок Opus Security. Opus дає змогу командам хмарної безпеки бачити не тільки сповіщення та загрози, а й отримувати контроль, знання та можливості для їх вирішення. Платформа інтегрується з існуючими інструментами безпеки та організовує весь процес виправлення для всіх зацікавлених сторін та організаційних середовищ.

Phylum.io

Phylum.io — це компанія з безпеки ланцюга постачання програмного забезпечення, яка пропонує платформу безпеки як коду, яка дає командам із безпеки та ризиків краще бачення життєвого циклу розробки коду та можливість застосовувати політику безпеки, не порушуючи інновації. Платформа захищає розробників і додатки на периметрі екосистеми з відкритим кодом, а також інструменти, які використовуються для створення вихідного коду. Компанія стала першим переможцем конкурсу Black Hat Innovation Spotlight у 2022 році та стверджує, що з червня першою виявила та пом’якшила три окремі атаки на розробників npm з боку державних зловмисників.

Piiano

Piiano пропонує два продукти: Piiano Scanner сканує вихідний код на наявність посилань на особисту інформацію (PII), а Piiano Vault захищає конфіденційні дані, дозволяючи їх використовувати. Сканер може сканувати будь-які проекти GitHub Java або Python одним клацанням миші та призначений для покращення співпраці між командами розробки та конфіденційності. Інфраструктура Vault на основі API дозволяє безпечно зберігати конфіденційні дані та забезпечує відповідність GDPR і CCPA. Piiano було засновано в 2021 році.

PingSafe

PingSafe — це хмарна платформа додатків (CNAPP), яка використовує інтелектуальні дані зловмисників і атакуючий механізм безпеки, щоб допомогти

клієнтам швидко та в масштабі усунути критичні вразливості, які можна використовувати. Платформа допомагає захищати хмарні середовища в гіпермасштабувальниках, таких як AWS, GCP, Azure, і різноманітних розгортаннях, як-от Kubernetes, віртуальних машинах і без сервера. Компанію заснували Ананд Пракаш і Нішант Міттал у 2021 році та базується в Сан-Франциско та Бангалорі.

Plerion

Plerion — це хмарна платформа безпеки, розташована в Сіднеї, Австралія, яка допомагає клієнтам визначати, визначати пріоритети та зменшувати ризики в хмарних операційних середовищах. Компанія, заснована у 2022 році, отримала 10 мільйонів доларів початкового фінансування в липні. Заснована у 2022 році компанія Plerion була визнана партнером з питань безпеки AWS.

Privya

Платформа Privya, заснована в 2021 році, забезпечує хмарний підхід до конфіденційності даних. Компанія стверджує, що це дозволить організаціям краще забезпечити конфіденційність і захист даних у процесі життєвого циклу розробки. Платформа Privya здатна виявляти та ідентифікувати особисті дані в багатьох джерелах даних і відображати потік даних і бізнес-логіку. Він також забезпечує автоматизовану архітектуру, щоб краще відповідати вимогам відповідності.

Protect AI

Protect AI – це безпекова компанія зі штучного інтелекту та машинного навчання, яка допомагає організаціям захищати системи машинного навчання та програми штучного інтелекту від унікальних вразливостей у безпеці, витоку даних і нових загроз. За словами компанії, її платформа, AI Radar, «допомагає організаціям створювати безпечніший ШІ, надаючи розробникам, інженерам ML і професіоналам AppSec спосіб бачити, знати та керувати середовищем ML». «AI Radar дозволяє клієнтам швидко виявляти та усувати ризики, а також підтримувати надійну безпеку систем машинного навчання та програм штучного інтелекту».

Savvy

Платформа автоматизації безпеки робочої сили Savvy усуває людські помилки, надаючи посібники з видимості та автоматизації безпеки SecOps для

організації реагування на інцидент SaaS до того, як відбудеться небезпечна дія. Компанія стверджує, що її платформа «надає сповіщення в режимі реального часу та підказки для покращення прийняття рішень користувачами. Зосередженість Savvy на «людській» поверхні атаки та захист співробітників у веб-переглядачах і робочих програмах вирішує величезну проблему, з якою стикаються всі підприємства, і вона лише погіршується.»

Sharepass

Sharepass, заснований у 2020 році, надає засоби для безпечного обміну конфіденційною інформацією між платформами. Компанія стверджує, що її веб-продукт не залишає цифрового сліду під час обміну даними. Sharepass спочатку шифрує інформацію, яка надається, і надсилає посилання одержувачу. Це посилання стає неактивним, коли одержувач відкриває його. Відправники можуть вказати адреси електронної пошти, встановити часові обмеження щодо тривалості дії посилання або вимагати PIN-код.

Silk Security

Silk Security пропонує стійку платформу вирішення кіберризиків, яка дозволяє зацікавленим сторонам у сфері безпеки та операцій спільно узгоджувати виявлення ризиків із усуненням ризиків, покращуючи безпеку підприємства та відповідність вимогам, а також централізовано переглядаючи статус вирішення ризиків. Платформа включає в себе технології штучного інтелекту для консолідації та контекстуалізації результатів багатьох інструментів виявлення, автоматизує визначення пріоритетів на основі серйозності, профілів активів і факторів навколишнього середовища, а також прогнозовано призначає право власності на виправлення.

SnapAttack

SnapAttack надає фіолетову об’єднану платформу, яка, як стверджує компанія, відповідає за весь процес виявлення загроз. Платформа містить бібліотеку сигналів атак, яка каталогізує загрози та симуляції атак. Червоні та сині команди можуть створювати власні сесії атаки. SnapAttack дозволяє фіолетовим командам виявляти прогалини в матриці MITER ATT@CK і створювати логіку

виявлення за допомогою конструктора виявлення без коду. Компанію засновано у 2021 році.

Socket

Платформа Socket розроблена для запобігання проникненню зловмисних залежностей із відкритим вихідним кодом у програми шляхом виявлення та блокування неочікуваних атак, які не вловлюються сканерами вразливостей CVE через зловмисне програмне забезпечення, прихований код, друкарські помилки та інші вектори. Платформа також знаходить актуальну інформацію про безпеку безпосередньо в GitHub. Компанію було засновано у 2021 році та запущено у 2022 році.

Spera

Платформа Spera забезпечує видимість і контекстуальне розуміння ідентифікаторів, дозволів і дій, зібраних від постачальників ідентифікаційних даних і додатків (SaaS, хмарних постачальників і локальних), використовуючи безагентний процес. Рішення розроблено для інтеграції з постачальниками ідентифікаційної інформації та хмарними та локальними програмами для створення звіту про зрілість ідентифікаційної інформації для всієї організації протягом однієї години після розгортання, надаючи картину поверхні атаки ідентифікаційної інформації в реальному часі, а також контекст дозволів ідентифікаційної інформації та використання. Компанія була запущена в березні 2023 року з фінансуванням у розмірі 10 мільйонів доларів.

SquareX

SquareX розробляє продукт кібербезпеки на основі браузера, щоб забезпечити безпеку споживачів в Інтернеті. Продукт компанії спрямований на боротьбу з такими загрозами, як фішинг, викрадення особистих даних, викрадення сесії та інші атаки на основі веб-переглядача за допомогою розширення для браузера, яке відстежує та захищає користувачів під час їхньої діяльності в Інтернеті. Компанія, заснована в 2023 році, планує запустити бета-версію з травня.

Stack Identity

Керівна компанія Stack Identity, що керує ідентифікацією та доступом (IAM), спрямована на вирішення проблеми тіньового доступу — неавторизованих, неконтрольованих і невидимих шаблонів доступу до хмарних даних, створених безліччю ідентифікаційних даних людей і машин, які отримують доступ до хмари. «Це наше бачення та переконання, що майбутнє хмарної безпеки має бути насамперед ідентифікацією, орієнтованою на доступ і з глибоким контекстом даних, додатків і програмного забезпечення», за словами генерального директора та засновника Венката Рагавана. Stack використовує свій алгоритм Breach Prediction Index, щоб зменшити ризик уразливості хмари та покращити IAM-аудит, відповідність і управління.

Sweet Security

Cloud Runtime Security Suite від Sweet Security забезпечує захист під час виконання на всіх етапах атаки, включаючи виявлення та реагування, виявлення та запобігання. За словами компанії, «Sweet використовує датчик на основі eBPF, щоб забезпечити видимість кластера в хмарі та передавати ключові дані додатків і бізнес-логіку на свої сервери. Використовуючи інноваційну структуру для профілювання аномалій поведінки робочого навантаження та контекстуалізації їх за допомогою традиційних TTP, її аналіз використовує глибоке розуміння хмарних атак і налаштованих клієнтських середовищ». Компанію заснували в 2021 році Дрор Кашті, колишній CISO Армії оборони Ізраїлю (ЦАХАЛ), і Еял Фішер, колишній керівник кібервідділу підрозділу 8200.

TrustCloud (раніше Kintent)

Платформа TrustCloud призначена для того, щоб допомогти компаніям проходити перевірки, керувати ризиками та виконувати аналізи безпеки. Він використовує програмний контроль на основі API та перевірку ризиків, які можуть автоматизувати робочі процеси та збір доказів. TrustCloud може проаналізувати програму відповідності та зіставити її з кількома стандартами. Він також має функцію на основі ШІ, яка допомагає заповнювати анкети безпеки. TrustCloud було засновано у 2020 році як Kintent.

Trustmi

Компанія з безпеки бізнес-платежів Trustmi пропонує комплексне рішення, спрямоване на те, щоб допомогти компаніям захистити свої прибутки, усунувши втрати від кібератак, внутрішньої змови та людських помилок. Trustmi, заснована в Ізраїлі в 2021 році, стверджує, що допомагає зменшити шахрайство з платежами B2B за допомогою «цілісного підходу до подолання фрагментації платіжних процесів, надаючи гнучке рішення, яке легко інтегрується в існуючі організаційні робочі процеси». Платформа використовує унікальну довірчу мережу, яка об'єднує краудсорсингові дані від тисяч постачальників і компаній, щоб допомогти виявити вразливості та виявити підозрілі сигнали для максимального захисту бізнес-платежів.

Valence Security

Valence Security, заснована в 2021 році, пропонує платформу для усунення ризиків безпеки SaaS, пов'язаних зі сторонньою інтеграцією, ідентифікацією, неправильною конфігурацією та обміном даними. Платформа надає власну перехресну модель даних і дозволів SaaS для підтримки контролю доступу. Він також поставляється з набором автоматизованих робочих процесів відновлення безпеки SaaS, щоб мінімізувати потребу в спеціальних знаннях для їх налаштування.

Vanta

Розробник платформи довірчого управління Vanta запустив свій продукт Vendor Risk Management, який забезпечує перевірку безпеки сторонніх постачальників і належну перевірку. Ця пропозиція розроблена, щоб скоротити час і витрати на перевірку, управління та звітування про ризик стороннього постачальника. Компанія запущена в 2018 році.

Vaultree

Компанія Vaultree, заснована в 2020 році, розробила, як вона стверджує, перший «повнофункціональний» набір програмного забезпечення для шифрування даних у використанні (SDK). Продукт розроблено для усунення ризику витоку чи викрадення даних у формі відкритого тексту. Згідно з Vaultree, може обробляти,

шукати та обчислювати дані в масштабі без передачі ключів шифрування або дешифрування на стороні сервера.

Vanta

Veza надає платформу авторизації для даних для використання в гібридних багатохмарних середовищах. Компанія стверджує, що це дає змогу організаціям краще розуміти, керувати та контролювати, хто може та повинен виконувати дії з даними. Він зосереджений на оптимізації управління доступом до даних, запровадженні безпеки озера даних, управлінні хмарними правами та модернізації привілейованого доступу. Веза була заснована в 2020 році.

Wing Security

Платформа Wing розроблена для виявлення та автоматичного усунення загроз додатків SaaS. Він постійно відстежує використання для кожного користувача, програми та файлу. Платформа може вимикати те, що вона вважає ризикованими з'єднаннями між програмами, обмежувати та керувати даними, які надаються зовнішнім користувачам через програми SaaS, і керувати вразливими місцями навколо ризикованої поведінки користувачів. Він також може керувати маркерами та дозволами програм SaaS. Компанія Wing була заснована в 2020 році». ***(Cybersecurity startups to watch in 2023 // CSO (https://www.csoonline.com/article/574053/cybersecurity-startups-to-watch-for-2023.html). 22.12.2023).***

***

Питання криптографії

«Оскільки квантові комп'ютери готові стати реальністю до кінця десятиліття, кіберпростір стикається з суворою реальністю, пов'язаною з можливістю того, що існуючі криптографічні протоколи стануть зайвими в найближчому майбутньому. Точний момент часу, коли це станеться, те, що тепер називають «Q-Day», швидко наближається. Відповідь на цей складний виклик прийшла у формі алгоритмів квантової стійкої криптографії (QRC) або

постквантової криптографії (PQC), яка незабаром стане реальністю завдяки широко поширеній глобальній ініціативі.

Важливість PQC

Більшість класичних схем шифрування, включаючи широко використовуваний алгоритм Рівест-Шаміра-Адлемана (RSA), покладаються на той факт, що розкладання на прості множники за своєю суттю є громіздким завданням, особливо для великих чисел, і класичним комп'ютерам для цього потрібно багато часу. З іншого боку, квантові алгоритми, як той, який задумав Пітер Шор ще в 1994 році, довели, що це буде базовим завданням для квантових комп'ютерів.

Наприклад, класичному комп'ютеру знадобилося б приблизно 300 трильйонів років, щоб зламати 2048-бітний ключ шифрування RSA грубою силою, тоді як ідеальний квантовий комп'ютер міг би зробити це протягом 10 секунд. Алгоритм Шора вдосконалюється і в наступні роки став більш ефективним, алгоритм Регева. прикладом цього є

Оскільки до створення ідеального квантового комп'ютера залишилося щонайменше десятиліття, це не може здатися неминучою загрозою. Однак це не так, оскільки квантові комп'ютери Annealing вже є реальністю. Хоча вони не здатні використовувати алгоритм Шора, вони можуть вирішити проблему факторингу, сформулювавши її як задачу оптимізації, і вже досягли значного прогресу.

Крім того, існує також проблема «збирати зараз, розшифрувати пізніше», що по суті означає, що зловмисник може викрасти дані зараз, дочекатися, поки квантові комп'ютери стануть практичною реальністю, і згодом розшифрувати їх пізніше. Це означає, що квантові комп'ютери вже становлять реальну загрозу, навіть не з'явившись на світ. Існує явна ймовірність того, що великі обсяги даних уже скомпрометовані, і вирішення цієї проблеми є невідкладним завданням, тому включення PQC у поточні протоколи шифрування є абсолютно необхідним. Наприклад, згідно зі звітом IBM «Cost of a data breach Report 2023», понад 95 відсотків досліджених організацій у всьому світі стикалися з більш ніж одним порушенням даних. Крім того, знадобиться багато часу, щоб повністю інтегрувати нові алгоритми в усі комп'ютерні системи, тому варто почати якнайшвидше.

Ключова роль Національного інституту стандартів і технологій (NIST)

Незважаючи на те, що в усьому світі існує кілька поточних ініціатив, спрямованих на розвиток PQC, найбільшого прогресу досяг NIST Сполучених Штатів (США). У 2016 році NIST ініціював свій «Проект стандартизації постквантової криптографії», в якому він запросив подати кандидати на алгоритми PQC. Із 69 придатних матеріалів для стандартизації було відібрано чотири: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ і FALCON. Алгоритм Kyber розроблено для загальних цілей шифрування, тоді як решта є схемами цифрового підпису. У серпні 2023 року NIST опублікував проекти стандартів для перших трьох із них, намагаючись отримати відгук громадськості. Він планує випустити їх до 2024 року разом із проектами стандартів для алгоритму FALCON.

Три алгоритми використовують те, що називається «Криптографія на основі решітки», яка базується на проблемі пошуку точки на решітці [i], найближчої до випадкової точки на ній. Як аналогія, це буде схоже на завдання знайти дерево, найближче до випадкового місця в лісі. Це виявляється особливо складною проблемою для граток із великими розмірами, яку, здавалося б, не можуть вирішити навіть квантові комп’ютери.

SPHINCS+, з іншого боку, використовує так звані «хеш-функції», криптографічну схему, яка вже є важливою частиною технології блокчейн. NIST також працює над другим набором алгоритмів, заснованих на різних математичних задачах, які покликані служити резервним копіюванням на випадок, якщо в майбутньому в криптографії на основі решітки виникнуть будь-які недоліки.

Крім цього, Агентство з кібербезпеки та безпеки інфраструктури США, Агентство національної безпеки (NSA) і NIST також опублікували аркуш під назвою «Квантова готовність: перехід до постквантової криптографії», у якому закликали всі організації, особливо ті, що підтримують критичну інфраструктуру, скласти «дорожню карту квантової готовності» для полегшення переходу на стандарти PQC.

Після цього у вересні 2023 року було створено коаліцію PQC, яка має на меті сприяти кращому розумінню PQC і публічному прийняттю алгоритмів NIST. Його

членами є такі технологічні гіганти, як IBM і Microsoft, а також MITRE, PQShield, SandboxAQ і Університет Ватерлоо.

Набіг Індії на PQC

У 2021 році армія Індії разом із Секретаріатом Ради національної безпеки заснували Квантову лабораторію у Військовому коледжі телекомунікаційної техніки, Мхоу, штат Мадья-Прадеш. Вона має на меті очолити дослідження та навчання в галузі квантових обчислень і зв'язку разом із PQC. як одна з головних областей тяги.

Центр розвитку телематики (C-DOT), автономний науково-дослідний центр при Департаменті телекомунікацій, досить активно працює над розвитком PQC. Вона власноруч розробила квантово-захищені продукти, що підтримують алгоритми PQC, наприклад квантово-безпечний шифратор під назвою «Компактний модуль шифрування» та квантово-безпечний відео IP-телефон із підтримкою штучного інтелекту під назвою «Quantum Secure Smart Video IP Phone».

Цікавою подією стала дедалі більша роль стартапів у цій галузі. QNu Labs із Бангалора стала лише четвертою компанією у світі, яка розробила квантово-безпечний продукт безпеки. Він створив алгоритм PQC під назвою «Hodos», який базується на одному з алгоритмів на основі решітки NIST і зробив його комерційно доступним для розгортання організацій. Він також підписав меморандум про взаєморозуміння з підрозділом оборонного державного сектору Bharat Electronics Limited на випадок, якщо в майбутньому буде потрібно створити квантово-безпечні системи безпеки через суб'єкт державного сектору. Інші стартапи, такі як Scytale Alpha і Qulabs, також активно цікавляться PQC.

Майбутні перспективи

Вищезазначені ініціативи, хоч і заслуговують похвали, недостатні, щоб протистояти навислій загрозі квантової переваги. Оскільки кількість витоків даних стрімко зростає протягом багатьох років і постійна загроза з боку Китаю та недержавних груп, Індія повинна забезпечити своєчасний перехід на алгоритми PQC у всіх секторах, особливо в критичній інфраструктурі. Він має створити

процвітаючу екосистему для академічних досліджень, а також підтримувати та стимулювати приватний сектор, який уже показав багато перспектив у цій галузі. Національна квантова місія (NQM), яка є провідною ініціативою Індії в галузі квантових технологій, відіграє ключову роль у цьому відношенні. Якщо NQM сподівається зробити Індію світовим лідером у квантових технологіях, PQC та його впровадження мають стати одним із його невід'ємних компонентів.

Протоколи безпеки працюють лише до тих пір, поки хтось не знайде спосіб їх зламати. Те саме стосується криптографії. Отже, хоча немає гарантії, що алгоритми NIST є герметичними, їм вдалося закласти основу для квантово безпечного майбутнього. Оскільки їх реліз запланований на наступний рік, ще невідомо, чи скористається Індія ситуацією, у неї, безумовно, є можливість це зробити». ***(Prateek Tripathi. Post-Quantum Cryptography: The Lynchpin Of Future Cybersecurity – Analysis // Eurasia Review (https://www.eurasiareview.com/05122023-post-quantum-cryptography-the-lynchpin-of-future-cybersecurity-analysis/?utm_source=flipboard&utm_content=EurasiaReview%2Fmagazine%2FEurasia+Review). 05.12.2023).***

***

«Може настати день, коли надпотужні машини, відомі як квантові комп'ютери, зможуть зламати коди, які захищають наші цифрові дані. Це включає коди, які шифрують дані в наших публічних мережах і захищають інформацію в таких місцях, як банки, державні установи та великі компанії.

Він відомий як «Q-Day». Це стане грандіозним поворотним моментом для того, як світ думає про цифрову конфіденційність, оскільки це може поставити конфіденційну інформацію під загрозу розкриття.

Експерти з кібербезпеки не погоджуються, коли цей день настане. Деякі дослідники прогнозують, що «Q-Day» настане десь у середині століття, повідомляє Reuters. Інші вважають, що це має з'явитися набагато раніше.

«День Q» може настати до 2025 року, заявив Тіло Кунц, виконавчий віце-президент канадської фірми з кібербезпеки Quantum Defen5e, представникам Міністерства оборони США, повідомляє Reuters.

Квантові комп’ютери набагато потужніші, ніж звичайні комп’ютери, оскільки вони покладаються на властивості субатомних частинок для серйозної обробки чисел. Вони можуть виконувати обчислення, які неможливі на сучасних комп’ютерах, і обробляти інформацію на значно вищих швидкостях.

Однією з головних проблем зараз є те, що ключові блоки обробки квантових комп’ютерів, відомі як кубіти, недостатньо стабільні, щоб розшифрувати великі обсяги даних. Тож сучасні квантові комп’ютери все ще досить малі та мають обмежену обчислювальну потужність.

Однак, коли технологія досягне цього, вона, «імовірно, буде настільки ж трансформаційною у 21 столітті, як використання електроенергії як ресурсу в 19 столітті», — сказав Reuters Майкл Берчук, засновник і генеральний директор квантової технологічної компанії Q-CTRL.

Тож глобальні супердержави, такі як Сполучені Штати та Китай, вливають тонни грошей у квантові дослідження напередодні Q-Day. Оскільки такі компанії, як IBM, Amazon, Intel, Google та інші, створюють квантові процесори, Північна Америка вважається лідером у розробці квантових обчислень у 2022 році Сполучені Штати інвестували 1,8 мільярда доларів у квантові дослідження, а Канада виділила ще 100 мільйонів доларів Згідно з оцінками консалтингової компанії McKinsey & Company.

Але Китай не відстає і вкладає гроші в дослідження з приголомшливою швидкістю. Китай оголосив про інвестиції в квантові обчислення на загальну суму понад 15 мільярдів доларів, що означає, що він «є найвищим показником у світі», – сказав McKinsey.

Можна лише здогадуватися, яка країна потрапить туди першою. Але що б з них не було, це може мати далекосяжні наслідки для глобальної безпеки». ***(Lakshmi Varanasi. Brace yourself for 'Q-Day,' a global cybersecurity event that could expose our most important secrets // Insider Inc. (https://www.businessinsider.com/q-day-2025-cybersecurity-quantum-computing-data-security-privacy-china-2023-12?utm_source=flipboard&utm_content=user%2FBusinessInsider). 17.12.2023).***

***