**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

№ 6 (червень)

Київ – 2024

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2024.– №6 (червень) . – 364 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

«Олександр Бабко – засновник компанії DigVel, яка спеціалізується на захисті від кіберзагроз. Олександр має 18-річний досвід у цій сфері. До 2022 року він обіймав посаду технічного директора в IT-компаніях Apriorit та Ekransystem (зараз Syteca), що розробляють інструменти кібербезпеки світового рівня. Після повномасштабного вторгнення вступив до лав ЗСУ.

Усвідомлюючи, що кількість кібератак проти українців продовжує зростати і ворог має певні успіхи на цьому фронті, Олександр вирішив боротися і з цією загрозою та зібрав команду, яка покриває всі аспекти кібербезпеки для малого та середнього бізнесу. У матеріалі для Forbes BrandVoice він розповів, чому під приціл кіберзлочинців потрапляють навіть малі підприємці, до яких втрат може призвести кібератака та як цьому запобігти.

Ризики для малого й середнього бізнесів

Зазвичай на старті підприємці не переймаються питаннями кібербезпеки: немає грошей, часу, фахових спеціалістів у команді. Водночас їм здається, що це не пріоритетний напрям. Мовляв, хакери полюють на великі компанії, а інший бізнес – поза увагою кіберзлочинців. Але це не так. У мене був випадок, коли власник компанії зі штатом 350 людей запевняв, що вони точно нікому не цікаві, а ми за місяць нарахували близько тисячі спроб атак на їхню інфраструктуру.

Сьогодні зловмисники у переважній кількості випадків беруть не якістю жертв, а кількістю. Їм байдуже, чи це великий концерн, чи домашній комп’ютер фрилансера – будь-яка інформація має свою цінність та ціну. Тому малий і середній бізнес може потрапити під кібератаку навіть випадково – й втратити приватні дані, інтелектуальні активи, а головне – довіру клієнтів.

Наведу два показові приклади, як кібератака може призвести до критичних втрат.

Конструкторська компанія зазнала атаки зловмисників, які зашифрували всі їхні креслення, розрахунки та моделі за кілька років роботи. Дані просто зникли й уже не підлягали відновленню.

У телеканала викрали Google-аккаунт, на якому зав’язана вся його онлайн-присутність: пошта, YouTube, соцмережі, реклама. Фактично у них залишився тільки прямий ефір, але охоплення миттєво упало на 60-80%.

Повномасштабна війна принесла нові кібервиклики. З 2022 року Україна – найбільш атакована країна світу. У 2023-му кількість зламів збільшилася на 62,5%.

Якщо йдеться про прицільні атаки, насамперед кіберзлочинців цікавить приватний сектор, який володіє обліковими даними споживачів. Так, зламавши онлайн-магазин із тактичним спорядженням, можна вкрасти інформацію про персональні дані та локації воїнів і волонтерів. Інший фокус атак – на медіа та підрядників державних установ. Наприклад, охоронна компанія встановлює камери відеонагляду, через які хакери намагаються отримати доступ до захищеного периметра.

Також протягом останніх двох років посилилася тенденція до знищення даних. Якщо раніше кіберзлочинність намагалася отримати вигоду й брала дані «в заручники», то зараз вони частіше намагаються саме завдати збитки: людям, компаніям, державі.

Краще щеплення, ніж лікування

Питання кібербезпеки малого та середнього бізнесу в Україні мало чим відрізняється від світового. Але варто зазначити, що у випадку з компаніями з України рівень захищеності не відповідає рівню загроз. За нашим досвідом, у чотирьох із п’яти компаній відсутній базовий контроль безпеки. Вони мають як витоки облікових даних, так і слабкі незахищені місця в інфраструктурі.

Нерідко підприємці замислюються про ті самі «базові засоби захисту», починають про них читати й тонуть в обсязі та складності інформації. Кібербезпека – широкий домен, у який важко увійти. Людина не знає, який варіант краще обрати та як його впровадити. А тому просто вирішує нічого не робити, бо занадто важко, дорого і «наразі на нас не нападали».

Але ідея кібербезпеки у тому, що вона має будуватися превентивно. Зазвичай ми робимо щеплення, а не лікуємось від гепатиту чи правця. Та й вилікувати бізнес не завжди можливо: якщо компанія втратила всі дані, це може призвести до

банкрутства й необхідності починати з нуля. Немає сенсу розгортати кіберзахист, коли вас уже «кібервбили».

Водночас це не означає, що коли стався кіберінцидент, то не треба звертатися за допомогою, бо «нічого не вдієш». Ймовірність того, що вам вдасться відновитися, якщо ви попередньо звертали увагу на кіберзахист, значно вища.

Наприклад, один із наших клієнтів – телекомунікаційна компанія – став жертвою атаки на свої новинні канали. Хакери здійснили напад пізно ввечері, але вже за кілька хвилин ми розпочали дії з усунення наслідків. Наша команда за години зробила те, що вимагає тижнів, і запобігла суттєвим збиткам. Уже наступного дня діяльність більшості функцій було відновлено.

Кіберзахист без бюджету та технічних фахівців

Створюючи компанію, ми від початку орієнтувалися на потреби малого та середнього бізнесу. В Україні загалом небагато компаній, які забезпечують кіберзахист. А ті, що є, здебільшого працюють із великими організаціями, фінансовими установами й об’єктами критичної інфраструктури. Водночас саме на малий та середній бізнес припадає понад 60% нашої економіки, тому ми поставили мету – не допустити зупинення їхньої діяльності.

Зараз ми працюємо над стандартом кіберстійкості, який плануємо викласти у відкритий доступ. На відміну від інших наявних матеріалів і стандартів, він написаний простою мовою і зрозумілий нетехнічним фахівцям. Тож навіть ті підприємці, у яких немає бюджету на надмірні витрати й команду професіоналів, можуть сфокусувати зусилля на простих і дієвих засобах.

Стандарт визначає п’ять послідовних рівнів стійкості з контрольними точками й осяжними результатами. Їхнє впровадження займає близько півтора року, залежно від розміру компанії та вмотивованості керівництва. Але навіть досягнення другого рівня, яке потребує до чотирьох місяців, уже закриває ключові ризики для бізнесу.

Наприклад, мінімальні дії, які кожен може зробити тут і зараз:

Максимально захищайте усе, куди можна увійти з інтернету: хмарні сервіси, соцмережі, сайти, сервери. Зробіть стійкі унікальні паролі, налаштуйте багатофакторну аутентифікацію.

Обмежте кількість публічно доступних (з інтернету) ресурсів і регулярно їх оновлюйте. У програмах щодня знаходять критичні вразливості, які хакери охоче використовують.

Робіть резервні копії критичних даних.

Ми надаємо клієнтам супровід і реагування на інциденти, проводимо аудити та пентести, консультуємо, допомагаємо побудувати політику безпеки. Та головне – намагаємося змінювати свідомість підприємців і менеджерів, аби вони краще зрозуміли масштаб і реальність загрози. Всі охоче інвестують у фізичну безпеку, міцні двері та ґрати на вікнах, але кіберпростір вимагає не меншої уваги.

Ще один напрям нашої роботи – створення в Україні партнерської мережі кіберзахисників. Ми впевнені, що одна окрема компанія не здатна покрити всі проблеми, пов’язані з кіберзагрозами. Тому налагоджуємо зв’язки з колегами по ринку. Завжди готові підхопити їхні завдання, які вони не встигають виконати, а також ділимося своїми, якщо не справляємося самостійно. Зараз час не для конкуренції, а для взаємодії заради спільної мети». ***(Кіберзахист для малого та середнього бізнесу: яким є масштаб загроз і що робити, якщо немає бюджету. Розповідає CEO DigVel Олександр Бабко // ТОВ "УЯВИ!" (https://forbes.ua/brandvoice/kiberzakhist-dlya-malogo-ta-serednogo-biznesu-masshtab-zagroz-i-shcho-robiti-yakshcho-nemae-byudzhetu-rozpovidae-seo-digvel-oleksandr-babko-30062024-21931). 27.06.2024).***

***

«20 червня Державна служба спеціального зв’язку та захисту інформації України відкрила перший Кваліфікаційний центр інформаційних технологій та кібербезпеки, який сприятиме впровадженню сучасної системи професійної сертифікації кіберспеціалістів.

Відкриття Кваліфікаційного центру сприятиме впровадженню сучасної системи професійної сертифікації кіберспеціалістів, що враховує кращі світові практики, зокрема Cybersecurity Workforce Framework USA (NICE NIST 800-801) та Європейської рамки навичок з кібербезпеки (ECSF ENISA).

Мета – сформувати в Україні спроможний, систематизований та професійний ринок праці в галузі кібербезпеки.

Уже зараз фахівці можуть підтвердити свої навички та компетенції у Кваліфікаційному центрі за двома новими професійними стандартами, а саме «Розробник безпеки інформаційних систем» та «Адміністратор безпеки мережі та систем». Надалі планується розширення переліку доступних кваліфікацій.

Відкриття Кваліфікаційного центру є кульмінацією допомоги та підтримки від Проєкту USAID Кібербезпека у розробленні та впровадженні Національної рамки професійних стандартів із кібербезпеки, яку реалізує Держспецзв’язку. Зміцнюючи кадровий потенціал України у сфері кібербезпеки разом з партнерами, ми підвищуємо захист України у кіберпросторі, – зазначив керівник Проєкту USAID Кібербезпека Петро Матіяшек». ***(Валерія Панасюк. В Україні відкрили перший Кваліфікаційний центр для фахівців з кібербезпеки // META.UA (https://meta.ua/uk/news/society/175652-v-ukrayini-vidkrili-pershii-kvalifikatsiinii-tsentr-dlya-fahivtsiv-z-kiberbezpeki/). 21.06.2024).***

***

«Держспецзв'язку презентувала представникам державних органів України нові технічні рішення для захисту установ від DDoS атак. Ці рішення забезпечують ефективне виявлення та блокування різних типів кіберзагроз та розширений моніторинг і аналіз інтернет-трафіку.

Про це повідомили у Держспецзв'язку.

Під час презентації представники Держспецзв'язку продемонстрували можливості програмної продукції та сервісної підтримки компаній Radware та Akamai Technologies, що розгорнуті в Державному центрі кіберзахисту.

Очільник відомства Юрій Мироненко закликав працівників з держсектору по максимуму використати ці можливості, щоб ефективніше захищатись від кібератак з боку противника.

Він також подякував проєкту USAID «Кібербезпека критично важливої інфраструктури України» за допомогу з програмною продукцією та сервісною підтримкою.

«Завдяки допомозі USAID ми оновили й суттєво покращили спроможності урядової команди реагування CERT-UA та Державного центру кіберзахисту. Ми також спільно впроваджуємо найкращі світові практики у сфері кібербезпеки, розвиваємо співпрацю з Агенцією США з кібербезпеки та інфраструктури CISA», – сказав Мироненко.

Директорка бюро з питань демократії та врядування місії USAID в Україні Енн Хоппер зазначила, що США твердо підтримують Україну у її протистоянні повномасштабному вторгненню Росії, у тому числі у кіберпросторі.

«Кібербезпека — це не лише про захист даних. Це й про те, що мільйони українців можуть безперебійно отримувати державні послуги щодня. Для цього USAID підтримало Держспецзв'язку у покращенні технічних спроможностей для захисту 70 державних інтернет-ресурсів та вебсервісів від DDoS атак і планує підтримати захист ще 170 ресурсів, інтегрувавши їх у Центр очищення трафіку Держспецзв'язку від DDoS атак», – наголосила вона». ***(Дмитро Михайлов. В Україні презентували нові технічні рішення для захисту держустанов від DDoS атак // АТ «НСТУ» (https://suspilne.media/777889-v-ukraini-prezentuvali-novi-tehnicni-risenna-dla-zahistu-derzustanov-vid-ddos-atak/). 27.06.2024).***

***

Кібервійна проти України

«Зловмисник намагається розгорнути постексплойтовий інструментарій Cobalt Strike на системах Windows, що належать користувачам в Україні.

Схоже, у центрі кампанії – отримати повний дистанційний контроль цільових систем для майбутнього розгортання корисного навантаження та потенційно інших шкідливих цілей, повідомили дослідники Fortinet у блозі цього тижня.

Документ на українську тему

Постачальник засобів безпеки описав загрозливого актора як використання файлу Excel на українську тематику з вбудованим макросом програми Visual Basic (VBA) як початкову приманку. Якщо необачний користувач вмикає макрос, він розгортає завантажувач бібліотеки динамічних посилань (DLL), обфускований за допомогою інструмента з відкритим кодом ConfuserEX, у системі жертви.

Одне з перших, що робить завантажувач DLL, це шукає наявність антивіруса та інших інструментів виявлення зловмисного програмного забезпечення в скомпрометованій системі. Якщо завантажувач виявляє наявність такого, він негайно припиняє подальшу діяльність. В іншому випадку він використовує веб-запит для отримання корисного навантаження наступного етапу з віддаленого місця. Завантажувач DLL розроблено таким чином, що він може завантажувати корисне навантаження другого етапу лише на пристрої, розташовані саме в Україні. Після цього завантажувач виконує ряд кроків, які призводять до розгортання Cobalt Strike на пристрої-жертві.

«У цій складній атаці зловмисник використовує багатоетапну тактику зловмисного програмного забезпечення, щоб перешкодити виявленню, забезпечуючи при цьому стабільність роботи», — написала в блозі дослідниця безпеки Fortinet Кара Лін. «Впроваджуючи перевірку на основі розташування під час завантажень корисного навантаження, зловмисник прагне замаскувати підозрілу активність, потенційно уникаючи уваги аналітиків», — додав Лін.

Інші механізми ухилення та збереження включають використання закодованих рядків у макросі VBA для полегшення розгортання файлів DLL, функцію самовидалення для ухилення від механізмів виявлення та інжектор DLL, який використовує тактику затримки, і механізми завершення батьківського процесу для уникнення пісочниці.

«Ці організовані маневри спрямовані на розгортання Cobalt Strike на цільових кінцевих точках, зокрема в межах геополітичного ландшафту України», — сказав Лінь.

Шаблон націлювання

Нова кампанія схожа на численні інші, спрямовані проти окремих осіб і організацій в Україні, про які Fortinet та інші повідомляли в останні роки, особливо після вторгнення Росії в 2022 році. Багато з цих атак включали спроби порушити та погіршити можливості критичної інфраструктури України. Інші нападали на український уряд і військові організації, часто для підтримки російських військових цілей у країні.

Кібергрупи, що базуються в Росії та ті, хто працює на її військову розвідку, часто були основними злочинцями. Їх обрана зброя включала все, починаючи від гучних очищувачів даних і програм-вимагачів і закінчуючи надзвичайно складними спеціальними інструментами, такими як «Industroyer», який російська група Sandworm використовувала для атак на українську електромережу.

Нові атаки, які нещодавно виявила компанія Fortinet, також не є першими випадками використання Cobalt Strike проти українських цілей. У 2022 році компанія спостерігала, як інший суб'єкт загрози використовував документ Excel на українську військову тематику для доставки Cobalt Strike на системи в Україні. Минулого року Українська команда реагування на комп'ютерні надзвичайні ситуації повідомила, що суб'єкт загрози UAC-0057 використовував XLS-файл із вбудованим макросом та зображенням-приманкою для розгортання шкідливого програмного забезпечення Cobalt Strike Beacon та PicassoLoader на комп'ютерах жертв в Україні». ***(Jai Vijayan. Ukrainian Systems Hit by Cobalt Strike Via a Malicious Excel File // Informa PLC (https://www.darkreading.com/cyberattacks-data-breaches/ukrainian-systems-hit-by-cobalt-strike-via-a-malicious-excel-file?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 05.06.2024).***

***

«Прокурори Міжнародного кримінального суду (МКС) розслідують ймовірні російські кібератаки на українську цивільну інфраструктуру як можливі військові злочини, повідомили Reuters чотири джерела, знайомі зі справою.

Це перше підтвердження того, що атаки в кіберпросторі розслідуються міжнародними прокурорами, що може призвести до видачи ордерів на арешт, якщо буде зібрано достатньо доказів.

За словами одного з чиновників, розслідування перевіряє атаки на інфраструктуру, які поставили під загрозу життя через порушення електропостачання та водопостачання, переривання з'єднань із службами екстреного реагування або виведення з ладу мобільних служб передачі даних, які передають попередження про повітряний наліт.

Прокурори МКС працюють разом з українськими командами над розслідуванням «кібератак, скоєних з початку повномасштабного вторгнення» в лютому 2022 року, сказав чиновник, який відмовився залишитися названим, оскільки розслідування ще не завершено.

Два інших джерела, близьких до офісу прокурора МКС, підтвердили, що вони досліджують кібератаки в Україні, і сказали, що вони можуть повернутися до 2015 року, року після захоплення Росією та односторонньої анексії Кримського півострова від України.

Москва раніше заперечувала, що здійснює кібератаки, а офіційні особи назвали такі звинувачення спробами розпалювання антиросійських настроїв.

Україна збирає докази на підтримку розслідування прокуратури МКС.

У п'ятницю прокуратура МКС відмовилася від коментарів, але раніше заявила, що має юрисдикцію розслідувати кіберзлочини. Він також заявив, що не може коментувати питання, пов'язані з поточними розслідуваннями.

РОСІЯН ЗВИНУВАЧУЮТЬ У ЗЛОЧИНАХ ПРОТИ ЛЮДЯНОСТІ

З початку вторгнення суд видав чотири ордери на арешт високопоставлених росіян. Серед них президент Володимир Путін, якого підозрюють у військовому злочині через депортацію українських дітей до Росії.

Росія, яка не є членом МКС, відкинула це рішення як «недійсне». Україна також не є членом, але надала юрисдикцію МКС переслідувати злочини, скоєні на її території.

У квітні палата попереднього судочинства видала ордери на арешт, стверджуючи, що двоє російських командирів скоїли злочини проти людяності, завдавши ударів по цивільній інфраструктурі. Міністерство оборони Росії тоді не відповіло на запит про коментар.

Щонайменше чотири великі атаки на енергетичну інфраструктуру розглядаються, повідомили Reuters два джерела, знайомі з розслідуванням.

Високопоставлене джерело повідомило, що одна група російських хакерів у прицілі ICC відома в дослідницьких колах кібербезпеки як «Sandworm», і українські чиновники та кіберексперти вважають її пов’язаною з російською військовою розвідкою.

Команда Центру з прав людини при Школі права Каліфорнійського університету в Берклі розслідує кібератаки Sandworm на українську цивільну інфраструктуру з 2021 року та подала конфіденційні подання до МКС у 2022 та 2023 роках, у яких виявила п’ять кібератак, які, за її словами, можуть бути визнані військовими злочинами.

Sandworm підозрюють у серії резонансних атак, включаючи успішну атаку на електромережу в західній Україні в 2015 році – одну з перших у своєму роді, за словами дослідників кібербезпеки.

Група хакерів-активістів, які називають себе «Солнцепьок» («гаряча точка»), взяла на себе відповідальність за велику атаку на українського оператора мобільного зв'язку «Київстар» 12 грудня минулого року. Українські спецслужби визначили цю групу як прикриття для Sandworm.

Київ також вважає, що Sandworm здійснював широке кібершпигунство проти західних урядів від імені російських спецслужб.

ЧИ МОЖЕ КІБЕРАТАКА БУТИ ВІЙСЬКОВИМ ЗЛОЧИНОМ?

Кібератаки, націлені на промислові системи управління, технологію, яка лежить в основі більшої частини світової промислової інфраструктури, рідкісні, але

Росія є однією з невеликого клубу країн, які мають для цього засоби, кажуть дослідники кібербезпеки.

Справа МКС, яка може створити прецедент для міжнародного права, уважно стежиться.

Міжнародне право, яке стосується збройних конфліктів, закріплене в Женевських конвенціях, забороняє напади на цивільні об’єкти, але немає загальноприйнятого визначення того, що є кібервійськовим злочином.

У 2017 році правознавці підготували довідник під назвою «Талліннський посібник із застосування міжнародного права до кібервійни та кібероперацій».

Але експерти, опитані Reuters, кажуть, що незрозуміло, чи можна вважати самі дані «об'єктом» атаки, забороненої міжнародним гуманітарним правом, і чи може їх знищення, яке може бути руйнівним для мирного населення, вважатися військовим злочином.

«Якщо суд візьметься за це питання, це створить для нас велику ясність», — сказав професор Майкл Шмітт з Редінгського університету, який очолює процес Талліннського посібника.

Шмітт вважає, що злом «Київстару», який належить голландській компанії Veon, відповідає критеріям воєнного злочину.

«Ви завжди дивитесь на передбачувані наслідки своєї операції. І, ви знаєте, це був передбачуваний наслідок, який поставив людей під загрозу».

Українська розвідка заявила, що передала деталі інциденту слідчим МКС у Гаазі. «Київстар» заявив, що аналізує атаку у партнерстві з міжнародними постачальниками та СБУ, спецслужбою України». ***(Anthony Deutsch, Stephanie van den Berg, James Pearson. Exclusive: ICC probes cyberattacks in Ukraine as possible war crimes, sources say // Reuters (https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/). 14.06.2024).***

***

«У Росії стався масштабний збій в роботі електронних сервісів, за яким стоять кіберфахівці Головного управління розвідки Міноборони України.

Про це у середу, 5 червня, пише «Українська правда» з посиланням на співрозмовників у ГУР МОУ.

Відомо, що фактично паралізовано роботу низки державних установ та приватних компаній РФ. Офіційне повідомлення «Роскомнадзора» стверджує, що збої є наслідком «аварії магістральної мережі зв'язку». Втім, за даними джерел ЗМІ, справжня причина у масштабній DDoS-атаці, яку зараз проводять кіберфахівці ГУР МОУ.

Станом на 11 годину 5 червня зник доступ до електронних сервісів сайту держпослуг, а також до послуг низки міністерств: міністерства оборони, фінансів, внутрішніх справ, юстиції, промисловості та енергетики, інформаційних технологій та зв'язку, надзвичайних ситуацій.

Заблоковано сайт та сервіси федеральної податкової служби РФ. Оприлюднено повідомлення від федеральної митної служби, де вказано що «у зв'язку з масованою DDoS-атакою на операторів зв'язку, інформаційний обмін з учасниками зовнішньоекономічної діяльності ускладнений».

Про відсутність доступу до мережі заявила «Об'єднана авіабудівельна компанія». Її роботу на певний час було паралізовано. Зафіксовано також збої в роботі серверів хмарного сховища РФ «гособлако». І наостанок в низці регіонів Росії вже кілька днів не працює "єдиний державний реєстр РАГС": росіяни масово скаржаться на скасовані весілля, додає джерело видання.

Недоступними є послуги деяких банківських установ, зокрема, "Сбербанка" та «Альфабанка».

За словами співрозмовника журналістів, також є серйозні перебої в роботі мережі «ВКонтакте» – низка сервісів недоступна». ***(ГУР влаштувало масштабну DDoS-атаку на держустанови та великі компанії РФ, – ЗМІ // Новинарня (https://novynarnia.com/2024/06/05/gur-vlashtuvalo-masshtabnu/). 05.06.2024).***

***

«Декілька російських інтернет-провайдерів зазнали масштабної кібератаки. Окупаційна влада півострова попередила місцевих жителів про те, що найближчим часом можуть виникнути проблеми із доступом до інтернету.

Як повідомив в інтерв'ю для «Суспільне Крим» представник ГУР, ця атака — наслідок роботи українських кіберфахівців воєнної розвідки.

Що відомо про атаку на окупаційних інтернет-провайдерів у Криму

За словами представника української розвідки, атаки одночасно зазнали одразу декілька надавачів інтернет-послуг на тимчасово окупованій території.

Окупаційна заступниця міністра внутрішньої політики, інформації та зв’язку окупаційної адміністрації Юлія Кирик заявила, що профілі DDos-атак постійно змінюються, а фахівці провайдерів нібито вживають заходів для протидії атакам.

«Здається, російським кібернетикам час згадати про імпортозамєщєніє, увімкнути свій «Чебурнет» замість Всесвітньої мережі та встановити ісконно-руський фаєрвол, відгородившися від усього вільного світу. Лише так у них є шанс убезпечитися від наших атак», — заявив співробітник ГУР.

Також експерт зазначив, що це вже не перша атака на російські сервери. Останнім часом таке відбувається систематично. Наприклад, на початку червня ГУР атакувало сайти Міністерства юстиції, Міністерства оборони, Міністерства інформаційних технологій і зв'язку, Міністерства фінансів, Міністерства внутрішніх справ, Міністерства надзвичайних ситуацій, Міністерства промисловості та енергетики РФ. А в так званий день Росії, 12 червня, атаки зазнали онлайн-платформи російських аеропортів, унаслідок чого затрималися авіарейси…». ***(Чекарьова Марія. ГУР здійснило атаку на російських інтернет-провайдерів у Криму // ТОВ «МЕДІАМЕРЕЖІ» (https://segodnya.novyny.live/gur-zdiisnilo-ataku-na-rosiiskikh-internet-provaideriv-u-krimu-182547.html). 26.06.2024).***

***

«Хакери атакують військових і держслужбовців у Signal. Про це повідомили в Центрі стратегічних комунікацій та інформаційної безпеки.

Зловмисники здійснюють кібератаки на держслужбовців, військових, представників оборонних підприємств України з використанням шкідливої програми DarkCrystal RAT, повідомили у CERT-UA.

Файл поширюють у Signal, при цьому відправником може бути людина зі списку контактів чи спільних груп.

Повідомлення, насправді надіслане хакерами, містить архів, пароль і повідомлення щодо необхідності відкриття файлу саме на комп'ютері.

Зазвичай архів містить виконуваний файл (розширення:.pif,.exe), запуск якого призведе до ураження комп'ютера шкідливою програмою DarkCrystal RAT.

Це створить технічну можливість прихованого несанкціонованого доступу до комп'ютера». ***(Хакери атакують військових і держслужбовців у Signal // Агенція інформації та аналітики (https://galinfo.com.ua/news/hakery_atakuyut_viyskovyh_i_derzhsluzhbovtsiv_u_signal_419639.html). 12.06.2024).***

***

«Група хакерів UAC-0020 (Vermin), пов'язаних з «силовими органами» окупованого Луганська, атакувала Сили оборони України, відправляючи шкідливі електронні листи, що містять шкідливе ПЗ SPECTR.

Група хакерів UAC-0020 (Vermin), пов'язана із силовими відомствами окупованого Луганська, атакувала Сили оборони України, передає УНН із посиланням на Держспецзв'язку.

Деталі

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA у взаємодії з Центром кібербезпеки ЗСУ виявила та дослідила ворожу активність угрупування UAC-0020 (Vermin) проти Сил оборони України.

Що сталося:

- група хакерів UAC-0020 (Vermin), пов'язана із силовими відомствами окупованого Луганська, атакувала Сили оборони України;

- зловмисники розсилали електронні листи з вкладенням у вигляді архіву «туррель.фоп.вовчок.rar», який містив файл-приманку «Wowchok.pdf»; EXE-інсталятор «sync.exe» та BAT-файл «run_user.bat»;

- файл «sync.exe» містив як легітимні компоненти програми SyncThing, так і файли шкідливих програм SPECTR;

- викрадена інформація (документи, файли, паролі) надсилалася на комп'ютер зловмисника за допомогою штатного функціоналу синхронізації SyncThing». ***(Антоніна Туманова. Пов'язані із «силовиками» окупованого Луганська: група хакерів атакувала Сили оборони України // Інформаційне агентство «Українські Національні Новини» (https://unn.ua/news/poviazani-iz-sylovykamy-okupovanoho-luhanska-hrupa-khakeriv-atakuvala-syly-oborony-ukrainy). 06.06.2024).***

***

Боротьба з кіберзлочинністю в Україні

«Житель Одеси розробляв віруси на телефони, за допомогою яких викрадав кошти з банківських рахунків та міг слідкувати за користувачем пристрою. Також свою «розробку» він продавав на форумах даркнету та закритих Телеграм-чатах, за що тепер може сісти за ґрати.

Про це повідомили у пресслужбі Управління СБ України в Одеській області.

Деталі діяльності

36-річний одесит створив та адміністрував закритий Телеграм-канал майже з тисячею підписників. Там пропонувалось придбати або орендувати його «розробку», ціна для покупців становила 1 500 доларів.

Вірусні файли маскував під різні мобільні додатки. У разі встановлення на пристрій зловмисник отримував віддалений доступ до онлайн-банкінгу, мобільних месенджерів та інших додатків «жертви».

Крім того, з телефонів потерпілих можна було дистанційно керувати дзвінками та камерою пристрою. Правоохоронці провели обшуки в помешканні

одесита та вилучили мобільну й комп’ютерну техніку зі зразками шпигунських програм.

Яке покарання загрожує

Наразі фігуранту повідомили про підозру за ч. 2 ст. 361-1 Кримінального кодексу України (створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут). Йому загрожує до п'яти років позбавлення волі.

Інші злочини на Одещині

Ми писали, що одесит шахрайським шляхом отримував кошти громадян, використовуючи фішингову схему. Він зімітував державний сайт "єПідтримка" та заволодів понад 120 тисячами гривень жертв, за що тепер йому загрожує ув'язнення.

Також ми повідомляли, що мешканець Ізмаїльської громади продавав фейкові електронні документи через інтернет. Хлопець завантажив підроблену «Дію», а згодом вирішив продавати копії застосунку. За це йому загрожує до п'яти років тюрми». ***(Верзілова Єлизавета. Хакер з Одеси продавав вірус для слідкування за чужими телефонами — що загрожує // ТОВ «МЕДІАМЕРЕЖІ» (https://odesa.novyny.live/khaker-z-odesi-prodavav-virus-dlia-slidkuvannia-za-chuzhimi-telefonami-shcho-zagrozhuie-182694.html). 27.06.2024).***

***

Світові тенденції в галузі кібербезпеки

«Пандемія COVID-19 різко змінила глобальний робочий ландшафт — віддалений офіс став новою нормою. Співробітники насолоджуються гнучкішим графіком і додатковими годинами свободи, приймаючи нову якість балансу між роботою та особистим життям, а роботодавці цінують економію коштів від відмови від оренди офісів та інших витрат.

Однак навігація цифровим робочим простором з дивана пов’язана з власним набором загроз: фішингові шахрайства, які виглядають як легальні електронні

листи, програми-вимагачі, які крадуть приватні файли за гроші, і хакери, які прослуховують чати Wi-Fi через те, що не дуже безпечна домашня мережа.

Основою безпеки даних компанії, незалежно від того, передаються чи зберігаються, є надійна політика віддаленого доступу. Цей набір інструкцій, який зазвичай встановлює IT-команда компанії або відділ безпеки даних, діє як дорожня карта для віддалених співробітників та їхніх пристроїв, забезпечуючи безпечний доступ до мереж компанії.

Він охоплює такі основні аспекти, як використання віртуальної приватної мережі (VPN) для безпечної онлайн-навігації, встановлення програмного забезпечення для захисту від зловмисного програмного забезпечення на всіх пристроях співробітників і впровадження багатофакторної автентифікації (MFA) для перевірки ідентичності користувачів.

Хоча розробка комплексної політики віддаленого доступу спочатку може здатися складною, зосередження уваги на основних стратегіях безпеки допомагає створити гнучку структуру, адаптовану до потреб вашої компанії. Дотримуйтеся прямолінійного підходу — націлюйтеся на такі важливі елементи, як контроль доступу, шифрування даних, захист кінцевої точки та навчання користувачів. За допомогою надійних основоположних практик ви зможете налаштовувати політику відповідно до розвитку свого бізнесу.

10 стратегій кібербезпеки для віддалених працівників

1. Захистіть дані під час передавання

Основною метою захисту даних під час передачі є захист конфіденційної інформації під час її переміщення мережами від перехоплення кіберзлочинцями. Це вкрай важливо для збереження конфіденційності та цілісності корпоративних даних, особистої інформації та інтелектуальної власності.

Ця стратегія використовує протоколи шифрування, такі як SSL (Secure Sockets Layer) і TLS (Transport Layer Security), щоб створити безпечний і зашифрований канал між двома системами. Завдяки обміну ключами шифрування ці протоколи забезпечують шифрування даних перед надсиланням і можуть бути

розшифровані лише на пристрої одержувача, що робить перехоплені дані неможливими для читання сторонніми особами.

2. Захист даних у спокої

Шифрування даних у стані спокою має на меті захистити дані, що зберігаються на пристроях, що особливо важливо у випадку втрати або крадіжки пристрою. Цей захід є основоположним для захисту конфіденційної інформації та дотримання різноманітних правил захисту даних.

Вбудовані інструменти шифрування, такі як BitLocker для Windows і FileVault для macOS, шифрують носій даних пристрою, наприклад жорсткі диски, за допомогою надійних алгоритмів шифрування. Цей процес робить дані на цих пристроях недоступними без правильного ключа шифрування або облікових даних користувача, ефективно захищаючи дані від несанкціонованого доступу, навіть якщо фізичну безпеку пристрою порушено.

3. Прийміть керування ідентифікацією та доступом

Системи IAM призначені для контролю та моніторингу доступу користувачів до ресурсів компанії, гарантуючи, що працівники мають відповідні рівні доступу відповідно до вимог їх роботи. Це життєво важливо для запобігання несанкціонованому доступу до конфіденційної інформації та для загальної безпеки цифрового середовища компанії.

Рішення IAM, такі як Okta або Microsoft Azure Active Directory, забезпечують централізоване керування ідентифікаторами користувачів і дозволами. Вони пропонують такі функції, як єдиний вхід (SSO), багатофакторна автентифікація (MFA) і автоматичне надання облікових записів користувачів. Завдяки управлінню цифровими ідентифікаторами ці технології гарантують, що лише авторизовані користувачі можуть отримати доступ до певних даних і додатків, підвищуючи безпеку та сприяючи дотриманню нормативних вимог.

4. Безпечний захист кінцевої точки для віддалених співробітників

Мета полягає в тому, щоб захистити кінцеві пристрої (ноутбуки, смартфони), якими користуються віддалені співробітники, від шкідливих програм, програм-вимагачів та інших кіберзагроз. Захищені веб-шлюзи також використовуються для

захисту доступу до Інтернету та запобігання доступу до шкідливих веб-сайтів, підвищуючи загальну кібербезпеку.

Це передбачає встановлення надійного антишкідного програмного забезпечення та антивірусного програмного забезпечення на всіх кінцевих пристроях для виявлення та усунення загроз. Захищені веб-шлюзи додатково захищають користувачів, фільтруючи небажане програмне забезпечення/зловмисне програмне забезпечення від Інтернет-трафіку, забезпечуючи безпечний перегляд і використання Інтернету.

5. Впровадити заходи захисту від DDoS

В офісному середовищі розподілені атаки на відмову в обслуговуванні (DDoS), які переповнюють мережу надмірним трафіком, можуть призвести до мінімальних збоїв. Однак для віддалених команд DDoS-атака на VPN може суттєво вплинути на роботу, порушуючи можливість доступу до критичних корпоративних ресурсів.

Щоб захиститися від цих атак, розгляньте можливість використання служб запобігання DDoS, які можуть виявляти та фільтрувати зловмисний трафік до того, як він досягне мережі. [Примітка редактора: компанія автора є однією з багатьох, які пропонують такі послуги.]

6. Розгорніть захист від фішингу та захоплення облікових записів

Ця стратегія зосереджена на мінімізації ризику фішингових атак і несанкціонованого доступу до облікового запису шляхом навчання співробітників розпізнаванню спроб фішингу та застосування суворих заходів безпеки, таких як MFA.

Регулярні тренінги з кібербезпеки, які інформують співробітників про новітні технології фішингу та способи їх уникнення, можуть зменшити ризик успішних атак. Надійна політика паролів і застосування MFA додають рівень безпеки, значно знижуючи ризик захоплення облікових записів.

7. Використовуйте аналітику поведінки користувачів (UBA) і Zero-Trust Framework

UBA має на меті виявляти аномалії в поведінці користувачів, які можуть вказувати на загрозу безпеці, наприклад зламані облікові дані або внутрішні загрози, шляхом аналізу звичайних моделей активності.

Такі інструменти, як Splunk або Exabeam, використовують машинне навчання для аналізу моделей доступу користувачів і виявлення відхилень від норми. Ці аномалії позначено для подальшого дослідження.

Структура нульової довіри працює за принципом «ніколи не довіряй, завжди перевіряй», який вимагає перевіряти особу користувачів і цілісність їхніх пристроїв перед наданням доступу до ресурсів компанії.

8. Захистіть параметри хмари та керуйте доступом

Виправлення та захист хмарних конфігурацій є важливими для захисту від зламів через неправильні конфігурації або вразливості, особливо в умовах збільшення впровадження хмарних служб.

Регулярні аудити та використання хмарних інструментів безпеки від таких постачальників, як AWS або Azure, допомагають виявити та виправити незахищені конфігурації. Ефективний контроль доступу користувачів гарантує, що лише авторизовані користувачі або групи користувачів можуть отримати доступ до певних хмарних ресурсів, зменшуючи ризик розкриття даних.

9. Впроваджуйте регулярні оновлення програмного забезпечення та керування виправленнями

Оновлення програмного забезпечення та систем є важливим для захисту від відомих уразливостей і експлойтів, які часто стають цілями кіберзлочинців.

Автоматизовані інструменти, такі як WSUS (Windows Server Update Services) для Windows або Jamf для macOS, гарантують, що всі пристрої в мережі отримають найновіші виправлення та оновлення безпеки, усуваючи вразливості та підвищуючи безпеку.

10. Запровадити (або оновити) плани реагування на інциденти

Наявність надійного плану реагування на інциденти допомагає мінімізувати збитки під час інциденту кібербезпеки та сприяє швидкому та організованому відновленню.

Це передбачає регулярний перегляд і тестування плану реагування на інциденти шляхом моделювання кібератак, а потім уточнення та оновлення його на основі отриманої інформації та отриманих уроків, забезпечуючи готовність до інцидентів у реальному світі.

Ще одна порада

Якщо ваша компанія працює в межах Європейського Союзу (або обробляє персональні дані осіб, які проживають у ЄС, незалежно від місця розташування), то вкрай важливо перевірити свою відповідність Загальному регламенту захисту даних (GDPR) — комплексному закону про конфіденційність даних, який містить правила управління персональними даними та запровадження можливих штрафів за недотримання». ***(Victor Zyamzin. Remote Work's Hidden Dangers // Informa PLC (https://www.darkreading.com/endpoint-security/remote-works-hidden-dangers?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 05.06.2024).***

***

«…державні інституції, зокрема, погано обладнані для виконання цифрової відповідальності, пов'язаної з керуванням такою величезною кількістю персональних даних. На відміну від приватних підприємств, державний сектор зазвичай не має належного фінансування чи персоналу або просто не зміг зробити кібербезпеку пріоритетом, яким він має бути.

Дійсно, останні кібератаки на державний сектор малюють жахливу картину. У 2023 році група програм-вимагачів Medusa атакувала систему державних шкіл Міннеаполіса, вимагаючи викупу в 1 мільйон доларів. Коли викуп не було сплачено, стався витік конфіденційних файлів. Серед них документи про жорстоке поводження, сексуальне насильство, психіатричне здоров'я студентів, медичні записи та ті маленькі шматочки золота, які називаються номерами соціального страхування.

Це лише один приклад.

Як це роблять зловмисники?

Соціальна інженерія залишається найпоширенішим вектором атак для кіберзлочинців. Фішинг і його різновиди, такі як компрометація бізнес-електронної пошти, становлять 70-90% усіх порушень і продовжують вловлювати працівників державного сектору. Хакери використовують ці точки входу, щоб обманом змусити державних службовців перейти за шкідливим посиланням і, як наслідок, розкрити свою установу та дані, які вони мають намір захистити.

Крім того, на радість кіберзлочинцям з'явився новий інструмент: генеративний штучний інтелект. GenAI може не тільки розробляти нове шкідливе програмне забезпечення, але також може допомагати зловмисникам розробляти більш складні атаки соціальної інженерії. Кіберзлочинцям більше не потрібно бути експертами в хакерстві або добре знати англійську мову; тепер штучний інтелект може зробити цю роботу за них.

Що з цим може зробити державний сектор?

Реальність така, що люди, які найменше обізнані про загрози безпеці, часто становлять найбільший ризик. Співробітники, які не знають про загрози, протоколи та процедури реагування, є найімовірнішими жертвами атак соціальної інженерії. З цієї причини навчання з питань безпеки має першочергове значення. Щоб зміцнити цей плямистий рівень кіберзахисту людини, агентства можуть запроваджувати різноманітні кампанії з підвищення обізнаності. Це навчання може приймати різні форми, наприклад тематичні дослідження, ігри, симуляції фішингу тощо. Мета полягає в тому, щоб навчити вразливу робочу силу, особливо тих, хто не вважає себе частиною проблеми.

Співробітники не люблять, коли їм кажуть, що вони роблять щось не так або що їм потрібно зробити щось інакше. Вони запитують, навіщо їм витрачати дорогоцінний час на дотримання процедур кібербезпеки та докладати зусиль, щоб звернути увагу на кожне ймовірно підозріле посилання в електронному листі, коли вони відчувають, що ніколи не попадуться на виверт соціальної інженерії. Вони можуть подумати, що це марна трата їхнього часу, коли вплинуть на організацію, а не на них.

Але справа в тому, що працівники зламаних організацій також піддаються особистому ризику.

Один із найефективніших способів змусити персонал звернути увагу та дотримуватися правил безпеки — це допомогти їм зрозуміти, чим вони ризикують як у своїй роботі, так і в особистому житті. Наприклад, якщо офіс постраждає від кібератаки та викрадено кадрову документацію, особиста інформація співробітників може бути використана зловмисниками, щоб подати заявку на кредитні картки та стягнути величезні витрати.

Висвітлення минулих кібератак, особливо тих, які були успішно спрямовані на технічно підкованих або кмітливих людей, також може допомогти змінити думку працівників про те, що соціальна інженерія не діє на розумних людей. На жаль, лікарі, юристи, педагоги та багато інших спритних людей стають жертвами атак соціальної інженерії. Це міф, що деякі люди занадто розумні, щоб їх обдурили.

Співробітники почнуть розуміти, наскільки вони вразливі та наскільки підступними можуть бути ці атаки, якщо вони беруть участь у імітованих атаках соціальної інженерії. Крім того, керівники агентств, які говорять про ризики та підтримують тренінги, можуть бути більш впливовими, ніж повідомлення, що надходить від IT-відділу. Коли лідери демонструють належну поведінку, це допомагає мотивувати інших робити те саме, зрештою зміцнюючи культуру безпеки в організації.

Деякі організації досягли великого успіху, перетворивши навчання та практику фішингу на ігри. Фішингові дербі можуть бути цікавим способом гейміфікації навчання, призначаючи бали за кожну правильно повідомлену симуляцію фішингового електронного листа та відстежуючи результати в організації. Деякі організації вибирають період часу (жовтень чудовий, оскільки це місяць обізнаності про кібербезпеку) і усувають негативні наслідки, наприклад додаткове навчання щодо помилок, одночасно значно збільшуючи кількість імітованих фішингових електронних листів, даючи співробітникам більше шансів підвищити свою ефективність. бали.

Цей конкурс можна проводити на індивідуальному рівні, рівні департаменту чи навіть філії з простими призами, починаючи від вечірки з піцою до спеціального місця для паркування чи навіть веселого трофею, щоб похвалитися. Усуваючи негативні наслідки та надаючи винагороду, багато співробітників справді сподіваються отримати симуляцію повідомлень, щоб покращити свій бал і статус, а організація отримує вигоду, забезпечуючи багато практики швидкого виявлення та повідомлення про те, що може бути значною загрозою.

Переформатувати культуру кібербезпеки в організації складно, особливо в державних установах, де недостатньо ресурсів. Однак організації, які знаходяться в зоні ризику, повинні визнати, що навчання та освіта з питань безпеки є хорошою інвестицією. Захист даних мешканців вартий роботи по розгортанню навчальних модулів і перегляду протоколів, навіть якщо це важко в короткостроковій перспективі.

Легко подумати: «О, нас ніколи не зламали, тому нам не потрібно хвилюватися», але це недалекоглядно. Завдяки групам кіберзлочинців організації державного сектору піддаються ще більшому ризику бути зламаними.

Запобігайте цьому, приділяючи пріоритет обізнаності, створюючи позитивну культуру безпеки та сприяючи спільній відповідальності». ***(Erich Kron. Why cybersecurity begins with users // route-fifty (https://www.route-fifty.com/cybersecurity/2024/06/why-cybersecurity-begins-users/397094/?utm_source=flipboard&utm_content=RouteFifty2018%2Fmagazine%2FRoute+Fifty). 04.06.2024).***

***

«Здавалося б, було б доцільно, щоб фінансові керівники міцно тримали свій гаманець у сфері кібербезпеки, оскільки такі рішення можуть визначити, чи є захист компанії достатньо міцним, щоб уникнути дорогих цифрових атак.

Однак у багатьох випадках саме керівники технічних компаній вирішують питання, коли справа доходить до розподілу грошей на безпеку цифрових операцій

компанії, згідно з результатами опитування керівників середнього ринкового бізнесу, вміщеного в нещодавній звіт консалтингової фірми RSM US.

Опитування, проведене протягом першого кварталу, показало, що більшість (51%) бюджетів на кібербезпеку «розташовується» під керівництвом директора з технологій або директора з інформаційної безпеки (42%), тоді як лише близько третини фінансових директорів (34%) і генеральних директорів (32%) тримають ключі від кібербюджету.

Це примітно, враховуючи, що кібератаки та кібербезпека можуть завдати фінансового удару. середній річний бюджет операцій центру безпеки для великих корпорацій становить близько 14,6 мільйонів доларів США. Згідно з нещодавнім опитуванням KPMG, Водночас фінансовий директор Dive раніше повідомляв, що середня кібератака, яка підтримується державою, коштує приблизно 1,6 мільйона доларів за інцидент.

Технічно кажучи, усі бюджети знаходяться під керівництвом фінансових керівників, але між компаніями існують великі відмінності щодо того, хто має більший контроль, за словами Таусефа Газі, національного лідера RSM з безпеки та конфіденційності. У багатьох компаніях структура бюджетування заслуговує перегляду, сказав він.

«Я думаю, що фінансовий директор контролює загальний бюджет, але покладайтеся на своїх керівників з IT або безпеки, щоб допомогти визначити потреби», — сказав Газі у відповіді електронною поштою на запитання.

«У багатьох випадках фінансові директори також вважають себе основними лідерами зі стримування витрат, що може спонукати до скорочення бюджетів, якщо потреби та ризики для організації не пояснюються належним чином... Вкрай важливо, щоб фінансові директори розуміли ці ризики та операційні бюджети. дуже детально, оскільки всі бюджети зрештою згортаються до них», – сказав він.

Є плюси і мінуси того, де розподіляється бюджет на кібербезпеку, сказав Газі в інтерв'ю минулого тижня, зазначивши, що його фірма навчила деякі компанії передавати бюджет іншим відділам, залежно від того, що відбувається всередині

фірми. Але є певні переваги, які фінансові директори можуть отримати, отримавши право власності, сказав він.

«З точки зору професіонала, я роблю це протягом 25 років, і коли я бачу, як фінансові директори розподіляють бюджети, зазвичай стратегія кібербезпеки більше узгоджується зі стратегією підприємства, що сприяє досягненню бізнес-результатів», — сказав Газі в інтерв'ю. Навпаки, коли технічні керівники мають більше контролю, може здатися, що це не пристосовано до стратегії організації. «Він більше орієнтований на інструменти».

Крім того, один із недоліків того, що кібервитрати виходять за рамки основної компетенції фінансового директора, полягає в тому, що вони можуть бути віддалені від наслідків певних рішень, сказав він.

Наприклад, вони можуть запитати, чому потрібні додаткові витрати на кібербезпеку, якщо компанія придбала певні хмарні продукти, які вважаються захисними. Але залежно від того, які підписки або типи хмарних сервісів купує компанія, їм все одно може знадобитися більший захист, сказав він.

Ще один недолік того, що технологічні лідери контролюють кібербюджет, полягає в тому, що витрати на кібербезпеку часто приносяться в жертву для фінансування інших проектів технологічної та цифрової трансформації, залишаючи компанії відкриті для великого ризику, поки вони завершують ці проекти, сказав Газі.

«Ми знайшли випадки, коли кіберкоманди роблять мінімум для виконання зобов'язань щодо відповідності, замість того, щоб розробляти цілісну програму кібербезпеки, яка може бути стійкою проти прогресуючих загроз, таких як програми-вимагачі», — сказав Газі в електронному листі. «Таким чином, для [кібербезпеки] має сенс мати гнучкість, щоб працювати окремо від IT-бюджетів і [мати] пряму видимість фінансового директора. IT-операції та безпека часто можуть конфліктувати». ***(Maura Webber Sadovi. Few CFOs control cybersecurity budgets. Here's why more should // Industry Dive (https://www.cfodive.com/news/few-cfos-control-cybersecurity-budgets-heres-why-more-***

should/718006/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 04.06.2024).

***

«Можливо, навіть більше, ніж в інших професійних областях, фахівці з кібербезпеки постійно стикаються з новими загрозами. Щоб ви залишалися на висоті, багато програм сертифікації вимагають отримання кредитів безперервної професійної освіти (CPE). CPE, по суті, є одиницями вимірювання, які використовуються для кількісної оцінки часу та зусиль, які фахівці витрачають на підтримку та вдосконалення навичок і знань у сфері кібербезпеки, і вони виступають як бали, які демонструють прагнення бути в курсі подій.

CPE найкраще зрозуміти з точки зору інших професій: так само, як медичні, юридичні та навіть CPA сертифікації вимагають безперервної освіти, щоб бути в курсі прогресу та змін у галузі, фахівцям з кібербезпеки потрібні CPE, щоб бути в курсі останніх тактик хакерства та стратегій захисту.

Кредити CPE мають вирішальне значення для підтримки сертифікацій, виданих різними організаціями з кібербезпеки, такими як (ISC)², ISACA та CompTIA. Отримання CPE передбачає різноманітні дії, як-от відвідування семінарів, проходження онлайн-курсів або участь у конференціях.

Основна мета CPE – забезпечити, щоб сертифіковані спеціалісти залишалися в курсі останніх тенденцій, технологій і загроз у кібербезпеці, таким чином зберігаючи цілісність і актуальність їхніх сертифікатів. Крім того, щоб ми залишалися чіткими, CPE зрештою зміцнюють загальну безпеку організації. Це безпрограшний варіант як для професіоналів, так і для їхніх організацій.

Навіщо спеціалістам із кібербезпеки потрібні CPE #

Ландшафт кібербезпеки — це постійна гонка озброєнь. Щоб залишатися актуальними та просувати свою кар’єру, спеціалісти з кібербезпеки потребують безперервної професійної освіти (CPE). І CPE – це не лише просування по службі; вони безпосередньо впливають на ефективність роботи.

З особистої точки зору, CPE – це як робота з тренером у вашому тренажерному залі. Вони допоможуть вам підвищити рівень вашої професійної підготовки, озброївши вас найновішими знаннями та навичками в таких сферах, як керування ризиками, тестування на проникнення або хмарна безпека. Це робить вас сильнішим і ціннішим активом для будь-якої організації, відкриваючи двері для просування по службі та можливостей для більш високої оплати праці.

У професійному плані CPE – це як відвідування бойових навчань. Вони захищають вас від кіберзагроз, що постійно розвиваються. Дізнавшись про нові методи злому та стратегії захисту, ви зможете краще захистити дані та системи вашої організації. Це зменшує ризик дорогих порушень і демонструє ваше прагнення до досконалості.

CPE – це інвестиція як у вашу кар'єру, так і у вашу здатність працювати на вищому рівні. Вони роблять вас більш цінним професіоналом і сильнішим захисником від кіберзагроз.

Відстеження вашого прогресу: демістифікація CPE з кібербезпеки #

Отримання CPE демонструє ваше прагнення бути в курсі подій. Але як ви відстежуєте свій прогрес?

Більшість органів сертифікації вимагають отримання певної кількості кредитів CPE протягом певного періоду, як правило, щорічно або протягом багаторічного циклу. Наприклад, (ISC)² вимагає від сертифікованих спеціалістів з безпеки інформаційних систем (CISSP) отримувати 120 кредитів CPE кожні три роки.

Розрахунок CPE зазвичай обертається навколо двох основних факторів: витраченого часу та типу діяльності. Більшість заходів присуджують CPE на основі інвестованих годин. Наприклад, відвідування конференції з безпеки може принести вам 8 CPE, тоді як онлайн-курс може надати 1 CPE за годину завершення.

Однак це не універсальна система. Органи сертифікації часто класифікують діяльність. Технічні семінари, зосереджені на нових методах злому, можуть мати більшу вагу (значення CPE), ніж, наприклад, семінари загальної обізнаності.

Дуже важливо перевірити конкретні вимоги вашої сертифікації. Вони часто окреслюють загальну кількість необхідних CPE, часові рамки для їх отримання та будь-які обмеження категорії. Відстежуючи свою навчальну діяльність і пов’язані з нею значення CPE, ви можете бути впевненими, що ви залишатиметеся кваліфікованими та удосконалите свої навички кібербезпеки.

Розширення арсеналу: пошук CPE з кібербезпеки #

Фахівці з кібербезпеки мають безліч варіантів отримання кредитів CPE. Ось деякі відправні точки для пошуку цих цінних ресурсів:

Формальне навчання. Такі організації, як (ISC)² і SANS, пропонують очні або онлайн-курси, розроблені спеціально для отримання CPE. Ці курси глибоко заглиблюються в теми безпеки, як-от реагування на інциденти, керування ризиками чи хмарну безпеку, гарантуючи, що ви отримаєте цінні знання, накопичуючи кредити

Галузеві події – конференції, семінари та вебінари, організовані охоронними компаніями, галузевими асоціаціями, відомими постачальниками кібербезпеки або навіть вашим власним роботодавцем, можуть бути скарбницею для CPE. Багато з цих заходів пропонують сесії, які не лише дають розуміння, але й сприяють вашим вимогам CPE.

Самостійне навчання - не недооцінюйте силу самостійного навчання! Читання публікацій з питань безпеки, відвідування безкоштовних вебінарів або навіть участь у проектах безпеки з відкритим кодом часто можуть претендувати на отримання CPE. Зверніться до свого сертифікуючого органу, щоб дізнатися, чи приймаються ці дії до кредиту.

Курс управління ризиками від XM Cyber - як професіонал, який прагне підвищити свій набір навичок із керування ризиками та виконати вимоги CPE, ви можете ознайомитися з курсом керування ризиками від XM Cyber. Цей комплексний курс пропонує цінну комбінацію професійного розвитку та кредитів CPE. Протягом 4-5 годин у самостійному темпі вивчаються основи керування загрозами та система керування безперервним загрозою (CTEM) Gartner, яка є

рекомендованим способом втілити керування загрозами в ефективний і повторюваний план.

Курс забезпечує глибоке розуміння різних кіберзагроз, які загрожують чутливим активам. Ви вивчите основні компоненти ефективної стратегії безперервного управління виявленням загроз і дізнаєтесь, як її реалізувати у своїй організації.

Курс також допоможе вам адаптувати стратегію до ваших конкретних потреб і допоможе оцінити рівень зрілості вашої організації щодо управління ризиками.

Програми підтримки сертифікації – багато сертифікацій пропонують вбудовані програми CPE. Поновивши свою сертифікацію через них, ви отримаєте доступ до ексклюзивних ресурсів і заходів, спеціально розроблених для виконання ваших вимог CPE.

Просто майте на увазі, що в усіх випадках важливо проконсультуватися з вашим конкретним сертифікуючим органом, щоб підтвердити відповідність кредиту CPE.

Кредити CPE – чудовий спосіб залишатися мотивованим і обізнаним #

Звісно, нікому не подобається постійна повторна сертифікація – але, правду кажучи, хто з нас продовжував би постійно оновлюватись, якби не потреба проходити сертифікацію? І, знаючи, як швидко все розвивається на цій арені, якщо професіонали в цій галузі бізнесу відстануть, це може призвести до проблем для організацій і даних, які вони зберігають. Сподіваємося, різноманітні джерела та поради, згадані тут, допоможуть вам у подальшому професійному зростанні». ***(Cybersecurity CPEs: Unraveling the What, Why & How // The Hacker News (https://thehackernews.com/2024/06/cybersecurity-cpes-unraveling-what-why.html). 10.06.2024).***

***

«Fortinet, світовий лідер у сфері кібербезпеки, який сприяє конвергенції мереж і безпеки, опублікував звіт про сталий розвиток за 2023 рік. У цьому щорічному звіті описано підхід компанії, її зобов’язання та прогрес у питаннях

сталого розвитку, які є найбільш важливими для Fortinet та її зацікавлених сторін, включаючи співробітників, інвесторів, постачальників, партнерів і клієнтів.

Як детально зазначено у звіті, підхід Fortinet до сталого розвитку має чотири стовпи: усунення кіберризиків для суспільства, диверсифікація талантів у сфері кібербезпеки, повага до навколишнього середовища та сприяння відповідальному бізнесу в ланцюжку створення вартості. На підтримку зобов'язань компанії щодо сталого розвитку та Цілей сталого розвитку (ЦСР), Fortinet приєдналася до Глобального договору ООН у 2023 році та дотримується його принципів у сфері прав людини, праці, навколишнього середовища та боротьби з корупцією. Крім того, другий рік поспіль Fortinet було визнано в рейтингу світових і Північноамериканських індексів Dow Jones Sustainability Indices (DJSI) за 2023 рік як свідчення постійних зусиль компанії в галузі сталого розвитку та відданості побудові більш сталого майбутнього для всіх.

Основні моменти зі звіту про сталий розвиток Fortinet за 2023 рік включають:

Прогрес у досягненні цільових показників чистого нульового викиду парникових газів: компанія продовжує інвестувати в екологічні джерела енергії, включаючи свій новий гараж у Саннівейлі, де сонячні батареї покриватимуть потреби в електроенергії для штаб-квартири Fortinet і прилеглих об'єктів. У 2024 році Fortinet надасть свій план декарбонізації на перевірку ініціативі Science-Based Targets (SBTi).

Підвищення енергоефективності продукту: Fortinet продовжує покращувати енергоефективність своїх пристроїв FortiGate — її моделі 2023 року споживають у середньому на 62% менше енергії, ніж еквівалентні моделі попереднього покоління.

Екологічна упаковка: Fortinet продовжує досліджувати та впроваджувати упаковку з біологічно розкладаних матеріалів, застосовуючи її до більш ніж 60 моделей у своїх лінійках продуктів. Екологічно чиста упаковка, виготовлена у 2023 році, допомогла Fortinet уникнути приблизно 455 тонн викидів CO2.

Прогрес у навчанні 1 мільйона людей кібербезпеці до 2026 року: станом на 31 грудня 2023 року Fortinet становить 43% від своєї п’ятирічної мети. Минулого року компанія розширила свої зусилля, щоб усунути прогалину в кібернавиках, надаючи безкоштовний доступ до різних навчальних програм, сприяючи обізнаності про безпеку в Інтернеті та виховуючи майбутніх фахівців з кібербезпеки серед студентів.

Різноманітність, справедливість та залучення (DEI): у 2023 році Fortinet посилила свою внутрішню програму розвитку лідерства, щоб ще більше зосередитися на залученні. У результаті понад 340 лідерів Fortinet пройшли навчання для сприяння інклюзії.

Партнерство для подолання кіберзлочинності: Fortinet продовжує розширювати співпрацю для боротьби з кіберзлочинністю. У 2023 році компанія приєдналася до Joint Cyber Defense Collaborative (JCDC) і через програму INTERPOL Gateway сприяла арешту 15 груп кіберзлочинців і запобіганню фінансових втрат на 40 мільйонів доларів.

Прихильність етичній бізнес-практикі та дотриманню законодавства: у 2023 році 100% дистриб’юторів компанії та ключових контрактних виробників пройшли навчання Fortinet з бізнес-етики та відповідності, визнаючи свою відповідність цінностям і принципам Fortinet.

Інформаційна безпека та конфіденційність: Fortinet запустив свій Центр ресурсів довіри, щоб запропонувати клієнтам доступ до інформації про сертифікати, відповідність і безпеку. Fortinet також оновив сертифікації та іспити з інформаційної безпеки та завершив нові, зокрема розширив продукти та послуги, які охоплюються ISO 27001, SOC 2 та HIPAA.

У Звіті про сталий розвиток Fortinet за 2023 рік згадуються Цільова група з розкриття фінансової інформації, пов’язаної з кліматом (TCFD), Стандарти Глобальної ініціативи звітності (GRI), Стандарти Ради зі стандартів звітності щодо сталого розвитку (SASB) і Цілі сталого розвитку ООН (ЦСР ООН). У звіті детально описано прогрес і показники Fortinet у восьми пріоритетних питаннях: інновації для безпечного Інтернету, інформаційна безпека та конфіденційність; вплив

продукції на навколишнє середовище; екологічне управління та вплив зміни клімату; різноманітність, справедливість та залучення; розрив навичок кібербезпеки; ділова етика; та відповідальне використання продукту». ***(Fortinet drives positive impact through cybersecurity and social responsibility // Manila Standard (https://manilastandard.net/tech/314460096/fortinet-drives-positive-impact-through-cybersecurity-and-social-responsibility.html). 16.06.2024.***

***

«Загальні нарікання серед CISO та інших керівників полягає в тому, що брак кваліфікованих спеціалістів із безпеки перешкоджає їхній здатності ефективно захищатися від дедалі більш ворожих загроз. Крім того, цим керівникам важко підвищити кваліфікацію наявного персоналу.

Згідно з дослідженням ISC2 Cybersecurity Workforce Study 2023, глобальна кіберробоча сила становила 5,5 мільйона з мільйонами незаповнених робочих місць. Гірше того, прогнозується, що розрив зросте на 12,6% за рік. З майже 15 000 опитаних міжнародних практиків 92% повідомили, що мають прогалини в навичках у своїй організації, причому найчастіше згадуються хмара та штучний інтелект (ШІ).

Економічна невизначеність ще більше змушує організації «робити більше з меншими витратами». Щоб вирішити ці проблеми, роботодавці повинні мислити нестандартно, стати більш гнучкими та креативними та визнати, що майбутні лідери безпеки вже можуть бути серед них. Ось чотири поради, які допоможуть вам на шляху:

1. Для посад початкового рівня будьте справжніми

Порівняйте очікування з реальністю безпеки. Початковий рівень означає відсутність досвіду. Посадові інструкції початкового рівня повинні містити вимоги, які відображають це. Не вимагайте сертифікатів на кшталт CISSP, які потребують п’ятирічного досвіду навіть для здачі іспиту. Також навчайте своїх рекрутерів і кадрового персоналу. Якщо ви шукаєте спеціалізовані кібернавички в нових

технологіях, таких як штучний інтелект і хмара, не розраховуйте на зарплату початкового рівня. Ми обмежуємо коло талантів, будучи нереалістичними.

В ідеалі кандидати, які роблять кар'єру в кіберпросторі, набувають навичок і отримують сертифікати, перш ніж подавати заявку на роботу, і я наводжу багато прикладів того, як це зробити в моїй книзі «Побачити себе в кібернетичному просторі: кар'єра безпеки поза межами хакерства». Керівництво з кібербезпеки та менеджери з найму можуть використовувати такі інструменти, як Workforce Framework for Cybersecurity (NICE Framework), як посібник для розвитку своєї робочої сили з кібербезпеки.

Програми наставництва є ще одним цінним інструментом для залучення та розвитку талантів. За даними Американського товариства навчання та розвитку (через YEC Women), 75% керівників кажуть, що наставництво було критичним фактором у їхній кар'єрі. Встановлення основоположних стосунків із досвідченими професіоналами галузі може прискорити навчання працівників і кар'єрний ріст.

2. (За іронією долі) Не зосереджуйтеся на своїй робочій силі з кібербезпеки

Більшість організацій покладаються на IT-команди для створення та експлуатації цифрової інфраструктури, на якій вони керують своїм підприємством. Ці IT-команди зазвичай перевершують команди з кібербезпеки, іноді навіть 100 до 1 з точки зору персоналу. Це величезна кількість талантів, які потрібно використовувати.

Ви хочете кібермасштаб? Починай тут. Навчіть цих будівельників і операторів лише кільком ключовим способам застосування безпеки в їхній роботі, і ви ефективно примножите свою кіберпотужність, не найнявши жодного працівника. Кілька порад для успіху:

• Не перевантажуйте їх занадто багато (наприклад, починайте з однієї атаки).

• Зробіть це реальним для них, показавши атаку на подібну IT-програму.

• Поговоріть з ними про те, що вони можуть зробити по-іншому у своєму проектуванні, розробці, тестуванні, експлуатації та обслуговуванні, щоб запобігти атаці.

3. Зосередьтеся менше на технічних навичках, більше на вирішенні проблем

Деякі з ваших найкращих кандидатів на роботу не матимуть ступеня з кібербезпеки, технічної освіти чи навіть відповідного досвіду. Деякі з сучасних рок-зірок кібербезпеки мають дипломи з психології, філософії, мов, фінансів, маркетингу та права, а також мають різні нетехнічні знання.

Боротьба з кіберзлочинністю — це як цікавість, вирішення проблем і терпіння, так і кодування та технології. Ці навички критичного мислення не можна знайти в певних ступенях чи галузевих сертифікатах, тому адаптуйте процес відбору кандидатів, щоб знайти те, що є важливим. Розумні люди з правильними рисами характеру «зрозуміють» і виконають роботу за вас — повірте.

4. Створюйте можливості через різноманітність

Шукайте способи створити різноманітність у вашій кіберкоманді. Усі організації отримують вигоду з різних точок зору, досвіду та наборів навичок; різні команди приймають кращі рішення та діють спритніше. Співпрацюйте з такими організаціями, як Cyversity, WiCyS, NPower та іншими некомерційними організаціями, які прагнуть диверсифікувати індустрію кібербезпеки, щоб підтримати ваші зусилля.

Очолюйте заряд

Кібербезпека — це величезна, різноманітна та захоплююча галузь, яка однаково стосується спеціалістів у сфері інформаційної безпеки та не пов’язаних із безпекою. Від нас як лідерів залежить створення більш реалістичних вимог і підготування наступного покоління до навичок, навчання та можливостей, необхідних для успіху. Наша промисловість залежить від цього». ***(Ed Adams. Four Tips For Ensuring A Strong Cybersecurity Workforce // Forbes (https://www.forbes.com/sites/forbestechcouncil/2024/06/14/four-tips-for-ensuring-a-strong-cybersecurity-workforce/). 14.06.2024).***

***

«MultiTeam Solutions, провідна компанія з розробки командної роботи в сфері кібербезпеки, орієнтована на людину, показала, що половина фахівців з

кібербезпеки очікує, що вони вигорають протягом наступних 12 місяців через стрес і тиск на своїй роботі.

Висновки були опубліковані в новому звіті MultiTeam Solutions під назвою «Стрес і вигорання в кібербезпеці: ризик тисячі паперових порізів». На основі опитування 173 міжнародних фахівців з кібербезпеки звіт розкриває тиск на психічне здоров'я, з яким вони стикаються, і підвищені шанси вигорання.

У звіті було виявлено, що хоча 52% фахівців з кібербезпеки почуваються досить стійкими до стресу, майже така ж кількість (50%) заявили, що протягом наступного року або раніше вони досягнуть точки вигорання. Ці показники вигорання також включають 35% респондентів, які збираються досягти вигорання протягом наступних шести місяців, і загалом 80% респондентів вказали, що вони досягнуть вигорання через три роки або менше.

У звіті виснаження визначається як «відсутність мотивації для ефективного виконання своєї роботи». У результаті фахівці з кібербезпеки відчувають себе змушеними залишити свою організацію або шукати нові можливості для боротьби зі стресом, який вони відчувають.

Коли їх запитали про існуючі структури підтримки, більшість (79%) відповіли MultiTeam Solutions, що їм принаймні певною мірою комфортно ділитися своїми проблемами з приводу вигорання зі своїми керівниками. Крім того, 81% респондентів вказали, що керівництво вищого рівня (SLM) принаймні певною мірою розуміє їхній стрес. Однак лише 23% фахівців з кібербезпеки вважають, що SLM активно допомагає зменшити їхній стрес, і фактично майже 50% респондентів зазначили, що SLM посилює їхній стрес, діючи як значний фактор, що сприяє вигоранню…» ***(Half of cybersecurity professionals expect to burnout in the next 12 months // Codel Software Ltd. (https://hrnews.co.uk/half-of-cybersecurity-professionals-expect-to-burnout-in-the-next-12-months/). 13.06.2024).***

***

«Trend Micro Incorporated (TYO: 4704; TSE: 4704), світовий лідер у галузі кібербезпеки, сьогодні оголосила результати свого річного звіту про

кібербезпеку за 2023 рік, у якому зазначено, що компанія заблокувала понад 161 мільярд загроз, що становить значні 10% річних зросли порівняно з глобальними цифрами попереднього року та випустили попередження, наголошуючи, що зловмисники використовують все більш складні методи, щоб націлитися на меншу кількість жертв, що потенційно може призвести до вищих фінансових прибутків.

Щорічний звіт Trend Micro про кібербезпеку за 2023 рік під назвою «Калібрування розширення» служить переконливим нагадуванням про те, що підприємства повинні дотримуватися проактивного підходу до управління ризиками на всій поверхні атак у сучасному динамічному ландшафті кібербезпеки. Крім того, у звіті виявлено сплеск виявлення зловмисного програмного забезпечення в електронній пошті на 349% порівняно з минулим роком у всьому світі. Натомість кількість виявлень шкідливих і фішингових URL-адрес зменшилася на 27% порівняно з минулим роком. Доступ до хмарних додатків становив найбільший ризик, оскільки Trend Attack Surface Risk Management (ASRM) зафіксував майже 83 мільярди спроб доступу.

Минулого року в Бахрейні Trend Micro виявила та заблокувала понад 8 мільйонів загроз. Це охоплює запобігання понад 1,9 мільйонам загроз електронною поштою та понад 1,1 мільйону атак зловмисних URL-адрес. Крім того, Trend Micro виявила та зупинила понад 3,5 мільйона атак зловмисного програмного забезпечення, демонструючи свою майстерність у захисті цифрових активів у країні.

«Оскільки частота та складність витоку даних продовжує зростати, організації повинні прийняти проактивний і комплексний підхід до захисту цифрової інфраструктури», — сказав Рашид Аль Ода, керуючий директор Trend Micro з Близького Сходу. «У Trend Micro ми глибоко прагнемо зміцнити ландшафт кібербезпеки Бахрейну шляхом використання передових технологій і досвіду. Наш щорічний звіт відображає наші зусилля та відданість справі створення стійкого та безпечного середовища, яке дає можливість бізнесу процвітати».

Зосереджуючись на забезпеченні успішної цифрової трансформації в країні, Національна стратегія кібербезпеки Бахрейну (NCSC) підкреслює критичну роль прийняття комплексної стратегії кібербезпеки, щоб організації могли процвітати в сучасну епоху. Trend Micro поділяє цю прихильність досконалості кібербезпеки, пропонуючи інноваційні рішення та сприяючи стійкості, щоб керувати організаціями в складному цифровому ландшафті». ***(Trend Micro's 2023 Annual Cybersecurity Report: Safeguarding Bahrain's digital frontiers amidst escalating threats // Zawya (https://www.zawya.com/en/press-release/research-and-studies/trend-micros-2023-annual-cybersecurity-report-safeguarding-bahrains-digital-frontiers-amidst-escalating-threats-xkvqd5ad). 13.06.2024).***

***

«2024 рік є важливим для виборів. Проходять десятки парламентських і президентських виборів, у тому числі в Сполучених Штатах, Великій Британії, Індії, Бразилії, Індонезії та Мексиці, і загроза кібератак і дезінформації, керованої штучним інтелектом, ніколи не була такою.

Відповідно до останнього звіту Всесвітнього економічного форуму про сприйняття глобальних ризиків, дезінформація та дезінформація є головними ризиками, і тенденція прагнення вплинути на виборців напередодні виборів і підірвати легітимність результатів, безсумнівно, продовжуватиметься та посилюватиметься.

Очікуваний сплеск дипфейків

У міру того як технологія глибокого підроблення аудіо- та відеопродукції розвивається і стає все більш доступною, ми повинні очікувати, що в найближчі місяці ми побачимо більше прикладів, які поширюватимуться в соціальних мережах. Нещодавні приклади включають «роботний дзвінок», у якому використовувався голос Джо Байдена, щоб відбити виборців від голосування на праймеріз у Нью-Гемпширі в січні 2024 року. Подібні практики більш зловмисно використовувалися у Словаччині та Великобританії.

Під час виборів у Словаччині у вересні 2023 року аудіозапис нібито був записом Міхала Сімецької, який очолює ліберальну партію «Прогресивна Словаччина», обговорюючи, як сфальсифікувати вибори. У другому ролику голос Сімецької був використаний для поширення фейкових новин про те, що він планує подвоїти ціни на пиво в країні, якщо виграє. Особу нападника не було доведено, а проросійський кандидат, колишній прем'єр-міністр Роберт Фіцо переміг на виборах.

У жовтні минулого року лідер Лейбористської партії Великої Британії сер Кейр Стармер став жертвою аудіо-дипфейку, опублікованого приурочено до першого дня щорічної конференції партії. На відео видно, як він лається зі співробітниками. Ситуація погіршилася тим, що X, колишній Twitter, відмовився видалити ролик, оскільки Лейбористська партія не змогла надати достатніх доказів того, що він був фейком.

Дипфейки аудіо, здається, більш неприємні, ніж відео, яке легше помітити як маніпульоване, принаймні в короткостроковій перспективі. Deepfakes також використовували публічних діячів на сьогоднішній день, але в майбутньому вони могли б націлитися на виборчих працівників у гострих округах, яких може бути важче швидко звільнити. Підроблені веб-сайти можна створювати, щоб підтверджувати претензії та поширювати подальшу дезінформацію, розміщувати в Інтернеті та розповсюджувати швидше, ніж будь-коли, розширюючи охоплення глибоких фейків.

Нещодавно агентство Associated Press опублікувало посібник про те, як розпізнати дипфейки, який усім нам варто вивчити.

Політики та експерти в усьому світі, але особливо у Великій Британії та США, де занепокоєння щодо маніпуляцій на виборах є найбільшими, закликають прийняти правила, які б зупинили створення та поширення дипфейків. Лист, підписаний сотнями лідерів спільноти штучного інтелекту в лютому цього року, закликав до кримінальної відповідальності для тих, хто створює та поширює шкідливий контент. Проте, навіть якщо нові правила будуть запроваджені вчасно до виборів, немає впевненості, що це щось змінить.

Загроза злому

Кібератаки залишаються ймовірними, і політики, їхні сім'ї, співробітники та партійні чиновники, ймовірно, постійно стають їх цілями протягом останніх кількох років. Відсутність звітів про викрадену інформацію з особистих і робочих пристроїв не означає, що цього не було; зловмисники можуть чекати найбільш сприятливого моменту виборчого циклу для витоку будь-якої інформації. Атаки на пристрої, які залишалися непоміченими протягом місяців або років, все одно можуть призвести до шкідливих витоків.

Хоча основна увага при втручанні у вибори в США на виборах 2020 року була зосереджена на Росії і, ймовірно, залишатиметься на Росії під час виборів 2024 року, інші країни, політичні групи та окремі особи також можуть бути мотивовані використовувати свої ресурси, щоб вплинути на виборців або порушити процес. В останніх звітах детально описано, як Китай втручався Китаю у федеральні вибори в Канаді в 2019 і 2021 роках, а також є докази наміру втрутитися у вибори в США в 2024 році. І Китай, і Росія вміють проводити довгострокові хакерські кампанії.

Інші державні суб'єкти, включно з Іраном і Північною Кореєю, також можуть намагатися втрутитися у вибори по всьому світу, але деякі хакерські атаки можуть відбуватися зсередини країни, оскільки сторонники намагаються перешкодити опозиції. Кілька країн проведуть вибори, які не вважаються ні вільними, ні чесними.

Націлена інфраструктура голосування

Машини для голосування можуть бути ще однією основною мішенню для хакерів, які фінансуються державою. Порушення або схоже на порушення безпеки машин для голосування під час виборів у США додасть олії у вогонь, що тліє після того, як колишній президент Трамп висунув звинувачення у фальсифікації голосування після своєї поразки у 2020 році. Там, де минулого разу не вистачало доказів, фактичні докази атак цього разу можуть бути використані, щоб знову поставити під сумнів результат 2020 року.

Агентство з кібербезпеки та безпеки інфраструктури (CISA) готувалося до таких атак. #protect2024 Веб-сайт містить велику кількість захисного вмісту

безпеки для державних і місцевих виборчих посадових осіб для покращення гігієни безпеки, підвищення безпеки систем і планування реагування на інциденти. Центр обміну та аналізу інформації про виборчу інфраструктуру (EI-ISAC) має надати пріоритет зв'язку та обміну розвідданими між виборчими посадовими особами в США та інших країнах, ймовірно, матимуть подібні групи.

Особливо цінною є робота, проведена етичними хакерами через Election Security Research Forum і MITER для перевірки апаратного та програмного забезпечення, що використовується виробниками виборчих технологій, на наявність вразливостей. Повністю перевірені дослідники та офіційні особи з кібербезпеки працювали разом, щоб виявити проблеми та виправити їх, запобігаючи потенційному використанню пізніше цього року.

Розподілені атаки на відмову в обслуговуванні (DDoS-атаки) використовувалися в спробах порушити роботу інфраструктури для голосування, включаючи тимчасові збої під час проміжних виборів у США у 2022 році. Однак їхній вплив обмежений і навряд чи зупинить процес голосування.

Під час виборів у Бангладеш у січні 2024 року програма, створена Виборчою комісією Бангладеш для надання виборцям інформації про кандидатів і історичних даних, стала мішенню невідомих зловмисників, що призвело до повільної роботи програми. Напередодні тих самих виборів телекомунікаційна та медіа-індустрія також зазнали серйозних мішеней DDoS-атак, які вважалися спробою уповільнити потік інформації до виборців.

Нарешті, ми не повинні виключати можливість того, що інсайдери намагаються підірвати безпеку виборів. Інсайдери можуть використовувати свій доступ для маніпулювання або знищення даних про вибори, включно з даними про реєстрацію виборців, або доступу до виборчих систем або даних. Вони також можуть спробувати вкрасти або втручатися в апаратне забезпечення виборчої інфраструктури або оприлюднити інформацію про виборців. CISA DOC.

Мікросвіт проблем кібербезпеки та ШІ

Проблеми, що впливають на безпеку виборів, — це мікрокосм кібербезпеки та проблем штучного інтелекту, які впливають на всі сфери: кількість загроз і

ризиків, якими необхідно керувати та пом’якшувати, зростає в геометричній прогресії, а зловмисники завжди матимуть перевагу, використовуючи технології швидше, ніж захисники.

З інцидентів, які вплинули на вибори цього року, ми будемо виносити уроки та ділитися ними, але ми, як професіонали безпеки, повинні бути пильними, щоб зрозуміти, як зловмисники можуть змінити ці інциденти, щоб загрожувати бізнесу, фінансовим ринкам і критичній інфраструктурі. Потім ми повинні застосовувати засоби пом’якшення скрізь, де це можливо, доки ми не зможемо використовувати ШІ для протидії атакам, перш ніж вони завдадуть нам шкоди». ***(Rob Sloan. How cybersecurity and AI will influence global elections in 2024 // IDG Communications, Inc. (https://www.networkworld.com/article/2145905/how-cybersecurity-and-ai-will-influence-global-elections-in-2024.html). 13.06.2024).***

***

«Сектор фінансових технологій, революціонізуючи фінансову індустрію за допомогою технологій, стикається зі значними проблемами кібербезпеки. Резонансні зломи, такі як злом Equifax у 2017 році, який розкрив особисту інформацію 147 мільйонів людей, підкреслюють критичну потребу в надійних заходах кібербезпеки. Фінтех-компанії, які мають справу з величезними обсягами конфіденційних фінансових даних, є головними цілями для кіберзлочинців. Основні ризики включають витік даних, атаки програм-вимагачів і вразливість системи. Ці загрози не тільки підривають довіру клієнтів, але й створюють серйозні фінансові та репутаційні ризики для компаній. Щоб пом’якшити ці проблеми, фінтех-компаніям важливо впровадити багаторівневі протоколи безпеки, включаючи шифрування, контроль доступу та регулярні перевірки безпеки. Крім того, виховання культури обізнаності про кібербезпеку серед співробітників може значно знизити ризик витоку даних через людську помилку. Тематичні дослідження, такі як атака на банківську мережу SWIFT, підкреслюють складність кіберзагроз, з якими стикається індустрія фінансових технологій, і важливість проактивних і комплексних стратегій безпеки.

Людський фактор: боротьба із соціальною інженерією та внутрішніми загрозами

Розуміння складності людської поведінки відіграє ключову роль у зміцненні кібербезпеки фінтех заходів. Соціальна інженерія використовує природну схильність людей довіряти, що робить її потужним інструментом у руках кіберзлочинців. Ці тактики часто передбачають маніпулювання співробітниками, щоб вони розкрили конфіденційну інформацію або вчинили дії, що загрожують безпеці. Тому підвищення обізнаності та навчання персоналу є надзвичайно важливими. Йдеться не лише про те, щоб мати найпередовіші технології; людський елемент має бути навченим і готовим розпізнавати ці загрози та ефективно реагувати на них.

Інсайдерські загрози, навмисні чи випадкові, становлять значний ризик для цілісності інфраструктур фінансових технологій. Вони можуть варіюватися від співробітників, які ненавмисно обмінюються конфіденційною інформацією, до зловмисників, які прагнуть отримати особисту вигоду. Вирішення цієї проблеми потребує комплексного підходу, який включає строгий контроль доступу, постійний моніторинг конфіденційних транзакцій і виховання культури безпеки в організації. Впроваджуючи ці стратегії, фінтех-компанії можуть значно пом’якшити ризики, пов’язані з людським фактором, і забезпечити більш безпечне середовище для своїх операцій і даних.

Посилення захисту: найкращі практики кібербезпеки Fintech

Зважаючи на швидкий розвиток цифрових фінансів, важливість надійних заходів кібербезпеки неможливо переоцінити. Компанії в секторі фінансових технологій є головними цілями для кіберзлочинців через величезні обсяги фінансових і особистих даних, які вони обробляють. Впровадження багатофакторної автентифікації (MFA) є критично важливим кроком у захисті облікових записів користувачів від несанкціонованого доступу. MFA вимагає від користувачів надати два або більше факторів перевірки, щоб отримати доступ до своїх облікових записів, що значно знижує ризик успішних кібератак. Наприклад, порівняння між компаніями, які впровадили MFA, і тими, які цього не зробили,

показує помітне зменшення випадків захоплення облікових записів на 99,9% згідно з дослідженнями Microsoft.

Технології шифрування відіграють ключову роль у захисті конфіденційних даних як у стані спокою, так і під час передачі. Використання передових стандартів шифрування (AES) гарантує, що дані, якщо їх перехоплять, залишаться нечитабельними та захищеними від несанкціонованого доступу. Порівняння методів шифрування, таких як 256-бітне шифрування AES, і старіших методів DES (стандарт шифрування даних), показує перевагу AES з точки зору безпеки та швидкості. Наприклад, 256-бітове шифрування AES наразі вважається незламним для атак грубої сили з використанням звичайних обчислень, що робить його золотим стандартом для захисту фінансових транзакцій і зберігання даних у фінтех-індустрії.

Регулярні аудити безпеки та перевірки відповідності є незамінними для виявлення вразливостей і забезпечення дотримання міжнародних стандартів кібербезпеки. Ці аудити допомагають визначити слабкі місця в захисті кібербезпеки фінтех-компанії, дозволяючи вчасно виправити ситуацію. Наприклад, компанії, які дотримуються стандарту безпеки даних індустрії платіжних карток (PCI DSS) і проходять регулярні аудити, мають значно менше порушень даних порівняно з тими, хто не дотримується цих вказівок. Дослідження, у якому порівнювали фінтех-компанії, які сумісні з PCI DSS, і невідповідні, показали на 50% нижчу кількість витоків даних серед відповідних компаній. Це підкреслює важливість регулярних аудитів і відповідності для зміцнення захисту кібербезпеки фінансових технологій.

Використання технологій: передові інструменти для безпеки Fintech

Оскільки фінтех-компанії продовжують розвиватися, зростають і загрози кібербезпеці, з якими вони стикаються. Вкрай важливо, щоб ці організації використовували передові технологічні інструменти для захисту своїх операцій і даних клієнтів. Серед найефективніших стратегій – впровадження алгоритмів машинного навчання для виявлення аномалій. Ці алгоритми можуть аналізувати

моделі поведінки та виявляти потенційні загрози в режимі реального часу, значно знижуючи ризик витоку даних і фінансового шахрайства.

Крім того, впровадження технології блокчейн стало потужним інструментом для підвищення безпеки фінансових технологій. Створюючи децентралізовану та незмінну книгу для транзакцій, технологія блокчейн забезпечує додатковий рівень безпеки, особливо стійкий до втручання та шахрайства. Ключові переваги:

Підвищена прозорість: кожна транзакція реєструється та легко перевіряється.

Покращена безпека: децентралізація ускладнює використання вразливостей хакерами.

Зменшення витрат: усунувши посередників, блокчейн може знизити комісію за транзакції.

Іншим важливим компонентом арсеналу безпеки фінтех є використання багатофакторної автентифікації (MFA). MFA додає додатковий рівень безпеки, вимагаючи від користувачів надати два або більше факторів перевірки, щоб отримати доступ до своїх облікових записів. Цей метод значно зменшує ймовірність несанкціонованого доступу, навіть якщо пароль користувача зламано. Застосування цих передових інструментів не тільки зміцнює захист фінтех-компанії, але й створює довіру з її клієнтами, забезпечуючи безпеку їхніх даних у все більш цифровому світі.

Відповідність і нормативні акти: Навігація правовою базою

Орієнтування в законодавчій базі в секторі фінансових технологій представляє унікальний набір проблем, насамперед через динамічний характер як технологій, так і фінансових норм. Компанії повинні переконатися, що вони не лише відповідають чинному законодавству, але й готові до майбутніх законодавчих змін. Це вимагає проактивного підходу, де постійний моніторинг і адаптація стратегій дотримання є важливими. Ключовим для цього є розуміння конкретних вимог, встановлених різними регуляторними органами, які можуть суттєво відрізнятися в різних юрисдикціях.

Щоб ефективно керувати проблемами відповідності та регулювання, фінтех-компанії повинні розглянути такі стратегії:

Впровадження надійних систем управління відповідністю, які є достатньо гнучкими, щоб адаптуватися до нових правил.

Участь у регулярних тренінгах для персоналу щодо останніх нормативних та нормативних вимог, гарантуючи, що кожен усвідомлює свої обов'язки.

Співпраця з юридичними експертами, які спеціалізуються на фінтехах, щоб отримати уявлення про те, як найкраще орієнтуватися в правовому ландшафті.

Використання технологічних рішень, таких як регуляторна технологія (RegTech), для оптимізації процесів відповідності та зменшення ризику невідповідності.

Ці кроки можуть суттєво пом'якшити ризики, пов'язані з проблемами відповідності та регулювання, дозволяючи фінтех-компаніям більше зосереджуватися на інноваціях і менше на юридичних перешкодах.

Створення стійкої культури: навчання та підвищення обізнаності у фінтех-компаніях

Створення культури кібербезпеки в фінтех-компаніях полягає не лише у впровадженні новітніх технологій; мова йде про надання кожному працівнику можливості бути частиною захисного механізму. Експерти сходяться на думці, що людські помилки часто призводять до порушень безпеки, тому для компаній вкрай важливо інвестувати в регулярні та комплексні навчальні програми. Ці програми мають не лише охоплювати основи кібербезпеки, але й бути адаптованими для вирішення конкретних загроз, з якими стикаються фінтех-компанії. Створюючи середовище, де співробітники постійно навчаються важливості кібербезпеки, фірми можуть значно зменшити свою вразливість до атак.

Залучення співробітників до роботи з кібербезпеки вимагає не лише періодичних тренінгів; це передбачає створення культури, де безпека є відповідальністю кожного. Цього можна досягти шляхом інтеграції практик кібербезпеки в повсякденні справи та заохочення співробітників бути пильними в будь-який час. Експерти рекомендують використовувати реальні приклади кібератак на навчальних заняттях, щоб проілюструвати можливі наслідки недбалості. Крім того, винагорода співробітників, які виявляють вразливі місця або

пропонують покращення заходів кібербезпеки фірми, може мотивувати інших брати активну роль у захисті цифрових активів компанії.

Адаптація до ландшафту кіберзагроз, що постійно змінюється, є постійним викликом для фінтех-компаній. Щоб залишатися попереду, компанії повинні не тільки оновити свої технічні засоби захисту, але й переконатися, що їхня робоча сила оснащена знаннями та інструментами для ефективного реагування. Це означає регулярну оцінку та оновлення навчальних програм, щоб вони відображали останні тенденції та загрози кібербезпеки. Співпраця з експертами з кібербезпеки та інституціями для отримання найновіших навчальних матеріалів і ідей також може підвищити ефективність цих програм. Зрештою, добре поінформована та пильна робоча сила є критично важливим компонентом комплексної стратегії кібербезпеки у секторі фінансових технологій.

Перспективні фінансові технології: нові тенденції та інновації в кібербезпеці

Кібербезпека в фінтех-секторі розвивається безпрецедентними темпами, керуючись як винахідливістю кіберзлочинців, так і інноваційним духом самої галузі. Щоб залишатися на випередженні, компанії повинні застосовувати проактивний підхід, зосереджуючись на нових тенденціях та інноваціях у сфері кібербезпеки. Це включає застосування вдосконалених методів шифрування, впровадження надійних систем контролю доступу та постійний моніторинг мережевої активності. Завдяки цьому фінтех-компанії можуть не лише захистити свою поточну діяльність, але й захистити свій бізнес від нових загроз.

Кілька ключових тенденцій формують майбутнє кібербезпеки у фінтех. До них належать:

Штучний інтелект (AI) і машинне навчання (ML) для прогнозного аналізу загроз і прийняття рішень щодо безпеки в реальному часі.

Технологія блокчейн для безпечних, захищених від несанкціонованих операцій і зберігання даних.

Біометричні заходи безпеки, такі як відбитки пальців і розпізнавання обличчя, для покращеної автентифікації користувача.

Застосування цих технологій може значно посилити захист фінтех-компанії, ускладнюючи кіберзлочинцям зламати їхні системи.

Щоб подолати виклики кібербезпеки у фінтех, потрібна багатогранна стратегія. Для компаній вкрай важливо не лише інвестувати в новітні технології безпеки, але й розвивати культуру обізнаності щодо кібербезпеки серед своїх співробітників. Регулярні тренінги, симуляції фішингових атак і оновлення останніх кіберзагроз можуть допомогти персоналу стати першою лінією захисту. Крім того, партнерство з експертами з кібербезпеки та використання їхньої інформації може забезпечити додатковий рівень захисту, гарантуючи, що фінтех-компанії залишатимуться стійкими перед обличчям нових кіберзагроз». ***(Understanding the Landscape: Key Cybersecurity Risks in Fintech // Techno FAQ (https://technofaq.org/posts/2024/06/understanding-the-landscape-key-cybersecurity-risks-in-fintech/). 13.06.2024).***

***

«Нове дослідження Keeper Security, (Keeper) провідного постачальника хмарного програмного забезпечення для кібербезпеки з нульовою довірою та нульовим знанням, показує, що майже половина спеціалістів із безпеки (48%) стверджують, що вони віддають перевагу автономним рішенням безпеки для конкретних проблем. Тим не менш, це призвело до того, що професіонали безпеки борються з 32 різними рішеннями безпеки у своїх технологічних стеках, а деякі керують сотнями різних інструментів безпеки.

Крім того, кожен 10-й професіонал з кібербезпеки визнає, що величезна кількість окремих інструментів у їхньому наборі змушує відчувати себе «неконтрольованим», що вказує на явну потребу в консолідації платформи.

Незалежні дослідники від імені Keeper опитали 218 професіоналів з кібербезпеки, включаючи CISO/CIO, старших менеджерів з кібербезпеки та осіб, які приймають рішення, на Infosecurity Europe, що відбулася в Лондоні цього місяця.

Основні фактори для фахівців із безпеки, які впливають на придбання рішень із кібербезпеки, включають:

Вартість

Простота виконання

Репутація постачальника

Ефективність проти конкретних загроз

Інтеграційні можливості

Незважаючи на фінансові вигоди від консолідації платформи, понад дві третини професіоналів підкреслили вартість як основну турботу та поставили можливості інтеграції як п’ятий фактор впливу при покупці рішень безпеки.

У той час як майже половина (48%) віддають перевагу окремим рішенням безпеки, лише 23% віддають перевагу можливостям інтеграції. Це може стати проблемою, оскільки вказує на те, що спеціалісти з безпеки зосереджуються на короткострокових виправленнях, а не на довгострокових покращеннях безпеки та бюджетному впливі.

З огляду на мінливий ландшафт загроз і широко поширені бюджетні обмеження на тлі глобального економічного спаду, організації можуть вважати неприйнятними продовжувати віддавати пріоритет рішенням на основі конкретних можливостей, а не цілісній стратегії кібербезпеки.

Попереднє дослідження, проведене Keeper, показало, що 92% бізнес-лідерів у всьому світі зазнали збільшення кількості кібератак з року в рік, причому 95% респондентів визнали, що загрози стали більш складними, частково завдяки прогресу ШІ. «Очевидно, що загрози кібербезпеці стають лише більш витонченими, змушуючи команди безпеки протистояти новим векторам атак», — сказав Даррен Гуччіоне, генеральний директор і співзасновник Keeper Security.

«Проблема полягає у високих витратах і складності управління розрізненими рішеннями для кожної конкретної загрози. Замість увічнення реактивного підходу «вдари крота», професіонали з безпеки повинні прийняти комплексну стратегію, яка об’єднує існуючі інструменти в єдину структуру. Це підвищить ефективність

пом’якшення загроз і розширить можливості керівників підприємств з більшим контролем і видимістю свого стану безпеки». – сказав Гуччіоне.

ІТ-лідери повинні визначити пріоритети відповідно до адаптації своєї позиції в галузі кібербезпеки. Менеджери паролів забезпечують надійну гігієну паролів і пом’якшують атаки на основі облікових даних, а керування привілейованим доступом (PAM) зміцнює захист, контролюючи та відстежуючи доступ високого рівня до критичних ресурсів.

Інтегруючи ці рішення в уніфіковану платформу, організації встановлюють багаторівневий підхід до безпеки, який значно обмежує несанкціонований доступ і підвищує загальну стійкість кібербезпеки, мінімізуючи потенційну шкоду під час кібератак, які можуть завдати руйнівних довгострокових наслідків для організацій». ***(Too Many Tools - Cybersecurity Professionals Feel Out Of Control // Cyber Security Intelligence (https://www.cybersecurityintelligence.com/blog/too-many-tools-leave-cybersecurity-professionals-feel-out-of-control-7717.html). 14.06.2024).***

***

«…Ландшафт кіберзагроз, що постійно змінюється, означає, що організації будь-якого розміру повинні надавати пріоритет обізнаності про кібербезпеку. Але чому саме обізнаність про кібербезпеку є такою важливою?

Захист від фінансових втрат

Кібератаки можуть завдати шкоди компанії фінансово. Порушення даних, атаки програм-вимагачів і шахрайство з компрометацією бізнес-електронної пошти (BEC) можуть призвести до великих штрафів, крадіжки коштів і значної втрати доходу. Уявіть собі сценарій, коли хакер проникає у вашу систему через фішинговий електронний лист і викрадає дані клієнтів. Розслідування та потенційні позови можуть коштувати вашій компанії мільйони.

Навчання з питань кібербезпеки допоможе вашим співробітникам виявляти та уникати цих загроз. Ознайомившись із проблемними прапорцями та найкращими практиками за допомогою ресурсів, таких як ті, що надаються постачальниками послуг, наприклад revotech-networks.com, ваші співробітники

стануть вашою першою лінією захисту. Це значно знижує ризики фінансових втрат і гарантує майбутнє вашої компанії.

Підвищення репутації бренду

Новини про кібератаку можуть швидко поширюватися через соціальні мережі та новинні видання, кидаючи тінь на репутацію вашого бренду. Негативний розголос може тривати місяцями, навіть роками, утримуючи потенційних клієнтів і партнерів від ведення бізнесу з вами.

Створення культури обізнаності про кібербезпеку демонструє ваш проактивний підхід до безпеки даних, позиціонуючи вашу компанію як надійну та надійну компанію. Це може дати вам конкурентну перевагу на сучасному ринку, де клієнти все більше стурбовані конфіденційністю даних. Демонструючи свою відданість кібербезпеці, ви викликаєте довіру та формуєте лояльність до бренду, зрештою зміцнюючи свою репутацію та стимулюючи зростання бізнесу.

Захист конфіденційної інформації

Компанії часто обробляють конфіденційні дані – інформацію про клієнтів, фінансові записи, інтелектуальну власність. Порушення даних може оприлюднити цю інформацію, що призведе до крадіжки особистих даних, підриву довіри клієнтів і юридичних наслідків. Розуміючи стратегії та найкращі практики кібербезпеки, співробітники стають першою лінією захисту у захисті цих конфіденційних даних.

Підтримуйте довіру клієнтів

Клієнти довіряють підприємствам свою особисту інформацію, від імен і адрес до номерів кредитних карток і номерів соціального страхування. Кібератака, яка скомпрометує ці дані, може порушити цю довіру, що призведе до:

Відтік клієнтів

Незадоволені клієнти, які зазнають порушення даних, з більшою ймовірністю переведуть свій бізнес в інше місце, що призведе до втрати доходу та потенційних амбасадорів бренду. У сучасному конкурентному середовищі лояльність клієнтів має першорядне значення. Порушення даних може підірвати цю лояльність, ускладнюючи повернення клієнтів, чия довіра була зраджена.

Шкода репутації

У сучасну епоху цифрових технологій новини про витік даних можуть швидко поширюватися, псуючи імідж вашого бренду та ускладнюючи залучення нових клієнтів. Негативний розголос також може вплинути на вашу здатність залучати й утримувати найкращих талантів.

Нормативні штрафи

Порушення даних може порушувати положення про конфіденційність, такі як Загальний регламент захисту даних (GDPR) і Каліфорнійський закон про конфіденційність споживачів (CCPA), що призведе до великих штрафів і судових зборів, які можуть навантажити ваші ресурси. Ці штрафи можуть сягати мільйонів доларів, залежно від тяжкості порушення та кількості постраждалих осіб.

Навчання з питань кібербезпеки демонструє вашу відданість захисту конфіденційності клієнтів. Вживаючи заходів для захисту їхніх даних, ви створюєте основу довіри, яка є важливою для довгострокового успіху. IT-підтримка від постачальників послуг, таких як generationix.com, також може відігравати вирішальну роль у забезпеченні надійних заходів безпеки та забезпеченні надійного захисту вашого бізнесу від потенційних загроз.

Підвищуйте моральний дух співробітників

Кібератаки можуть бути стресом для співробітників, залишаючи їх уразливими та невпевненими. Навчання з питань кібербезпеки дає їм знання та інструменти для впевненого орієнтування в цифровому ландшафті. Це створює відчуття безпеки та покращує загальний моральний стан працівників.

Дотримуватись Регламенту

Різні галузі регулюються суворими правилами захисту даних. Недотримання цих правил може призвести до великих штрафів і судових позовів. Поінформованість про кібербезпеку гарантує, що ваші співробітники ознайомлені з цими правилами та дотримуються необхідних протоколів, щоб дотримуватися їх. Це не тільки захистить ваш бізнес від юридичних наслідків, але й вселить довіру у ваших клієнтів і партнерів.

Створіть проактивну культуру безпеки

Кібербезпека – це не одноразове рішення. Це постійний процес, який вимагає постійної пильності. Віддаючи пріоритет обізнаності про кібербезпеку, ви створюєте культуру, у якій безпека є частиною повсякденної практики. Співробітники стають активними учасниками захисту даних компанії, а не просто пасивними спостерігачами. Ось кілька способів розвитку проактивної культури безпеки:

Регулярне спілкування та навчання

Тримайте співробітників в курсі останніх кіберзагроз і найкращих практик за допомогою регулярних тренінгів, моделювання фішингу та внутрішніх комунікаційних кампаній.

Повідомлення про інциденти

Встановіть чіткі процедури повідомлення про підозрілу діяльність і створіть безпечний простір для співробітників, щоб повідомляти про інциденти, не боячись помсти. Це можна зробити, створивши анонімну гарячу лінію або електронну адресу.

Чемпіони безпеки

Допоможіть співробітникам стати чемпіонами безпеки в своїх командах. Ці чемпіони можуть допомогти підвищити обізнаність своїх однолітків щодо кібербезпеки та відповісти на основні запитання.

Підтримка лідерства

Відданість керівництва кібербезпеці є важливою для створення культури безпеки. Лідери повинні задавати тон, дотримуючись протоколів безпеки та беручи участь у тренінгах.

Створення проактивної культури безпеки передбачає постійні зусилля та залучення всіх рівнів організації. Застосувавши ці методи, ви зможете підвищити загальну кібербезпеку вашої компанії.

Висновок

Віддаючи пріоритет обізнаності про кібербезпеку, ви не просто захищаєте свої дані та системи – ви захищаєте майбутнє своєї компанії. У світі, де

кіберзагрози постійно присутні, проактивний підхід до кібербезпеки більше не є варіантом – це необхідність». ***(Fabrice Beaux. Cyber Threat Preparedness: Why Is Cybersecurity Awareness Important for Businesses // BBN Times (https://www.bbntimes.com/technology/cyber-threat-preparedness-why-is-cybersecurity-awareness-important-for-businesses). 14.06.2024).***

***

«…зараз настав час почати думати про них [кіберінциденти у космосі] і планувати їх.

Такий висновок із нового дослідження кібератак у космосі, яке фінансується Національним науковим фондом США (NSF), яке провели дослідники Каліфорнійського політехнічного університету (Cal Poly). У 95-сторінковому звіті розглядається злиття потенційних рушійних сил для нового рубежу в кібератаках протягом наступних кількох десятиліть, коли країни — і приватний бізнес — борються за домінування та вплив у космосі.

Таксономія космічної кібербезпеки

Доповідь насамперед пропонує таксономію космічної кібербезпеки, яку дослідники можуть використовувати для розробки мільйонів нових сценаріїв кібер-атак із залученням інфраструктури запуску та наземної інфраструктури, супутників, космічних станцій, супутникових телефонів і терміналів, а також каналів зв’язку з землі в космос.

Теоретична атака на місячний дверний замок і викрадення зграї CubeSat — це два з 42 сценаріїв, які автори надають як зразок того, як дослідники можуть використовувати цю таксономію, щоб уявити різні способи, якими кібератаки можуть розгортатися в космосі. Інші приклади включають введення підроблених даних, пов’язаних із позаземним життям, у місії в глибокому космосі, щоб викликати незаслужену, дорогу та трудомістку відповідь; або зараження критично важливих запасів їжі для космічного табору шляхом атаки на системи, що контролюють ці запаси.

Сама таксономія представлена у формі матриці під назвою ICARUS (що розшифровується як «Imagining Cyberattacks to Anticipate Risks Unique to Space»). Матриця перераховує всі основні змінні, які становлять кібератаку, і впорядковує їх за вектором атаки, типом експлойтів, мотивацією потенційних учасників загрози, жертвами та різними космічними можливостями, які атака може скомпрометувати. За словами дослідників, вибравши змінну з двох або більше з цих категорій, дослідники можуть створити понад 4 мільйони нових сценаріїв кібератак у космосі.

«Є кілька причин вважати, що кібератаки стануть домінуючою формою конфлікту в космосі», — каже Патрік Лін, провідний автор звіту та директор групи етики та нових наук Cal Poly.

Проте більшість дискусій — принаймні тих, які не є секретними — які стосуються кіберзагроз у космосі, рідко мають тенденцію виходити за межі деяких загальних сценаріїв злому супутників або глушіння, фальсифікації сигналу або вимкнення зв’язку GPS, каже Лін.

Частково це тому, що всі зареєстровані випадки кібератак на космічні цілі наразі стосувалися лише одного з цих компонентів. Останнім прикладом є атака Росії на американську комунікаційну компанію Viasat у лютому 2022 року, яка порушила супутникове з’єднання десятків тисяч клієнтів по всій Європі. Інша — дедалі небезпечніша неспроможність розглянути або визнати всі різні поверхні атак, які відкриваються, коли урядові та приватні організації поспішають розгортати безліч нових технологій у космосі — від гігантських космічних кораблів до крихітних CubeSat для наукових досліджень.

Нездатність уявити космічні атаки

«Оскільки нездатність уявити повний спектр загроз може бути катастрофічним для будь-якого планування безпеки, нам потрібно більше, ніж звичайні сценарії, які зазвичай розглядаються в дискусіях про кібербезпеку в космосі», — говорить Лін. «Наша матриця ICARUS заповнює цю прогалину «уяви».

Лін та інші автори звіту — Кейт Абні, Брюс Де Брюл, Кіра Аберкромбі, Генрі Деніелсон і Райан Дженкінс — визначили кілька факторів, які збільшують

потенціал для кібератак, пов’язаних із космосом, протягом наступних кількох років і десятиліть.

Серед них – стрімке завантаження космічного простору в останні роки в результаті гонки держав і приватних компаній у розгортанні космічних технологій; віддаленість простору; і технологічна складність.

Як зазначається у звіті, кількість зареєстрованих об’єктів у космосі, більшість з яких є супутниками, нещодавно зросла неймовірною швидкістю після стабільного становлення близько 150 нових об’єктів на рік у період з 1965 по 2012 рік. Протягом останніх двох років це число не змінювалося. в середньому на 2600 нових об'єктів щороку.

Віддаленість — і величезність космосу — також ускладнює для зацікавлених сторін — як державних, так і приватних — вирішення проблеми вразливості космічних технологій. Є численні об’єкти, які були розгорнуті в космосі задовго до того, як кібербезпека стала основною проблемою, які могли стати цілями для атак.

«І, як би божевільно це не звучало, супутники все ще запускаються без кібербезпеки, такі як CubeSats, які популярні в університетських лабораторіях та інших через недорогу вартість створення та запуску», — зазначається у звіті. «У них, як правило, немає ні місця, щоб втиснути компоненти кібербезпеки, ні бюджету на це».

Космічний мотлох, технологічна складність і багато іншого

Ситуацію погіршує зростаюча складність космічних систем — які часто все ще залишаються прототипами на етапі розгортання — і відносна відсутність спроб зрозуміти або вивчити вразливі місця в них, які можна використовувати в кібернетичному просторі. Існує загальний брак публічної інформації про потенційні кіберпроблеми в космічних технологіях — і космічному ланцюжку поставок загалом — іноді через технологічну новизну, або через міркування секретності, або через небажання виробника розкривати деталі.

Цікаво, що власний інтерес зацікавлених сторін, щоб уникнути сприяння зростаючій проблемі космічного сміття, може за іронією долі змусити супротивників уникати кінетичного конфлікту в космосі та використовувати

кіберзасоби як спосіб звести рахунки. На даний момент існує близько 35 000 частин космічного сміття, яке можна відстежити, і більше 1 мільйона дрібніших бітів — і ніхто насправді не хоче збільшувати цей обсяг шляхом збою або підриву інших космічних об'єктів, зазначається у звіті.

Лін і його колеги також визначили нечіткі правові режими та потенційно високу видимість і вплив кібератак на космічні активи як потенційно потенційну причину інтересу противника в майбутньому.

«Оцінка можливостей у сфері кібербезпеки ніколи не буває легкою, і це ще гірше для космічної сфери через внутрішні проблеми національної безпеки, які можуть засекречувати велику частину цієї інформації», — каже Лін. «Космічна кібербезпека оповита таємницею з самого початку, що не дивно, оскільки космічні запуски почалися як військові місії».

Але захист через невідомість не буде довго доступним, каже він. Дослідники вже почали шукати вразливості в космічних технологіях, каже він, вказуючи на кілька команд, які успішно зламали 3U CubeSat на DEFCON минулого року. обізнаність щодо космічної кібербезпеки заважає більшій кількості практиків із кібербезпеки займатися цією проблемою тут».

Лін каже, що є кілька ключових аудиторій для звіту, серед яких професіонали з космічної кібербезпеки — як технічні, так і пов'язані з політикою — є головними: «Навіть якщо вони розуміють причини проблеми — і дуже важливо зрозуміти проблему, щоб її вирішити. — планувальники безпеки завжди можуть скористатися допомогою, щоб передбачити нові загрози».

По-друге, доповідь також прагне підвищити обізнаність дослідників з інших дисциплін, особливо нетехнічних, таких як соціальні та гуманітарні науки, про проблему, каже Лін. І по-третє, «ми також хочемо підвищити обізнаність широкої громадськості, тому що всі ми є зацікавленими сторонами, оскільки є можливими жертвами», — додає він». ***(Jai Vijayan. Space: The Final Frontier for Cyberattacks // Informa PLC (https://www.darkreading.com/cyber-risk/space-final-frontier-cyberattacks?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 17.06.2024).***

***

«Контрольний список кібербезпеки є важливим для посилення безпеки як персональних пристроїв, так і корпоративних мереж у сучасному цифровому середовищі. Незважаючи на те, що ці заходи в основному спрямовані на забезпечення кібербезпеки для своїх співробітників і робочих місць, ці заходи однаково важливі для безпеки окремих пристроїв.

У цьому контрольному переліку описано основні методи захисту від кіберзагроз, що розвиваються, забезпечуючи наявність стратегій проактивного захисту.

Необхідний контрольний список кібербезпеки

1. Шифрування даних

Шифрування даних перетворює конфіденційну інформацію в закодований формат, що робить її нечитабельною для неавторизованих користувачів. Цей захід безпеки забезпечує конфіденційність і дотримання правил конфіденційності. Навіть якщо зловмисники отримають доступ до зашифрованих даних, вони не зможуть розшифрувати їх без правильного ключа дешифрування, таким чином зберігаючи цілісність даних.

2. Політика аварійного відновлення

Політика аварійного відновлення життєво важлива для організацій, щоб швидко реагувати на кібератаки чи системні збої та відновлюватися після них. Він включає процедури для відновлення даних, мінімізації часу простою та забезпечення безперервності бізнесу. Регулярні оновлення та тренування забезпечують готовність до ефективного вирішення надзвичайних ситуацій.

3. Резервне копіювання зовнішнього жорсткого диска

Зберігання резервних копій на зовнішньому жорсткому диску забезпечує резервування даних в автономному режимі. Ця практика захищає важливі дані незалежно від первинних систем. У сценаріях, таких як атаки програм-вимагачів або збої мережі, офлайн-резервне копіювання сприяє швидкому відновленню даних, доповнюючи резервне копіювання в хмарі.

4. Оновлене програмне забезпечення

Регулярне оновлення програмного забезпечення має вирішальне значення для виправлення відомих уразливостей, якими користуються кіберзлочинці. Оновлення не тільки покращують безпеку, але й покращують функціональність програмного забезпечення та продуктивність. Нехтування оновленнями робить системи вразливими до кіберзагроз і порушує загальну цілісність системи.

5. Страхування кібербезпеки

Страхування кібербезпеки пропонує фінансовий захист від збитків у результаті кіберінцидентів. Він покриває такі витрати, як витрати на розслідування, судові збори та зусилля з пом’якшення наслідків. Це страхування служить запобіжним засобом, гарантуючи, що підприємства можуть відновити роботу після значних подій у сфері кібербезпеки.

6. Антивірусні оновлення

Часті оновлення антивірусного програмного забезпечення необхідні для захисту від нових загроз зловмисного програмного забезпечення. Оновлені антивірусні рішення виявляють і блокують шкідливі дії, підвищуючи загальну безпеку системи. Безперервні оновлення забезпечують захист систем від нових кіберзагроз.

7. Принцип найменших привілеїв

Реалізація принципу найменших привілеїв обмежує права доступу користувачів лише тим, що необхідно для їхніх ролей. Це зменшує ризик внутрішніх загроз і несанкціонованого доступу, зберігаючи контроль над конфігураціями системи та підвищуючи загальну безпеку.

8. Безпечні з'єднання

Захищені з’єднання, яким часто сприяють VPN (віртуальні приватні мережі), шифрують дані під час передачі через загальнодоступні чи незахищені мережі. Ця практика запобігає перехопленню та несанкціонованому доступу до конфіденційної інформації, забезпечуючи конфіденційність і цілісність даних.

9. Надійний брандмауер

Надійний брандмауер діє як бар’єр між довіреними внутрішніми мережами та зовнішніми мережами, фільтруючи вхідний і вихідний трафік. Він блокує

зловмисний трафік і спроби неавторизованого доступу, захищаючи мережеву інфраструктуру та конфіденційні дані від кіберзагроз.

10. Політика кібербезпеки

Створення всебічної політики кібербезпеки має вирішальне значення для сприяння обізнаності щодо кібербезпеки та передового досвіду серед працівників. Ці політики охоплюють вказівки щодо паролів, протоколи використання Інтернету та заходи безпеки електронної пошти. Регулярне навчання підсилює ці політики, зменшуючи вразливість до фішингових атак і спроб неавторизованого доступу.

Висновок

Цей контрольний список кібербезпеки містить важливі заходи для підготовки до потенційних кіберзагроз. Він наголошує на проактивних стратегіях як в Інтернеті, так і фізично, включаючи використання зовнішніх жорстких дисків для резервного копіювання та впровадження надійних політик кібербезпеки. Застосовуючи ці практики, окремі особи та організації можуть підвищити свою стійкість проти мінливого середовища кіберзагроз.

У світі, де загрози кібербезпеці стають дедалі поширенішими, виконання цих пунктів контрольного списку має вирішальне значення». ***(Samiksha Jain. Don't Be a Sitting Duck: The Cybersecurity Checklist You Need Right Now // The Cyber Express (https://thecyberexpress.com/cybersecurity-checklist-you-need-right-now/?utm_source=flipboard&utm_content=FlipboardCanada%2Fmagazine%2FTechnology). 17.06.2024).***

***

«Світ праці зазнав значних змін, навіть коли компанії прагнуть залучати більше талантів і створювати плани безперервності бізнесу. Такі тенденції, як гібридна робота, стали поширеними, особливо з широким впровадженням віддаленої роботи.

Співробітники все більше цікавляться роботами, які керуються дистанційно. У звіті FlexJobs.com за січень 2023 року зазначено, що з 2021 по 2022 рік кількість оголошень про віддалену роботу зросла з 12% до 20%.

Однак віддалена робота створює унікальну проблему для інформаційної безпеки, оскільки віддалене робоче середовище не має таких же гарантій, як офіси. Співробітники повинні вивчити різні методи забезпечення мінімізації ймовірності кібератак.

Помилкою багатьох людей, працюючи вдома, є використання персональних комп'ютерів для виконання «незначних» робочих проектів. Це особливо, якщо ваш робочий комп'ютер знаходиться в іншій кімнаті. Такі операції становлять ризик для компанії та даних компанії.

Якщо ви працюєте з компанією, яка має хороший IT-відділ, вони можуть запускати регулярні оновлення, перевірки безпеки та блокувати шкідливі сайти на робочих комп'ютерах без вашого відома. Наприклад, розробники використовують різні форми тестування, включаючи SAST і DAST, щоб перевірити, чи їхні програми вразливі до атак.

Користуючись своїм персональним комп'ютером, ви ризикуєте стати легкою мішенню, оскільки висока ймовірність того, що ви не дотримуєтесь тих самих протоколів, що й робочі комп'ютери. Без різноманітних заходів безпеки, що працюють у фоновому режимі, ваш персональний комп'ютер небезпечний для роботи з робочими даними.

Якщо роботодавець надає вам доступ до віддаленого доступу, наприклад Office 365, ви можете вибрати роботу в Інтернеті. Утримайтеся від завантаження файлів або синхронізації електронних листів із вашим особистим пристроєм, оскільки завжди рекомендується розділяти ваші особисті та робочі справи.

Одна з найкращих інвестицій, яку ви можете зробити для безпеки вдома, — комплексний антивірусний пакет.

Очікується, що у 2028 році вартість кіберзлочинності в усьому світі зросте до 13,82 трильйона доларів США. Ця цифра може бути навіть вищою, враховуючи збільшення кількості хакерів, які намагаються зламати домашній Інтернет людей, а корпоративні мережі VPN мають доступ до конфіденційних файлів.

Антивірусні пакети дозволяють вам бути в безпеці, пропонуючи автоматичний захист віддаленої роботи від таких загроз, як:

Шкідливе програмне забезпечення, шпигунське програмне забезпечення та віруси

- Фішингові шахрайства
- Атаки нульового дня
- Трояни та хробаки

Комплексний антивірусний пакет забезпечить додаткову лінію захисту на захищених і оновлених пристроях.

Завжди слід уникати публічних мереж Wi-Fi, оскільки вони становлять значний ризик для безпеки. Якщо ви отримуєте доступ до Інтернету через публічного провайдера, ви повинні бути готові вирішити дві основні проблеми.

По-перше, є також інші люди, які використовують цю мережу Wi-Fi, і оскільки між вами та ними немає брандмауера, загрози можуть легко дістатися до вашого пристрою в будь-який час. По-друге, зацікавлений спостерігач, який працює в поточній мережі або іншій публічній мережі, через яку проходять ваші дані, може легко контролювати ваш трафік. Тому важливо знайти спосіб захистити робочий пристрій і зашифрувати трафік.

Хорошим варіантом для використання є особиста точка доступу з телефону або спеціального пристрою. Перевага цього полягає в тому, що навіть якщо трафік між точкою доступу та пунктом призначення незашифрований, ви усуваєте ризик злому користувачами загальнодоступної мережі Wi-Fi. Вартість може бути вищою за використання стільникових даних, але потенційний недолік загальнодоступної мережі Wi-Fi становить більший ризик.

Іншим варіантом є встановлення зашифрованих віддалених з’єднань із віддаленим робочим столом. Типи з’єднань, задіяні в такому налаштуванні, не потребують додаткової служби шифрування для захисту даних під час передачі.

Хоча ви можете довіряти своїм робочим пристроям, працюючи вдома, вони піддаються доступу членів сім’ї та маленьких дітей. Ці люди не мають повноважень або досвіду, необхідних для належного керування пристроями, і можуть створити лазівки, якими можуть скористатися хакери.

Переконайтеся, що всі пристрої знаходяться далеко від членів сім'ї. Вам також потрібно переконатися, що пристрої постійно захищені паролем, щоб запобігти сторонньому доступу до конфіденційних файлів. Бажано мати довгі паролі, які містять великі та малі літери, цифри та символи. Це створює надійні паролі.

Працюючи віддалено, ви повинні переконатися, що ви використовуєте корпоративний пристрій через різні протоколи, які застосовуються для захисту пристроїв. Ви також повинні переконатися, що на всіх пристроях є антивірусні пакети та програмне забезпечення безпеки в Інтернеті для боротьби зі зловмисним програмним забезпеченням, шпигунським програмним забезпеченням та іншими атаками.

Оскільки загальнодоступний Wi-Fi ніколи не є безпечним варіантом, ви можете вдатися до інших варіантів мережі, як-от точка доступу стільникового зв'язку, оскільки це зменшує ризик публічних хакерів. Крім того, ви повинні бути пильними, щоб ваш пристрій використовувався лише вами та був недоступним для інших членів родини.

Дотримуючись таких заходів, ви можете бути впевнені, що зменшите загрози кібербезпеці під час роботи поза офісом». ***(Cyber Security Practices For Remote Working // TechRound (https://techround.co.uk/business/cyber-security-practices-remote-working/). 14.06.2024).***

***

«Згідно з новим звітом, виснаження, пов'язаний із роботою стрес і втома фахівців з кібербезпеки обходяться підприємствам США в 626 мільйонів доларів втрати продуктивності на рік, а підприємствам Великобританії – 130 мільйонів фунтів стерлінгів.

Дослідження, проведене навчальною компанією з кібербезпеки Hack The Box, виявило, що 80% працівників у всьому світі відчувають виснаження та стрес.

Майже три чверті фахівців з кібербезпеки повідомляють про те, що брали відпустку через проблеми з психічним самопочуттям, пов'язані з роботою, причому

в середньому 3,4 дні психічної хвороби на рік втрачаються через напругу, пов’язану з роботою.

Згідно з дослідженням, це означає втрату в середньому 3,4 години роботи на місяць або близько 5 днів на рік, що призводить до погіршення психічного самопочуття.

У звіті стверджується, що зростання кіберзагроз на 600% після пандемії Covid-19 призвело до підвищення рівня стресу для тих, хто працює в секторі кібербезпеки. У ньому також згадується поява новітніх технологій і поширення злочинних груп як проблеми, що посилюють тиск на персонал.

Хоча 90% CISO стурбовані впливом стресу на благополуччя членів їхньої команди, згідно зі звітом, менше половини CEO поділяють таку ж стурбованість.

Однак існує прогалина в тому, що, як вважають, є причиною посилення внутрішнього тиску: 66% керівників підприємств вважають, що їхні спеціалісти з кібербезпеки працюють понаднормово через зростання загроз, тоді як майже 90% фахівців із кібербезпеки називають причиною обсяг проектів, які необхідно виконати за обмежений проміжок часу.

Щоб вирішити цю проблему, трохи менше половини (44%) компаній інвестують у тимчасовий персонал для підтримки команд, а майже 50% інвестують у платформи підвищення кваліфікації, щоб підвищити впевненість членів команди.

Харіс Піларінос, засновник і генеральний директор Hack The Box, каже: «Фахівці з кібербезпеки знаходяться на передовій битви, яку знають, що колись програють, це лише питання часу».

«Ми закликаємо бізнес-лідерів тісніше співпрацювати з професіоналами з кібербезпеки, щоб зробити психічне благополуччя пріоритетом і фактично надавати рішення, необхідні для досягнення успіху», – додає він. «Це не просто правильна річ, це має бізнес-сенс».

Сарб Сембхі, технічний директор Virtually Informed і голова відділу психічного здоров’я в кібербезпеці, каже: «Стрес, виснаження та психічне здоров’я в сфері кібербезпеки досягли найвищого рівня за весь час. Це не лише молодші члени команди, а й аж до рівня CISO. У цій темі складно орієнтуватися, оскільки

вона дуже особиста для кожної людини, але створення правильної підтримки та процесів має так багато переваг для людей і підприємства».

Як зменшити вигорання?

Під час вебінару, присвяченого обговоренню звіту, ТІ почула професіоналів з кібербезпеки про те, як вони зменшують вигоряння, і поради тим, хто має проблеми.

«Підготовленість», — каже Андреа Суччі, керівник відділу інформаційних технологій у логістичній фірмі Ferrari Group. «Якщо ви перейдете в режим паніки, ваша команда перейде в режим паніки. Ви повинні вміти цим керувати».

«Це частина вашої роботи. Вам потрібно вчитися, вам потрібно працювати, вам потрібно готуватися і вам потрібно тренуватися, щоб контролювати стрес. Це як грати в шахи, тому що якщо ви перемістите коня в неправильну позицію, то ви будете в стресі до кінця партії».

У тому ж дусі Піларінос додає, що це допомагає бути готовим до несподіванок і тренуватися для симуляції кризових ситуацій – настільки, що це стає «ще одним днем в офісі».

«Імітація всього досвіду, розвиток емоцій, стресу готує вас до живих подій», — радить він.

Джесс Берн, головний аналітик дослідницької компанії Forrester, рекомендує, зокрема, робочим, які працюють на офісах, виходити на вулицю та прогулятися.

«Погуляти й очистити голову справді допомагає, тому що справи починають здаватися досить важкими, якщо у вас багато конкуруючих пріоритетів», — каже вона.

«Крім того, у мене є чудовий менеджер, і коли на моїй тарілці надто багато справ, ми вирішуємо, що є пріоритетним», — додає Берн. «[Є] хтось інший, щоб сказати те, що вони думають, що має найбільший сенс для мене, щоб визначити пріоритети, коли все терміново, і відкинути ідеї, це неймовірно корисно».

Насамкінець Сембхі додає, що «Психічне здоров’я в кібербезпеці» виявило, що коли люди перебувають у стресі, у них з’являються шкідливі звички, як-от

неправильне харчування, більше споживання кави та алкоголю, більше куріння, брак сну та фізичних вправ.

«Щодо мене, я завжди намагався бути впевненим, що я займаюся спортом, правильно харчуюся, зменшую споживання алкоголю та правильно сплю. Усі ці прості речі».

Сембхі також пропонує скоротити час розмови, щоб дозволити перерви між зустрічами. Наприклад, годинний дзвінок займає 50 хвилин, а півгодини 25 хвилин. Крім того, видалення сповіщень з електронної пошти, щоб зменшити стресові відволікання та відвідування електронних листів, коли є можливість». ***(Cyber security burnout costing US enterprises over $620m // TechInformed (https://techinformed.com/cyber-security-burnout-is-costing-us-enterprises-over-620-million-a-year/). 17.06.2024).***

***

«Нова група, яка називає себе Міжнародна організація з кібербезпеки на морі (IMCSO), створює незалежний сторонній стандарт для покращення послуг кібербезпеки в морському світі. За даними організації, незважаючи на те, що існує багато кіберпрофесіоналів, небагато мають спеціалізовані морські знання, тоді як загроза для суден та інтересів судноплавства продовжує зростати.

Хоча жодного конкретного прикладу конфіскації судна чи жертви кібератаки задокументовано не було, судноплавні компанії, портові адміністрації та навіть Міжнародна морська організація (ІМО) зазнали атак. У міру того, як кораблі стають більш зв’язаними, і в той час як у майбутньому вимальовуються перспективи дистанційного керування кораблями, експерти підкреслюють, що кібернебезпеки для морського світу лише зростають.

«Кібербезпека була визначена Міжнародною морською організацією (ІМО), яка вимагає від судноплавних компаній впроваджувати заходи для захисту своїх бортових систем управління безпекою та проводити їх регулярний аудит. Однак зміни в законодавстві спричинили появу нової індустрії морської кібербезпеки, яка

виявилася мінливою у своєму підході до оцінки систем та тлумачення стандартів», — пояснює Кемпбелл Мюррей, генеральний директор IMCSO.

Він пояснює, що метою організації є підвищення рівня оцінки ризиків кібербезпеки в морській галузі. IMCSO повідомляє, що розробить програми сертифікації для консультантів з безпеки та професійний реєстр, а також перевірить результати звітів для забезпечення узгодженості. Вони планують надати інструменти як для ідентифікації експертів з морської кібербезпеки, так і для відстеження ризиків для окремих суден.

Вони зазначають, що капітани, офіцери та члени екіпажу зайняті й не обов'язково мають досвід, щоб наглядати за кібер-аудиторами, які проводять оцінювання. IMCSO прагне вирішити проблеми, що виникають у секторі, спорядивши індустрію безпеки для проведення цих тестів у належний, безпечний та однаковий спосіб, таким чином дозволяючи сектору порівнювати відповідність вимогам. Однією з проблем, на яку вони вказують, є низка різних методологій, що існують на даний момент, і різні вимоги до інформації, яку необхідно надати портовій владі та страховикам.

Окрім програми сертифікації з навчанням, IMCSO планує надати реєстри. Він виділить постачальників кібербезпеки в рамках спеціальності морської кібербезпеки. Транспортні компанії, про які вони повідомляють, зможуть здійснювати пошук у базі даних, щоб знайти персонал, який має досвід роботи в певній сфері та місці.

IMCSO також підтримуватиме базу даних реєстру ризиків, яка міститиме результати оцінок і аудитів суден, що дозволить відповідним сторонам отримати доступ до профілю кіберризиків будь-якого конкретного судна. Завдяки стандартизації даних і форматів, за їхніми словами, споживачам цієї інформації, наприклад портовим адміністраціям і страховим компаніям, буде набагато простіше враховувати кіберризик судна». ***(New Organization Seeks to Build Maritime Cyber Security Capabilities // The Maritime Executive, LLC. (https://maritime-executive.com/article/new-organization-seeks-to-build-maritime-cyber-security-capabilities). 18.06.2024).***

***

«…Сучасний маркетинговий ландшафт кібербезпеки завалює керівників дивовижними повідомленнями. Величезний обсяг, загальні повідомлення та тактика FOMO створюють ринок шуму. Відсутність прозорості з використанням жаргону, прихованих витрат і нереалістичної рентабельності інвестицій обіцяє подальше незрозуміле судження. Подібним чином, конкурентний ландшафт навколо використання штучного інтелекту в кібербезпеці сам по собі викликає здивування, коли постачальники рекламують хибні можливості рішень, блокування постачальників і фрагментований ринок.

На жаль, маркетингові повідомлення, які переконали команди безпеки придбати рішення цих постачальників, залишилися завалені сповіщеннями та пошуком помилкових спрацьовувань.

Ця плутанина призводить до марної витрати ресурсів, затримки рішень і підриву довіри. Маркетинг повинен перейти від викидання нісенітниці до обговорення того, як він задовольняє потреби клієнтів. Прозора комунікація має життєво важливе значення для того, щоб допомогти керівникам і командам безпеки зробити обґрунтований вибір і побудувати надійний захист безпеки.

Шлях вперед

Рішення полягає в дивовижній паралелі: прорізання шуму. Подібно до того, як штучний інтелект допомагає аналітикам безпеки визначити пріоритети реальних загроз, інтелектуальне лідерство може подолати маркетинговий шум для підприємств. Обидва ці підходи зосереджені на релевантності, достовірності та практичних ідеях.

Фільтрування шуму

Подібно до того, як штучний інтелект фільтрує нескінченні дані безпеки, щоб виявити справжні загрози, інтелектуальне лідерство усуває маркетинговий шум і позиціонує компанію як надійного радника.

Подібності:

Зосередьтеся на релевантності:

• AI визначає пріоритетність сповіщень на основі їх потенційного впливу, зосереджуючись на найбільш релевантних загрозах.

• Контент, спрямований на лідерство думок, створено для вирішення конкретних проблемних моментів і проблем, з якими стикається цільова аудиторія, забезпечуючи його відповідність процесу прийняття рішень.

Довіра та досвід:

• AI використовує дані про загрози та дані про вразливості, щоб зміцнити довіру до своїх оцінок загроз.

• Контент, спрямований на лідерство думок, демонструє глибоке розуміння компанією галузевих проблем і робить її інноваційними, надійними експертами.

Корисна інформація:

• AI не просто визначає загрози; він надає контекст і дієві рекомендації для команд безпеки.

• Лідерство думки виходить за межі усвідомлення; він пропонує практичні рішення та найкращі практики, щоб допомогти підприємствам долати складні виклики.

Забезпечення переваг для всіх

Такий підхід вигідний усім. Незалежно від того, чи використовується штучний інтелект для фільтрації сповіщень, чи інтелектуальне лідерство для посилення маркетингових зусиль, маркетингові команди залучають кваліфікованих потенційних клієнтів і зміцнюють довіру. Команди безпеки спостерігають зменшення втоми від оповіщення та приймають кращі рішення. Підприємства отримують більш надійну безпеку.

Маркетингові групи:

Поєднуючи інтелектуальне лідерство з традиційними маркетинговими зусиллями, маркетингові групи можуть:

Привертайте увагу: інтелектуальне лідерство привертає увагу потенційних клієнтів, демонструючи досвід і пропонуючи цінну інформацію, підвищуючи впізнаваність бренду та зміцнюючи довіру.

Кваліфіковані потенційні клієнти: контент, спрямований на лідерство думки, приваблює потенційних клієнтів, які стикаються з конкретними проблемами, які ви можете вирішити, залучаючи кваліфікованих потенційних клієнтів, які щиро зацікавлені у ваших рішеннях.

Диференціація бренду: продумане лідерство позиціонує вашу компанію як далекоглядного експерта галузі, вирізняючи вас серед конкурентів, які пропонують ті самі продукти чи послуги.

Підвищена довіра: демонстрація досвіду зміцнює довіру потенційних клієнтів, роблячи їх більш сприйнятливими до ваших маркетингових повідомлень.

Стимулюйте залучення до продажів: довіра, створена завдяки інтелектуальному лідерству, полегшує взаємодію з потенційними клієнтами, оскільки вони вже сприймають вашу компанію як експерта, який має знання для вирішення їхніх проблем.

Команди безпеки:

Ефективне використання штучного інтелекту в кібербезпеці дає аналітикам такі можливості:

Зменшення втоми від сповіщень: штучний інтелект визначає пріоритетність загроз на основі їх релевантності, що дає змогу аналітикам безпеки зосередитися на розслідуванні справжніх загроз.

Швидший час відповіді: відфільтровуючи хибні спрацьовування, AI дозволяє швидше ідентифікувати та реагувати на реальні інциденти безпеки.

Покращений процес прийняття рішень: штучний інтелект надає контекст і інформацію разом із загрозами, дозволяючи командам із безпеки приймати більш обґрунтовані рішення.

Підвищена ефективність: AI автоматизує повторювані завдання, дозволяючи командам безпеки присвятити свій досвід більш стратегічним ініціативам.

Винос

У вік інформаційного перевантаження кібербезпека та маркетинг потребують стратегій, щоб подолати шум. Подібно до того, як штучний інтелект має вирішальне значення для професіоналів у сфері кібербезпеки, ідейне лідерство є

життєво важливим у маркетингу для корпоративних організацій. Зосереджуючись на релевантності, довірі та практичних ідеях, ШІ та інтелектуальне лідерство можуть допомогти організаціям визначити, що справді важливо, і досягти своїх цілей.

Отже, наступного разу, коли ви розроблятимете свою маркетингову стратегію, пам'ятайте про силу лідерства думки. Це ваш ШІ для залучення потрібних клієнтів і взаємодії з ними у світі, переповненому марною інформацією». ***(Joe Ariganello. How Thought Leadership Mirrors Utilizing AI In Cybersecurity // Forbes (https://www.forbes.com/sites/forbescommunicationscouncil/2024/06/21/how-thought-leadership-mirrors-utilizing-ai-in-cybersecurity/). 21.06.2024).***

***

«…Оскільки бізнеси стають все більш взаємопов'язаними та залежними від даних, потреба в надійній стратегії кібербезпеки стає першочерговою. Одним із підходів, який набирає популярності в усьому світі, є концепція Zero Trust.

Але що таке Zero Trust?

За своєю суттю Zero Trust кидає виклик традиційному уявленню про те, що суб'єктам у мережі слід безперечно довіряти. Натомість він виступає за постійний процес перевірки, гарантуючи, що довіра ніколи не припускається, а безпека підтримується під час кожної взаємодії. Простіше кажучи, Zero Trust базується на передумові, що кожен і все, хто запитує будь-що у вашому IT-середовищі, має бути перевірено, перш ніж йому можна буде довіряти.

Розуміння ландшафту

Південноафриканські компанії працюють у середовищі, де кіберзагрози не тільки зростають, але й стають все більш витонченими. Традиційні моделі безпеки, побудовані на припущенні безпечного периметра, виявляються неадекватними в сучасному динамічному ландшафті загроз. Це усвідомлення підкреслює необхідність стратегічного зрушення, яке б відповідало реаліям сучасних проблем кібербезпеки: нульова довіра.

Нульова довіра, безсумнівно, завойовує великий інтерес, оскільки галузеві дослідження показують, що 60% організацій планують або активно впроваджують стратегію нульової довіри. Однак, згідно з дослідженнями Gartner, хоча багато організацій мають стратегію «нульової довіри» та працюють над впровадженням технологій «нульової довіри», мало хто є зрілими. Відсутність інтеграції між продуктами безпеки ускладнює досягнення наскрізного розгортання Zero Trust, а організації, які прийняли Zero Trust, намагаються перевірити покращення свого стану безпеки, оскільки немає ефективних методів вимірювання впливу.

До 2025 року понад 90% корпоративних мережевих продуктів все ще не відповідатимуть основним вимогам мережі Zero Trust.

До 2026 року 75% організацій включатимуть у свою стратегію Zero Trust лише керовані пристрої та сучасні програми, щоб зменшити складність і витрати.

До 2027 року 25% організацій, які використовують мережевий доступ з нульовою довірою (ZTNA), перейдуть від статичних одноразових правил доступу до постійного динамічного контролю на основі ризиків.

Незважаючи на складнощі, фахівці з кібербезпеки одностайно виступають за підхід «нульової довіри» або принаймні за шлях до нього.

Розробка Zero Trust для південноафриканських малих і середніх підприємств

Що робить Zero Trust привабливим, так це те, що його впровадження не означає, що вам доведеться капітально переглядати існуючі системи. Натомість це передбачає стратегічний поетапний підхід, який відповідає унікальним потребам і обмеженням вашого бізнесу.

Безпека, орієнтована на користувача: Zero Trust обертається навколо принципу «ніколи не довіряй, завжди перевіряй». Це робить сильний акцент на автентифікації та авторизації користувачів. Цього можна досягти шляхом впровадження багатофакторної автентифікації, керування доступом на основі ролей і регулярних перевірок доступу користувачів. Починаючи зі статичних політик на основі сигналів користувачів і пристроїв, організації починають шлях до зрілості Zero Trust.

Визначення критично важливих активів. Організації повинні визначити та визначити пріоритети для своїх найважливіших активів. Це можуть бути дані клієнтів, фінансові записи або конфіденційна інформація. Визначивши ці активи, компанії можуть адаптувати впровадження Zero Trust для захисту найважливішого. У рамках цього процесу організації повинні визначити ресурси, які виграють від динамічних політик доступу, а не ті, які можуть бути належним чином захищені статичними політиками на основі ролей.

Встановлення управління: щоб подолати проблему невимірності, організації повинні налагодити управління навколо своїх програм Zero Trust, щоб гарантувати, що реалізовані переваги є вимірними та кількісно визначеними.

Безперервний моніторинг: на відміну від традиційних моделей безпеки, які зосереджуються на периметрі, Zero Trust вимагає постійного моніторингу всіх мережевих дій. Цей проактивний підхід дозволяє компаніям виявляти потенційні загрози та реагувати на них у реальному часі, мінімізуючи вплив потенційного інциденту безпеки.

Безпека постачальників і ланцюгів постачання: багато південноафриканських організацій співпрацюють із зовнішніми партнерами та постачальниками. Zero Trust поширює свої принципи за межі організації, наголошуючи на необхідності безпечних з'єднань і постійної перевірки в усьому ланцюжку постачання.

Юридичні перспективи

Кіберстійкість і нульова довіра — це не просто технологічні вимоги; це також важливі юридичні міркування. З юридичної точки зору компанії повинні переконатися, що їхні стратегії кібервідмовостійкості відповідають нормативним вимогам і галузевим стандартам. Це передбачає не лише впровадження надійних заходів безпеки, але й документування цих зусиль, щоб продемонструвати відповідність законам про захист даних, таким як Закон про захист персональних даних 2013 року (POPIA) (переважний закон Південної Африки про захист конфіденційності) та будь-які інші закони про конфіденційність у всьому світі які можуть застосовуватися до використання компанією особистої інформації (наприклад, GDPR, Закон Великобританії про захист даних, CCPA та інші).

Невиконання цього може призвести до серйозних юридичних наслідків, включаючи штрафи, пеню та репутаційну шкоду.

Як згадувалося вище, архітектура Zero Trust вимагає ретельного підходу до контролю доступу та керування даними. З юридичної точки зору цей підхід є безцінним, оскільки він мінімізує ризик несанкціонованого доступу та витоку даних, які є головною проблемою багатьох нормативних актів щодо захисту даних. Організації повинні встановити чітку політику та процедури перевірки особи, постійного моніторингу та реагування на інциденти. Ці політики слід регулярно переглядати та оновлювати, щоб йти в ногу з мінливими кіберзагрозами та правовими вимогами.

Крім того, ризик, позначений вище в розділі «Безпека постачальників і ланцюгів постачання», викликає правову думку про те, що контракти зі сторонніми постачальниками повинні відображати зобов'язання щодо кіберстійкості та принципів нульової довіри. Це включає в себе включення конкретних положень, які вимагають дотримання суворих стандартів кібербезпеки, регулярні перевірки безпеки та негайне сповіщення про інциденти безпеки. Такі положення допомагають пом'якшити правові ризики та гарантують, що всі сторони однаково зобов'язані підтримувати надійну систему кібербезпеки.

Важливо пам'ятати, що нульова довіра, як і всі підходи до кібербезпеки, не є срібною кулею, і вона сама по собі не може усунути всі кіберзагрози. Кібербезпека є багаторівневою, і будь-яка хороша практика кібербезпеки захищатиме перекриваючі рівні, призначені для спільної роботи для виявлення та припинення вторгнень. Таким чином, Zero Trust має бути доповнено або підтримано цілісною стратегією кібербезпеки, щоб бути повністю ефективним.

Впровадження кіберстійкості

У цифровому середовищі, повному невизначеності, застосування принаймні основ стратегії нульової довіри є кроком до стійкої позиції кібербезпеки для південноафриканських організацій. Йдеться не лише про запобігання порушенням, а й про формування здатності адаптуватися, реагувати та швидко відновлюватися

після будь-якого інциденту безпеки. Відмовтеся від спокуси стежити за останніми тенденціями кібербезпеки та дотримуйтесь основ.

Інтеграція правових аспектів у стратегії кіберстійкості та нульової довіри є надзвичайно важливою. Узгодивши заходи безпеки з вимогами законодавства та гарантуючи, що контракти з третіми сторонами включають суворі зобов'язання щодо кібербезпеки, організації можуть краще захистити себе від кіберзагроз і юридичної відповідальності.

Починаючи шлях до нульової довіри, організації повинні прийняти прагматичний підхід, узгоджений із унікальним ландшафтом загроз, що розвивається. Щоб повністю зрозуміти нюанси та спланувати подорож відповідно до потреб і цілей вашої організації, партнерство з експертом допоможе вам впевнено орієнтуватися в цій мінливій цифровій місцевості…» ***(Priyanka Raath and Ridwaan Boda. Building Cyber Resilience: The Strategic Imperative of Zero Trust // ENSafrica (https://www.ensafrica.com/news/detail/8746/building-cyber-resilience-the-strategic-imper). 06.2024).***

***

«У сучасному цифровому ландшафті стратегії зберігання даних відіграють вирішальну роль у загальному підході організації до кібербезпеки. Незалежно від того, чи йдеться про захист конфіденційної інформації клієнтів, захист інтелектуальної власності чи забезпечення безперервності бізнесу, спосіб зберігання даних може покращити або порушити здатність організації захищатися від кіберзагроз.

Підприємства стикаються з безпрецедентним сплеском інформації. Оскільки дані зростають експоненціально завдяки інноваціям, взаємодії з клієнтами та бізнес-операціям, організації повинні балансувати між використанням їхнього потенціалу та забезпеченням їх безпеки та доступності.

Зростання кіберзлочинності

Оскільки кібератаки стають все більш частими та витонченими, компанії повинні приділяти пріоритет захисту даних. Зокрема, значний ризик становлять

атаки програм-вимагачів. У цих зловмисних інцидентах кіберзлочинці блокують або шифрують доступ до даних організації та вимагають викуп за їх оприлюднення.

Відповідно до останнього звіту Verizon 2023 Data Breach Investigations, програмне забезпечення-вимагач присутній у понад 62% інцидентів, скоєних діячами організованої злочинності, і в 59% інцидентів з фінансовою мотивацією. Вплив також є значним – підприємствам потрібно в середньому 9,9 днів, щоб відновити нормальну роботу після початкової атаки програм-вимагачів, причому 1 з 31 компанії в усьому світі щотижня стикається з атаками програм-вимагачів.

У середовищі загроз, що швидко розвивається, компанії стикаються з постійною боротьбою з кібератаками. Оскільки частота та складність цих атак зростає, захист критичних даних стає першорядним.

Дані служать наріжним каменем для зростання, інновацій і задоволеності клієнтів. Незважаючи на величезну цінність, багатьом організаціям важко повністю використовувати дані, які вони генерують. Крім того, забезпечення безпечного та надійного зберігання даних залишається проблемою. Однак існуючі стратегії зберігання даних можна використовувати для захисту від кіберзагроз і запобігання інцидентам втрати даних.

Роль незмінного зберігання даних

Введіть незмінне сховище даних – потужну зброю в боротьбі з кіберзагрозами. Незмінне сховище гарантує, що дані, записані, не можуть бути видалені або змінені. Це означає, що безпека даних підвищується, а організації мають можливість відновлювати дані зі 100% точністю у разі порушення.

Незмінне сховище виступає останнім бар’єром проти кібератак. Навіть якщо інші заходи безпеки не спрацюють, цілісність збережених даних залишається незмінною. Кіберзлочинці не можуть підробити або змінити важливу інформацію.

Коли програми-вимагачі атакують, наявність незмінних резервних копій стає вирішальною. Організації, які платять викуп, часто не відновлюють свої дані повністю, тоді як організації, які мають надійні резервні копії, можуть відновити свої системи без шкоди для цілісності даних. Ця стійкість проти програм-вимагачів є життєво важливою у світі, де програми-вимагачі стають все більш плідними.

Крім того, після нападу час має велике значення. Незмінне зберігання даних забезпечує відому відправну точку для швидкого відновлення, мінімізації часу простою та забезпечення безперервності бізнесу.

Впровадження незмінних рішень для зберігання

Щоб захиститися від кіберзагроз, компаніям слід запровадити політику захисту даних, яка включає незмінне зберігання з розширеним виявленням загроз на додаток до ретельного процесу резервного копіювання та відновлення даних. Раннє виявлення дозволяє діяти проактивно, запобігаючи ескалації атак.

Це особливо важливо для критично важливих даних, таких як записи клієнтів, фінансові операції та інтелектуальна власність, щоб забезпечити безпеку даних.

Резервне копіювання, щоб мінімізувати шкоду від програм-вимагачів

Важливо мати надійні рішення для резервного копіювання. Організації повинні регулярно створювати резервні копії даних у незмінному сховищі та тестувати процес відновлення, щоб перевірити точність. Ці резервні копії служать критично важливим заходом на випадок втрати даних через програми-вимагачі або інші кіберінциденти. Ефективні рішення для резервного копіювання мінімізують час простою та забезпечують безперервність бізнесу.

Коли підприємства створюють резервні копії даних, зловмисник втрачає контроль. Організації продовжують володіти даними та мати доступ до них, навіть якщо вони викрадені. Однак важливо зазначити, що багато зловмисників будуть шукати та видаляти резервні копії, тому потрібно вживати запобіжних заходів, щоб захистити їх. Щоб ускладнити доступ до резервної копії, компаніям слід зберігати її в хмарі або на іншому холодному диску.

Політики захисту даних на рівні підприємства мають реалізовувати стратегію резервного копіювання 3-2-1, яка включає як точку відновлення, так і цільовий час відновлення (RPO/RTO). Стратегія повинна використовувати незмінне сховище, щоб дані можна було відновити, якщо інші резервні копії були змінені.

Організації також повинні переконатися, що багатофакторна автентифікація, ротація паролів і рольовий контроль доступу є частиною загальної стратегії. Якщо

зловмисники отримають доступ до систем зберігання даних, вони можуть видалити кластери, що містять незмінні резервні копії. Вони також можуть скорочувати або видаляти один раз, читати багато (WORM) позначення. Життєво важливо захистити бекдори систем зберігання за допомогою систем управління ідентифікацією та доступом (IAM), таких як багатофакторна автентифікація та брандмауери.

Більшість сучасних постачальників хмарних сховищ пропонують незмінні політики зберігання. Зберігання об'єктів добре підходить як незмінна ціль не лише через його високу довговічність, але й завдяки таким функціям, як блокування об'єктів, керування версіями та політики збереження даних. Сучасні постачальники програмного забезпечення для захисту даних розуміють, як використовувати ці функції, і впровадили їх у набір функцій свого продукту.

Ті самі постачальники програмного забезпечення для захисту даних можуть реалізувати незмінну стратегію для локального зберігання на додаток до хмари. Найкращі стратегії захисту даних використовують поєднання як локальних, так і хмарних технологій разом із незмінним сховищем.

Захист на майбутнє

Оскільки кіберризики продовжують розвиватися, компанії повинні надавати пріоритет цілісності даних. Незмінне сховище є життєво важливим компонентом інструментарію кібербезпеки організації, забезпечуючи стійкість, захист і душевний спокій.

Незмінне зберігання даних і надійне резервне копіювання забезпечують багаторівневий захист від кіберзагроз. Розставляючи пріоритети для цих методів, організації можуть впевнено рухатися в епоху цифрових технологій, використовуючи весь потенціал даних і одночасно захищаючись від ризиків.

У боротьбі з кіберзагрозами цілісність даних не підлягає обговоренню. Дуже важливо, щоб компанії впроваджували надійні стратегії даних зараз, щоб захистити їх у майбутньому». ***(Melyssa Banda. Why immutable data storage is key to cybersecurity strategy // Future US, Inc. (https://www.techradar.com/pro/why-immutable-data-storage-is-key-to-cybersecurity-strategy). 25.06.2024).***

***

«Оскільки підприємства та організації значною мірою покладаються на технології для ефективної роботи, потреба в надійних заходах кібербезпеки є першочерговою. Мережеві інженери відіграють важливу роль у захисті конфіденційних даних і забезпеченні безпеки мереж від кіберзагроз. У цій публікації в блозі ми розглянемо важливість кібербезпеки для мережевих інженерів і розглянемо, чому для захисту нашої цифрової інфраструктури важливо бути на крок попереду зловмисників.

Кібербезпека та її значення для мережевих інженерів

Ласкаво просимо на цифровий рубіж, де мережеві інженери є неоспіваними героями, які захищають наш онлайн-світ! У цю взаємопов'язану епоху кібербезпека – це не просто модне слово; це критичний щит від загроз, що постійно розвиваються. Отже, візьміть свій кібер-інструмент, коли ми заглибимося в життєво важливу роль мережевих інженерів у зміцненні нашої цифрової сфери від зловмисників.

Типи загроз кібербезпеці, з якими стикаються мережеві інженери

Коли мережеві інженери орієнтуються в цифровому ландшафті, вони стикаються з безліччю загроз кібербезпеці, які постійно розвиваються та адаптуються. Однією з поширених загроз є фішинг, коли зловмисники намагаються обманом змусити людей надати конфіденційну інформацію за допомогою електронних листів або повідомлень. Іншою поширеною небезпекою є зловмисне програмне забезпечення, яке може проникати в системи та сіяти хаос, викрадаючи дані або порушуючи роботу.

Мережеві інженери також стикаються з ризиком DDoS-атак, коли мережі переповнюються трафіком, що призводить до збою та стає недоступним. Крім того, програми-вимагачі становлять значну загрозу, оскільки шифрують дані, доки не буде сплачено викуп. Тактика соціальної інженерії, як-от створення приводів або цькування, спрямована на вразливі місця людини для отримання несанкціонованого доступу до мереж.

Щоб ефективно боротися з цими загрозами, мережеві інженери повинні залишатися пильними та проактивними у впровадженні надійних заходів безпеки.

Загальні заходи безпеки, реалізовані мережевими інженерами

Оскільки мережеві інженери відіграють важливу роль у захисті конфіденційних даних і забезпеченні цілісності мереж, вони впроваджують різні заходи безпеки для захисту від кіберзагроз. Однією з поширених практик є встановлення брандмауерів для моніторингу та контролю вхідного та вихідного мережевого трафіку. Вони діють як бар'єр між внутрішніми системами та зовнішніми загрозами, фільтруючи шкідливі пакети даних.

Мережні інженери також використовують методи шифрування для захисту каналів зв'язку, що ускладнює неавторизованим користувачам перехоплення або підробку конфіденційної інформації. Впровадження надійних протоколів автентифікації, таких як багатофакторна автентифікація, додає додатковий рівень безпеки, вимагаючи кількох форм перевірки перед наданням доступу.

Регулярне оновлення патчів програмного забезпечення та проведення оцінки вразливостей є ключовими кроками, які здійснюються мережевими інженерами для виявлення та усунення потенційних недоліків у системі. Крім того, впровадження систем виявлення вторгнень допомагає виявляти підозрілі дії в мережі, які можуть свідчити про злом або кібератаку.

Вплив витоку даних на підприємства та організації

Порушення даних може мати руйнівні наслідки для підприємств і організацій. Коли конфіденційна інформація потрапляє в чужі руки, це може призвести до фінансових втрат, шкоди репутації та юридичних наслідків.

Клієнти втрачають довіру до компаній, які не захищають їхні дані. Ця втрата довіри може призвести до падіння продажів і довгострокової шкоди лояльності до бренду.

Наслідки витоку даних часто включають дорогі розслідування, регулятивні штрафи та можливі судові позови. Ці фінансові навантаження можуть зруйнувати діяльність організації та перешкодити можливостям майбутнього зростання.

Крім того, час і ресурси, необхідні для відновлення після порушення, відволікають увагу від основної діяльності бізнесу. Ця зміна фокусу може вплинути на продуктивність і загальну ефективність компанії.

Як підвищити кібербезпеку як мережевий інженер?

Як мережевий інженер, посилення кібербезпеки має вирішальне значення для захисту конфіденційних даних і забезпечення цілісності мережі вашої організації. Один із способів підвищити кібербезпеку – це регулярне оновлення програмного забезпечення та мікропрограми на всіх мережевих пристроях. Це допомагає виправити будь-які вразливості, якими можуть скористатися кіберзагрози.

Застосування надійних заходів автентифікації, таких як багатофакторна автентифікація, додає додатковий рівень безпеки, крім паролів. Це значно знижує ризик несанкціонованого доступу до критично важливих систем або даних. Проведення регулярних перевірок і оцінок безпеки може допомогти завчасно виявити будь-які слабкі місця у вашій мережевій інфраструктурі.

Інвестування в надійні протоколи шифрування для передачі даних може запобігти перехопленню зловмисниками. Крім того, будьте в курсі останніх тенденцій кібербезпеки та відвідуйте навчальні сесії, щоб покращити свої знання та навички щодо ефективної боротьби з кіберзагрозами, що розвиваються.

Найкращі методи підтримки безпечної мережевої інфраструктури

Коли мова заходить про підтримку безпечної мережевої інфраструктури як мережевий інженер, є кілька найкращих практик, які можуть допомогти посилити заходи кібербезпеки. Регулярне оновлення програмного забезпечення та мікропрограми має вирішальне значення для усунення вразливостей і посилення захисту від потенційних загроз.

Впровадження надійних протоколів автентифікації, таких як багатофакторна автентифікація, додає додатковий рівень безпеки, вимагаючи більше, ніж просто пароль для доступу. Сегментація мережі також може обмежити вплив зломів шляхом ізоляції конфіденційних даних від інших частин мережі.

Регулярний моніторинг і аналіз шаблонів мережевого трафіку можуть допомогти виявити будь-яку підозрілу активність на ранніх стадіях, дозволяючи

своєчасно втручатися, щоб зменшити ризики. Проведення регулярних перевірок безпеки та тестування на проникнення допомагає виявити слабкі місця в системі до того, як ними зможуть скористатися кібер-зловмисники.

Навчання співробітників питанням кібербезпеки та передовим практикам має важливе значення для створення культури пильності в організації. Бути в курсі останніх тенденцій у кіберзагрозах і технологіях, що постійно розвиваються, є ключем до того, щоб залишатися попереду в умовах кібербезпеки, що постійно змінюється.

Безперервна освіта та сертифікація з кібербезпеки для мережевих інженерів

Безперервне навчання та сертифікація з кібербезпеки мають вирішальне значення для мережевих інженерів, щоб бути в курсі загроз і технологій, що постійно змінюються. Проходження курсів підвищення кваліфікації та отримання сертифікатів не тільки підвищує технічні навички, але й демонструє прагнення до професійного зростання.

Такі сертифікати, як Certified Information Systems Security Professional (CISSP) або Certified Ethical Hacker (CEH), підтверджують досвід у ключових сферах кібербезпеки, роблячи мережевих інженерів більш затребуваними в галузі. Крім того, постійне навчання на семінарах, вебінарах і конференціях дає цінну інформацію про нові тенденції та найкращі практики.

Вкладаючи час і зусилля в постійне навчання, мережеві інженери можуть завчасно адаптуватися до нових проблем безпеки. Ці ініціативи не тільки зміцнюють їхні власні можливості, але й сприяють створенню надійних механізмів захисту в організаціях від кіберзагроз.

Висновок

Підсумовуючи, неможливо переоцінити попит на потужні заходи кібербезпеки в сучасному взаємопов’язаному світі. Мережеві інженери відіграють вирішальну роль у забезпеченні безпеки та цілісності мереж передачі даних, тому їм важливо бути в курсі останніх досягнень і методів кібербезпеки. Впроваджуючи надійні протоколи безпеки та зберігаючи пильність щодо потенційних загроз, мережеві інженери можуть допомогти захистити організації від кібератак, які

можуть мати катастрофічні наслідки. Давайте пам’ятати, що кібербезпека – це не просто додаткова відповідальність, а життєво важлива для будь-якої успішної організації чи професіонала». ***(The Importance of Cybersecurity for Network Engineers // TechBullion (https://techbullion.com/the-importance-of-cybersecurity-for-network-engineers/). 27.06.2024).***

***

«Оскільки світ продовжує рухатися до хмари, кібербезпека стає все більш важливою для захисту конфіденційних даних і забезпечення цілісності та доступності систем.

Сучасна кібербезпека охоплює ряд методів, технологій і політик, призначених для захисту мереж, пристроїв і даних від кіберзагроз.

Ці небезпеки постійно розвиваються та стають дедалі складнішими, варіюються від зловмисного програмного забезпечення та програм-вимагачів до вдосконалених постійних загроз (APT) і експлойтів нульового дня. Це зробило для організацій життєво важливим постійну адаптацію та посилення захисту.

DFIR (цифрова криміналістика та реагування на інциденти) постає тут як важливе рішення завдяки його здатності методично працювати з кіберінцидентами та вирішувати їх, що, отже, зміцнює здатність організації протистояти мінливим загрозам.

Продовжуйте читати цю статтю, щоб дізнатися про значення DFIR у сучасній екосистемі кібербезпеки.

Розуміння цифрової криміналістики

У галузі кібербезпеки головна мета полягає в тому, щоб виявити та зрозуміти кіберінциденти, щоб допомогти організаціям ефективно реагувати та запобігати майбутнім атакам. Цифрова криміналістика передбачає збір, збереження, аналіз і представлення цифрових доказів. Його ключові компоненти:

1. Отримання та збереження даних: збір доказів із забезпеченням їх цілісності та захисту від підробки чи втрати

2. Аналіз та інтерпретація: перегляд зібраної інформації для розпізнавання закономірностей, реконструкції подій і отримання значущих ідей

3. Звітування та презентація: чітке та стисле документування результатів для використання в судових розглядах або внутрішніх розслідуваннях.

Загальні інструменти, які тут використовуються, включають EnCase та FTK (Forensic Toolkit), які допомагають у зборі, аналізі та звітності даних. Зображення (створення точних копій цифрового сховища) і вирізання даних (вилучення фрагментів даних із великих наборів даних) є ключовими методами для виявлення загроз і ефективного реагування на інциденти.

Взаємодія між цифровою криміналістикою та реагуванням на інциденти

Надійний план кібербезпеки повинен включати цифрову криміналістику та реагування на інциденти (DFIR). Цифрова криміналістика допомагає реагувати на випадки, пропонуючи структурований підхід до збору та дослідження цифрових доказів. Наприклад, розслідування доказів може виявити шкідливе програмне забезпечення, зламані облікові записи та несанкціоновані входи, що є життєво важливим для розуміння ситуації та врегулювання ситуації.

Під час реагування на інциденти цифрова криміналістика надає детальну інформацію, щоб висвітлити причину та послідовність подій у порушеннях. Ці дані життєво важливі для успішного стримування, усунення небезпеки та відновлення. Проведення судово-медичних звітів після інцидентів також може підвищити безпеку шляхом точного визначення вразливостей системи та пропонування дій для запобігання майбутнім порушенням.

Включення цифрової криміналістики в реагування на інциденти, по суті, дозволяє вам ретельно досліджувати інциденти, що призводить до швидшого відновлення, покращення заходів безпеки та підвищення стійкості до кіберзагроз. Це партнерство покращує вашу здатність виявляти, оцінювати та ретельно реагувати на кіберзагрози.

Виклики в DFIR

З DFIR пов’язано кілька проблем:

1. Технічні перешкоди

Це стосується керування шифруванням і методами, які використовують злочинці, щоб приховати свої дії. Ефективне керування великими обсягами даних також може бути обтяжливим і потребувати значного часу.

2. Правові та етичні перешкоди

Проблеми, пов’язані з законністю та етикою, виникають під час доступу до конфіденційних персональних даних для проведення судових розслідувань, що викликає занепокоєння щодо конфіденційності. Переконатися, що цифрові докази є юридично прийнятними в суді, важко і вимагає ретельного документування та обробки.

3. Операційні виклики

Вони передбачають ефективну координацію та спілкування всередині організацій, особливо під час інциденту. Наявність добре продуманого плану та готовності до інцидентів є важливими, але часто недостатніми, що призводить до неефективної реакції на кіберзагрози. Подолання цих перешкод має вирішальне значення для успіху зусиль DFIR.

Майбутнє DFIR у кібербезпеці

Нові тенденції та технології формують майбутнє DFIR у сфері кібербезпеки. Штучний інтелект і машинне навчання підвищують швидкість і ефективність виявлення загроз і реагування на них. Хмарні обчислення революціонізують процеси завдяки масштабованим можливостям зберігання та аналізу даних. Крім того, покращена координація з іншими секторами кібербезпеки, такими як розвідка про загрози та мережева безпека, призводить до більш узгодженого плану захисту.

Навчання та спеціалізація фахівців DFIR також продовжують розвиватися. Основні здібності включають використання інструментів цифрової криміналістики, керування реагуванням на інциденти та не відставати від мінливих загроз. Вони можуть розглянути можливість отримання таких сертифікатів, як CISSP (Сертифікований спеціаліст з безпеки інформаційних систем) і GIAC (Глобальна сертифікація забезпечення інформації).

Кінцева виноска

Цифрова криміналістика та реагування на інциденти мають вирішальне значення для кібербезпеки, ефективного вирішення та пом'якшення загроз, що робить їх життєво важливими для захисту цифрових середовищ. Організації повинні інвестувати в можливості DFIR і бути в курсі нових загроз і технологій, щоб забезпечити надійний і стійкий захист від кібербезпеки». ***(DFIR and its role in modern cybersecurity // Information Age (https://www.information-age.com/dfir-and-its-role-in-modern-cybersecurity-123510868/). 26.06.2024).***

***

«Кібербезпека є важливою частиною технологічної гігієни кожної організації. У деяких випадках стійка кібербезпека навіть є критично важливим елементом дотримання організацією правил і законів. Проте дотримання урядових вимог при дотриманні надійних заходів кібербезпеки та покращенні кіберстійкості може бути величезним викликом. На додаток до ландшафту кіберзагроз, що постійно змінюється, організації стикаються зі складною мережею пересічних і часто непослідовних нормативних актів щодо кібербезпеки на федеральному, штатному та місцевому рівнях. Складність цієї ситуації була визнана в Національній стратегії кібербезпеки президента Джо Байдена на 2023 рік, і в липні 2023 року Офіс Національного директора з кібербезпеки Білого дому (ONCD) опублікував запит на інформацію (RFI) щодо нормативної гармонізації. Регуляторна гармонізація спрямована на спрощення та узгодження суперечливих або дублюючих норм і полегшення адміністративного тягаря та витрат для регульованих установ. Зрештою, цей RFI отримав 86 унікальних відповіді з різних секторів.

Наш аналіз

Інститут R Street опублікував новий звіт «Розшифровка відповідей організацій на зусилля з гармонізації законодавства в галузі кібербезпеки США з наукою про дані», у якому аналізуються ці відповіді, щоб виявити важливі ідеї, які слід враховувати політикам, виконуючи важке завдання гармонізації регулювання кібербезпеки. Зокрема, наш звіт зосереджується на відповідях на RFI та пропонує

рекомендації, що мають відношення до уточнення намірів і надання дорожньої карти для майбутніх зусиль федерального уряду; він не пропонує та не аналізує рішення для гармонізації правил. Крім того, у нашому звіті зосереджено лише обсяг RFI щодо мінімальних вимог до кібербезпеки (тобто не вимог до реагування на інциденти чи інших дій, які необхідно вжити після кіберінциденту).

Наш аналіз відповідей на RFI виявив такі тенденції на сукупному рівні:

Бажання консолідувати вимоги: існувало загальне переконання, що консолідація вимог до звітності та аудиту під керівництвом меншої кількості регуляторних органів може значно зменшити тягар відповідності.

Перевага галузевим підходам: більшість респондентів висловили перевагу галузевим спільним нормам кібербезпеки, а не універсальному підходу. Це контрастує з очевидним наміром ONCD розробити базові заходи кібербезпеки в різних секторах.

Занепокоєння щодо приписів: респонденти підкреслили, що занадто приписи, засновані на контрольних списках, часто відволікають ресурси від усунення реальних загроз кібербезпеці та не встигають за кібернетичним ландшафтом, який швидко розвивається.

Неузгодженість у розумінні RFI: Здається, існує розбіжність між урядовим визначенням гармонізації та інтерпретаціями респондентів. Багато пропозицій не повністю узгоджувалися із запропонованою метою гармонізації, як зазначено в RFI.

Потім ми запропонували п’ять ключових рекомендацій на основі нашого аналізу відповідей на RFI та нашого розуміння регуляторного середовища:

Узгодити визначення та наміри: Уряд повинен роз’яснити значення та мету гармонізації, щоб уникнути непорозумінь і забезпечити узгодженість із зацікавленими сторонами.

Узгодьте пріоритети із зацікавленими сторонами: ONCD та інші агенції повинні продовжувати взаємодію з політиками, регуляторними органами, фахівцями галузі та експертами з кібербезпеки, щоб визначити наступні кроки та досягти консенсусу.

Залучайте менші організації: слід докладати зусиль, щоб врахувати перспективи менших організацій, яким може не вистачати ресурсів для реагування на RFI.

Спрощення регулятивної координації: розгляньте можливість призначення федерального органу для координації нормативних актів між установами та регуляторами, що потенційно посилить існуючі зусилля ONCD та Агентства з кібербезпеки та безпеки інфраструктури.

Проведіть подальший аналіз: шукайте додаткові цільові RFI та застосовуйте більш складні методи науки про дані щодо відповідей поточного RFI, щоб визначити глибше розуміння ключових сфер інтересу.

Аналіз ONCD та наступні кроки

Нещодавно ONCD опублікував свій власний підсумковий звіт про відповіді на RFI та надав свідчення Конгресу, у яких розглядалися деякі з тих самих проблем, які ми підняли. ONCD визнає широке занепокоєння з приводу відсутності нормативної гармонізації та взаємності в сфері кібербезпеки.

Зокрема, ONCD працює з партнерами над розбудовою пілотної схеми взаємності для підсектору критичної інфраструктури. Якщо він виявиться успішним, ця пілотна структура дасть цінну інформацію про ефективні регулятивні підходи до кібербезпеки, хоча це вимагатиме ширшої участі регуляторних органів, щоб однаково застосовуватись у всіх секторах.

На щастя, і Конгрес, і адміністрація Байдена визнають, що ця проблема впливає на бізнес усіх секторів і розмірів, впливаючи на результати кібербезпеки та конкурентоспроможність бізнесу. Ми сподіваємося, що підтримка Конгресу може допомогти об’єднати відповідні агентства для розробки міжгалузевої структури для гармонізації та взаємності базових вимог до кібербезпеки.

Шлях вперед для гармонізації

Шлях до регулятивної гармонізації кібербезпеки є складним і вимагає тонкого балансу між встановленням узгоджених базових показників і врахуванням галузевих потреб. Визнання ONCD цих викликів і зобов'язання щодо їх вирішення є позитивним кроком вперед. Їх запланована пілотна програма та заклик до

підтримки Конгресу демонструють проактивний підхід до цієї давньої проблеми. Щоб підтримати зусилля ONCD, урядові, галузеві та експерти з кібербезпеки повинні брати участь у постійному діалозі, який зосереджується на ефективності, результативності та адаптивності будь-якої запропонованої нормативної бази кібербезпеки. Крім того, важливими будуть зусилля уряду щодо покращення взаємності та сприяння співпраці. Коротше кажучи, розробники політики, включно з ONCD, повинні надавати пріоритет нормам, які сприяють зменшенню ризиків кібербезпеки та покращують стійкість, зберігаючи при цьому прозорість і уникаючи надмірних дій. Будь-які кроки, зроблені для вирішення цієї «важкої проблеми», дають надію на створення більш спрощеного та ефективного нормативно-правового середовища кібербезпеки, яке підвищує національну стійкість, одночасно враховуючи проблеми, пов'язані з конкретними галузями». ***(Amy Chang, Haiman Wong. Navigating the Complexities of U.S. Cybersecurity Regulation Harmonization // R Street Institute (https://www.rstreet.org/commentary/navigating-the-complexities-of-u-s-cybersecurity-regulation-harmonization/). 27.06.2024).***

***

«Відповідно до звіту Rockwell Automation, заснованого на результатах глобального опитування, виробники автомобілів заявили, що ризик кібербезпеки є їх основною зовнішньою перешкодою у 2024 році.

Згідно зі звітом, 35% респондентів назвали кібербезпеку головною проблемою.

«Кібербезпека викликає ще більше занепокоєння в автомобільній промисловості, ніж в інших галузях: респонденти в нашому загальногалузевому звіті поставили її нижче, під № 3 у списку зовнішнього тиску», — йдеться у звіті. «Недавні резонансні витоки даних і поширення підключення до Інтернету в автомобільній галузі, можливо, сприяли тому, що кібербезпека підскочила з дев'ятого найбільшого ризику минулого року на перше місце цього року».

Респонденти сказали, що енергетична криза та зростання цін на енергоносії є другою за величиною перешкодою, інфляція — третьою, збої в ланцюзі поставок — четвертою, а робоча сила — п’ятою.

Автомобільна промисловість також перевершила інші галузі за інвестиціями в технології, йдеться у звіті. Витрати у 2024 році становили 31% операційних бюджетів OEM, що на 35% більше, ніж у минулому році, йдеться у звіті.

«Впровадження інтелектуальних технологій і ШІ розглядається виробниками як найкращий спосіб пом’якшити як зовнішні, так і внутрішні ризики», — йдеться у звіті. «Автомобільні виробники отримують найбільшу рентабельність інвестицій завдяки інвестиціям, які створюють покращене підключення та ефективність заводу, наприклад 5G, системи управління виробництвом (MES) і програмовані логічні контролери (PLC)».

Дев’яносто сім відсотків виробників автомобілів використовують або оцінюють технології інтелектуального виробництва, йдеться у звіті. Відсоток збільшився з 85% минулого року.

У звіті йдеться, що на виробництві відбувається найбільше технологічних оновлень. Це включає оновлення датчиків і приладів, підключених пристроїв і промислових комп’ютерів.

«Впровадження промислового метавсесвіту в автомобільному секторі, схоже, випередить інші галузі», — йдеться у звіті. «Хоча ця технологія стоїть у нижній частині таблиці найсучасніших інструментів, у які вже інвестували всі сектори в нашому опитуванні, це одна з найбільших респондентів автомобільної галузі, у яку планують інвестувати протягом року».

Сорок шість відсотків автомобільних респондентів заявили, що планують інвестувати в промисловий метавсесвіт наступного року.

Компанія «Делойт» визначає «промисловий метавсесвіт» як конвергенцію окремих технологій, які за умови використання в поєднанні можуть створити захоплююче тривимірне віртуальне або віртуальне/фізичне промислове середовище.

Генеративний штучний інтелект або причинно-наслідковий штучний інтелект разом із носимими пристроями та роботами були іншими технологічними досягненнями, які зайняли високе місце в автомобільній промисловості, йдеться у звіті.

Завдяки вдосконаленню технологій і підключень не лише на заводі, але й у дизайні транспортних засобів, цілком зрозуміло, що кібербезпека є головною проблемою для OEM-виробників. Це також не нова проблема.

Центр обміну та аналізу автомобільної інформації (Auto-ISAC) був запущений у 2015 році державними зацікавленими сторонами та автовиробниками, згідно з даними Alliance for Automotive Innovation. Того ж року було створено найкращі практики автомобільної кібербезпеки.

У 2016 році Національне управління безпеки дорожнього руху (NHTSA) випустило посібник із найкращих практик автомобільної кібербезпеки.

У 2021 році ISO та SAE завершили розробку глобального стандарту кібербезпеки транспортних засобів.

«Ця нова багаторічна робота об’єднала понад 100 експертів із 17 країн, охоплюючи різноманітну групу з понад 80 організацій державного та приватного секторів», — повідомляють Auto Innovators. «ISO/SAE 21434 надає промисловості надійні процеси та процедури для управління ризиками кібербезпеки протягом усього життєвого циклу транспортного засобу – від проектування до виведення з експлуатації».

Кібербезпека – це те, що зміниться разом зі зміною технологій, йдеться в документі Auto Innovators.

«Залишатися спритним і адаптивним перед обличчям швидкого, динамічного середовища загроз кібербезпеці є першорядним для автомобільної промисловості», – йдеться в документі. «Зростаюча цифрова та зв’язана екосистема створює кілька складнощів і ризиків кібербезпеки, які більше не обмежуються самим транспортним засобом і не контролюються виключно автомобільною промисловістю. Взаємовідносини між транспортними засобами, підключеною інфраструктурою, продуктами та послугами, а також із споживачами сприяють

розвитку автомобільних інновацій, тому кібербезпека має залишатися в основі. Від цього залежить довіра споживачів і майбутнє нашого чистішого, безпечнішого та розумнішого транспорту». ***(Teresa Moss. Cybersecurity top 2024 concern for auto manufacturers, report says // DRIVEN COMMUNICATIONS Inc. (https://www.repairerdrivennews.com/2024/06/25/cybersecurity-top-2024-concern-for-auto-manufacturers-report-says/). 25.04.2024).***

***

«Занепокоєння щодо кібератак зростає за останні 20 років. Перша атака була здійснена на комунальне підприємство в Квінсленді (Австралія) у 2000 році, тоді як останні атаки вразили водопостачання Ізраїлю в 2020 році та станцію очищення води у Флориді в 2021 році. Нам достатньо ввести термін «кібербезпека» в Google, щоб побачити важливість цього явища.

Нові технологічні тенденції у водному циклі, такі як автоматизація, системи раннього попередження та інтелектуальне вимірювання, приносять значні переваги та інновації у водний сектор, але також відкривають нові вектори атак для кіберзлочинців. Тому, як зазначено у звіті Idrica Water Technology Trends 2024, комунальні підприємства витрачають більше часу та зусиль на зміцнення та розширення своїх ініціатив у сфері кібербезпеки.

Захід для покращення кібербезпеки в Європі

У 2023 році в Іспанії було зареєстровано 107 777 кібератак, що на 94% більше, ніж у попередньому році. Такі дані взяті з річного звіту про національну безпеку за 2023 рік, складеного Департаментом національної безпеки.

Згідно зі звітом, той факт, що зловмисники володіють «більшими технічними та операційними можливостями», призвів до збільшення частоти, витонченості та серйозності кібератак. Ця ситуація погіршується через «високу залежність суспільства від інформаційно-комунікаційних технологій», як зазначено у звіті. Дійсно, другою найбільшою загрозою для Іспанії сьогодні є вразливість кіберпростору, поступаючись лише кампаніям дезінформації, хоча вона має потенційно більший вплив.

З цієї причини, за словами Бегонья Гонсалеса, керівника відділу інформаційної безпеки компанії Idrica, «оператори водопостачання повинні розробити низку стратегій, спрямованих на посилення їх кібербезпеки». Експерт виділяє шість:

Оцінка ризиків: необхідно проводити регулярні оцінки ризиків для виявлення вразливостей і потенційних загроз.

Постійний моніторинг: системи постійного моніторингу мають бути запроваджені для виявлення підозрілої активності в реальному часі.

Навчання та підвищення обізнаності: співробітники повинні пройти навчання щодо найкращих практик кібербезпеки, щоб створити культуру безпеки.

Резервування та стійкість: резервні системи та плани аварійного відновлення повинні бути створені для забезпечення безперервності роботи.

Оновлення та виправлення: системи мають бути оновлені з останніми виправленнями безпеки.

Шифрування та автентифікація: для захисту конфіденційної інформації необхідно розгорнути шифрування даних і надійну автентифікацію.

У цьому сценарії «уряди та інші зацікавлені сторони посилюють законодавство, щоб пом'якшити ситуацію», - підкреслив Гонсалес. Такі нормативні акти, як ACN в Італії, щодо хмарних послуг; ENS в Іспанії, з інформаційної безпеки; ANSSI у Франції, зосереджена на сертифікації продукції; і BIO в Нідерландах, з управління інформаційними системами, є лише кількома прикладами.

З цього приводу експерт Idrica каже: європейські країни повинні імплементувати директиву NIS2, яка передбачає правові заходи для просування кібербезпеки в Європейському Союзі, забезпечуючи:

Держави-члени добре оснащені для реагування на будь-які інциденти, які можуть статися.

Створення Групи співпраці для забезпечення співпраці між державами-членами, а також обміну інформацією між ними.

Сприяння розвитку культури безпеки в усіх основних секторах (Європейський Союз).

Idrica, компанія, заснована Fomento Urbano de Castellón, SA, усвідомлює важливість впровадження відповідних організаційних, технічних і операційних заходів для управління ризиками безпеки. Таким чином, він сертифікував інформаційну систему, яка керує проектуванням, розробкою, впровадженням, підтримкою та обслуговуванням платформи GoAigua відповідно до ISO 27001 та Схеми національної безпеки Іспанії (ENS).

Крім того, у квітні 2024 року було опубліковано посібник, щоб усім компаніям, сертифікованим ENS, було легше виконувати вимоги NIS2. Логічно, відповідність директиві NIS1 не означає відповідності новішій NIS2.

Цей посібник містить дорожню карту для навігації між обома нормативними актами, щоб переконатися, що компанії дотримуються нової директиви. Нарешті, у 2024 році Idrica почала впроваджувати сертифікацію кібербезпеки SOC2». ***(Service and Organization Controls), орієнтовану на американський ринок. (Cybersecurity: A Must for European Water Utilities // Automation.com (https://www.automation.com/en-us/articles/june-2024/cybersecurity-must-european-water-utilities). 26.06.2024).***

***

Сполучені Штати Америки та Канада

«Дії Конгресу необхідні для впорядкування регуляторного ландшафту кібербезпеки, заявив представник Білого дому в середу під час слухань, на яких законодавці і свідки виступили проти того, що, за їхніми словами, є надто складною клаптиковою тканиною кіберправил, яка перешкоджає здатності приватного сектору протистояти загрозам.

Слухання в середу в Сенатському комітеті з питань внутрішньої безпеки і урядових справ, що відбулися наступного дня після того, як Офіс національного кібердиректора опублікував звіт у відповідь на запит про гармонізацію нормативно-правового регулювання кібербезпеки, продемонстрували відносно

широку згоду між членами комітету і федеральними чиновниками щодо необхідності законодавчого вирішення проблеми.

Хоча таке рішення ще не було представлено, законопроект голови комітету сенатора Гері Пітерса (штат Мічиган) неодноразово згадувався під час слухань як спосіб вирішити проблему впорядкування. Проект закону Пітерса про гармонізацію регулювання кібербезпеки, отриманий The Record, передбачає створення міжвідомчого комітету для координації кіберрегулювання.

Гармонізація регулювання «є проблемою, яка існує десятиліттями, і тенденція загалом спрямована до більшої фрагментації, а не до більшої гармонізації», - сказав Ніколас Лейзерсон, помічник національного кібердиректора з питань кіберполітики та кіберпрограм. «Це проблема, яка вимагає лідерства з боку ONCD і Конгресу, поінформованого приватним сектором».

Лейзерсон заявив, що адміністрація Байдена підтримує законопроект Пітерса, назвавши його «таким, що відповідає поглядам», якими ONCD раніше ділився з комітетом. Він додав, що законопроект «дозволить ONCD краще виконувати нашу місію, залучаючи незалежні регуляторні комісії до процесу вироблення політики разом з міжвідомчими органами».

Нормотворчість незалежних відомств викликала багато гніву з боку приватного сектору, особливо у випадку з правилами Комісії з цінних паперів і бірж щодо розкриття інформації про інциденти в сфері кібербезпеки.

У своїй вступній промові Пітерс зазначив, що за останні чотири роки федеральні регулятори прийняли 48 правил щодо стандартів кібербезпеки. Хоча він сказав, що регулятивний поштовх «приходить з хорошого місця», за відсутності вищого рівня координації «немає способу гарантувати, що ці вказівки не збігаються, не дублюють або просто не суперечать одна одній», що призводить до результатів, які «часто заплутані та неефективні».

Сенатор Джеймс Ленкфорд, штат Оклахома, повторив занепокоєння Пітерса, особливо щодо незалежних агентств, які «все ще потребують додаткового контролю».

«Є незалежні агентства, які відчувають себе незалежними від усіх. Вони не є незалежними від усіх», – сказав Ланкфорд. «Існують певні межі, які повинні бути там, коли вони створюють нові правила, щоб вони не були абсолютно незалежною четвертою гілкою влади».

ONCD «обмежений» у своїх можливостях залучати незалежні регуляторні комісії, сказав Лейзерсон, підкреслюючи необхідність участі Конгресу. Залучення всіх відповідних сторін до переговорів має першочергове значення, додав він, що стало особливо очевидним, коли ONCD проаналізувала понад 2000 сторінок коментарів у відповідь на свій запит на інформацію. У звіті, опублікованому в середу, ONCD намагався узагальнити 86 унікальних відповідей на цей запит.

Наприклад, бізнес-круглий стіл зазначив, що обтяжливі та часто суперечливі норми «вимагають від компаній виділяти більше ресурсів на виконання вимог технічної відповідності без покращення результатів кібербезпеки». Інститут банківської політики зазначив, що опитування великих фінансових установ показало, що керівники відділу інформаційної безпеки або аналогічні старші кіберкерівники витрачають від 30% до 50% свого часу на питання дотримання нормативних вимог. А Національна асоціація оборонної промисловості заявила, що нормативні «невідповідності» створюють «бар'єри для входу» для малого та середнього бізнесу.

«Коли у вас є кілька режимів звітності з кількома вимогами, які не однакові, ви витрачаєте багато часу на оформлення документів, а не на роботу, тому що вам потрібно відповідати вимогам обох цих рамок, яким ви підпорядковуєтесь», сказав Девід Хінчман, директор відділу інформаційних технологій та кібербезпеки в Управлінні підзвітності уряду, який опублікував відповідний звіт у середу про кібергармонізацію.

Відсутність федеральної кібергармонізації також негативно впливає на здатність американських компаній конкурувати на міжнародному рівні, сказав Лейзерсон, зазначивши, що європейським компаніям потрібно лише турбуватися про роботу в рамках ЄС. І в той час, коли Росія та Китай дедалі сміливіше атакують

критично важливу інфраструктуру США, оптимізація стандартів стає ще більш критичною.

За словами Лейзерсона, створення належної структури мало б показати секторам, «як ви повинні підходити до захисту ваших корпоративних IT-систем, на що націлені зловмисники, щоб отримати початковий доступ для встановлення цих плацдармів».

У електронному листі до CyberScoop Емі Чанг, старший науковий співробітник з питань кібербезпеки та нових загроз правого R Street Institute, сказала, що на слуханнях і в звіті ONCD з'явилося «більш узгоджене повідомлення» про гармонізацію, ніж те, що було повідомлено раніше. приватний сектор.

Забігаючи вперед, Чанг сказав, що ONCD і, певною мірою, Конгрес «повинні залучити додаткову підтримку з боку регуляторів, щоб підтримати гармонізацію, і створити узгодженість пріоритетів і очікувань із зацікавленими сторонами, такими як політики, регуляторні органи, професіонали галузі та експертів з кібербезпеки». ***(Matt Bracken. Congress needs to step in on cybersecurity harmonization, White House official says // CyberScoop (https://cyberscoop.com/congress-cybersecurity-harmonization-oncd-report/?utm_source=flipboard&utm_content=other). 05.06.2024).***

***

«У Сполучених Штатах нинішні фахівці з кібербезпеки можуть задовольнити лише 85% попиту роботодавців, залишаючи майже півмільйона (469 930) вакансій. Про це йдеться в CyberSeek, спільному проекті між організацією технічної сертифікації CompTIA, аналітиком ринку праці Lightcast і NICE, федеральною програмою США, спрямованою на кібербезпеку.

NICE (раніше абревіатура від National Initiative for Cybersecurity Education), яка входить до складу Національного інституту стандартів і технологій, надала грант компаніям CompTIA і Lightcast на розробку «теплової карти» кар'єри в галузі кібербезпеки, яка стала CyberSeek. Відвідувачі можуть побачити різницю між наявними працівниками з кібербезпеки та попитом роботодавців у відсотках,

переходячи до мегаполісів, щоб побачити, де робочих місць більше. Наприклад, якщо ви шукали роботу в Каліфорнії, вам краще було б перевірити Сан-Дієго, де задовольняється лише 87% попиту на робочі місця, аніж Фресно, де співвідношення змінюється на інший бік, оскільки попит на робочі місця задовольняється на 120%.

Інтерактивна карта CyberSeek дає цікаву підказку про те, чому досвідчені професіонали можуть відчувати себе непоміченими менеджерами з найму. Унизу сторінки ви можете порівняти кількість професіоналів, які мають різні сертифікати, з тим, скільки списків вакансій запитують ці сертифікати – і вони не дуже збігаються. Наприклад, найпопулярнішою сертифікацією серед практиків є CompTIA Security+; Цей сертифікат мають 265 992 людини. Однак лише 69 906 списків вакансій вимагають такого сертифікату. З іншого боку, 47 230 оголошень запитують Сертифікованого аудитора інформаційних систем (CISA), а 36 162 запитують Сертифікованого менеджера з інформаційної безпеки (CISM). Серед потенційних претендентів 35 812 CISA та 20 300 CISM, що недостатньо для задоволення потреб роботодавців. Узгодження навчання та сертифікації з тим, чого насправді шукають менеджери з найму, може допомогти вирішити проблеми найму та підбору персоналу». ***(Cybersecurity Job Hunting May Come Down to Certifications // Informa PLC (https://www.darkreading.com/cybersecurity-careers/cybersecurity-jobs-gap-may-come-down-to-certifications-gap?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 07.06.2024).***

***

«На горизонті значні зміни у дотриманні вимог кібербезпеки, і підприємствам потрібно підготуватися. Починаючи з 2024 року, організації зіткнуться з новими вимогами повідомляти федеральному уряду про інциденти кібербезпеки та платежі за програми-вимагачі. Ця зміна пов’язана з публікацією Агентства інфраструктури кібербезпеки та безпеки (CISA) Міністерства внутрішньої безпеки США (DHS) 4 квітня 2024 року Повідомлення про

запропоновану нормотворчу діяльність (NPRM). Це повідомлення спрямоване на виконання Закону про звітність про кіберінциденти для критичної інфраструктури. 2022 (CIRCIA). По суті, це означає, що «охоплені організації» повинні повідомляти CISA про конкретні кіберінциденти та виплати викупу протягом визначених часових рамок.

Фон

Ще в березні 2022 року президент Джо Байден підписав закон CIRCIA. Це був великий крок до покращення кібербезпеки Америки. Закон вимагає, щоб CISA створювала та вводила в дію правила, які зобов'язують суб'єктів звітування про кіберінциденти та виплату викупу. Мета полягає в тому, щоб допомогти CISA швидко допомогти жертвам, проаналізувати тенденції в різних секторах і поділитися важливою інформацією з захисниками мережі, щоб запобігти іншим потенційним атакам.

Запропоноване правило відкрито для громадських коментарів до 3 липня 2024 року. Після цього періоду CISA має 18 місяців, щоб завершити це правило, з очікуваною датою впровадження приблизно 4 жовтня 2025 року. Правило має набути чинності на початку 2026 року. Цей документ передбачає огляд NPRM, висвітлюючи його ключові моменти з детального повідомлення Федерального реєстру.

Ініціативи звітування про кіберінциденти

CIRCIA містить кілька ключових вимог щодо обов'язкового звітування про кіберінциденти:

Вимоги щодо звітування про кіберінциденти – CIRCIA наказує CISA розробити правила, які вимагають від охоплених організацій повідомляти про будь-які кіберінциденти протягом 72 годин з моменту, коли організація обґрунтовано вважає, що інцидент стався.

Обмін федеральними звітами про інциденти. Будь- який федеральний орган, який отримує звіт про кіберінцидент після дати набрання чинності остаточним правилом, повинен надати цей звіт CISA протягом 24 годин. CISA також має

надати інформацію, отриману в рамках CIRCIA, доступною певним федеральним агентствам протягом того ж терміну.

Рада зі звітування про кіберінциденти – Міністерство внутрішньої безпеки (DHS) має створити та очолити міжурядову Раду зі звітування про кіберінциденти для координації, усунення конфліктів та узгодження федеральних вимог щодо звітування про інциденти.

Ініціативи програм-вимагачів

CIRCIA також санкціонує або наказує кілька ініціатив для боротьби з програмами-вимагачами:

Вимоги щодо звітування про виплату викупу – CISA має розробити правила, які вимагатимуть від охоплених організацій звітувати CISA протягом 24 годин після здійснення будь-яких виплат викупу через атаку програм-вимагачів. Ці звіти мають надаватися федеральним агентствам, як і звіти про кіберінциденти.

Пілотна програма попередження про вразливість програм-вимагачів – CISA має створити пілотну програму для виявлення систем, уразливих до атак програм-вимагачів, і може повідомити власників цих систем.

Об’єднана робоча група з програм-вимагачів – CISA оголосила про запуск Об’єднаної робочої групи з програм-вимагачів, щоб на основі існуючих зусиль координувати загальнонаціональну кампанію проти атак програм-вимагачів. Ця цільова група тісно співпрацюватиме з Федеральним бюро розслідувань і Офісом національного кібердиректора.

Сфера застосування

Постанова спрямована на багатьох «охоплених суб’єктів» у секторах критичної інфраструктури. CISA пояснює, що «охоплені суб’єкти» охоплюють більше, ніж просто власників і операторів систем і активів критичної інфраструктури. Суб’єкти, які активно беруть участь у цих секторах, можуть вважатися «в секторі», навіть якщо вони самі не є критичною інфраструктурою. Організаціям, які не впевнені щодо свого статусу, рекомендується звертатися до CISA.

Сектори критичної інфраструктури

Інтерпретація CISA включає суб'єкти в одному з 16 секторів, визначених Президентською політичною директивою 21 (PPD 21). Ці сектори включають хімічну промисловість, комерційні об'єкти, зв'язок, критичне виробництво, дамби, оборонно-промислову базу, екстрені служби, енергетику, фінансові послуги, продовольство та сільське господарство, державні установи, охорону здоров'я та громадське здоров'я, інформаційні технології, ядерні реактори, матеріали та відходи, Транспортні системи, системи водопостачання та водовідведення.

Суб'єкти, на які поширюється дія

CISA має на меті охопити малі підприємства, які володіють і керують критично важливою інфраструктурою, встановлюючи додаткові галузеві критерії. Запропоноване правило стосується організацій, що належать до однієї з двох категорій:

- Суб'єкти господарювання, що працюють у секторах критичної інфраструктури, крім малого бізнесу
- Суб'єкти в секторах критичної інфраструктури, які відповідають галузевим критеріям, навіть якщо вони є малими підприємствами

Критерії на основі розміру

Критерії на основі розміру використовують стандарти малого бізнесу (SBA), які відрізняються залежно від галузі та базуються на річному доході та кількості працівників. Суб'єкти у секторах критичної інфраструктури, які перевищують ці порогові значення, є «охопленими суб'єктами». Стандарти SBA періодично оновлюються, тому організації повинні бути в курсі поточних порогових значень, застосовних до їх галузі.

Секторальні критерії

Критерії, засновані на секторі, націлені на основні суб'єкти в секторі, незалежно від розміру, на основі потенційних наслідків збою. Запропоноване правило визначає конкретні критерії для майже всіх 16 секторів критичної інфраструктури. Наприклад, у секторі інформаційних технологій критерії включають:

- Організації, що надають IT-послуги для федерального уряду
- Організації, що розробляють, ліцензують або обслуговують критичне програмне забезпечення
- Виробники, постачальники або інтегратори апаратного чи програмного забезпечення операційних технологій
- Суб'єкти, задіяні в інформаційно-комунікаційних технологіях, пов'язаних з виборами

У сфері охорони здоров'я та охорони здоров'я критерії включають:

- Лікарні на 100 і більше ліжок
- Лікарні критичного доступу
- Виробники певних ліків або медичних приладів
- Висвітлені кіберінциденти

Організації, на яких поширюється дія, повинні повідомляти про «захищені кіберінциденти», які включають значну втрату конфіденційності, цілісності або доступності інформаційної системи, серйозний вплив на безпеку та стійкість операційної системи, порушення ділових або промислових операцій і несанкціонований доступ через треті сторони компроміси постачальників послуг або порушення ланцюга постачання.

Значні інциденти

Це визначення охоплює значні кіберінциденти незалежно від їх причини, наприклад компрометацію сторонніми засобами, атаки типу «відмова в обслуговуванні» та вразливості у відкритому коді. Однак загрози або дії, що відповідають запитам власника/оператора, не включені. Значні інциденти включають шифрування основних систем, експлуатацію, що спричиняє тривалий простой, і атаки програм-вимагачів на промислові системи керування.

Вимоги до звітності

Підприємства, на яких поширюється дія, повинні повідомляти CISA про кіберінциденти протягом 72 годин після обґрунтованих припущень, що інцидент стався. Звіти необхідно подавати через веб-форму «CIRCIA Incident Reporting

Form» на веб-сайті CISA та містити детальну інформацію про інцидент і виплату викупу.

Типи звітів і терміни

Звіти про висвітлені кіберінциденти протягом 72 годин після виявлення інциденту

Звіти про виплату викупу внаслідок атаки програм-вимагачів протягом 24 годин після оплати

Спільні закриті кіберінциденти та звіти про виплату викупу протягом 72 годин для випадків виплати викупу

Додаткові звіти протягом 24 годин у разі появи нової інформації або додаткових платежів

Організації повинні зберігати дані, які використовуються для звітів, щонайменше два роки. Вони можуть уповноважити третю сторону подавати звіти від їх імені, але залишаються відповідальними за дотримання вимог.

Винятки для подібного звітування

Охоплені організації можуть бути звільнені від звітності CIRCIA, якщо вони вже звітували в іншому федеральному агентстві, за умови наявності угоди між CISA та цим агентством. Ця угода має забезпечувати суттєву схожість вимог до звітності, а агентство має ділитися інформацією з CISA. Федеральні агентства, які підпорядковуються CISA згідно з Федеральним законом про модернізацію інформаційної безпеки (FISMA), звільняються від звітності CIRCIA.

Ці угоди ще знаходяться в стадії розробки. Суб’єкти, які звітують перед іншими федеральними агентствами, повинні бути в курсі свого прогресу, щоб зрозуміти, як вони вплинуть на свої зобов’язання щодо звітності відповідно до CIRCIA.

Виконання та покарання

Директор CISA може зробити запит на інформацію (RFI), якщо організація не подає необхідний звіт. Невиконання вимог може призвести до цивільного позову або ухвали суду, включно з такими покараннями, як позбавлення права та

обмеження майбутніх державних контрактів. Неправдиві твердження у звітах можуть призвести до кримінальної відповідальності.

Захист інформації

CIRCIA захищає звіти та відповіді на RFI, включаючи імунітет від примусових дій, заснованих виключно на поданні звітів, і захист від юридичного виявлення та використання в судочинстві. Звіти звільняються від розкриття Закону про свободу інформації (FOIA), і організації можуть позначати звіти як «комерційну, фінансову та конфіденційну інформацію». Інформація може бути передана федеральним агентствам для цілей кібербезпеки або конкретних загроз.

Бізнес на винос

Хоча це правило набуде чинності лише наприкінці 2025 року, компаніям слід почати готуватися вже зараз. Організаціям слід переглянути запропоноване правило, щоб визначити, чи відповідають вони вимогам до звітності та чи розуміють вони вимоги до звітності, а потім відповідно відкоригувати свої програми безпеки та плани реагування на інциденти. Створення таблиці нормативних повідомлень може допомогти відстежувати різні зобов'язання щодо звітування про інциденти. Профілактичні заходи та потенційні офіційні коментарі до запропонованого правила можуть допомогти досягти відповідності після завершення розробки правил.

Ці кроки призначені для керівництва компаніями при підготовці до CIRCIA, хоча кожна компанія повинна оцінити власні потреби та процедури в рамках свого конкретного операційного, бізнесового та нормативного контексту». ***(Sinan Pismisoglu. Mandatory Cybersecurity Incident Reporting: The Dawn of a New Era for Businesses // Bradley Arant Boult Cummings LLP (https://www.onlineandonpoint.com/2024/06/mandatory-cybersecurity-incident-reporting-the-dawn-of-a-new-era-for-businesses/#page=1). 03.06.2024).***

***

«21 травня 2024 року директор Відділу фінансів корпорацій Комісії з цінних паперів і бірж США (SEC) Ерік Гердіг опублікував заяву, в якій

уточнював, що пункт 1.05 форми 8-K слід використовувати лише для розкриття суттєвих інцидентів кібербезпеки. Вирішуючи добровільно розкрити інформацію про інцидент кібербезпеки, який компанія визнала несуттєвим або щодо якого вона ще не визначила суттєвість, компанія повинна використовувати інший пункт форми 8-K, наприклад пункт 8.01.

У сучасному цифровому середовищі інциденти з кібербезпекою, як-от атаки програм-вимагачів, стають все більш поширеними та можуть суттєво вплинути на публічні компанії. Щоб підвищити прозорість і захистити інвесторів, у липні 2023 року SEC прийняла правила розкриття інформації про кібербезпеку, які вимагають, серед іншого, щоб публічні компанії розкривали інформацію про суттєві інциденти кібербезпеки згідно з пунктом 1.05 форми 8-K. Відколи ці правила набули чинності в грудні 2023 року, було подано кілька 8-K, які розкривають інциденти кібербезпеки, подані відповідно до пункту 1.05, і лише незначна меншість (приблизно 10%) заявили, що інцидент був суттєвим.

Одним із факторів, який може вплинути на кількість 8-K, які розкривають інциденти кібербезпеки, подані згідно з пунктом 1.05, не вказуючи, що інцидент є суттєвим, може бути скарга SEC, подана проти SolarWinds Corporation у листопаді 2023 року. У скарзі також зазначено ім’я головного інформаційного директора компанії. Офіцер безпеки як особистість у дії. Така агресивна позиція SEC могла сприяти тому, що компанії розкривали інформацію про несуттєві інциденти через страх бути підданими примусовим діям, пов’язаним із недостатнім розкриттям інформації.

Згідно із заявою, «інвесторів може ввести в оману, якщо компанії розкриють або несуттєві інциденти кібербезпеки, або інциденти, для яких визначення суттєвості ще не було зроблено відповідно до пункту 1.05». Відповідно, «це розрізнення між формою 8-K, поданою згідно з пунктом 1.05 щодо інциденту кібербезпеки, визначеного компанією як істотний, і формою 8-K, добровільно поданою відповідно до пункту 8.01 для інших інцидентів кібербезпеки, дозволить інвесторам легше розрізняти між два та приймати кращі рішення про інвестиції та голосування щодо суттєвих інцидентів кібербезпеки».

Застосовуючи такий підхід, SEC повідомила, що вона не намагається перешкоджати добровільному розголошенню інцидентів кібербезпеки. Згідно з SEC, це добровільне розкриття інформації згідно з пунктом 8.01 є цінним і забезпечує прозорість, але його слід чітко відрізняти від розкриття інформації про суттєві інциденти кібербезпеки, щоб інвестори могли приділяти суттєвим інцидентам відповідний рівень уваги.

Крім того, у заяві повторюється, що при оцінці суттєвості компанії повинні враховувати кількісні та якісні фактори. Компанії повинні враховувати можливу репутаційну шкоду, вплив на відносини з клієнтами чи постачальниками або конкурентоспроможність компанії, а також можливість судового розгляду чи розслідування регуляторних органів. У заяві також зазначається, що можуть бути настільки серйозні інциденти кібербезпеки, що компанія може визначити, що це суттєвий інцидент, перш ніж зрозуміти його вплив. У такому випадку Комісія з цінних паперів та цінних паперів наказує, що інцидент має бути подано відповідно до пункту 1.05 із достатньою інформацією, щоб інвестори могли зрозуміти природу, масштаб і час інциденту, а розкриття має містити заяву про те, що компанія ще не визначила вплив інциденту. Компанія повинна внести зміни до форми 8-K після визначення впливу». ***(Timothy Howard, Megan M. Kayo and David Benger. New SEC Guidance for Disclosing Cybersecurity Incidents // Freshfields Bruckhaus Deringer (https://blog.freshfields.us/post/102j8x2/new-sec-guidance-for-disclosing-cybersecurity-incidents#page=1). 03.06.2024).***

***

«15 травня 2024 року Департамент охорони здоров'я штату Нью-Йорк (NYSDOH) опублікував зміни до запропонованих правил кібербезпеки лікарень, які він вперше опублікував у листопаді 2023 року. Раніше ми підсумували спочатку опубліковані запропоновані нормативні акти («Початкові запропоновані нормативні акти») у сповіщенні клієнта за листопад 2023 року. Незважаючи на те, що переглянута версія запропонованих нормативних актів («Переглянуті запропоновані нормативні акти») все ще перебуває в статусі

«запропонованих» і ще не завершена, перегляди дають уявлення про реакцію галузі на початкові запропоновані нормативні акти та відповіді NYSDOH.

Більшість вимог Початкового запропонованого регламенту було збережено у Переглянутому запропонованому регламенті з деякими змінами. Нижче наведено основні вимоги переглянутих запропонованих правил:

Вимоги, що застосовуються до непублічної інформації. Переглянуті запропоновані правила встановлюватимуть вимоги кібербезпеки щодо «непублічної інформації», яка включає конфіденційну ділову інформацію лікарні та інформацію, яка може бути використана для ідентифікації фізичної особи. Це ширше, ніж федеральний Закон про перенесення та підзвітність медичного страхування (HIPAA), що стосується «захищеної медичної інформації», яка може бути використана для ідентифікації пацієнта.

Програма кібербезпеки: Переглянуті запропоновані правила вимагатимуть від лікарень створення програми кібербезпеки, яка містить певні можливості, зокрема ідентифікацію та оцінку ризиків кібербезпеки, захисну інфраструктуру та реагування на виявлені або виявлені події кібербезпеки для пом'якшення будь-яких негативних наслідків.

У переглянутих запропонованих положеннях NYSDOH вилучило положення початкових запропонованих правил, яке вимагало, щоб програма кібербезпеки лікарні була розроблена таким чином, щоб доповнювати HIPAA. NYSDOH внесло цю зміну у відповідь на коментарі, які закликали до зменшення надмірності та кращої відповідності вимогам HIPAA. Однак у письмових коментарях NYSDOH зазначило, що переглянуті запропоновані правила все ще мають на меті доповнити HIPAA.

У той час як початкові пропоновані правила зосереджувалися на заходах кібербезпеки для захисту безпеки та цілісності непублічної інформації, переглянуті пропоновані правила додатково зосереджені на безперервності бізнесу та операцій лікарні. Переглянута Заява про вплив на регулювання також містить додаткові посилання на безперервність бізнесу та операцій. Можливо, на збільшення уваги до

безперервності бізнесу вплинула нещодавня кібератака Change Healthcare, яка мала далекосяжні наслідки для діяльності організацій охорони здоров'я по всій країні.

Переглянуті запропоновані правила вводять нову вимогу до лікарень запроваджувати засоби контролю безпеки, щоб зменшити ризики, що виникають через загрози електронної пошти (таких як спуфінг, фішинг і шахрайство), а також регулярно переглядати та оновлювати такі засоби контролю, щоб забезпечити їх ефективність проти загроз, що розвиваються. Крім того, політика кібербезпеки лікарні має бути прийнята відповідно до оцінки ризиків лікарні та чинного державного та федерального законодавства.

CISO: Лікарні повинні будуть призначити кваліфікованого старшого або керівного персоналу з належною підготовкою, досвідом і знаннями на посаду головного спеціаліста з інформаційної безпеки («CISO»). CISO має рекомендувати політику кібербезпеки лікарні для затвердження керівним органом лікарні та надавати керівному органу щорічний письмовий звіт про програму кібербезпеки лікарні та суттєві ризики кібербезпеки.

Початкові запропоновані положення вимагали від CISO розробити політику та процедури кібербезпеки лікарні. Однак переглянуті запропоновані положення передбачають, що лікарня повинна нести відповідальність за розробку та впровадження політики кібербезпеки лікарні, а також нагляд і впровадження програми кібербезпеки лікарні. Цей перегляд надає лікарням додаткову гнучкість у впровадженні процесів кібербезпеки.

У відповідь на запитання коментаторів щодо того, чи потрібна кожна лікарня в багатолікарняній системі мати власну CISO, NYSDOH пояснила, що керівний орган кожної лікарні повинен визначити на основі оцінки ризиків та організаційної структури, чи може один CISO обслуговувати декілька лікарень у межах мережі організації або якщо для кожної лікарні потрібні окремі CISO.

Персонал із кібербезпеки: лікарні повинні будуть залучати кваліфікованого персоналу з кібербезпеки або стороннього постачальника послуг для керування програмою кібербезпеки. У разі використання стороннього постачальника послуг лікарня повинна буде впроваджувати письмові правила та процедури, розроблені

для забезпечення безпеки інформаційних систем і непублічної інформації, до якої має доступ така третя сторона. Переглянуті запропоновані положення також визначають вимоги до контрактів із сторонніми постачальниками послуг. Лікарням, які залучають сторонніх постачальників послуг для допомоги у своїх програмах кібербезпеки, можливо, доведеться переглянути умови таких залучень, щоб забезпечити відповідність цим новим вимогам.

Автентифікація користувача інформаційної системи: лікарням потрібно буде використовувати багатофакторну автентифікацію, автентифікацію на основі оцінки ризику або інші компенсаційні засоби контролю автентифікації користувачів для захисту від несанкціонованого доступу до закритої інформації або інформаційних систем. Для доступу до внутрішньої мережі лікарні із зовнішньої мережі необхідна багатофакторна автентифікація, якщо CISO не схвалить інше в письмовій формі.

Переглянуті запропоновані правила вводять додаткові вимоги щодо привілеїв доступу користувачів і привілейованих облікових записів, які можна використовувати для виконання функцій безпеки, які звичайні користувачі не мають права виконувати (наприклад, можливість додавати, змінювати або видаляти інші облікові записи або вносити зміни в конфігурацію до інформаційних систем). Зокрема, лікарні повинні обмежити привілеї доступу користувачів до інформаційних систем, які надають доступ до непублічної інформації лише тим, хто необхідний для виконання роботи користувача. Крім того, лікарні повинні мати окремі привілейовані облікові записи, які обмежені за кількістю та функціями доступу лише до кількості та можливостей, необхідних для виконання необхідних привілейованих функцій. Лікарні також повинні переглядати всі привілеї доступу користувачів і принаймні раз на рік видаляти або вимикати облікові записи та доступ, які більше не потрібні, негайно припиняти доступ після від’їзду та вимикати або безпечно налаштовувати всі протоколи, які дозволяють дистанційне керування пристроями.

Тестування, оцінка вразливості та оцінка ризику: лікарні повинні будуть проводити щорічну оцінку потенційних ризиків і вразливості щодо конфіденційності, цілісності та доступності закритої інформації та інформаційних

систем. Лікарням також потрібно буде розробити моніторинг і тестування відповідно до оцінки ризику, який призначений для оцінки ефективності програми кібербезпеки лікарні та оцінки змін в інформаційних системах, які можуть створювати або вказувати на вразливі місця. Такий моніторинг і тестування повинні включати тестування на проникнення в інформаційні системи лікарні кваліфікованою внутрішньою або зовнішньою стороною принаймні раз на рік, а також автоматичне сканування або ручне або автоматизоване перевірка інформаційних систем, розумно призначених для виявлення загальновідомих вразливостей кібербезпеки в інформаційних системах лікарні на основі оцінка ризику. Ці вимоги є більш жорсткими, ніж вимоги HIPAA щодо «періодичного» аналізу ризиків, і лікарням може знадобитися переглянути свої плани аналізу ризиків HIPAA, щоб забезпечити відповідність цим новим вимогам.

Переглянуті запропоновані правила загалом зберігають початково запропоновані вимоги до тестування, оцінки вразливості та оцінки ризиків, водночас додатково вимагаючи оцінки ризиків лікарні для оцінки ризиків та вразливості для безперервності діяльності та операцій лікарні; своєчасне усунення вразливостей на основі ризику, який вони становлять для лікарні; і що тестування на проникнення повинно проводитися на основі оцінки ризику лікарні.

Журнали аудиту та ведення записів: лікарні повинні будуть зберігати записи, що стосуються проектування, безпеки та обслуговування систем, а також журнали аудиту, які можуть виявляти значні загрози кібербезпеці та боротися з ними протягом щонайменше шести років. Це відображає зобов’язання щодо зберігання записів HIPAA, які вимагають зберігання записів, що стосуються політик HIPAA, протягом шести років після їх створення або впровадження політики.

Плани реагування на інциденти: Лікарні будуть зобов’язані прийняти письмовий план реагування на інциденти, розроблений для швидкого реагування на інциденти матеріальної безпеки та відновлення після них відповідно до вимог, визначених у правилах.

72-годинне звітування про інциденти: одразу після завершення переглянутого пропонованого положення лікарні будуть зобов’язані повідомляти NYSDOH

якнайшвидше, але не пізніше ніж через 72 години після визначення того, що стався інцидент кібербезпеки. Лікарні повинні зберігати документацію, пов'язану з такими інцидентами, принаймні шість років і надавати її до NYSDOH на запит.

Декілька коментаторів висловили занепокоєння вимогою в Початкових запропонованих правилах повідомляти про інциденти безпеки в NYSDOH протягом двох годин після визначення того, що інцидент стався та мав суттєвий негативний вплив на лікарню, зазначивши, що цей термін не відповідає галузевим стандартам. У відповідь Департамент продовжив термін подання звітності.

Приблизні витрати на відповідність і фінансування кібербезпеки. Штат оцінює значні витрати на відповідність, коливаючись від десятків тисяч до десятків мільйонів доларів на лікарню. Тим не менш, держава вважає, що переглянуті запропоновані правила необхідні, враховуючи високий ризик кібербезпекового середовища, в якому працюють лікарні. У 2023 році NYSDOH реагував на більш ніж один інцидент кібербезпеки на місяць, кілька з яких змушували лікарні відмовляти пацієнтам, зупиняли процедури виставлення рахунків і ускладнювали надання медичної допомоги. Ці інциденти вплинули на багатьох жителів Нью-Йорка, причому лише одне порушення може постраждати понад 225 000 пацієнтів. У відповідь на коментарі, у яких висловлювалося занепокоєння щодо витрат на відповідність вимогам, NYSDOH знову висловив переконання, що значний фінансовий вплив зрештою буде переважений додатковими рівнями безпеки, які ці правила нададуть лікарням і системі охорони здоров'я в Нью-Йорку. NYSDOH також зазначив, що 500 мільйонів доларів США у вигляді грантів на кібербезпеку лікарень і 650 мільйонів доларів США на загальнодержавне фінансування медичних інформаційних технологій, телеохорони здоров'я та заходів, пов'язаних з кібернетичними засобами, потенційно можуть полегшити фінансовий тягар відповідності для постраждалих лікарень.

Наступні кроки. Переглянуті запропоновані правила підлягають повідомленню та коментарям до 1 липня 2024 року, і, якщо вони будуть остаточно розроблені, вони набудуть чинності через рік після завершення — за винятком вимоги щодо звітування про інциденти безпеки протягом 72 годин, які набудуть

чинності негайно. Щоб відповідати вимогам, лікарням доведеться оновити свою політику та процедури кібербезпеки, найняти спеціалістів із кібербезпеки, змінити свої процедури реагування на інциденти та переглянути заплановану оцінку ризиків безпеки.

Ці запропоновані нормативні акти з'являються після розширення вимог щодо управління кібербезпекою, заходів безпеки та звітності про інциденти, які застосовуються до організацій, діяльність яких регулюється страховим законодавством Нью-Йорка (включаючи компанії медичного страхування), банківським законодавством або законодавством про фінансові послуги. Загалом ці нормативні зміни вказують на збільшення очікувань і ретельний контроль щодо програм кібербезпеки для сектору охорони здоров'я». ***(Christine Moundas, Gideon Zvi Palte, William Shefelman and Peyton Brooks. New York State Revises Proposed Cybersecurity Program and Incident Reporting Requirements for Hospitals // Ropes & Gray LLP (https://www.ropesgray.com/en/insights/alerts/2024/06/new-york-state-revises-proposed-cybersecurity-program-and-incident-reporting-requirements?utm_source=alert&utm_medium=email&utm_campaign=new-york-state-revises-proposed-cybersecurity-program-and-incident-reporting-requirements). 05.06.2024).***

***

«7 травня 2024 року Офіс національного кібердиректора (ONCD) оприлюднив Звіт про стан кібербезпеки Сполучених Штатів за 2024 рік (Звіт). У Звіті окреслено головні тренди 2023 року, серед яких:

1. Розвиток ризиків для критичної інфраструктури

Противники національних держав розробляють стратегії нападу на критично важливу інфраструктуру США без шпигунської чи розвідувальної цінності, і мають намір порушити або знищити критично важливу інфраструктуру США та союзників. Ці атаки можуть бути спрямовані на те, щоб «сприяти зриву оперативних технологічних систем у критичній інфраструктурі та втручатися у

бойові можливості США та союзників», а також можуть бути мотивованими для досягнення «геополітичних цілей».

2. Програми-вимагачі

«Програми-вимагачі залишаються постійною загрозою національній безпеці, громадській безпеці та економічному процвітанню». Центр розгляду скарг на злочини в Інтернеті (ICS) Федерального бюро розслідувань (ФБР) отримав на 22% більше повідомлень про випадки програм-вимагачів від американських жертв, а вартість атак програм-вимагачів у 2023 році, про які повідомляє ICS, зросла на 74% порівняно з 2022 роком. Зловмисники більше співпрацюють і більше про розробку зловмисного програмного забезпечення, здійснення атак і збір викупу.

3. Експлуатація ланцюга поставок

Зловмисники використовують переваги складних і взаємопов'язаних відносин між постачальниками, клієнтами, продавцями та постачальниками послуг. Це надає їм можливість «доступу до жертв у масштабі та ускладнює зусилля захисників щодо виявлення та управління ризиками кібербезпеки».

4. Комерційні шпигунські програми

Ринок комерційного шпигунського програмного забезпечення значно виріс, і той, хто запропонує найвищу ціну, може отримати доступ до складних і інвазивних наскрізних інструментів кіберспостереження для віддаленого доступу до електронних пристроїв, моніторингу та вилучення вмісту та маніпулювання компонентами без відома чи згоди власника пристрою. Більше того, ці загрозливі суб'єкти тепер націлені на «журналістів, активістів, правозахисників та урядовців все частіше». Комерційне шпигунське програмне забезпечення також «використовується проти урядового персоналу США, інформації та комп'ютерних систем, створюючи значні контррозвідувальні та безпекові ризики для Сполучених Штатів».

5. Штучний інтелект (AI)

Швидкий і безперервний розвиток штучного інтелекту створить можливості та виклики для управління кіберризиками. Хоча штучний інтелект надасть можливості для захисту критичної інфраструктури, кіберзлочинці, хакери та інші

«можуть використовувати ці можливості для проведення фішингових кампаній, інформаційних операцій та іншої зловмисної кіберактивності». Для захисту конфіденційності американців можуть знадобитися заходи безпеки щодо використання та розвитку технологій ШІ.

У звіті також описано 12 заходів, вжитих Федеральним урядом протягом звітного періоду, серед яких:

Встановлення та використання кібервимог для захисту критичної інфраструктури, у тому числі шляхом розробки та гармонізації нормативних вимог у багатьох секторах критичної інфраструктури.

Розширення федерального співробітництва та партнерства для кращої підтримки кіберзахисників, у тому числі шляхом посилення оперативної співпраці, покращення потенціалу Агентства управління ризиками сектору (SRMA) та інтеграції можливостей федерального кіберзахисту.

Поліпшення готовності до інцидентів і реагування на них шляхом швидкого обміну інформацією про загрози, надання пріоритетної підтримки жертвам і перегляду значних інцидентів і кампаній для отримання отриманих уроків.

Знищення та приниження активності противника з використанням усіх інструментів національної влади, що призводить до скоординованих, потужних кампаній зриву проти широкого кола зловмисних кіберакторів.

Швидкий і масштабний захист федеральних мереж, зокрема шляхом інтеграції принципів Zero Trust Architecture у федеральне підприємство, модернізації застарілих технологічних систем і розширення використання спільних служб.

Зміцнення національної робочої сили в кіберпространстві, зокрема шляхом оприлюднення Національної стратегії щодо робочої сили та освіти в кіберпространстві (NCWES) і взаємодії з працівниками, роботодавцями, студентами та освітянами по всій країні.

Підвищення безпеки програмного забезпечення для створення безпечніших продуктів і послуг, у тому числі шляхом вдосконалення принципів безпеки за

проектом, номенклатури програмного забезпечення (SBOM) і безпечних для пам’яті мов програмування.

Створення цифрової економіки, яка розширює можливості та захищає споживачів, у тому числі шляхом запуску програми сертифікації та маркування Cyber Trust Mark у США та сприяння конкуренції та підзвітності в усій галузі технологій.

Інвестування в стійкі технології наступного покоління в економіці чистої енергії, видача виконавчого наказу, який керуватиме федеральними зусиллями, пов’язаними зі штучним інтелектом, і вирішення проблем безпеки, наявних у технічних основах Інтернету.

Управління ризиками для безпеки та конфіденційності даних шляхом забезпечення безпечної транскордонної торгівлі з багатим даними та сприяння розвитку технологій, що покращують конфіденційність.

Підвищення стійкості в усьому світі шляхом створення коаліцій країн-однодумців для надання підтримки жертвам програм-вимагачів та інших кібератак, узгодження національної політики та сприяння безпечним і стійким глобальним ланцюжкам поставок.

У звіті зазначається, що «Федеральний уряд спиратиметься на досягнення минулого року, продовжуватиме впровадження нещодавно опублікованої версії Плану впровадження національної стратегії кібербезпеки та Національної стратегії щодо робочої сили та освіти в кіберпространстві та адаптуватиме свій підхід для вирішення нових проблем і можливостей. представлений стратегічним ландшафтом, що розвивається». ***(Trisha Sircar. The Office of the National Cyber Director Releases 2024 Report on Cybersecurity Posture // Katten Muchin Rosenman LLP (https://quickreads.ext.katten.com/post/102j9iw/the-office-of-the-national-cyber-director-releases-2024-report-on-cybersecurity-p#page=1). 06.06.2024).***

***

«12 березня 2024 року Міністерство оборони США випустило остаточне правило, що переглядає критерії прийнятності для його добровільної

Програми кібербезпеки оборонно-промислової бази («DIB»). Остаточне правило «розширює право на участь у програмі DIB CS лише з підрядників, які мають активний дозвіл на об’єкт, на всіх оборонних підрядників, які володіють або керують несекретною інформаційною системою, яка обробляє, зберігає або передає контрольовану несекретну інформацію (CUI)».

Програма DIB, започаткована в 2013 році, є добровільною програмою, спрямованою на підвищення та доповнення можливостей учасників щодо захисту секретної оборонної інформації, яка обробляється, зберігається або передається в несекретних інформаційних системах. Правило створило веб-сайт Міністерства оборони для дозволених оборонних підрядників («CDC»), щоб полегшити: (1) обмін інформацією щодо права та участі в програмі з потенційними учасниками, (2) подання заявки на участь у програмі онлайн та (3) виконання необхідних договори з Урядом. Правило 2013 року визначило CDC як будь-яку «приватну юридичну особу, яка отримала дозвіл Міністерства оборони на доступ, отримання або зберігання секретної інформації з метою участі в торгах за контрактом або проведення заходів на підтримку будь-якої програми Міністерства оборони».

Програма DIB надає учасникам доступ до: «конференцій для технічного обміну, спільної веб-платформи (DIBNet-U) та продуктів і послуг з інформацією про загрози через Центр боротьби з кіберзлочинністю Міністерства оборони (DC3). DC3 реалізує операції програми, обмінюючись інформацією про кіберзагрози та розвідкою з DIB, а також пропонуючи різноманітні продукти, інструменти, послуги та заходи. DC3 служить єдиним інформаційним центром для некласифікованих обов’язкових звітів про інциденти (MIR) і добровільних звітів про обмін інформацією про загрози».

До зміни правил 12 березня 2024 року, щоб мати право брати участь у програмі DIB, підрядник повинен був бути CDC, який: (1) має сертифікат середньої гарантії, затверджений Міністерством оборони; (2) має наявний доступ до об’єкта («FCL») принаймні до секретного рівня; і (3) може виконувати Рамкову угоду DIB (надається лише відповідним підрядникам після перевірки). З урахуванням цих

вимог 45% із 266 заявників на участь у програмі DIB у 2022 році не мали права брати участь у програмі. Наразі Програма налічує близько 1000 учасників-підрядників.

Останнє правило (1) скасовує вимогу щодо схваленого Міністерством оборони сертифіката середньої впевненості, замінюючи його вимогою реєстрації в інтегрованому корпоративному середовищі Міністерства оборони («PIEE»); та (2) скасовує вимогу щодо наявного секретного FCL.

Крім того, останнє правило замінює посилання на CDC на «підрядники, які володіють або керують охопленою інформаційною системою підрядника» (інформаційна система, якою володіє або керує підрядник, яка обробляє, зберігає або передає федеральну контрактну інформацію. FAR 52.204-21).

Очікується, що ці зміни до критеріїв прийнятності збільшать кількість відповідних оборонних підрядників приблизно на 68 000.

Підрядники повинні відповідати таким критеріям, щоб отримувати секретну інформацію про кіберзагрози в електронному вигляді: (1) мати наявний FCL принаймні до секретного рівня; (2) мати або придбати обліковий запис Communication Security (COMSEC); (3) мати або отримати затверджений захист принаймні секретної інформації; та (4) отримати доступ до безпечних систем передачі голосу та даних Міністерства оборони, які підтримують програму DIB.

Остаточне правило набуло чинності 11 квітня 2024 року. Слідкуйте за оновленнями, щоб отримати додаткову інформацію про вплив і програми, які будуть оновлені після того, як програма діятиме протягом тривалого періоду часу». ***(Abby Bello Salinas. Department of Defense Expands Voluntary Cybersecurity Information Sharing Program // Peckar & Abramson PC (https://www.pecklaw.com/government-contract-law-blog/department-of-defense-expands-voluntary-cybersecurity-information-sharing-program/#page=1). 10.06.2024).***

***

«Загрози кібербезпеці, які впливають на Канаду та її бізнес, швидко розвиваються, оскільки світ продовжує спостерігати наплив політичної та

економічної нестабільності. Порушення даних, кібератаки та інші інциденти інформаційної безпеки займають центральне місце в дискусіях про національну безпеку, оскільки більше не можна покладатися на кордони та фізичну відстань для захисту канадців та їх власності.

У відповідь на ці нові загрози уряд Канади намагається вдосконалити режим національної безпеки, запровадивши заходи, спрямовані на захист від загроз кібербезпеці своєї критичної інфраструктури. У рамках цих ініціатив уряд запропонував законопроект C-26, Закон про кібербезпеку, внесення змін до Закону про телекомунікації та внесення відповідних поправок до інших законів, який запроваджує Закон про захист критичних кіберсистем («CCSPA»).

Запропонований закон випливає з визнання урядом того, що деякі кіберсистеми є критично важливими для інфраструктури, економіки та національної безпеки Канади, і їх збій може мати серйозні наслідки для нації. CCSPA створить основу для захисту критично важливих кіберсистем і послуг, життєво важливих для національної або громадської безпеки. Багато з цих систем є головною мішенню для кіберзлочинців і спонсорованих державою акторів, враховуючи їхню чутливість до шкідливих збоїв.

Якщо CCSPA стане законом, він накладе ряд зобов’язань на призначених операторів, а також на їхні ланцюги поставок і постачальників послуг у чотирьох федерально регульованих секторах: телекомунікації, фінанси, енергетика та транспорт.

Згідно з CCSPA, призначені оператори в цих чотирьох секторах повинні будуть:

Впровадити програму кібербезпеки із заходами щодо зменшення ризиків і структурою управління;

Зменшити ризики кібербезпеки в рамках свого ланцюжка поставок;

Повідомляти про інциденти кібербезпеки;

Дотримуватися вказівок, наданих Губернатором у Раді; і

Ведіть записи щодо відповідності.

CCSPA також надасть регуляторам широкі правозастосовні повноваження для запобігання невідповідності та надасть повноваження губернатору в Раді керувати призначеними операторами дотриманням будь-яких заходів, викладених у вказівці, з метою захисту критичної кіберсистеми.

Широке охоплення CCSPA

Хоча сфера діяльності CCSPA на перший погляд може здатися обмеженою, це законодавче рішення має далекосяжні наслідки для багатьох канадських компаній. Насправді, компанії, що надають продукти або послуги федерально регульованим організаціям, перерахованим CCSPA, потенційно можуть взяти на себе певний тягар встановлення більш надійного кіберзахисту в цих секторах.

У рамках своїх обов'язків призначені оператори повинні будуть відстежувати вразливі місця в системі кібербезпеки в межах свого ланцюжка поставок і сторонніх постачальників послуг. Це ключова частина CCSPA, оскільки суб'єкти загроз все частіше атакують організації через їхні зовнішні мережі, знаходячи найслабшу ланку.

Зосередженість на критичній інфраструктурі ланцюга поставок і постачальників послуг є результатом здатності суб'єктів загрози проникати на периметр мережі організації, скомпрометувавши одного з учасників ланцюга поставок або постачальників послуг. У зв'язку з тим, що компанії використовують більше цифрових зв'язків у ланцюгах постачання та сторонніх постачальників послуг, технологічна інфраструктура стає більш розподіленою по всьому світу, що призводить до збільшення точок уразливості. Виявлення будь-яких компромісів у цьому розширеному ланцюжку підключених компаній може бути складним, що робить цілі мережі вразливими для атак.

Ці нові зобов'язання означають, що призначені оператори відповідно до CCSPA почнуть вимагати від своїх постачальників і сторонніх постачальників вжити серйозних заходів для підвищення їх кіберстійкості. Очікується, що великі організації будуть особливо суворими до своїх вимог, оскільки вони значною мірою покладаються на багаторівневий аутсорсинг для виконання своїх повсякденних операцій. Це, безсумнівно, спричинить подальший ефект для

багатьох компаній, які зараз працюють практично без власних програм кібербезпеки.

У своєму посланні до канадців CCSPA чітко стверджує, що для створення національної кіберстійкості Канади потрібні спільні зусилля в усіх секторах. Наслідки кібератак, якими б незначними вони не були, можуть мати серйозні та руйнівні наслідки для бізнесу, а також несподівані наслідки для країни. Оскільки законопроект С-26 продовжує розгляд у Палаті громад, компаніям слід розглянути можливість впровадження проактивних заходів для підготовки до цих змін. Підвищення стану кібербезпеки, ізоляція критично важливих активів і навчання співробітників — все це важливі кроки, які можна зробити зараз, щоб захиститися від кіберризиків і підготуватися до нових загроз». ***(Paige Backman and Michelle Slipanchuk. Canada Is Protecting Its Critical Infrastructure: What Does This Mean for Your Business's Cybersecurity? // Aird & Berlis LLP | Aird & McBurney LP (https://www.airdberlis.com/insights/publications/publication/canada-is-protecting-its-critical-infrastructure-what-does-this-mean-for-your-business-s-cybersecurity). 11.06.2024).***

***

«Президент Microsoft (MSFT.O) Бред Сміт відповів на запитання про практику безпеки технологічного гіганта і його зв'язки з Китаєм на засіданні Комітету з питань національної безпеки Палати представників у четвер, через рік після того, як хакери, пов'язані з Китаєм, зламали електронну пошту федерального уряду США.

Минулого літа хакери отримали доступ до 60 000 електронних листів Державного департаменту США, зламавши системи Microsoft, а цього року кіберзлочинці, пов'язані з Росією, окремо шпигували за електронною поштою вищого керівництва Microsoft, згідно з розкриттями компанії.

Слухання в Конгресі відбуваються на тлі посилення федерального контролю над Microsoft, найбільшим у світі виробником програмного забезпечення, який також є ключовим постачальником для уряду США та установ національної

безпеки. На бізнес Microsoft припадає близько 3% федерального IT-бюджету США, сказав Сміт на слуханні.

Законодавці критикували Microsoft за її нездатність запобігти російським і китайським хакерським атакам, які, на їхню думку, поставили під загрозу федеральні мережі, незважаючи на те, що вони не використовували складні засоби.

Електронні листи компанії, до яких отримали доступ російські хакери, також «включали листування з урядовцями», заявив демократ Бенні Томпсон.

«Microsoft є одним із найважливіших партнерів федерального уряду в області технологій і безпеки, але ми не можемо дозволити собі дозволити, щоб важливість цих відносин створювала самовдоволення або втручатися в наш нагляд», — додав він.

Законодавці спиралися на висновки різкого звіту в квітні Комісії з аналізу кібербезпеки (CSRB) - групи експертів, сформованої міністром внутрішньої безпеки США Алехандро Майоркасом, - який критикував Microsoft за відсутність прозорості щодо злому в Китаї, називаючи його можна запобігти.

«Ми беремо на себе відповідальність за кожен висновок у звіті CSRB», — сказав Сміт на слуханні, додавши, що Microsoft почала діяти відповідно до більшості рекомендацій звіту.

«Ми маємо справу з грізними ворогами в Китаї, Росії, Північній Кореї, Ірані, і їм стає краще», — сказав Сміт. «Вони стають більш агресивними... Вони ведуть напади з надзвичайною швидкістю».

Томпсон розкритикував компанію Сміта за те, що вона не змогла виявити злом, натомість його виявив Державний департамент США. Сміт відповів: «Це має працювати саме так. Жодна сутність в екосистемі не може бачити все».

Але конгресмена Томпсона це не переконало.

«Це не наша робота - знаходити винних. Це те, за що ми вам платимо», - сказав Томпсон.

Члени комісії також досліджували Сміта для отримання подробиць про бізнес Microsoft у Китаї, зазначивши, що компанія вклала значні кошти у створення стимулів для досліджень там.

«Присутність Microsoft у Китаї створює комплекс складних проблем і ризиків», — сказав конгресмен Марк Грін з Міссісіпі, який очолював групу.

Microsoft отримує близько 1,5% свого доходу в Китаї і працює над скороченням своєї інженерної присутності там, сказав Сміт.

Протягом останнього року компанія зіткнулася з посиленою критикою з боку колег із галузі безпеки через порушення та відсутність прозорості.

Відповіді Сміта на слуханнях заслужили похвалу деяких членів колегії, таких як конгресмен-республіканець Марджорі Тейлор Грін. «Ви сказали, що берете на себе відповідальність, і я просто хочу похвалити вас за це», — сказав йому Грін.

Після критики правління Microsoft заявила, що працює над удосконаленням своїх процесів і дотриманням контрольних показників безпеки. У листопаді компанія запустила нову ініціативу з кібербезпеки та заявила, що робить безпеку головним пріоритетом компанії «понад усе — над усіма іншими функціями». ***(Zeba Siddiqui. US lawmakers grill Microsoft president over China ties, hacks // Reuters (https://www.reuters.com/technology/microsoft-president-testify-before-house-panel-over-security-lapses-2024-06-13/). 13.06.2024).***

***

«Американська бібліотечна асоціація (ALA) вітає сьогоднішнє голосування Федеральної комісії зі зв'язку (FCC) щодо запуску пілотної програми для публічних бібліотек і шкіл із придбання передових інструментів кібербезпеки. Пілотна програма, яка планується запустити пізніше цього року, надасть 200 мільйонів доларів США на допомогу бібліотекам і школам у захисті цифрової інфраструктури.

«Сьогоднішнє рішення FCC створити пілотну програму кібербезпеки є важливим кроком вперед для бібліотек і бібліотечних працівників нашої країни, надто багато з яких стикаються з ескалацією витрат на захист систем і даних своєї установи», — сказала президент ALA Емілі Драбінські. «Ми залишаємося непохитними у своєму заклику до довгострокового механізму фінансування, який

забезпечить можливість бібліотек і надалі пропонувати доступ та інформацію, на яку покладаються їхні спільноти».

ALA постійно виступає за створення ширшого плану фінансування та підтримки кібербезпеки для бібліотек Америки через програму E-rate. У коментарях, поданих до FCC, ALA закликала Комісію створити довгостроковий план фінансування для підтримки інструментів кібербезпеки. У спільному листі, поданому разом із партнерами по коаліції, ALA закликала внести кілька ключових змін у дизайн пілотного проекту, щоб зменшити перешкоди для доступу бібліотек і шкіл і уточнити суми фінансування. Зокрема, суми фінансування великих бібліотечних систем недостатньо покриють витрати на кібербезпеку для найбільших бібліотечних систем країни.

Зіштовхнувшись зі зростанням витрат на мережеву безпеку та зростанням рівня загроз кібербезпеці, бібліотеки по всій країні потребують нової та постійної підтримки для належного захисту своїх систем. Резонансні випадки порушень безпеки, включаючи атаки програм-вимагачів у численних бібліотеках по всій країні, підкреслили необхідність додаткової підтримки безпеки бібліотечної мережі.

Оскільки рішення про програму будуть ухвалені в найближчі місяці, ALA продовжуватиме отримувати відгуки від місцевих бібліотек і виступати за зміни пілотної програми кібербезпеки, щоб вона захищала цінну інформацію публічних бібліотек по всій країні та мільйонів відвідувачів, яких вони обслуговують. Найближчими днями працівники ALA також нададуть відповіді на поширені запитання потенційним кандидатам на бібліотеку, щоб краще допомогти членам і бібліотечним професіоналам, які шукають фінансової підтримки». ***(American Library Association welcomes FCC cybersecurity funding pilot for libraries, calls for long-term funding // American Library Association (https://www.ala.org/news/2024/06/american-library-association-welcomes-fcc-cybersecurity-funding-pilot-libraries-calls). 06.06.2024).***

***

«Публічна бібліотека Сіетла досягла важливої віхи в четвер, оскільки вона оговталася після події минулого місяця, пов'язаної з кібербезпекою.

25 травня публічна бібліотека Сіетла була змушена припинити роботу через подію з кібербезпекою, яка вплинула на її технологічні системи.

У четвер бібліотека опублікувала оновлення, в якому повідомляється, що читачі знову матимуть доступ до колекції цифрових книг бібліотеки.

Відповідно до заяви публічної бібліотеки Сіетла від травня, бібліотека залишалася в автономному режимі з моменту першої атаки програм-вимагачів, і немає графіка, коли всі служби будуть відновлені.

Незважаючи на те, що бібліотека залишається відкритою, багато інших послуг, які покладаються на онлайн-з'єднання, перешкоджають роботі, зокрема каталогізація, програмне забезпечення для прокату, громадські комп'ютери та публічна друкарня.

Кібератака почалася на початку травня 25, лише за день до того, як бібліотека планувала вивести свої системи з мережі, щоб провести планове технічне обслуговування сервера на вихідних у День пам'яті. Атака завадила доступу до комп'ютерів персоналу та загальнодоступних комп'ютерів, онлайн-каталогів та систем прокату, електронних книг та електронних аудіокниг, Wi-Fi у будівлі та веб-сайту публічної бібліотеки Сіетла (SPL).

За словами SPL, вони швидко залучили сторонніх спеціалістів-криміналістів, зв'язалися з правоохоронними органами та повністю перевели свої системи в автономний режим, щоб перервати та краще оцінити характер і наслідки події.

Співпрацюючи із зовнішніми партнерами, SPL продовжує розслідувати атаку. У своїй заяві про подію вони заявили: «Ми працюємо якнайшвидше та старанніше, щоб підтвердити ступінь впливу та відновити повну функціональність наших систем. Конфіденційність і безпека інформації про клієнтів і співробітників є головними пріоритетами».

Проте всі двадцять сім закладів публічної бібліотеки Сіетла залишатимуться відкритими за розкладом для таких послуг, як перевірка друкованих книг, компакт-дисків і DVD-дисків, або забирання книг, які вже є на полицях із фізичною

бібліотечною карткою чи номером бібліотечної картки. Відвідувачі також можуть отримати відповіді на довідкові та рекомендаційні запитання, а приміщення та зручності будуть доступні для використання.

Наразі SPL не може перевірити фізичні матеріали, заохочуючи гостей зберігати ці матеріали, доки вони не відновлять роботу системи та не зможуть оновити терміни для матеріалів.

Бібліотека підтвердила, що продовжуватиме оновлювати інформацію, щойно стане доступною додаткова інформація, і заздалегідь вибачилася за потенційно довший час очікування через великий відставання повернених і щойно доставлених елементів, якими потрібно керувати, коли системи знову будуть онлайн». ***(After cybersecurity event, Seattle Public libraries slowly coming back online // Yahoo (https://www.yahoo.com/news/cybersecurity-event-seattle-public-libraries-202707054.html?fr=sycsrp_catchall). 13.06.2024).***

***

«Річні бонуси найвищих посадових осіб Microsoft залежатимуть від того, наскільки уважно вони ставилися до кібербезпеки, повідомив віце-голова та президент компанії

Напередодні слухань у комітеті Палати представників Конгресу США, присвячених питанням безпеки Microsoft, Бред Сміт представив доповнення до своїх письмових свідчень, в якому детально описав майбутнє нововведення.

Керівники вищої ланки компанії, які часто зустрічаються з генеральним директором, отримують річні бонуси, які розраховуються на основі ряду факторів, включаючи так звану «індивідуальну ефективність».

У 2025 фінансовому році, який розпочнеться 1 липня, третина цієї частини «індивідуальної ефективності» буде безпосередньо пов’язана з перевіркою їхньої з кібербезпеки роботи. Перегляд буде проведено комітетом ради директорів з компенсацій, але також включатиме думку неідентифікованої незалежної третьої сторони.

Деякі зміни в структурі бонусів також можуть відбутися в цьому фінансовому році, пояснив Сміт:

«Правління також вирішило, що в поточному фінансовому році, який закінчується 30 червня, Комітет з компенсацій буде чітко розглядати показники кібербезпеки кожного члена SLT під час щорічної оцінки ефективності виконавчої влади», — написав він. «Окрім структурних змін у нашій програмі оплати праці керівників, які передбачають посилення відповідальності за кібербезпеку, Рада також має можливість використовувати на свій розсуд результати компенсацій, які вона вважає доцільними».

Останнім часом корпорація Майкрософт зазнала великої критики через її нібито погану роботу з серйозними інцидентами кібербезпеки.

Влітку 2023 року Microsoft Exchange Online зазнав серії вторгнень з боку підтримуваного Китайською Народною Республікою (КНР) актора під іменем Storm-0558, який отримав доступ до поштових скриньок 22 організацій. Поштовими скриньками користувалися понад 500 осіб, і вони скомпрометували ряд представників уряду США, включаючи міністра торгівлі Джину Раймондо, посла США в КНР Р. Ніколаса Бернса та конгресмена Дона Бекона.

Відповідно до звіту Міністерства внутрішньої безпеки (DHS) і Комісії з аналізу кібербезпеки (CSRB), було встановлено, що нападу можна було запобігти, в якому зазначено, що було прийнято рішення, яке вказує на «корпоративну культуру, яка віддає перевагу безпеці підприємства». інвестиції та суворе управління ризиками, що суперечить центральній ролі компанії в технологічній екосистемі та рівню довіри, яку клієнти надають компанії щодо захисту своїх даних і операцій».

Перевірка показала, що недбалість Microsoft у підписанні ротації ключів призвела до того, що ключ 2016 року залишився активним у 2023 році. Крім того, низка критичних елементів керування безпекою, які були стандартною практикою для інших CSP на момент атаки, не використовувалася, що могло виявити і запобігли вторгненню такого масштабу.

Було також виявлено, що під час інциденту корпорація Майкрософт надсилала суперечливі повідомлення, в яких говорилося, що ключ 2016 року, ймовірно, було вкрадено під час «аварійного дампа», а потім заявлялося, що немає жодних доказів того, що ключ було вкрадено в цьому сценарії.

Виконувач обов'язків заступника голови CSRB Дмитро Альперович сказав: «Ця пов'язана з Китайською Народною Республікою група хакерів має можливість і має намір скомпрометувати системи ідентифікації для доступу до конфіденційних даних, включаючи електронні листи осіб, які становлять інтерес для китайського уряду. Постачальники хмарних послуг повинні терміново впровадити ці рекомендації, щоб захистити своїх клієнтів від цієї та інших постійних і згубних загроз з боку національних держав». ***(Sead Fadilpašić. Microsoft set to dock bosses' pay — if they haven't shown good cybersecurity performance // Future US, Inc. (https://www.techradar.com/pro/security/microsoft-set-to-dock-bosses-pay-if-they-havent-shown-good-cybersecurity-performance).16.06.2024).***

***

«13 травня 2024 року уряд Онтаріо вніс законопроект 194 «Про зміцнення кібербезпеки та розбудову довіри в державному секторі» 2024 року. Законопроект пропонує Закон про посилення цифрової безпеки та довіри 2024 року («EDSTA») і спрямований на внесення змін до Закону про свободу інформації та захист конфіденційності («FIPPA»).

Законопроект не пропонує змін до Закону про муніципальну свободу інформації та захисту конфіденційності («MFIPPA») або Закону про захист особистої інформації про здоров'я («PHIPA»), але EDSTA застосовуватиметься до муніципальних установ державного сектору.

Закон про посилення цифрової безпеки та довіри, 2024 (EDSTA)

У додатку 1 законопроекту 194 буде введено в дію EDSTA. Згідно з пропозицією, EDSTA запровадить нові вимоги в державному секторі щодо кібербезпеки, штучного інтелекту (ШІ) і технологій, що впливають на неповнолітніх (визначаються як особи віком до 18 років). EDSTA

поширюватиметься на всі установи, які охоплюються FIPPA та MFIPPA, а також на товариства допомоги дітям і шкільні ради.

Незважаючи на те, що EDSTA встановлює основу для регулювання штучного інтелекту та кібербезпеки в державному секторі, багато з його ключових положень залишаються обґрунтованими майбутніми нормативними актами.

Кібербезпека

EDSTA дозволить уряду створювати правила, які вимагатимуть від суб'єктів державного сектору розробки та впровадження програм кібербезпеки. Положення можуть передбачати конкретні елементи, які повинні бути включені в такі програми, зокрема:

Внутрішні ролі та обов'язки в організації для забезпечення кібербезпеки.

Процедури звітування про прогрес щодо забезпечення кібербезпеки.

Громадська освіта та обізнаність.

Заходи реагування та відновлення після інциденту кібербезпеки.

Нагляд за програмою.

Міністр надання державних і ділових послуг («Міністр») також може приймати правила, що встановлюють технічні стандарти або встановлюють директиви щодо програм кібербезпеки.

Норми можуть вимагати від організацій державного сектору подавати звіти міністру або будь-якій іншій уповноваженій особі у разі виникнення інцидентів, пов'язаних з кібербезпекою. Зверніть увагу, що «інциденти, пов'язані з кібербезпекою» не визначені, але вони відрізняються від порушень конфіденційності. Відповідно, ця вимога звітування, ймовірно, буде спричинена нижчим порогом, ніж зобов'язання сповіщати про порушення конфіденційності відповідно до FIPPA (описано нижче).

Штучний інтелект

Вимоги до штучного інтелекту відповідно до EDSTA будуть застосовуватися до суб'єктів державного сектора, які використовують або мають намір використовувати системи штучного інтелекту, передбачені нормативними актами. Суб'єкти господарювання, на які поширюються такі правила, повинні будуть:

Надавати громадськості інформацію про використання ними систем ШІ.

Розробити та впровадити систему підзвітності, застосовну до використання ними систем ШІ.

Вжити заходів для управління ризиками, пов’язаними з використанням систем ШІ.

Не використовувати системи штучного інтелекту у спосіб, заборонений нормативними актами.

На додаток до цих загальних вимог, передбачених майбутніми правилами, організації, які використовують або мають намір використовувати системи ШІ, повинні будуть призначити особу, відповідальну за нагляд за системами ШІ в межах організації.

Крім того, міністр може приймати правила, що встановлюють технічні стандарти використання систем ШІ.

Технологія, що впливає на неповнолітніх

Згідно з EDSTA, уряд може приймати правила щодо обробки «встановленої цифрової інформації» осіб віком до 18 років (неповнолітніх) товариствами допомоги дітям і шкільними радами. Майбутні нормативні акти встановлюватимуть, що таке «прописана цифрова інформація».

Правила можуть бути прийняті для:

Визначте спосіб збору, використання, зберігання або розкриття встановленої цифрової інформації.

Вимагати, щоб організації надавали звіти міністру або іншій уповноваженій особі про збір, використання, зберігання та розкриття встановленої цифрової інформації.

Заборонити обробку цифрової інформації неповнолітніх за встановлених обставин або для встановлених цілей.

Міністр може приймати правила, що встановлюють технічні стандарти, яких повинні дотримуватися шкільні ради та товариства допомоги дітям під час обробки цифрової інформації неповнолітніх, а також приписувати цифрові технології, які можуть бути доступні для використання неповнолітніми.

Оновлення Закону про свободу інформації та захист приватного життя (FIPPA)

Додаток 2 законопроекту 194 пропонує низку поправок до FIPPA. Оновлення FIPPA стосуються обов'язкової оцінки впливу на конфіденційність (PIA), зобов'язань повідомляти про порушення та нових повноважень Уповноваженого з питань інформації та конфіденційності Онтаріо (IPC).

PIA

Законопроект 194 пропонує нову вимогу до установ заповнювати письмові PIA перед збором персональної інформації. Відповідна PIA повинна містити:

Мета, з якою особиста інформація збирається, використовується та розкривається, якщо це застосовно, а також пояснення того, чому особиста інформація потрібна для досягнення мети.

Законні повноваження для збирання, використання та розкриття особистої інформації.

Типи особистої інформації, яку планується збирати, і для кожного типу зібраної персональної інформації вказівку того, як тип персональної інформації планується використовувати або розкривати.

Джерела персональної інформації, яку планується зібрати.

Посади посадових осіб, співробітників, консультантів або агентів установи, які матимуть доступ до особистої інформації.

Будь-які обмеження, накладені на збір, використання або розкриття особистої інформації.

Період часу, протягом якого особиста інформація зберігатиметься установою.

Пояснення адміністративних, технічних і фізичних заходів безпеки та практики, які будуть використовуватися для захисту особистої інформації, а також стислий опис будь-яких ризиків для осіб у разі крадіжки, втрати або несанкціонованого використання чи розкриття особистої інформації.

Заходи, які має вжити установа:

Щоб запобігти або зменшити ймовірність крадіжки, втрати або несанкціонованого використання чи розкриття особистої інформації.

ii. Щоб зменшити ризики для окремих осіб у разі таких подій.

Така інша інформація, яка може бути встановлена.

Відповідно до законопроекту 194 установи повинні постійно оновлювати PIA та надавати копію PIA IPC на запит.

Повідомлення про порушення та звітування

Законопроект 194 вводить обов'язковий обов'язок для установ повідомляти IPC та постраждалих осіб про порушення конфіденційності, як «будь-яку крадіжку, втрату або несанкціоноване використання або розголошення особистої інформації, що знаходиться на зберіганні або під контролем установи». Майбутні нормативні акти визначатимуть форму та зміст повідомлень про порушення, але в законопроекті 194 зазначено, що повідомлення повинні містити заяву про те, що постраждалі особи мають право подати скаргу до IPC.

Законопроект 194 встановлює поріг «обґрунтованого ризику значної шкоди» (РРОШ) для зобов'язань щодо повідомлення та звітності. Установи повинні повідомляти IPC та постраждалих осіб лише тоді, коли існує обґрунтований ризик того, що за цих обставин особа може завдати значної шкоди.

Законопроект вимагає від установ вести записи про кожну крадіжку, втрату або несанкціоноване використання або розголошення особистої інформації, яку вони повідомляють IPC.

Повноваження IPC

Законопроект 194 пропонує розширити наглядові та правозастосовні повноваження IPC. Це включає в себе повноваження переглядати інформаційну практику установ після скарги або якщо IPC має підстави вважати, що сталася невідповідність FIPPA. IPC може здійснювати слідчі повноваження, щоб розпорядитися про виготовлення записів і видавати розпорядження щодо відповідності після завершення свого перегляду. Відповідно до змін, внесених до законопроекту 194, інституції матимуть обов'язок сприяти перевіркам IPC.

Законопроект запроваджує захист для інформаторів, вимагаючи від IPC зберігати конфіденційність особи, яка повідомляє IPC про їхнє обґрунтоване переконання, що установа порушила FIPPA.

Відповідно до поправок, запропонованих у законопроекті 194, IPC матиме повноваження консультуватися з працівником правоохоронних органів або будь-якою особою, яка має повноваження, обов'язки та функції, подібні до тих, які має IPC, щодо захисту особистої інформації.

Наступні кроки

Законопроект 194 зараз розглядається у другому читанні в Законодавчих зборах Онтаріо. Законодавча асамблея піднялася на літо і не планує повернутися до 21 жовтня 2024 року.

Період початкових громадських консультацій щодо законопроекту 194, під час якого громадськості було запропоновано надати коментарі уряду Онтаріо щодо законопроекту, завершився 11 червня 2024 року». ***(Michael Walsh and Wendy J. Wagner. Ontario Introduces Bill 194 to address cyber security in the public sector // Gowling WLG (https://gowlingwlg.com/en/insights-resources/articles/2024/ontario-introduces-bill-194/). 18.06.2024).***

***

«Збройні сили США нещодавно запустили новаторську ініціативу щодо зміцнення зв'язків з комерційною космічною галуззю. Метою є інтеграція комерційного обладнання у військові космічні операції, включаючи супутники та інше обладнання. Це підвищить кібербезпеку військових супутників.

Оскільки космос стає все більш важливим для критичної інфраструктури світу, зростає ризик того, що ворожі національні держави розгорнуть кібератаки на важливі супутники та іншу космічну інфраструктуру. Цілі включатимуть супутники-шпигуни або військові супутники зв'язку, а також комерційні космічні апарати.

Міністерство оборони США вважає, що його нове партнерство під назвою Commercial Augmentation Space Reserve (CASR) посилить національну безпеку США та конкурентну перевагу країни в космосі. Це дещо виходило б за межі відносин між урядом і приватним підрядником, які вже існують.

У деяких випадках комерційний сектор швидко вийшов за межі державних можливостей. Така ситуація існує в багатьох країнах, що мають космічний потенціал, і також може застосовуватися в деяких районах США.

Тому уряди деяких національних держав стикаються з вибором. Вони можуть використовувати спеціальні системи для захисту своїх супутників, навіть якщо вони можуть бути застарілими, або вони можуть використовувати інші комерційні – і потенційно більш просунуті – готові компоненти. Однак комерційне апаратне забезпечення може бути менш зрозумілим з точки зору його вразливості до кібератак.

Незважаючи на це, армія США вважає, що CASR надасть їй передові стратегічні можливості, і що потенційні ризики можна мінімізувати, активно уникаючи надмірної залежності від будь-якої окремої комерційної організації.

Метою ланцюжка постачання є перехід армії США від обмеженого кола комерційних постачальників до ширшого кола партнерів. Однак існують ризики з більшим пулом комерційних постачальників. Деякі можуть бути не в змозі задовольнити вимоги військових контрактів, можуть зіткнутися з фінансовою нестабільністю або зіткнутися з іншим тиском, який перешкоджає їхній здатності постачати критичні компоненти.

Нові пріоритети

У 2022 році відбулася кібератака на споживчий супутниковий широкосмуговий сервіс KA-Sat. Він націлився на супутники, що надають широкосмуговий зв’язок, і порушив роботу послуги.

Існує багато способів атакувати супутники іншої держави, наприклад протисупутникова зброя (ASAT), яка часто призначена для фізичного знищення або виведення з ладу космічного корабля. Однак, порівняно з ASAT, кібератаки можна здійснювати дешевшими, швидшими способами, які важче відстежити.

Частина критичної потреби в пріоритеті кібербезпеки в результаті цієї стратегії полягає в тому, що США є привабливим ринком для глобальних гравців у космосі. Таким чином, ця стратегічна зміна Міністерства оборони США, ймовірно, заохотить більше глобальних компаній до участі.

Стійкість до кібератак у космічній галузі не завжди була головним пріоритетом. Ймовірно, потрібен час, щоб це увійшло в думку головних гравців у космічному секторі.

Ця історична відсутність акценту на кібербезпеці в космосі підкреслює очевидну потребу. Існують також неузгодженості та прогалини щодо основних кібервимог до уряду та промисловості, які відрізняються залежно від позиції кожної національної держави.

Збройні сили США стверджують, що оперативна сумісність у військових стандартах – здатність різного обладнання безперебійно працювати разом – зміцнить нові державно-приватні відносини. Це також залишило відкритими двері для прийняття комерційних стандартів у певних випадках. Але існує ризик того, що відхід від військових стандартів (які зазвичай суворіші, ніж комерційні стандарти) може підірвати військові активи та призвести до тих самих несприятливих наслідків, яких стратегія прагне уникнути.

Незважаючи на найкращі наміри, складність роботи з багатьма новими комерційними партнерами також може призвести до неузгодженості в застосуванні стандартів у різних проектах і системах. Комерційні стандарти кібербезпеки навряд чи віддадуть пріоритет рівню безпеки, необхідному для військових застосувань, особливо в екстремальних умовах.

У світлі цих викликів успіх цих ініціатив залежить від наявності ініціативних і добре поінформованих лідерів. Здатність діяти в комерційному та оборонному секторах вимагатиме ключових навичок, одним із яких є інформування та освіта з кібербезпеки.

Нещодавно я розробив курс з космічної кібербезпеки для керівників із дипломами для аспірантів у партнерстві з Міжнародним космічним університетом. Цей курс для керівних кадрів залучив професіоналів із різних секторів, у тому числі юристів, регуляторів, консультантів, комерційних компаній та інвесторів.

Подолаючи розрив між різними секторами та дисциплінами, курс сприяв всебічному міждисциплінарному підходу до космічної кібербезпеки. Керівники змогли глибше зрозуміти взаємозв’язок різних систем і потенційні вразливості, які

можуть виникнути. Це не лише збагатило навчальний досвід, але й спонукало учасників мислити нестандартно та досліджувати нові стратегії пом'якшення кіберзагроз у космосі.

Оскільки Пентагон і комерційна космічна галузь просуваються вперед у своїй новаторській співпраці, важливо, щоб ті, хто приймає рішення, розуміли критичну природу кібербезпеки. Ця зміна не позбавлена проблем. Але це також відкриває можливості для інновацій і нових партнерств, які можуть сформувати майбутнє дослідження космосу та привести до нових підходів до кібербезпеки для супутників та іншої космічної інфраструктури». ***(Sharon Lemac-Vincere. US military project aims to prevent hackers targeting satellites and recognises rising threat of cyberattacks in space // Conversation Media Group Ltd (https://theconversation.com/us-military-project-aims-to-prevent-hackers-targeting-satellites-and-recognises-rising-threat-of-cyberattacks-in-space-233028). 27.06.2024).***

***

«7 травня 2024 року Офіс національного кібердиректора (ONCD) оприлюднив Звіт про стан кібербезпеки Сполучених Штатів за 2024 рік (Звіт). У Звіті окреслено головні тренди 2023 року, серед яких:

1. Розвиток ризиків для критичної інфраструктури

Противники національних держав розробляють стратегії нападу на критично важливу інфраструктуру США без шпигунської чи розвідувальної цінності, і мають намір порушити або знищити критично важливу інфраструктуру США та союзників. Ці атаки можуть бути спрямовані на те, щоб «сприяти зриву оперативних технологічних систем у критичній інфраструктурі та втручатися у бойові можливості США та союзників», а також можуть бути мотивованими для досягнення «геополітичних цілей».

2. Програми-вимагачі

«Програми-вимагачі залишаються постійною загрозою національній безпеці, громадській безпеці та економічному процвітанню». Центр розгляду скарг на злочини в Інтернеті (ICS) Федерального бюро розслідувань (ФБР) отримав на 22%

більше повідомлень про випадки програм-вимагачів від американських жертв, а вартість атак програм-вимагачів у 2023 році, про які повідомляє ICS, зросла на 74% порівняно з 2022 роком. Зловмисники більше співпрацюють і більше про розробку зловмисного програмного забезпечення, здійснення атак і збір викупу.

3. Експлуатація ланцюга поставок

Зловмисники використовують переваги складних і взаємопов'язаних відносин між постачальниками, клієнтами, продавцями та постачальниками послуг. Це надає їм можливість «доступу до жертв у великому обсязі та ускладнює зусилля захисників щодо виявлення та управління ризиками кібербезпеки».

4. Комерційні шпигунські програми

Ринок комерційного шпигунського програмного забезпечення значно виріс, і той, хто запропонує найвищу ціну, може отримати доступ до складних і інвазивних наскрізних інструментів кіберспостереження для віддаленого доступу до електронних пристроїв, моніторингу та вилучення вмісту та маніпулювання компонентами без відома чи згоди власника пристрою. Більше того, ці загрозливі суб'єкти тепер націлюються на «журналістів, активістів, правозахисників та урядовців все частіше». Комерційне шпигунське програмне забезпечення також «використовується проти урядового персоналу США, інформації та комп'ютерних систем, створюючи значні контррозвідувальні та безпекові ризики для Сполучених Штатів».

5. Штучний інтелект (AI)

Швидкий і безперервний розвиток штучного інтелекту створить можливості та виклики для управління кіберризиками. Хоча штучний інтелект надасть можливості для захисту критичної інфраструктури, кіберзлочинці, хакери та інші «можуть використовувати ці можливості для проведення фішингових кампаній, інформаційних операцій та іншої зловмисної кіберактивності». Для захисту конфіденційності американців можуть знадобитися заходи безпеки щодо використання та розвитку технологій ШІ.

У звіті також описано 12 заходів, вжитих Федеральним урядом протягом звітного періоду, серед яких:

Встановлення та використання кібервимог для захисту критичної інфраструктури, у тому числі шляхом розробки та гармонізації нормативних вимог у багатьох секторах критичної інфраструктури.

Розширення федерального співробітництва та партнерства для кращої підтримки кіберзахисників, у тому числі шляхом посилення оперативної співпраці, покращення потенціалу Агентства управління ризиками сектору (SRMA) та інтеграції можливостей федерального кіберзахисту.

Поліпшення готовності до інцидентів і реагування на них шляхом швидкого обміну інформацією про загрози, надання пріоритетної підтримки жертвам і перегляду значних інцидентів і кампаній для отримання отриманих уроків.

Знищення та приниження активності противника з використанням усіх інструментів національної влади, що призводить до скоординованих, потужних кампаній зриву проти широкого кола зловмисних кіберакторів.

Швидкий і масштабний захист федеральних мереж, зокрема шляхом інтеграції принципів Zero Trust Architecture у федеральне підприємство, модернізації застарілих технологічних систем і розширення використання спільних служб.

Зміцнення національної робочої сили в кіберпространстві, зокрема шляхом оприлюднення Національної стратегії щодо робочої сили та освіти в кіберпространстві (NCWES) і взаємодії з працівниками, роботодавцями, студентами та освітянами по всій країні.

Підвищення безпеки програмного забезпечення для створення безпечніших продуктів і послуг, у тому числі шляхом вдосконалення принципів безпеки за проектом, номенклатури програмного забезпечення (SBOM) і безпечних для пам’яті мов програмування.

Створення цифрової економіки, яка розширює можливості та захищає споживачів, у тому числі шляхом запуску програми сертифікації та маркування Cyber Trust Mark у США та сприяння конкуренції та підзвітності в усій галузі технологій.

Інвестування в стійкі технології наступного покоління в економіці чистої енергії, видача виконавчого наказу, який керуватиме федеральними зусиллями, пов’язаними зі штучним інтелектом, і вирішення проблем безпеки, наявних у технічних основах Інтернету.

Управління ризиками для безпеки та конфіденційності даних шляхом забезпечення безпечної транскордонної торгівлі з багатим даними та сприяння розвитку технологій підвищення конфіденційності.

Підвищення стійкості в усьому світі шляхом створення коаліцій країн-однодумців для надання підтримки жертвам програм-вимагачів та інших кібератак, узгодження національної політики та сприяння безпечним і стійким глобальним ланцюжкам поставок.

У звіті зазначається, що «Федеральний уряд спиратиметься на досягнення минулого року, продовжуватиме впровадження нещодавно опублікованої версії Плану впровадження національної стратегії кібербезпеки та Національної стратегії щодо робочої сили та освіти в кіберпространстві та адаптуватиме свій підхід для вирішення нових проблем і можливостей. представлений стратегічним ландшафтом, що розвивається». ***(Trisha Sircar. The Office of the National Cyber Director Releases 2024 Report on Cybersecurity Posture // National Law Forum, LLC (https://natlawreview.com/article/office-national-cyber-director-releases-2024-report-cybersecurity-posture). 26.06.2024).***

***

«У стрімко змінюваному ландшафті цифрової ери кібербезпека стала першорядною проблемою для окремих осіб, організацій та урядів у всьому світі. Поширення підключених пристроїв, Інтернету речей (IoT), хмарних обчислень і соціальних медіа створило взаємопов’язаний світ, наповнений можливостями та викликами. Оскільки дані стають новою валютою, їх захист від кіберзагроз стає надзвичайно важливим. Захистіть цінні дані вашого бізнесу за допомогою команди Managed IT Services Fresno.

Цей блог досліджує багатогранну сферу кібербезпеки, проливаючи світло на важливість захисту даних у зв'язаному світі та стратегії її досягнення.

Важливість кібербезпеки

Захист персональних даних

У сучасну цифрову епоху люди довіряють величезні обсяги особистої інформації онлайн-платформам і службам. Від профілів у соціальних мережах і онлайн-банкінгу до медичних записів і транзакцій електронної комерції – особисті дані всюди. У разі зламу ці дані можуть призвести до крадіжки особистих даних, фінансових втрат і порушення конфіденційності. Заходи кібербезпеки мають важливе значення для захисту людей від цих ризиків і забезпечення безпеки їх цифрового життя.

Захист бізнес-активів

Для компаній дані є цінним активом, який стимулює прийняття рішень, інновації та зростання. Однак такі кіберзагрози, як витік даних, атаки програм-вимагачів і крадіжка інтелектуальної власності, можуть серйозно вплинути на репутацію організації, фінансову стабільність і безперервність роботи. Ефективні стратегії кібербезпеки допомагають компаніям захистити конфіденційну інформацію, зберегти довіру клієнтів і дотримуватися нормативних вимог.

Забезпечення національної безпеки

На національному рівні кібербезпека має вирішальне значення для захисту критичної інфраструктури, державних даних і систем захисту від кібератак. Як національні держави, так і кіберзлочинці націлюються на ці активи, щоб порушувати послуги, викрадати секретну інформацію та здійснювати політичний вплив. Надійні рамки кібербезпеки необхідні для захисту національної безпеки та підтримки цілісності державних установ.

Ландшафт загроз, що розвивається

Складні кібератаки

З розвитком технологій змінюються і тактики та методи, які використовують кіберзлочинці. Сучасні кібератаки стають все більш складними, використовують штучний інтелект (ШІ), машинне навчання та автоматизацію, щоб обійти

традиційні засоби захисту. Фішингові атаки, зловмисне програмне забезпечення та експлойти нульового дня — це лише кілька прикладів загроз, що розвиваються, з якими мають орієнтуватися організації та окремі особи.

Розвиток програм-вимагачів

Атаки програм-вимагачів стали поширеною та дуже руйнівною кіберзагрозою. Ці атаки спрямовані на широкий спектр організацій, від малих підприємств до великих корпорацій і навіть державних установ, таких як лікарні та школи. Фінансові та операційні наслідки програм-вимагачів можуть бути руйнівними, що підкреслює необхідність проактивних заходів кібербезпеки.

Внутрішні загрози

Хоча зовнішні загрози привертають значну увагу, внутрішні загрози становлять не менш критичний ризик. Інсайдерські загрози можуть виходити від співробітників, підрядників або ділових партнерів, які мають доступ до конфіденційної інформації. Ці особи можуть навмисно чи ненавмисно скомпрометувати безпеку даних через такі дії, як крадіжка даних, шпигунство або недбалість. Щоб подолати внутрішні загрози, потрібне поєднання технічних рішень, навчання співробітників і надійних засобів контролю доступу.

Стратегії кібербезпеки для підключеного світу

Реалізація надійної автентифікації

Одним із основоположних елементів кібербезпеки є надійна автентифікація. Одних паролів часто недостатньо для захисту конфіденційних даних. Багатофакторна автентифікація (MFA) додає додатковий рівень безпеки, вимагаючи від користувачів надати кілька форм підтвердження, наприклад пароль і відбиток пальця або одноразовий код, надісланий на мобільний пристрій. Запровадивши MFA, організації можуть значно знизити ризик несанкціонованого доступу.

Шифрування та захист даних

Шифрування є критично важливим інструментом для захисту даних як під час передачі, так і в стані спокою. Перетворюючи дані в закодований формат, шифрування гарантує, що навіть у разі перехоплення даних або доступу до них без

авторизації вони залишаються нечитабельними. Організації повинні впроваджувати протоколи шифрування для конфіденційної інформації, такої як фінансові дані, персональні ідентифікатори та конфіденційна бізнес-інформація. Крім того, мають існувати безпечні рішення для резервного копіювання, щоб забезпечити можливість відновлення даних у разі кіберінциденту.

Регулярне оновлення програмного забезпечення та керування виправленнями

Кіберзлочинці часто використовують уразливості програмного забезпечення для отримання несанкціонованого доступу до систем і даних. Регулярне оновлення програмного забезпечення та застосування патчів безпеки є важливими для усунення цих вразливостей і захисту від нових загроз. Організації повинні встановити надійний процес керування виправленнями, щоб гарантувати, що всі системи та програми оновлюються з останніми виправленнями безпеки.

Навчання та обізнаність співробітників

Людська помилка є суттєвим фактором багатьох інцидентів кібербезпеки. Співробітники можуть ненавмисно поставити під загрозу безпеку, піддавшись фішингу, використовуючи ненадійні паролі або неправильно обробляючи конфіденційну інформацію. Комплексне навчання з кібербезпеки та програми підвищення обізнаності є важливими для навчання співробітників передовим практикам, потенційним загрозам і тому, як реагувати на підозрілу діяльність. Розвиваючи культуру обізнаності про кібербезпеку, організації можуть зменшити ризики порушень безпеки, пов’язаних з людьми.

Безпека та сегментація мережі

Заходи безпеки мережі, такі як брандмауери, системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS), відіграють вирішальну роль у захисті цифрової інфраструктури організації. Ці інструменти допомагають контролювати мережевий трафік, виявляти зловмисні дії та блокувати спроби несанкціонованого доступу. Сегментація мережі додатково підвищує безпеку, розділяючи мережу на менші ізольовані сегменти. Такий підхід обмежує поширення кіберзагроз і мінімізує вплив потенційного зламу.

Реагування на інциденти та планування відновлення

Незважаючи на найкращі профілактичні заходи, жодна організація не застрахована від кіберінцидентів. Чітко визначений план реагування на інциденти необхідний для швидкого й ефективного усунення порушень безпеки. У плані реагування на інцидент описано кроки, яких необхідно вжити у випадку кібератаки, включаючи виявлення загрози, локалізацію збитку, усунення загрози та відновлення постраждалих систем. Регулярне тестування та оновлення плану реагування на інциденти забезпечують готовність реагувати на нові загрози. Якщо у вас виникнуть труднощі під час планування чи відновлення даних, зверніться до спеціалістів IT Consulting Sacramento.

Впровадження архітектури нульової довіри

Традиційна модель безпеки, яка спирається на надійну внутрішню мережу та захисний периметр, потребує перегляду перед обличчям сучасних кіберзагроз. Архітектура нульової довіри — це структура безпеки, яка працює за принципом «ніколи не довіряй, завжди перевіряй». Він вимагає постійної перевірки користувачів, пристроїв і програм, незалежно від їхнього місцезнаходження. Прийнявши підхід нульової довіри, організації можуть підвищити безпеку шляхом мінімізації ризику несанкціонованого доступу та бокового переміщення в мережі.

Роль нових технологій у кібербезпеці

Штучний інтелект і машинне навчання

Штучний інтелект (AI) і машинне навчання (ML) трансформують сферу кібербезпеки. Ці технології сприяють створенню складних систем виявлення загроз і реагування на них, які можуть аналізувати великі обсяги даних у режимі реального часу, щоб ідентифікувати моделі та аномалії, що вказують на кіберзагрози. Рішення безпеки на основі штучного інтелекту можуть автоматично адаптуватися до нових загроз, забезпечуючи проактивний захист від нових кібератак.

Технологія блокчейн

Технологія блокчейн, відома своїми децентралізованими та незмінними характеристиками, демонструє великий потенціал для підвищення кібербезпеки. Він може захищати транзакції, захищати цілісність даних і перевіряти

автентичність цифрових ідентифікаторів. Його децентралізований характер ускладнює маніпулювання даними для кіберзлочинців, пропонуючи надійне рішення для захисту конфіденційної інформації та забезпечення прозорості цифрових взаємодій.

Безпека Інтернету речей (IoT).

Широке впровадження пристроїв IoT створює нові виклики безпеці, оскільки ці пристрої часто не мають потужних функцій безпеки та можуть виступати в якості точки входу для кібератак. Захист пристроїв IoT вимагає багатогранного підходу, включаючи надійну автентифікацію, регулярні оновлення мікропрограми та сегментацію мережі. Крім того, організації повинні впроваджувати протоколи безпеки та стандарти безпеки для Інтернету речей, щоб зменшити ризики, пов'язані з підключеними пристроями.

Висновок

У цифрову епоху кібербезпека є фундаментальним аспектом захисту даних у підключеному світі. Зростаюча складність кіберзагроз, зростання кількості програм-вимагачів і розповсюдження пристроїв Інтернету речей підкреслюють потребу в надійних заходах кібербезпеки. Запровадивши надійну автентифікацію, шифрування, регулярні оновлення та навчання співробітників, організації можуть покращити рівень безпеки та зменшити ризики, пов'язані з кіберзагрозами. Крім того, впровадження нових технологій, таких як штучний інтелект, блокчейн і квантові обчислення, може надати нові шляхи захисту даних. Оскільки цифровий ландшафт продовжує розвиватися, проактивний і комплексний підхід до кібербезпеки буде необхідним для захисту особистих, бізнесових і національних активів». ***(Cybersecurity in the Digital Age: Protecting Data in a Connected World // Big News Network (https://www.bignewsnetwork.com/news/274434694/cybersecurity-in-the-digital-age-protecting-data-in-a-connected-world). 27.06.2024).***

***

«Німеччина посилює заходи безпеки під час підготовки до Чемпіонату Європи з футболу, борючись із широким спектром загроз, включаючи тероризм, хуліганство та кібербезпеку.

Безпека є «головним пріоритетом» для Німеччини, оскільки вони готуються прийняти майбутній Чемпіонат Європи з футболу.

Виступаючи на прес-конференції за десять днів до офіційного старту Євро-2024 у вівторок, міністр внутрішніх справ Німеччини Ненсі Фезер заявила, що нація готується до «усіх мислимих небезпек».

Вона назвала такі загрози, як тероризм, хуліганство та кібератаки, але сказала, що співпраця «йде дуже добре» на федеральному рівні та рівні штатів.

«Поліція матиме потужну присутність скрізь, де пересувається велика кількість людей. Це буде серйозна робота для поліції штату та федеральної поліції, але це також має вирішальне значення для турніру», – сказала вона.

Тимчасовий поліцейський центр був створений у Північному Рейні-Вестфалії, де розташовані чотири з десяти стадіонів, на яких проводяться ігри.

«Ми ніколи не можемо гарантувати 100% безпеки», — сказав Герберт Реул, губернатор землі Північний Рейн-Вестфалія, але додав, що «ми можемо підготуватися якнайкраще»…». ***(Germany preparing for 'all conceivable' security threats during Euro 2024, interior minister says // Euronews (https://www.euronews.com/my-europe/2024/06/04/germany-preparing-for-all-conceivable-security-threats-during-euro-2024-interior-minister-?utm_source=flipboard&utm_content=euronews%2Fmagazine%2FNews). 04.06.2024).***

***

«Наприкінці квітня Рада міністрів Польщі опублікувала проект змін до Закону про національну систему кібербезпеки. Закон імплементує положення Директиви NIS 2 у польське законодавство. Його набрання чинності стане революцією для багатьох підприємств, на які будуть накладені нові зобов’язання.

Звертаємо вашу увагу, що в проект поправок можуть бути внесені зміни.

1. Кого це стосується?

Нові правила значно розширять перелік секторів, які будуть зобов’язані застосовувати норми кібербезпеки. У результаті, за підрахунками Мінцифри, приблизно 38 тис організації можуть бути зобов'язані адаптуватися до нових правил. Зобов'язання поширюватимуться на підприємства та організації, які працюють у таких секторах:

Додаток № 1 до проекту змін

Енергія

Транспорт

Банківська справа та інфраструктура фінансового ринку

Охорона здоров'я

Постачання та розподіл питної води

Стічні води

Цифрова інфраструктура

Управління послугами ІКТ

Зовнішній простір

державне управління

Виробництво, виробництво та розподіл хімічних речовин

Виробництво, переробка та розподіл харчових продуктів

виробництво

Додаток № 2 до проекту змін

Поштові послуги

Поводження з відходами

Постачальники цифрових послуг

дослідження

Нові зобов'язання стосуватимуться не всіх підприємств. Вимога щодо адаптації до нових нормативних актів залежатиме від розміру суб’єкта господарювання – закон застосовуватиметься лише до великих або середніх підприємств у розумінні Додатку I до Регламенту Комісії (ЄС) № 651/2014.

Крім того, Закон визначає суб’єкти, до яких застосовуватимуться його положення, незалежно від їх розміру. До них увійдуть, наприклад, постачальники кваліфікованих довірчих послуг і підприємці в сфері електронних комунікацій.

Крім того, за рішенням компетентного органу малі та мікропідприємства можуть бути зобов’язані застосовувати положення Закону, якщо вони працюють у секторах, зазначених у таблиці вище, і мають особливості, зазначені в проекті змін (наприклад, вони є єдиними ті, хто надає послуги ключового значення для критичної соціальної чи економічної діяльності або збій у наданні їхніх послуг призведе до серйозної загрози державній безпеці).

Суб’єкти, зобов’язані застосовувати положення, будуть поділені на ключові та важливі. Проект змін передбачає досить складні критерії віднесення суб’єктів до однієї з цих двох категорій.

2. Які зобов'язання запровадять нові положення?

Суб’єкти, на яких поширюються розглянуті положення, будуть зобов’язані:

а. Незалежна реєстрація в списку, який веде Міністерство цифровізації.

Підприємства, які працюють у зазначених вище секторах, повинні самостійно оцінити, чи стосуватимуться їх нові правила. Лише у виняткових випадках адміністративні органи визначатимуть зобов’язаних суб’єктів згідно з рішенням. Щоб спочатку оцінити, чи застосовуватимуться нові правила до певної організації, ми пропонуємо скористатися інструментом, створеним Bird & Bird – NIS2 Tool – який простим і доступним способом проведе вас через індивідуальні кваліфікаційні вимоги як зобов’язаної організації згідно з Директива NIS 2 Звертаємо вашу увагу лише на те, що цей інструмент створений на основі директиви NIS2, а не на основі проекту змін до польських правил, які дещо відрізняються від директиви NIS2.

б) Впровадження системи управління інформаційною безпекою.

Значні організації та важливі організації повинні будуть запровадити систему управління інформаційною безпекою для процесів, що впливають на надання послуг.

Система управління інформаційною безпекою включає низку заходів, що дозволяють управляти ризиками, наприклад, систематичну оцінку ризику

інциденту та управління ним, відповідні технічні та організаційні заходи, управління інцидентами. Якщо система управління інформаційною безпекою відповідає вимогам стандартів PN-EN ISO/IEC 27001 та PN-EN ISO/IEC 22301, зазначені вище зобов’язання вважаються виконаними.

c. Забезпечення нагляду за виконанням вищезазначеного обов'язків керівника ключової організації або важливої організації.

керівник Відповідальність за правильне виконання посадових обов'язків несе. Керівниками суб’єкта господарювання можуть бути, наприклад, члени правління, повний учасник товариства з обмеженою відповідальністю, учасники повного товариства. Керівник суб'єкта буде відповідати, серед іншого, за: для впровадження, застосування та перевірки системи управління інформаційною безпекою, надання фінансових ресурсів для виконання обов’язків та забезпечення знань персоналу з кібербезпеки.

d. Підготовка документації з безпеки інформаційної системи.

Розробка документації безпеки для IT-системи, яка використовується для надання послуги, також призначена для забезпечення кібербезпеки значущих суб’єктів та організацій. Він має складатися з:

- нормативна документація, в тому числі: система управління інформаційною безпекою, захист інфраструктури або система управління безперервністю обслуговування
- експлуатаційна документація, яка засвідчує виконання зобов'язань, що містяться в нормативній документації.

e. Повідомлення про інциденти.

Ключові та важливі суб’єкти будуть зобов’язані повідомляти відповідну CSIRT про серйозні інциденти кібербезпеки. Зобов’язані суб’єкти підприємницької діяльності повинні будуть зробити це протягом визначеного терміну з моменту виявлення такої події:

- раннє попередження про серйозний інцидент має бути повідомлено протягом 24 годин після виявлення інциденту (виняток: підприємець електронних комунікацій - 12 годин)

- повідомлення про серйозний інцидент протягом 72 годин після його виявлення (виняток: постачальник довірчих послуг – 24 години).

f. Проведення аудиту безпеки.

Ключові та важливі суб'єкти щонайменше раз на два роки. будуть зобов'язані проводити аудит безпеки інформаційної системи, яка використовується для надання послуг,

3. Якими будуть штрафи за невиконання?

Про важливість нової норми свідчать санкції, передбачені за невиконання зобов’язань. За порушення нормативно-правових актів на головних і важливих суб’єктів господарювання може бути накладено штраф у розмірі:

- до 10 мільйонів євро або 2% доходів, отриманих у попередньому фінансовому році, але не менше 20 000 злотих - у випадку ключових суб’єктів,
- до 7 мільйонів євро або 1,4% доходів, отриманих у попередньому фінансовому році, не менше 15 000 злотих – у випадку важливих суб’єктів.

В обох випадках застосовується більша сума. Якщо порушення також спричинило пряму та серйозну загрозу безпеці, життю та здоров’ю або могло завдати серйозної шкоди майну чи серйозних труднощів у наданні послуг, влада зможе накласти штраф у розмірі до 100 мільйонів злотих.

Керівник підрозділу також нестиме матеріальну відповідальність за порушення регламенту, незалежно від ключового чи важливого суб’єкта. Розмір фінансового штрафу не може перевищувати 600% винагороди, отриманої покараною особою, розрахованої згідно з правилами визначення грошового еквівалента відпустки.

4. Скільки часу є на підготовку?

Наразі закон знаходиться на стадії громадського обговорення. У Мінцифри планують, що він набуде чинності в четвертому кварталі цього року. Однак це не означає, що після набуття Законом чинності необхідно буде продемонструвати дотримання всіх зобов’язань.

Суб’єкти господарювання, які вже відповідають умовам для визнання ключовими та важливими суб’єктами господарювання, матимуть 6 місяців для

впровадження нових норм з дати набрання чинності поправками. Суб'єкти, які стануть ключовими або важливими після набрання чинності поправкою, повинні будуть адаптуватися до своїх зобов'язань протягом 6 місяців після виконання умов для визнання ключовим або важливим суб'єктом.

Перший аудит необхідно буде провести протягом 12 місяців з дати виконання умов для визнання ключовою або важливою юридичною особою.

5. Для кого це важливо?

Підприємства, на які поширюватимуться нові правила, повинні якнайшвидше розпочати процес впровадження нових правил. Постачальники хмарних та ІКТ-послуг, а також виробники регульованих товарів повинні звернути на це особливу увагу.

Практичний досвід щодо імплементації існуючих правил кібербезпеки показує, що відповідність вимогам законодавства та впровадження необхідних змін (зокрема наймання людей у внутрішню команду, впровадження ІТ-інструментів) може тривати до року для суб'єктів, на які досі не поширювалися ці правила». ***(Tomasz Zalewski, Kuba Ruiz, Aleksandra Cywinska and Michal Smiechowski. Rewolucja w obszarze cyberbezpieczeństwa - projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa // Bird & Bird LLP (https://www.twobirds.com/pl/insights/2024/poland/240607-rewolucja-w-obszarze-cyberbezpieczenstwa). 07.06.2024).***

***

«Минулого місяця Офіс Уповноваженого з питань інформації Великобританії (ICO) опублікував свій звіт про «Навчання на помилках інших» (ICO Звіт). Звіт ICO, зібраний на основі фактичних звітів про порушення даних, надісланих до ICO, заглиблюється в найпоширеніші проблеми з інформаційною безпекою – і як найкраще їх уникнути.

У 2023 році ICO отримала понад 3000 повідомлень про кіберзломи, причому найбільш інтенсивна діяльність була у фінансовому, роздрібному та освітньому секторах. У 2024 році також спостерігалося збільшення активності в цьому

просторі. З травня 2022 року по травень 2023 року 25,9% порушень даних, про які повідомили в ICO, були пов'язані з кібернетичною інформацією. Цей показник зріс до 32,5% за той самий період наступного року, що на 6,6% більше за кіберзломи. Оскільки ми з нетерпінням чекаємо кінця 2024 року та далі, очікується, що ці цифри продовжуватимуть зростати, оскільки кібератаки стануть різноманітнішими та витонченішими.

Отже, згідно з ICO, які найпоширеніші причини порушення безпеки та як їх уникнути?

Шкідливе програмне забезпечення

Що це? «Шкідливе програмне забезпечення» — це зловмисне програмне забезпечення, яке має намір порушити роботу комп'ютерних систем, пошкодити їх або отримати доступ до них. Відповідно до звіту ICO, кількість атак зловмисного програмного забезпечення зростає з кожним роком, причому найчастіше використовують програмне забезпечення-вимагач – форму шкідливого програмного забезпечення, яке використовується злочинцями та передбачає шифрування файлів організації, щоб запобігти доступу будь-кого в організації. Зловмисне програмне забезпечення найбільш поширене через фішингові електронні листи або через використання вразливостей програмного забезпечення для віддаленого робочого столу.

Як краще захиститися від нього? Багатофакторна аутентифікація; часте навчання персоналу з безпеки; регулярне тестування планів реагування та відновлення.

Фішинг

Що це? Фішинг полягає в тому, що зловмисники вводять в оману людей для виконання дій, які приносять користь зловмиснику (на шкоду відповідній особі та/або організації). Це включає надсилання конфіденційної інформації чи грошей зловмиснику або клацання посилання зловмисника, яке додає вірус до комп'ютера, який потім потенційно може заразити всю мережеву інфраструктуру організації. Зазвичай це робиться електронною поштою, текстовим повідомленням або телефонним дзвінком – покладаючись на те, що особа вірить, що повідомлення

зловмисника справжнє. Департамент науки, інновацій і технологій у рамках свого опитування про порушення кібербезпеки за 2024 рік заявив, що 56% компаній, які повідомили про порушення минулого року, назвали фішингові атаки найбільш руйнівними для організацій. Це опитування також показало, що кількість фішингових атак зростає (79% у 2023–2024 роках порівняно з 72% у 2017 році).

Як краще захиститися від нього? Навчіть персонал остерігатися відкривати або натискати вміст електронних листів від незнайомих відправників; засоби захисту від спуфінгу, щоб запобігти зловмисникам імітувати мережевий домен вашої організації.

Атаки грубою силою

Що це? Зловмисники намагатимуться вгадати імена користувачів і паролі методом проб і помилок із різними комбінаціями. Зловмисники використовують широкий спектр методів, зокрема використання штучного інтелекту (ШІ), щоб спробувати багато комбінацій за короткий проміжок часу, або використання загальних фраз чи відомих паролів для систематичного отримання несанкціонованого доступу. У нещодавньому звіті Microsoft про цифровий захист зазначено, що тільки в квітні 2023 року вона зазнавала 11 000 атак грубою силою на секунду.

Як краще захиститися від нього? Уникайте паролів, що містять відповідну або особисту інформацію; унікальні паролі для різних облікових записів; CAPTCHA для запобігання спробам автоматичного вгадування пароля; відключити невикористовувані облікові записи.

Відмова в обслуговуванні (DoS)

Що це? Атака DoS спрямована на те, щоб веб-сайт або мережа не працювали належним чином, перевантажуючи систему, створюючи надзвичайно високий рівень мережевого трафіку. Це також може мати форму розподіленої атаки на відмову в обслуговуванні (DDoS), яка все ще перевантажує систему, але з кількох підключених пристроїв, що робить атаку набагато важчою для зупинки та/або підтримки. Зазвичай зловмисник виконує DoS-атаку з метою грошової вигоди або соціальних чи політичних причин. Ознаки DoS-атаки включають винятково низьку

швидкість мережі, не завантаження веб-сторінок або втрату з'єднання. Управління з питань фінансового контролю (FCA) повідомило, що DDoS-атаки спричинили 25% хакерських інцидентів, про які повідомили FCA, за перші 6 місяців 2022 року, порівняно з лише 4% за той самий період у 2021 році.

Як краще захиститися від нього? Впроваджуйте служби, які можуть розпізнавати законне збільшення мережевого трафіку в порівнянні з порушеннями від можливих атак; регулярно перевіряйте брандмауери та маршрутизатори, щоб переконатися, що вони правильно налаштовані; часто тестувати безперервність бізнесу та плани на випадок аварій.

Атака на ланцюг поставок

Що це? Організацію атакують через скомпрометовані продукти або послуги, які їй надає постачальник, що призводить до потенційного порушення систем організації. Це показує небезпеку довіри стороннім постачальникам без відповідної належної обачності.

Як краще захиститися від нього? Впроваджувати програму управління ризиками ланцюга постачання для перегляду, моніторингу та керування системами та процесами в ланцюзі постачання організації; бути повністю обізнаним про те, якою інформацією ділиться постачальник і як вона обробляється; провести належну перевірку потенційних нових постачальників, щоб переконатися, що вони мають відповідні заходи безпеки; регулярно переглядати/аудит існуючих постачальників.

Людська помилка

Наскільки це ймовірно? Звіт про ICO підсилює роль самих людей у сприянні атаці або злому через бездіяльність або виконання дії неправильно. У звіті Verizon про порушення даних за 2023 рік зазначено, що 74% усіх пляжів пов'язані з людським фактором (включно з усіма типами атак, які ми вже описали вище). Звіт ICO також визначає, як неправильні конфігурації, зроблені людьми, є одними з найшкідливіших помилок, що спричиняють витік даних. Це включає конфігурації безпеки, які погано обслуговуються або налаштовані неточно (наприклад, залишення елементів керування безпекою за замовчуванням на відміну від

адаптації налаштувань до потреб організації). Неправильна конфігурація може дати зловмисникам можливість отримати доступ до систем і серверів, вимкнути погано підтримувані елементи керування безпекою та викрасти дані з невеликим опором.

Як краще захиститися від нього? Прийміть підхід до безпеки за проектом; перевірити процедури безпеки перед тим, як їх додати до живих середовищ; навчити персонал чому трапляються помилки та як найкраще керувати засобами контролю; багаторазові перевірки контролю якості та системи затвердження безпеки за участю щонайменше двох осіб; реагуйте на системні попередження або необхідні оновлення та виправлення якнайшвидше.

З нетерпінням – що це означає для вас

Організаціям зростає потреба більш серйозно ставитися до інформаційної безпеки. Стає все більш очевидним, що «загальних» порад і рішень буде недостатньо – організації повинні справді розуміти власні специфічні слабкі сторони інформаційної безпеки та діяти відповідно, щоб усунути ці слабкі місця та якомога швидше посилити свій захист.

Важливо також визнати, що методи кібератак постійно розвиваються та розвиваються, і організації повинні забезпечити їх розвиток, щоб відповідним чином реагувати. Наприклад, загроза фішингових електронних листів продовжуватиме зростати в міру розвитку штучного інтелекту – великі мовні моделі, такі як Chat GPT, використовуються для сприяння фішинговому шахрайству (зменшення таких проблем, як погана орфография/граматика), а також спостерігається зростання у використанні клонування голосу та відео «deepfake» для копіювання осіб, відомих об’єкту зловмисника. Під час атак Brute Force також розробляються нові технології, які можуть обійти паролі відбитків пальців, використовуючи слабкі місця в системі автентифікації відбитків пальців смартфонів.

Кожна монета має дві сторони. Штучний інтелект і машинне навчання також покладаються на покращення захисту від кібератак. Наприклад, машинне навчання тепер використовується для вивчення моделей мережевого трафіку, щоб виявляти аномалії з частотою трафіку – і, отже, швидко реагувати на DoS-атаку. Для

організацій вкрай важливо бути в курсі цих подій, щоб було чітке розуміння того, з якими новими проблемами вони можуть зіткнутися, і які інноваційні рішення можуть пом’якшити загрози, пов’язані з кібератакою.

Тим часом у звіті ICO висвітлюється кілька чітких дій, щоб запобігти потраплянню організацій у пастку того, що ICO описує як «цілком запобігти» витоку кіберданих:

- використовувати багатофакторну аутентифікацію для захисту зовнішніх з'єднань;
- контролювати системи та діяти, коли виявлено незвичайну/несподівану активність;
- використовувати надійні й унікальні паролі для внутрішніх облікових записів, особливо для привілейованих облікових записів або облікових записів адміністратора;
- належним чином перевірити захист кібербезпеки та якнайшвидше усунути будь-які відомі недоліки (і протягом 14 днів для будь-яких критичних прогалин, які потребують виправлень); і
- реагувати на сповіщення, отримані від програмного забезпечення для захисту кінцевих точок (захист від зловмисних програм/вірусів), і проводити подальші перевірки після видалення шкідливих програм». ***(Junior Mbulu. Fortifying defences: ICO publishes new report on common information security mistakes and pitfalls // TLT LLP (https://www.tlt.com/insights-and-events/insight/fortifying-defences-ico-publishes-new-report-on-common-information-security-mistakes-and-pitfalls/). 10.06.2024).***

***

«Польща витратить понад 3 мільярди злотих (760 мільйонів доларів) на посилення кібербезпеки, заявив міністр цифровізації в понеділок після того, як державне інформаційне агентство PAP постраждало від, за словами влади, ймовірної російської кібератаки.

Оскільки в неділю в Польщі відбудуться вибори до Європейського парламенту, влада перебуває у стані підвищеної готовності щодо спроб Москви втрутитися у голосування. Побоювання, які посилилися в п’ятницю, коли на РАР з’явилася неправдива стаття про військову мобілізацію.

Варшава неодноразово звинувачувала Москву в спробі дестабілізувати Польщу через її роль у постачанні військової допомоги сусідній Україні, Росія звинувачення відкинула.

«Ми хочемо виділити понад 3 мільярди злотих на «Кіберщит», – сказав Кшиштоф Гавковський на прес-конференції. «Сьогодні Польща знаходиться на передовій кіберборотьби з Росією. На Польщу припадає найбільше атак».

Гавковський повідомив, що в неділю і понеділок Польща заблокувала кілька кібератак на критичну інфраструктуру.

«РФ має одну мету - дестабілізувати ситуацію і забезпечити користь тим силам, які підтримують розпад ЄС», - сказав він.

Посольство Росії у Варшаві в п'ятницю заявило, що нічого не знає про атаку на РАР. Він відкинув звинувачення в тому, що Росія намагається дестабілізувати Польщу.

Польща також пов’язує Росію з інцидентами саботажу та підпалів на своїй території та каже, що російські спецслужби активно намагаються збирати інформацію про поставки зброї в Україну після повномасштабного вторгнення Росії в лютому 2022 року.

Вона оголосила про відновлення комісії з розслідування російського впливу». ***(Poland to boost cybersecurity after fake news attack // Reuters (https://www.reuters.com/technology/cybersecurity/poland-spend-3-bln-zlotys-cybersecurity-after-attack-news-agency-2024-06-03/). 03.06.2024).***

***

«Після свого створення у 2021 році Європейський центр компетенції з кібербезпеки (ECCC) знаходиться на порозі автономної роботи та готовий взяти на себе управління грантами Horizon Europe у цій сфері.

Це наблизить центр до основної амбіції щодо об’єднання інвестицій у дослідження, розробки та розгортання та створення єдиної європейської екосистеми для зміцнення європейського кіберзахисту та координації планування Horizon Europe та Програми цифрової Європи (DEP).

Пізніше цього року ECCC візьме на себе реалізацію дзвінків Horizon Europe у сфері кібербезпеки, а Європейська комісія передасть цю функцію, коли центр стане фінансово незалежним.

На дослідження кібербезпеки припадає близько третини витрат у Кластері 3 Horizon Europe «Громадянська безпека для суспільства», бюджет якого у 2024 році становить 60,4 мільйона євро. Наразі ECCC підтримує Генеральний директорат з комунікацій, DG Connect, у впровадженні дзвінків, а дати повної передачі до ЄЦКК ще немає.

В останні роки спостерігається сплеск кібератак на критичну інфраструктуру, таку як лікарні та енергетичні мережі. У той час як нові закони, зокрема Закон про кібер-стійкість і Закон ЄС про кібер-солідарність, спрямовані на встановлення суворіших правил для цифрових продуктів і їх розгортання, дослідження та інновації відіграють ключову роль, оскільки загрози стають все складнішими.

«Технології стають настільки поширеними, що нам потрібно паралельно забезпечити належний рівень захисту не лише на фінансовому ринку, який історично був краще захищеним, але й у секторі охорони здоров’я, у транспорті тощо», — заявив керівник ECCC. Режисер Лука Тальяретті розповів Science|Business.

Керівна рада ECCC складається з представників держав-членів і Комісії, але Тальяретті хоче якомога більше взаємодіяти з галуззю при визначенні пріоритетів і допомагати створювати партнерства. Центр приділяє велике значення підтримці малого та середнього бізнесу. «Це компанії, які не мають ресурсів, необхідних для захисту», — сказав він.

Що стосується розробки нових технологій кібербезпеки, він не вважає, що Європа перебуває в поганому становищі, але каже, що їй потрібно активізувати

зусилля, щоб залишатися конкурентоспроможною. «Вам потрібно продовжувати бігти, щоб не відстати», — сказав Тальяретті.

ЕССС підтримується 27 національними координаційними центрами (NCC), які сприяють обміну між урядом, промисловістю та дослідниками на національному рівні та спрощують пошук партнерів для транснаціональних проектів. Вони нададуть ЕССС зворотній зв'язок щодо того, які сфери слід фінансувати.

Центр уже взяв на себе управління чотирма грантами DEP, підтримуючи 113 проектів по всій Європі, і сподівається розподілити 700 мільйонів євро фінансування до кінця року. DEP зосереджена на розгортанні цифрових технологій, а ЄС покриває 50% вартості проекту.

ЕССС також буде взаємодіяти з іншими програмами, які мають кібернетичний елемент, включаючи Європейський оборонний фонд (EDF), щоб уникнути дублювання. EDF нещодавно опублікував свої конкурси на 2024 рік, включаючи конкурс на суму 48 мільйонів євро на розробку кооперативного кібернетичного ряду нового покоління – віртуального середовища, яке використовується для навчання або технологічного розвитку.

Надання посилання

Наявність НКС, які будуть виконувати функції координаційних центрів у державах-членах, є гарною ідеєю, і хоча деякі країни, такі як Бельгія та Італія, швидко підтримали цю концепцію, решта зараз наздоганяють згаяне, сказав Маттео Меріалдо з бельгійської компанії з кібербезпеки Nexova.

Він вважає, що ЕССС відіграватиме важливу роль у забезпеченні зв'язку між Horizon Europe та DEP, уникаючи збігів між темами досліджень та об'єднуючи екосистему. «Координація є важливою, оскільки є галузі знань, де зусиль однієї країни-члена недостатньо, щоб конкурувати на глобальному ринку», — сказав він.

Європейські програми можуть допомогти створити критичну масу, необхідну для подолання залежності ЄС від продуктів кібербезпеки США. «Я не думаю, що нам є чому заздрити США з точки зору знань, але з точки зору координації безумовно все ще є важлива прогалина», — сказав Меріальдо.

Меріальдо був керівником проекту ECHO, одного з чотирьох пілотних проектів Horizon 2020, створених для закладення основи для ECCC. ECHO об'єднала 32 партнери та 15 афілійованих партнерів для роботи над конкретними темами дослідження, включаючи моделювання та кібердальності.

За словами Меріальдо, у випадку дзвінків із питань кібербезпеки Horizon мережевий аспект навіть важливіший, ніж технологія. Половина консорціуму ECHO знову об'єдналася для проекту EDF ACTING, який базується на роботі проекту Horizon 2020.

Виникаючі загрози

Агентство Європейського Союзу з кібербезпеки (ENISA) також відповідає за зміцнення співпраці на континенті. У 2019 році йому було надано розширені повноваження відповідно до Закону ЄС про кібербезпеку, включаючи нову роль у моніторингу досліджень і розробок в академічних і промислових колах, а також консультування органів ЄС щодо потреб у дослідженнях.

Прокопіос Дрогкаріс, експерт з кібербезпеки ENISA, каже, що фінансування досліджень та інновацій має важливе значення для вирішення нових загроз. «З розвитком технологій контрзаходи повинні рухатися з тією ж швидкістю, якщо не швидше, і для цього вам потрібно мати на європейському рівні можливість проактивно передбачати майбутні загрози та реагувати на них», — сказав він.

Drogkaris вітає важливість, яку надають кібербезпеці в стратегічному плані Horizon Europe на 2025-2027 роки, в якому зазначено, що необхідні додаткові інвестиції у відповідь на «зростаючу кількість інцидентів у кіберпросторі та поточний геополітичний контекст».

Існують основні технології, включаючи хмарне зберігання даних, цифрові близнюки, програми метавсесвіту та розгортання штучного інтелекту та перехід до постквантової криптографії, які необхідно захистити. «Потрібно забезпечити кібербезпеку нових технологій», — йдеться в плані на 2025-2027 роки.

ENISA публікує щорічний звіт про ландшафт загроз, і Drogkaris каже, що за останні роки спостерігалося значне зростання кількості шкідливих програм, дезінформації, а також загроз для ланцюгів постачання та атак на відмову в

обслуговуванні, які намагаються перевантажити мережу, щоб вона стала недоступною. Загроза посилилася через триваючі війни та геополітичну напруженість.

Як яскраво ілюструє вторгнення Росії в Україну, кібератаки є помітною рисою сучасної війни, і багато нових технологій можуть мати як цивільне, так і військове застосування. Однією з цілей ECCC є сприяння співпраці між цивільним і оборонним секторами, хоча Тальяретті каже, що бюджет на технології подвійного використання невеликий і його ще належить використати повністю. «Для цього нам потрібно налагодити відносини з Європейським оборонним агентством і, можливо, з НАТО», — сказав він.

Європейська комісія хоче посилити підтримку технологій подвійного призначення та розглядає можливість перегляду ексклюзивного цивільного положення в частині наступної програми Horizon Europe, причому кібербезпека є однією з сфер, на яку можуть бути спрямовані нові правила». ***(Martin Greenacre. Cybersecurity centre gets ready to direct EU research // Science Business Publishing Ltd. (https://sciencebusiness.net/news/cybersecurity/cybersecurity-centre-gets-ready-direct-eu-research). 13.06.2024).***

***

«У Європі 26 галузевих груп попередили, що запропонована схема сертифікації кібербезпеки (EUCS) для хмарних сервісів не повинна дискримінувати Microsoft (MSFT), Amazon (AMZN) і Alphabet (GOOGL (GOOG) Google, повідомляє Reuters.

Європейська комісія, Агентство Європейського Союзу з кібербезпеки ENISA та країни ЄС зберуться у вівторок, щоб обговорити схему, яка зазнала багатьох змін після того, як ENISA представила проект у 2020 році, додається у звіті.

EUCS має намір допомогти урядам і компаніям визначити безпечного постачальника послуг для хмарних обчислень.

Попередня версія, оприлюднена в березні, видалила так звані вимоги суверенітету з попереднього проекту, згідно з яким американські технологічні

компанії повинні були створити спільне підприємство або співпрацювати з компанією з ЄС для зберігання та обробки даних клієнтів у регіоні, щоб мати право на знак кібербезпеки ЄС, зазначається у звіті.

У спільному листі до країн ЄС групи заявили, що вірять у те, що інклюзивна та недискримінаційна EUCS, яка підтримує вільне переміщення хмарних послуг у Європі, допоможе членам процвітати вдома та за кордоном.

«Усунення як засобів контролю власності, так і вимог щодо захисту від незаконного доступу/імунітету до законодавства, що не входить до ЄС, або PUA/INL, гарантує, що вдосконалення хмарної безпеки відповідають найкращим галузевим практикам і принципам недискримінації», – заявили організації.

Крім того, групи відзначили, що надзвичайно важливо, щоб їхні учасники мали доступ до низки стійких хмарних технологій, розроблених відповідно до їхніх конкретних вимог для зростання на конкурентному глобальному ринку.

Американська торгова палата в ЄС у Чехії, Норвегії, Румунії, Іспанії, Естонії, Фінляндії, Італії, Європейська федерація платіжних установ, Цифрова асоціація Польщі, ірландська бізнес-лобістська група IBEC, нідерландська NL Digital та іспанська Асоціація стартапів, Чеська конфедерація промисловості, Dansk Industry з Данії, Bundesverband deutscher Banken з Німеччини були серед тих, хто підписав листа.

Постачальники хмарних послуг у ЄС, такі як Deutsche Telekom (OTCQX:DTEGY) (OTCQX:DTEGF), Orange (ORAN) (OTCPK:FNCTF) і Airbus, закликали до вимог суверенітету в EUCS на тлі побоювань, що уряди країн, які не входять до ЄС, можуть отримати незаконний доступ до даних європейців через їхні закони, додається у звіті». ***(Ravikash Bakolia. EU groups urge cybersecurity certification should not discriminate against Big Tech – report // Seeking Alpha (https://seekingalpha.com/news/4116524-eu-groups-urge-cybersecurity-certification-should-not-discriminate-against-big-tech?utm_content=user%2Fseekingalpha). 17.06.2024).***

***

«За загальними виборами у Великій Британії уважно стежать після різких попереджень про те, що швидкий розвиток кібертехнологій, зокрема штучного інтелекту, і зростання суперечок між великими країнами загрожують чесності знакових голосувань 2024 року.

«Ці шахрайські та нерегульовані технологічні досягнення становлять величезну загрозу для всіх нас. Їх можна озброїти для дискримінації, дезінформації та розколу», – заявила у квітні глава Amnesty International Агнес Калламар.

Вибори у Великій Британії 4 липня – за чотири місяці до Сполучених Штатів – будуть розглядатися як «піддослідний кролик» для безпеки виборів, сказав Брюс Снелл, стратег з кібербезпеки американської фірми Qwiet AI, яка використовує ШІ для запобігання кібератакам.

Хоча ШІ займає більшість заголовків, більш традиційні кібератаки залишаються основною загрозою.

«Це дезінформація, це зрив вечірок, це витік даних і атаки на конкретних осіб», — сказав Рам Ельбоїм, керівник фірми з кібербезпеки Sygnia та колишній старший оперативний співробітник ізраїльського відділу кіберрозвідки 8200.

Очікується, що головною загрозою стануть державні актори, а Велика Британія вже попереджає про Китай і Росію.

«Головне — це, можливо, просування конкретних кандидатів або планів», — сказав Елбоїм.

«Другий — це створення певної внутрішньої нестабільності чи хаосу, чогось, що вплине на почуття громадськості».

Велика Британія має перевагу над Сполученими Штатами через короткий проміжок часу між оголошенням і проведенням виборів, що дає зловмисникам мало часу для розробки та реалізації планів, сказав Елбоїм.

Він також менш вразливий до атак на виборчу інфраструктуру, оскільки голосування не автоматизоване, додав він.

Діпфейки

Але хакерські атаки установ залишаються загрозою, і Великобританія вже звинуватила Китай у нападі на виборчу комісію.

«Вам не потрібно порушувати основну систему голосування, — пояснив Елбоїм. «Наприклад, якщо ви порушуєте роботу сторони, її комп'ютерів або третьої сторони, яка впливає на цю сторону, це може вплинути».

Він додав, що люди найбільше ризикують стати мішенями. Будь-яка незручна інформація може бути використана для шантажу кандидатів.

Але більш імовірно, що зловмисник просто видасть інформацію, щоб сформувати громадську думку, або використає зламаний обліковий запис, щоб видати себе за жертву та поширити дезінформацію.

Колишній лідер Консервативної партії Ієн Дункан Сміт, лютий критик Пекіна, вже заявив, що китайські державні діячі видають себе за нього в Інтернеті, надсилаючи підроблені електронні листи політикам по всьому світу.

Однак саме розширення можливостей використання ШІ для створення та поширення дезінформації є справжньою невідомою величиною на цьогорічних виборах, сказав Снелл.

Головне занепокоєння викликає розповсюдження «дипфейків» — підроблених відео, зображень чи аудіо.

«Рівень потенціалу для підробок просто величезний. Це те, чого ми точно не мали на останніх виборах», — сказав Снелл, назвавши Великобританію «піддослідним кроликом» для голосів у 2024 році.

Він підкреслив програмне забезпечення, яке може відтворити чийсь голос із 30-секундного зразка, і як цим можна зловживати.

Речник Лейбористської партії з питань охорони здоров'я Вес Стрітінг заявив, що став жертвою глибокого фейку аудіо, у якому він ображав колегу.

Ботоферми

Снелл порадив владі зосередитися на «швидкому» рішенні «поінформувати людей, щоб люди зрозуміли, що це проблема».

Інше програмне забезпечення можна використовувати для створення підроблених фотографій і відео, незважаючи на фільтри в багатьох додатках ШІ, розроблених для запобігання зображенню реальних людей.

«Хоча штучний інтелект дуже складний, його також надзвичайно легко обдурити», щоб створити зображення реальних людей, сказав Снелл.

ШІ також використовується для створення «ботів», які автоматично наповнюють соціальні мережі коментарями, щоб формувати громадську думку.

«Раніше ботів було дуже легко виявити. Ви бачите такі речі, як те саме повідомлення, яке повторюється та повторюється кількома обліковими записами», — сказав Снелл.

«Але завдяки витонченості штучного інтелекту… дуже легко створити ботоферму, яка може мати 1000 ботів, і кожен із них матиме різний стиль спілкування», — додав він.

Хоча вже існує програмне забезпечення для перевірки того, чи були створені відео та зображення за допомогою штучного інтелекту на «високому рівні компетентності», воно ще не використовується достатньо широко, щоб приборкати цю проблему.

Снелл вважає, що індустрія штучного інтелекту та компанії соціальних медіа повинні взяти на себе відповідальність за стримування дезінформації, «оскільки ми живемо в чудовому новому світі, де законодавці не мають уявлення про те, що відбувається». ***(Shajil Kumar. Election security: Cyber-attacks, bot farms, deepfakes pose threat // Garavi Gujarat Publications Ltd (https://www.easterneye.biz/election-security-deepfakes-bot-farms-threats/). 16.06.2024).***

***

«Оскільки Велика Британія виконує свій план стати технологічною та науковою наддержавою до 2030 року, кібербезпека матиме вирішальне значення для досягнення цієї мети.

Нові технології, такі як штучний інтелект (AI), квантові обчислення та Інтернет речей (IoT), швидко трансформують усі сектори економіки Великої Британії, створюючи кілька захоплюючих можливостей для економічного зростання та процвітання.

Однак ці технології також становлять численні ризики, оскільки нові досягнення створюють спектр потенційних вразливостей і векторів атак, використання яких може призвести до значних збоїв.

Кібернетичні загрози, з якими стикається Велика Британія, мають широкий спектр і постійно розвиваються, починаючи від атак програм-вимагачів, які руйнують життєво важливі служби, і закінчуючи державним шпигунством, націленим на державні установи. Організації будь-якого розміру повинні мати стратегію захисту своїх активів і захисту від нових загроз, що виникають.

Постійна загроза, яка стоїть перед найважливішою інфраструктурою Великобританії

Однією з найбільших кіберзагроз, з якими стикається Великобританія, є атаки на її критичну національну інфраструктуру (CNI). За даними Національного центру кібербезпеки (NCSC), цей тип інфраструктури, який, серед іншого, відповідає за забезпечення нас електроенергією, транспортом, підключенням до Інтернету та безпечною питною водою, знаходиться під «постійною та значною загрозою» з боку країни -державні довірені особи.

Недавній звіт Palo Alto Networks і ABI Research показав, що понад три чверті (76%) промислових організацій Великобританії повідомили, що вони стають жертвами кібератак щомісяця, щотижня, а в деяких випадках навіть щодня. Крім того, більше ніж кожна четверта (27%) британська промислова фірма повідомила, що їй принаймні раз за останній рік припиняли свою діяльність через успішну атаку.

Дослідження NCSC показує, що Велика Британія є третьою країною за кількістю кібератак, після США та України, із зростанням геополітичної напруженості, що призводить до зростання атак на національні держави, особливо з боку загрозливих суб’єктів, що базуються в таких країнах, як Китай, Іран, Росії та КНДР.

Оскільки цифровізація галузей прискорюється, поява нових технологічних додатків і швидка еволюція штучного інтелекту розширюють зону атаки, особливо

в критичних галузях та інфраструктурі, підвищуючи їхню вразливість до складних кіберзагроз.

Про це свідчать резонансні міжнародні інциденти, зокрема атаки на Colonial Pipeline та Irish Health Service Executive, а також інциденти у Великобританії, такі як інциденти проти South Staffordshire Water, Royal Mail International і навіть один, що вплинув на NHS 111.

Існує також зростаючий ризик збоїв у результаті кібератак на постачальників, які можуть мати слабший захист і, таким чином, являти собою привабливу можливість для зловмисників.

Дослідження розвідки про загрози, проведене Unit 42, показує, як середовища ОТ стали привабливою мішенню для загроз. Великобританії Було встановлено, що у 2023 році обробна промисловість була найбільш вразливою до атак програм-вимагачів, ставши жертвою майже п'ятої частини (17%) усіх атак програм-вимагачів.

Оскільки кіберзлочинці стають все більш досвідченими, інноваційними та наполегливими, ланцюжок постачання програмного забезпечення, зокрема, також зазнає значних атак.

У разі проникнення ланцюжки постачання програмного забезпечення надають прямий доступ до привілейованих облікових даних, власних кодових баз, конфіденційних даних та інфраструктури для майнінгу криптовалют, програм-вимагачів тощо, що робить їх особливо привабливими цілями для кіберзлочинців.

За даними Gartner, до 2025 року 45% організацій у всьому світі зазнають кібератак на ланцюги поставок, і бізнес Великобританії не є винятком. Захист ланцюгів постачання є ключовою сферою уваги для британських організацій будь-якого розміру.

Чому Великобританія стає все більш привабливою для організацій з кібербезпеки

Зараз більшість компаній усвідомлюють важливість ефективного управління кіберризиками в умовах дедалі динамічнішого середовища загроз. Це особливо вірно у Великобританії, де дані свідчать про те, що британські організації

піддаються більшій частоті атак порівняно з міжнародними партнерами. Наприклад, дослідження Unit 42 ставить Великобританію відразу після США як країну з другою за величиною кількістю жертв сайтів витоку програм-вимагачів у 2023 році.

Зараз більшість компаній усвідомлюють важливість ефективного управління кіберризиками в умовах дедалі динамічнішого середовища загроз. Це особливо вірно у Великобританії, де дані свідчать про те, що британські організації

піддаються більшій частоті атак порівняно з міжнародними партнерами. Наприклад, дослідження Unit 42 ставить Великобританію відразу після США як країну з другою за величиною кількістю жертв сайтів витоку програм-вимагачів у 2023 році.

Враховуючи свій статус провідного світового фінансово-економічного центру, Великобританія незмінно привертає увагу учасників загроз. Визнаючи цю реальність, уряд Великої Британії став одним із найбільш далекоглядних світових лідерів щодо стратегії та політики кібербезпеки. країни Ця проактивна позиція закріплена в Національній кіберстратегії, яка демонструє глибоке розуміння критичної важливості надійних заходів кібербезпеки.

Стратегія встановлює низку цілей, спрямованих на досягнення бачення уряду, яке полягає в тому, що у 2030 році Великобританія продовжить залишатися провідною відповідальною та демократичною кібердержавою, здатною захищати та просувати свої інтереси в кіберпросторі та через нього на підтримку національних цілей.

Він використовує підхід до кібербезпеки, який базується на «всесуспільстві», стверджуючи, що для підвищення стійкості Великобританії до кібератак уряду потрібно буде працювати в партнерстві з організаціями приватного сектору та фахівцями з кібербезпеки.

Однією з основних цілей стратегії є перенесення тягаря кібербезпеки з окремих громадян на організації, які найкраще підходять для управління кіберризиками. Це є ключовим фактором у створенні середовища, де кібербезпека є першочерговим завданням для компаній, і це дає значну можливість для партнерів

із кібербезпеки продемонструвати свою цінність для бізнесу, допомагаючи їм керувати цими ризиками та захищати їх від загроз, що постійно розвиваються. з якими вони стикаються.

Уряд та організації Великої Британії визнають, що для того, щоб скористатися перевагами нових технологій, надійна стратегія кібербезпеки є надзвичайно важливою. У поєднанні з яскравою технологічною екосистемою, резервом талантів світового рівня та одними з найкращих університетів у світі Великобританія є дуже привабливим місцем для таких компаній, як Palo Alto Networks.

Великобританія є однією з найбільш привабливих країн світу для інвестицій у технології. Це домівка для талантів світового рівня, одні з найкращих університетів у світі та понад три мільйони людей, які зараз працюють у технологічній індустрії Великобританії. Крім того, технологічний сектор Великої Британії, що швидко розвивається, сприяв розвитку культури підприємництва та інновацій, що дозволило Великій Британії стати однією з найпривабливіших країн Європи для інвестицій і третьою за привабливістю у світі, згідно з даними уряду.

У поєднанні з сильним структурним попитом на партнерів із кібербезпеки з місцевим досвідом Великобританії, особливо з огляду на зростаючі кіберзагрози, з якими стикаються підприємства будь-якого розміру, це робить Великобританію все більш привабливим місцем для організацій кібербезпеки, які можуть створювати та розвивати свою присутність, допомагаючи країні досягти своєї амбіції стати однією з провідних світових технологічних і наукових супердержав». ***(Gavin Mee. The role of cyber security in the UK's tech renaissance // Future US, Inc. (https://www.itpro.com/security/the-role-of-cyber-security-in-the-uks-tech-renaissance). 14.06.2024).***

***

«В останні роки британські університети постійно стають об'єктами атак кібер-зловмисників. Вони є особливо вразливими установами через велику кількість студентів і співробітників, розпорошених по кампусах, що ускладнює для

невеликих IT-команд відстеження тисяч кінцевих точок, кожна з яких має доступ до IT-систем установи.

Як повідомляється, основними суб'єктами загроз, які націлені на академічний сектор через вторгнення - будь-яку діяльність, спрямовану на порушення безпеки даних, - є хактивісти, противники, пов'язані з Китаєм, та суб'єкти електронної злочинності. Згідно з тим же дослідженням CrowdStrike, поряд з технологіями та телекомунікаціями, наукові кола є одним з найбільш націлених секторів для інтерактивних вторгнень на базі Linux. І це відбувається не лише у Великій Британії, загроза посилилася і в Америці, де зловмисники, пов'язані з Китаєм, використовують експлойти нульового дня, щоб скомпрометувати організації в академічному секторі.

Демістифікація супротивника

Щоб зупинити цих ворогів, служби безпеки в навчальних закладах повинні розуміти, як вони працюють.

Противники проникають у оточення та виходять із нього швидше, ніж будь-коли. Середній час розкриття електронного злочину впав до 79 хвилин, а найшвидший зафіксований час становив лише сім хвилин. Крім того, суб’єкти загроз електронної злочинності також знаходять ефективніші способи проникнення. Серед них – зловживання законними інструментами віддаленого моніторингу та керування, яке зросло на 312% з 2022 року.

VICE SPIDER — один із супротивників електронних злочинів, який, як було зафіксовано, використовує клавіатурні дії проти організацій в академічному секторі. Компрометації пов’язані з кількома хостами в інфраструктурі віртуального робочого столу (VDI), причому суб’єкт загрози виконує базову розвідку хостів, щоб перерахувати доменні довіри за допомогою nltest, потім перераховує групи дозволів адміністратора та виконує тести підключення до вихідної інфраструктури.

Зловмисники також стають експертами з хмар, знаючи про хмарні середовища стільки ж, а то й більше, ніж організації. Оскільки служби безпеки впроваджують більше хмарних технологій, зловмисники стають більш вправними у використанні неправильних конфігурацій і зловживання інструментами керування

хмарою. Насправді противники використовують хмару більше, ніж будь-коли. кількість крадіжок Кількість хмарних атак зросла на 95%, а зросла на 160%. облікових даних через API метаданих хмарних екземплярів

Вестмінстерський університет

Університет, заснований у 1838 році, наразі нараховує понад 19 000 студентів із 169 країн світу, багатьом із них пропонується стажування у майже 200 організаціях по всій Великобританії та працює понад 2 000 людей.

У 2021 році університет зіткнувся з ландшафтом кіберзагроз, який різко змінився під час пандемії COVID-19, включаючи такі серйозні виклики безпеці: високий ризик атак програм-вимагачів, які завдають шкоди репутації, відсутність цілодобового виявлення загроз і реагування на них, реактивний захист положення, спричинене обмеженнями ємності та відсутністю уніфікованої видимості в різних операційних системах.

Через непомірно високу вартість впровадження внутрішнього центру безпеки (SOC) і додаткове навантаження на персонал, пов’язане з цілодобовою безпекою, лідери безпеки університету визнали модель послуги керованого виявлення та реагування (MDR) привабливою — і достатньо стійкий, щоб задовольнити існуючі та майбутні потреби університету в кібербезпеці.

Сандерлендський університет

Викликає занепокоєння те, що того ж року Університет Сандерленда став жертвою порушення кібербезпеки. Зовнішні групи безпеки виявили, що облікові дані особи були зламані, що дозволило зловмиснику отримати доступ до спеціалізованого навчального середовища, а потім перейти до інших систем. Рішення кінцевої точки від постачальника безпеки рідної ОС, яке використовувалося під час атаки, не змогло зупинити злом. Це надто поширене явище.

Інцидент продемонстрував, що зловмисники використовували атаки на основі ідентифікації, щоб обійти застарілі рішення безпеки. Ці зловмисники все частіше використовують кінцеву точку як опору для переходу до хмарної інфраструктури. Завдяки об’єднанню захисту кінцевих точок, ідентичності та

хмари на одній платформі університет тепер має керований захист на всіх етапах шляху атаки противника.

Сем Селдон, спеціаліст із захисту даних Університету Сандерленда, сказав: «Ми зобов'язані захищати не лише нашу інфраструктуру, але й наших людей. Наші старші керівники знаходяться в соціальних мережах і на веб-сайтах, де зловмисники активно полюють за їхньою інформацією. Для цих керівників компроміс у житті може призвести до компромісу на роботі».

Чи готові групи безпеки?

Запитання, які університети мають поставити своїм командам і партнерам із безпеки: «Чи стали ми швидше ідентифікувати, досліджувати та усувати сучасні загрози?» Чи можемо ми виявити супротивника за сім хвилин або навіть сім годин? Чи виявили ми нові потенційні вразливості, враховуючи, що ландшафт супротивника змінився? Чи ділимося ми своїми знаннями з екосистемою, щоб інші навчальні заклади не стали жертвами?»

Комплексна стратегія кібербезпеки абсолютно необхідна в сучасному підключеному світі, особливо для організацій, які мають стільки кінцевих точок, скільки навчальні заклади. Захист цифрових активів вашої організації має очевидну перевагу у вигляді зниження ризику втрати, крадіжки чи знищення, а також потенційної необхідності платити викуп за відновлення контролю над даними чи системами компанії. Бездіяльність може призвести до катастрофічного порушення, де репутаційна шкода буде такою ж занепокоєною, як і втрата конфіденційних даних». ***(Zeki Turedi. Cyber threat actors are targeting UK universities. Are security teams prepared? // HEPI (https://www.hepi.ac.uk/2024/06/14/cyber-threat-actors-are-targeting-uk-universities-are-security-teams-prepared/). 14.06.2024).***

***

«Згідно з новим дослідженням, понад вісім із десяти спеціалістів із кібербезпеки у Великій Британії працюють у вихідні через напруженість своєї роботи.

У новому звіті охоронної компанії Bitdefender, заснованому на опитуванні 1200 кіберпрофесіоналів у Франції, Німеччині, Італії, Сінгапурі, Великобританії та США, компанія заявила, що тиск означає, що 71% респондентів у Великобританії планують шукати нова робота протягом наступного року.

У всьому світі сім із десяти сказали, що їм часто доводиться працювати у вихідні, а у Великобританії цей показник зріс до 81%. У Сінгапурі лише 59%.

З точки зору того, що їх хвилює, основними загрозами були програми-вимагачі, які назвали третиною, за якими йшли вразливості програмного забезпечення та експлойти нульового дня, а також фішинг/соціальна інженерія (28%).

Майже половина (44%) респондентів назвали порушення або витік даних серйозною проблемою, тоді як 43% висловили занепокоєння через несанкціонований доступ до хмарних сервісів, а ще 42% турбували неправильно налаштоване хмарне сховище.

Дослідники попереджають, що нинішній ландшафт загроз у поєднанні з нестримним браком навичок створює більш інтенсивну культуру надмірної роботи для спеціалістів із безпеки.

Це, у свою чергу, має шкідливий вплив на їхнє здоров’я та загальну кіберстійкість.

«Дефіцит кваліфікованих фахівців із хмарної кібербезпеки робить це ще більш складним», — кажуть дослідники.

«Багато IT-фахівців можуть володіти глибокими знаннями в одній конкретній хмарній платформі, такій як Azure, але виявляти себе менш знайомими з іншими, такими як Google Cloud або AWS. Ця невідповідність навичок може призвести до прогалин у загальній системі хмарної безпеки організації».

Через відсутність внутрішнього досвіду двоє з п’яти професіоналів залучають сторонніх експертів з кібербезпеки, щоб полегшити навантаження.

Вигорання у сфері кібербезпеки є шаленим

Результати опитування тісно збігаються з попередніми дослідженнями надмірної роботи в галузі кібербезпеки. Минулого року дослідження Centripetal

показало, що одна третина спеціалістів із безпеки зазнає перерв у своєму особистому житті через тиск роботи.

70% респондентів сказали фірмі, що їхнє життя переривається принаймні раз на тиждень, тоді як майже одна п'ята щотижня працювала понад повний день неоплачуваної понаднормової роботи.

У подібному дослідженні, проведеному CyberArk цього року, понад дві третини керівників C-suite сказали, що професійне вигорання впливає на їхню здатність приймати важливі рішення високого рівня». ***(Emma Woollacott. Cyber security staff are working weekends more than ever before – and it needs to stop // Future US, Inc. (https://www.itpro.com/security/cyber-security-staff-are-working-weekends-more-than-ever-before-and-it-needs-to-stop). 18.06.2024).***

***

Австралія та Нова Зеландія

«3 червня 2024 року Управління пруденційного регулювання Австралії (APRA) написало всім організаціям, які регулюються APRA, щоб підкреслити свої очікування щодо кібербезпеки, зокрема щодо резервного копіювання даних і захисту від втрати даних.

APRA закликала підприємства негайно переглянути та усунути прогалини в будь-якій практиці, яка може перешкоджати відновленню системи на етапі відновлення кіберінциденту. Зокрема, посилаючись на «поширені проблеми, які можуть обмежити корисність…резервних копій у відновленні систем під час інциденту».

APRA рекомендує підприємства:

- періодично самооцінювати себе щодо практик безпеки в APRA Prudential Guide CPG 234 (Інформаційна безпека) (CPG 234);
- перевірити їхні механізми резервного копіювання на предмет поширених проблем, які обмежують корисність резервних копій на етапі відновлення після кіберінциденту:
- недостатня сегрегація між виробничим і резервним середовищами;

- недостатнє охоплення контрольним тестуванням і суворість для забезпечення захисту резервних копій від компрометації; і
- недостатнє тестування можливості відновлення систем і даних із резервних копій у межах допустимих рівнів.

APRA зазначила, що:

- прогалини, виявлені під час перегляду механізмів резервного копіювання, можуть бути недоліком, про який потрібно повідомити, згідно з параграфом 36 Пруденційного стандарту APRA CPS 234 (Інформаційна безпека) (CPS 234); і
- використання регулярного резервного копіювання є однією з Essential Eight. пріоритетних стратегій пом'якшення кібернетичних наслідків

Рекомендації APRA щодо того, як підприємства можуть вирішувати типові проблеми

Контрольний список APRA щодо забезпечення безпеки та адекватності резервного копіювання включає:

- підтримання достатньої ізоляції резервних копій від виробничого середовища, щоб компрометація виробничого середовища не скомпрометувала резервні копії. Включаючи заборону будь-якому окремому обліковому запису, який має дозвіл змінювати або видаляти робочі та резервні копії (CPG 234, пункти 44 і 45);
- забезпечення того, щоб програма тестування підтверджувала, що резервні копії є ефективними та захищеними від несанкціонованого доступу, модифікації або зміни (CPG 234, параграф 45 і Додаток G); і
- забезпечення того, щоб програма тестування підтверджувала, що покриття резервного копіювання є достатнім для відновлення критично важливих бізнес-операцій, а також технічної можливості відновлення систем і даних у межах допустимих рівнів (CPG 234 і Додаток G).

APRA також скеровує суб'єкти до восьми основних стратегій пом'якшення інцидентів кібербезпеки для пріоритетних стратегій пом'якшення загальних недоліків.

Винос

Лист APRA містить вказівки для регульованих установ щодо регуляторних пріоритетів, а також очікування APRA щодо етапу відновлення кіберінциденту.

Зокрема:

- оскільки ландшафт кіберзагроз продовжує швидко розвиватися, APRA підкреслив вирішальну роль резервного копіювання даних у кібервідмовостійкості та те, що тепер, як ніколи, очікується, що регульовані організації продемонструють, що вони вжили пильних і проактивних кроків для зменшення ризиків і наслідків кібер -атаки через їхню практику резервного копіювання даних;
- APRA пояснила, що від регульованих організацій очікується, що вони самостійно перевірять свої механізми резервного копіювання (і усунуть будь-які недоліки), щоб забезпечити ефективне відновлення критичних бізнес-операцій у рамках CPS 234 (тобто уникнути збоїв і збоїв у контролі операційного ризику); і
- APRA наголошує, що недоліки в практиці резервного копіювання даних можуть прирівнюватися до події, що підлягає сповіщенню, через «слабкість контролю безпеки інформації» (згідно з параграфом 36 CPS 234), що вимагає повідомлення APRA не пізніше ніж за 10 робочих днів.

Ми очікуємо, що APRA продовжуватиме наголошувати на необхідності суб’єктів упереджувати самооцінку, виправляти будь-які недоліки та покращувати свою кіберстійкість.

Лист APRA узгоджується з ширшою тенденцією кількох австралійських регуляторів, які наголошують на важливості надійних процесів і методів безпеки даних під час перевірки та забезпечення відповідності австралійським законам про захист даних, конкуренцію, корпорації, телекомунікації та критичну інфраструктуру. Пріоритет APRA щодо нагляду за резервним копіюванням даних нагадує організаціям, регульованим APRA, про активне вдосконалення своїх процесів і методів управління даними не тільки для забезпечення ефективного відновлення системи та мінімальних збоїв у роботі в разі кіберінциденту, але й як важливої частини виконання своїх CPS 234 зобов'язання». ***(Hamish Fraser, Julie Cheeseman, Emma Croft and Evelyn Park. The importance of cyber resilience stressed***

by Australian Prudential Regulator // Bird & Bird LLP (https://www.twobirds.com/en/insights/2024/australia/the-importance-of-cyber-resilience-stressed-by-australian-prudential-regulator#page=1). 06.06.2024).

***

Китай

«У вівторок уряд Гонконгу запропонував нове законодавство для посилення кібербезпеки критично важливих інфраструктур, таких як банки, залізничні системи та постачальники електроенергії, згідно з яким оператори зобов'язані повідомляти про інциденти кібербезпеки, а тих, хто не виконує, штрафують до 5 мільйонів гонконгських доларів.

Згідно з документом, поданим до Законодавчої ради Бюро безпеки, критична інфраструктура — це «об'єкти, необхідні для підтримки нормального функціонування суспільства Гонконгу».

Існує дві основні категорії критичної інфраструктури. Перший охоплює об'єкти, що надають «основні послуги» у восьми секторах, а саме енергетиці, інформаційних технологіях, банківських і фінансових послугах, наземному транспорті, повітряному транспорті, морському транспорті, послугах охорони здоров'я, а також зв'язку та радіомовлення. Друга включає «іншу інфраструктуру для підтримки важливої соціальної та економічної діяльності», таку як основні спортивні та виступальні майданчики.

Буде створено новий офіс уповноваженого при Бюро безпеки для моніторингу операторів і спостереження за невідповідністю.

Згідно із запропонованою законодавчою базою, оператори зобов'язані створити підрозділ управління безпекою комп'ютерної системи, проводити оцінку ризиків безпеки принаймні раз на рік і незалежний аудит безпеки принаймні раз на два роки, а також повідомляти про серйозні інциденти безпеки протягом двох годин.

До організацій, які не дотримуються вимог, застосовуватимуться штрафні санкції від 500 000 гонконгських доларів до 5 мільйонів гонконгських доларів.

У дописі на Facebook міністр безпеки Кріс Танг заявив, що ця пропозиція спрямована не на окремих осіб, а на великі організації, додавши, що вона не порушуватиме свободу людей користуватися Інтернетом.

Законодавці обговорять цю пропозицію на засіданні групи безпеки 2 липня, після чого відбудеться період консультацій, який триватиме місяць.

Бюро безпеки заявило, що сподівається внести рахунок до Legco до кінця цього року». ***(New law to boost infrastructure cybersecurity mooted // rthk.hk (https://news.rthk.hk/rthk/en/component/k2/1759011-20240625.htm). 25.06.2024).***

***

Інші країни

«У 2024 році минуло майже шість місяців, і цей рік уже став кардинальним для законодавства та регулювання IT та кібербезпеки на Бермудських островах.

І всі ці події продовжують нещодавню та потужну тенденцію реформування IT та кіберзаконодавства на Бермудських островах.

22 січня 2024 року фінансово-кредитне управління Бермудських островів (BMA) у своєму бізнес-плані на 2024 рік підтвердило свою постійну увагу до нагляду за кіберризиками, свою зацікавленість у розгляді того, як штучний інтелект вплине на фінансові послуги, і свою відданість своїй IT-стратегії: бачення 2025.

Крім того, BMA чітко вказав на реальний зв'язок, який існує між IT та кібероперaційними ризиками, аутсорсинговими транзакціями, плануванням безперервності бізнесу та захистом даних у критичній інфраструктурі, яку регулює BMA.

Нещодавно уряд Бермудських островів ухвалив Закон про неправомірне використання комп'ютерів 2024 року, щоб забезпечити вдосконалену законну зброю для боротьби з кіберзлочинністю. Спираючись на законодавство Великої Британії з цих питань, новий закон замінює попередній однойменний статут Бермудських островів 1996 року та має на меті відобразити найкращі міжнародні

практики як щодо інновацій у сфері обчислювальної техніки, так і для значного посилення штрафів.

Проте наш найновіший Закон про неправомірне використання комп'ютерів 2024 року може не стати остаточним словом щодо реформи кримінального законодавства щодо неправомірного використання комп'ютерів, враховуючи численні рекомендації щодо реформування законодавства, які містяться у звіті Мережі реформи кримінального права Великобританії за 2020 рік під назвою «Реформування Закону про неправомірне використання комп'ютерів 1990 року». На цьому фронті може бути більше.

31 травня палата прийняла новий Закон Бермудських островів про кібербезпеку 2024 року, щоб вирішити потребу в регулятивному нагляді за численними основними службами та критичною інфраструктурою на Бермудських островах, які уряд більш конкретно визначить найближчими тижнями.

Прийнявши Закон про кібербезпеку, уряд вирішив створити новий режим регулювання під наглядом міністерства, а не просто наказати існуючим регуляторам, таким як Рада охорони здоров'я Бермудських островів і Регуляторний орган, впроваджувати власні моделі регулювання IT та кібербезпеки на основі пропорційних ризиків, який, ймовірно, буде слідувати за дуже успішним формулюванням, впровадженням та управлінням такими правилами BMA в останні роки.

Проте очікується, що кінцевий результат буде дуже схожим для всіх основних служб та їхніх регуляторів, навіть якщо відповідно до цього Закону передбачено різні пропорційні стандарти безпеки, практики та вимоги до управління, що базуються на ризиках. Очікується, що процес імплементації цього Закону, включно з впровадженням усіх таких регулятивних стандартів у найближчі тижні, включатиме ретельні консультації з галуззю та реагування Урядом на підвищення актуальності та ефективності цього Закону.

Нарешті, як багато хто слідкував, Закон Бермудських островів про захист особистої інформації 2016 року (PIPA) набуде повної чинності наприкінці цього року. Дійсно, PIPA також містить закони, які вимагають захисту IT та кібербезпеки,

і стосується послуг третіх сторін, таких як аутсорсинг, передача особистої інформації за кордон, а також відповідні обов'язки та відповідальність щодо захисту даних.

Безсумнівно, правовий ландшафт IT та кібербезпеки на Бермудських островах зазнає трансформаційних змін у всіх своїх аспектах, від фундаментальних стандартів сумлінного корпоративного управління до всіх комерційних IT-послуг і угод про аутсорсинг, які кожен учасник критичної інфраструктури укладає з їхні філії та постачальники комерційних послуг». ***(Duncan Card. Bermuda's Cybersecurity Law Transformation Is Well Underway // Appleby (https://www.applebyglobal.com/publications/bermudas-cybersecurity-law-transformation-is-well-underway/). 04.06.2024).***

***

«31 травня 2024 року Департамент комунікацій і цифрових технологій Південної Африки офіційно опублікував Національну політику щодо даних і хмарних технологій (GG № 50741) відповідно до розділу 3(1) Закону про електронні комунікації 2005 року («Політика»).

Яка мета політики?

Політика визнає, що дані та хмарні технології відіграють ключову роль у соціально-економічному розвитку, наданні державних послуг і цифровому економічному зростанні в Південній Африці.

Основні цілі включають:

Покращена безпека даних

Політика спрямована на захист приватної та конфіденційної інформації від кібератак шляхом встановлення протоколів захисту даних, як того вимагає Закон про захист персональних даних 2013 року («POPIA»).

Цифрова трансформація

Політика спрямована на сприяння використанню технологій у різних секторах для підвищення продуктивності та ефективності

Поліпшення надання державних послуг

Політика спрямована на сприяння використанню хмарних рішень, щоб допомогти урядовим департаментам пропонувати кращі послуги громадянам і підприємствам

Економічного зростання

Політика дозволить більшій кількості підприємств використовувати технології, що призведе до збільшення кількості робочих місць та економічного зростання

Розширена співпраця

Політика спрямована на сприяння поглибленій співпраці між урядовими департаментами, приватними організаціями та дослідницькими установами, сприяючи обміну знаннями, даними та досвідом

На кого поширюється політика?

Політика має широке застосування, оскільки її сфера дії поширюється на:

національний і провінційний уряд

органи державних/громадських підприємств

приватний сектор

громадськість/окремі громадяни та

контролери та зберігачі даних.

Крім того, Політика визначає обов'язки центрів обробки даних, що працюють у Південній Африці, зокрема:

Центри обробки даних мають будуватися й експлуатуватися з дотриманням екологічного законодавства та будівельних нормативних актів.

Центри обробки даних не можна будувати в обмежених зонах, таких як об'єкти культурної спадщини, ключові національні точки або землі, призначені для земельної реформи.

Центри обробки даних не можна розташовувати в районах, схильних до стихійних лих або соціальних заворушень.

Центри обробки даних повинні відображати або мати можливість надавати перевірені облікові дані сертифікації всім потенційним клієнтам.

Центри обробки даних, які використовуються урядом, повинні відповідати відмовостійкій конструкції, яка забезпечує мінімальний час безвідмовної роботи 99,995%.

Пріоритет повинен бути наданий самостійному забезпеченню електроенергією та водою для роботи центрів обробки даних, щоб забезпечити безперервну роботу та зменшити залежність від національних мереж.

Вищезазначене мають враховувати (1) організації, які використовують центри обробки даних у Південній Африці для розміщення своїх даних і переконатися, що їхні контракти з такими центрами обробки даних оновлюються відповідно до вищезазначеного, і (2) центри обробки даних, які працюють у Південній Африці, повинні враховувати вплив Політики на їх діяльність і взаємодію з клієнтами.

Що там сказано про децентралізацію хмарних служб?

Нова політика спрямована на перенесення всіх державних IT-сервісів у хмару, сприяючи взаємодії між різними державними відомствами та покращуючи цифрові послуги для громадян. Децентралізуючи постачальників хмарних послуг, Політика визнає досвід і ресурси, доступні в приватному секторі, які можуть підвищити ефективність та інновації в державних послугах. Це відхилення від проекту версії, в якому говорилося, що всі державні сектори повинні покладатися на єдиний державний центр обробки даних для своїх IT-потреб, що викликало занепокоєння багатьох секторів і ключових зацікавлених сторін.

Одним із важливих положень Політики є вимога, згідно з якою інфраструктура центрів обробки даних, яка використовується державними установами, має бути розташована в межах країни.

Чи є політика обов'язковою?

Оскільки вже існують політики та законодавство, як-от POPIA, Рамкова основа політики кібербезпеки та Закон про кіберзлочини, які стосуються управління даними та безпеки, Політика спрямована на посилення цих законів.

Політику все ще потрібно впровадити, що відбуватиметься шляхом урядових консультацій із ключовими зацікавленими сторонами та виконавцями, такими як

SITA, відповідні урядові департаменти та, за необхідності, зацікавлені сторони галузі та сектора. Будуть створені структури, що складатимуться з різних професіоналів, щоб надавати консультації щодо розробки структур, необхідних для підтримки реалізації Політики, включаючи консультативну раду з питань даних із представниками державного та приватного секторів, академічних кіл, а також цільову групу з технічного впровадження даних і хмари, до складу якої входять різні державні установи…» ***(Priyanka Raath, Shaaista Tayob and Ridwaan Boda. South Africa's new National Cloud and Data Policy: A strategic shift // ENSafrica (https://www.ensafrica.com/news/detail/8715/south-africas-new-national-cloud-and-data-pol). 10.06.2024).***

***

«7 травня 2024 року парламент Сінгапуру прийняв законопроект про кібербезпеку (з поправками) № 15/2024 («Законопроект»), щоб внести ключові поправки до Закону про кібербезпеку Сінгапуру 2018 року («Закон про кібербезпеку»). Законопроект надає Агентству кібербезпеки Сінгапуру («CSA») більші повноваження та розширює сферу дії Закону про кібербезпеку за межі власників критичної інформаційної інфраструктури («CII»), тобто комп'ютерних систем, безпосередньо залучених до надання основних послуг. Секторами ICI є енергетика, водопостачання, банківська справа та фінанси, охорона здоров'я, транспорт (що включає сухопутний, морський та авіаційний), інформаційний зв'язок, засоби масової інформації, служби безпеки та надзвичайних ситуацій, а також уряд.

Законопроект спрямований на вирішення нових проблем кібербезпеки, спричинених, серед іншого, розвитком хмарних обчислень. Початкові положення Закону про кібербезпеку регулюють лише власні комп'ютерні системи ICI, але все частіше комп'ютерні системи ICI розміщуються на хмарних платформах, що також вимагає регулювання для комп'ютерних систем ICI, що належать третім особам. Крім того, зловмисники все частіше атакують постачальників і ланцюжки поставок організацій, як продемонструвала атака на ланцюг постачання SolarWinds кілька

років тому. Збільшення цифрової інтеграції в повсякденне життя також розширило «поверхню атаки», в результаті чого жителі та підприємства піддаються більшим ризикам кібербезпеки.

Ключові поправки до Закону про кібербезпеку

Регулювати як фізичні, так і віртуальні системи ICI

Законопроект розширює сферу застосування Закону про кібербезпеку, охоплюючи віртуальні комп'ютерні системи CII. Уточнюючи, що «комп'ютер» і «комп'ютерна система» включають віртуальні структури, такі як CII у хмарному середовищі, ці зміни гарантують, що власники CII несуть відповідальність за кібербезпеку своїх систем, фізичних чи віртуальних.

До Закону про кібербезпеку додано новий розділ, який гарантує, що власники ICI, а не сторонні постачальники ICI, залишатимуться відповідальними за свої зобов'язання щодо кібербезпеки для зовнішніх систем, наданих сторонніми постачальниками. Власники ICI повинні встановлювати юридичні зобов'язання, такі як контракти, щоб гарантувати, що системи їхніх постачальників відповідають порівнянним стандартам кібербезпеки.

Регулювати власників ICI, які підтримують важливу послугу з-за кордону

Оригінальний Акт про кібербезпеку дозволяє CSA лише позначати комп'ютерні системи як CII, якщо вони повністю або частково розташовані в Сінгапурі. Нові поправки дозволять CSA регулювати комп'ютерні системи, які повністю розташовані за межами Сінгапуру, якщо (i) власник таких комп'ютерних систем перебуває в Сінгапурі; та (ii) такі комп'ютерні системи були б визначені як ICI, якби вони були розташовані в Сінгапурі.

Управляйте ризиками власників ICI в ланцюжку поставок

Відповідно до оригінального Закону про кібербезпеку, власник ICI зазвичай зобов'язаний лише повідомляти про інциденти кібербезпеки, що стосуються комп'ютерів або комп'ютерних систем, які взаємопов'язані з ICI або спілкуються з ним. Нові поправки вимагатимуть від власників ICI додатково повідомляти про інциденти, які впливають на: (i) інші комп'ютери чи комп'ютерні системи, які знаходяться під контролем власника ICI, навіть якщо вони не пов'язані з ICI та не

спілкуються з ним; та (ii) комп'ютери, які знаходяться під контролем зовнішнього постачальника, якщо такі комп'ютери взаємопов'язані з ICI власників ICI або спілкуються з ними.

Перша вимога спрямована на вирішення інцидентів кібербезпеки, подібних до атаки на ланцюг поставок SolarWinds, тоді як друга вимога сприяє ранньому втручанню, якщо системи, надані зовнішніми постачальниками, скомпрометовані. Слід зазначити, що вимога повідомляти про інциденти, що стосуються зовнішніх постачальників, застосовуватиметься лише в тому випадку, якщо ICI належить власнику ICI. Цей підхід є практичним, оскільки власники ICI, які використовують ICI третіх сторін, часто не мають достатньої інформації про своїх зовнішніх постачальників, щоб виконати зобов'язання щодо звітності.

Суб'єкти, окрім власників ICI, також підпадають під дію CSA

Законопроект розширює сферу застосування Закону про кібербезпеку, охоплюючи три нові типи організацій, окрім власників ICI:

Системи тимчасової занепокоєності кібербезпекою («STCC») — це тимчасові системи високого ризику, які, якщо їх зламано, завдадуть серйозної шкоди національним інтересам. STCC охоплює системи, які мають вирішальне значення для реагування на кризу або підтримки великих міжнародних подій, наприклад тих, які використовуються для підтримки розповсюдження критичних вакцин під час COVID.

Суб'єкти, що становлять особливий інтерес у сфері кібербезпеки («ESCI») — це організації, які обробляють конфіденційну інформацію, що впливає на національні інтереси (наприклад, суб'єкти, які можуть бути особливо привабливими цілями для зловмисників через порушення функції, яку вони виконують, або розкриття конфіденційної інформації, що міститься в їх комп'ютерні системи, матиме значний шкідливий вплив на оборону Сінгапуру, зовнішні відносини, економіку, охорону здоров'я, громадську безпеку чи громадський порядок). Наприклад, ESCI можуть потенційно включати університети або окремі фінансові установи. Хоча список призначених ESCI не

буде опубліковано з міркувань безпеки, CSA буде взаємодіяти з організаціями, перш ніж призначати їх як такі.

Постачальники «Основної послуги цифрової інфраструктури» («FDIS») є постачальниками, які мають важливе значення для функціонування цифрової економіки, що забезпечує повсякденні потреби громадян. Список постачальників FDIS було визначено в новому Третьому додатку, який наразі охоплює хмарні обчислення та послуги центру обробки даних. Список може бути розширений, щоб охопити нові типи цифрової інфраструктури в майбутньому.

Розширені регуляторні повноваження

Законопроект розширює регуляторні повноваження CSA, включаючи повноваження щодо:

- перевіряти ICI у разі невиконання їх власниками своїх зобов'язань або надання недостовірної інформації;
- проводити перевірки та вимагати документацію від постачальників ліцензованих послуг кібербезпеки для забезпечення дотримання умов ліцензування; і
- продовжувати строки виконання з поважних причин.

Що стосується забезпечення виконання Закону про кібербезпеку, було запроваджено новий режим цивільного покарання за порушення окремих частин Закону про кібербезпеку (на додаток до кримінальних покарань згідно з чинним Законом про кібербезпеку). Законопроект дозволяє Уповноваженому з кібербезпеки за згодою прокурора подавати позов до суду проти особи, яка порушила певні частини Закону про кібербезпеку, щоб вимагати накладення цивільного покарання замість судового переслідування. Штрафи можуть сягати 10% річного обороту такої особи в Сінгапурі або 500 000 сінгапурських доларів, залежно від того, що більше.

Наші спостереження

Нові поправки до Закону про кібербезпеку надають CSA ширші повноваження для підвищення стійкості кібербезпеки Сінгапуру та готовності до боротьби з кібератаками. Щоб орієнтуватися в регулятивному ландшафті

кібербезпеки, що розвивається в Сінгапурі, компанії повинні розуміти наслідки Закону про кібербезпеку для їх діяльності. Наприклад, вони можуть безпосередньо підпадати під дію Закону про кібербезпеку та/або зіткнутися з аудитом і суворішими вимогами щодо кібербезпеки, які встановлюються їхніми бізнес-партнерами чи клієнтами через контракти чи іншими способами». ***(Peggy Chow. Singapore expands the scope of the cybersecurity act // Herbert Smith Freehills LLP (https://www.herbertsmithfreehills.com/notes/data/2024-posts/singapore-expands-the-scope-of-the-cybersecurity-act-#page=1). 12.06.2024).***

***

«2024 рік знаменує собою переломний момент в історії Південної Африки. Це не тільки рік, який відзначає три десятиліття з моменту перших демократичних виборів, але й може стати роком, який потенційно віщує нам відродження.

Оскільки країна відзначає День молоді, надзвичайно важливо пам’ятати та вшановувати стійкість і мужність, виявлені молоддю 1976 року. Їхня хоробрість перед лицем труднощів є свідченням сили південноафриканського духу. У той же час ми повинні задуматися про стан країни та численні виклики, з якими стикається сучасна молодь, такі як безробіття, нерівність в освіті та відсутність доступу, зокрема до справедливих можливостей у технологічному секторі.

Визначність цифрового гендерного розриву в таких секторах, як кібербезпека Хоча розширення можливостей молоді домінує в національному та міжнародному порядку денному, відсутність значного прогресу викликає занепокоєння. Збільшується розрив між кількістю молоді, яка шукає роботу, особливо молодих дівчат, і можливостями працевлаштування. Згідно зі статистикою Південної Африки, рівень поглинання молодих чоловіків на ринку праці становить 31,9%, випереджаючи показник молодих жінок, який становить 24,2%. Ця тенденція, посилена різними соціально-економічними викликами, включаючи цифровий гендерний розрив, відображає нагальну потребу в діях для вирішення широко поширеної гендерної нерівності в нашому суспільстві.

Жінки ООН визначають цифровий гендерний розрив як невідповідність між жінками, чоловіками, дівчатами та хлопцями щодо цифрової адаптації та їхніх відносних можливостей доступу до цифрових технологій, їх використання та отримання вигоди від них. Ця прогалина є актуальною проблемою, яка потребує негайної уваги, особливо в нашому цифровому світі. Занадто багато молодих жінок стримуються через суспільні норми та упередження. Як наслідок, вони дуже мало представлені в галузях науки, технологій, інженерії та математики (STEM). У всьому світі 35% випускників STEM – жінки, а в Південній Африці ця цифра нижча – лише 13%. Недопредставленість жінок також очевидна в таких критично важливих сферах, як кібербезпека, де жінки становлять 20-25% світової робочої сили.

Чому усунення гендерного розриву в кібербезпеці є критично важливим? Усунення гендерного розриву в кібербезпеці має бути на передньому плані стратегічного планування кожної організації. Різноманітність у поглядах, лідерстві та досвіді має важливе значення для успіху бізнесу, і це особливо вірно у сфері кібербезпеки. Нам потрібні професіонали з різним досвідом і віком для ефективної боротьби з безліччю загроз і кібертактик. Чим ширша різноманітність людей і досвіду, які захищають наші мережі, тим кращі наші шанси на успіх. Крім того, галузь кібербезпеки відчуває значний дефіцит робочої сили, оскільки багато посад незаповнені. Ця нестача посилюється, коли гендерні упередження обмежують коло потенційних кандидатів. Попит на кваліфікованих, обізнаних і відданих фахівцям з кібербезпеки величезний, і як жінки, так і чоловіки можуть знайти в цій галузі вражаючу та корисну кар’єру. Заохочуючи більше жінок до участі в кібербезпеці, ми можемо не лише підвищити справедливість робочої сили, але й покращити нашу здатність захищати критично важливі мережі від кіберзагроз.

Як компанії можуть усунути цифровий гендерний розрив у кібербезпеці Організації можуть усунути гендерний розрив у галузі кібербезпеки, впроваджуючи різні стратегічні заходи. По-перше, вони можуть віддавати перевагу потенціалу над професійними досягненнями, наприклад, залучати нещодавніх випускників або підвищувати кваліфікацію наявних співробітників. Програми

наставництва та гнучкі умови праці також можуть мати вирішальне значення для залучення та утримання жінок. Крім того, знайомство дівчат із технологіями з раннього віку через освітні ініціативи та програми охоплення може надихнути майбутніх фахівців з кібербезпеки. Компанії також можуть зробити посади в сфері кібербезпеки привабливими для молоді та жінок, використовуючи культурні переваги своєї організації та пропонуючи персоналізовані переваги для створення інклюзивного середовища, яке підтримує різноманітні таланти. Ці кроки не лише вирішать проблему нестачі робочої сили, але й покращать здатність галузі боротися з кіберзагрозами з ширшого спектру точок зору та досвіду.

Як Mimecast підвищує кваліфікацію молоді та жінок у галузі Ми в Mimecast відіграємо свою роль у ліквідації гендерного розриву, навмисно орієнтуючись на молодь і жінок у Південній Африці. Завдяки програмі для випускників Mimecast ми пропонуємо безробітним випускникам комплексне навчання та річне занурення в технічну службу або підтримку клієнтів. Ця ініціатива дає учасникам практичний досвід роботи, підвищуючи їхню впевненість і працевлаштування. Завдяки програмі ми залучили до нашої робочої сили 63% випускників, з яких 53% — жінки. Зокрема, 51% робочої сили та 60% технічних працівників Mimecast – жінки, що відображає прихильність компанії до гендерного розмаїття. Крім того, у нас є внутрішня стипендіальна програма, яка допомагає працівникам підвищувати освіту та навички. У нас також є громадська стипендіальна програма з допоміжними структурами, щоб допомогти вченим завершити атестацію або продовжити вищу освіту. Нарешті, 60% співробітників Mimecast є молодими (віком від 18 до 35 років), що підкреслює прагнення компанії збільшити кількість майбутніх фахівців з кібербезпеки в країні.

Висновок. Оскільки цього місяця ми відзначаємо День молоді, вкрай важливо вшановувати минуле, а також вирішувати сучасні виклики, з якими стикається молодь, наприклад цифровий гендерний розрив у таких критичних секторах, як кібербезпека. Заохочуючи різноманітність та залученість і розширюючи можливості молодих жінок за допомогою цільових ініціатив і стратегічних дій, країна може забезпечити надійну та стійку робочу силу, готову протистояти

майбутнім кіберзагрозам». ***(Why is Closing The Cybersecurity Gender Gap Critical? // Fusion Media Limited (https://za.investing.com/news/technology-news/why-is-closing-the-cybersecurity-gender-gap-critical-3196291). 14.06.2024).***

***

«Звіт Ocean опублікував останній звіт про дослідження ринку кібербезпеки Індонезії. Щоб цілісно зрозуміти ринок, необхідно оцінити низку факторів, включаючи демографічні показники, бізнес-цикли та мікроекономічні вимоги, які стосуються саме досліджуваного ринку. Крім того, дослідження ринку кібербезпеки в Індонезії демонструє детальний аналіз стану бізнесу, який представляє креативні шляхи розвитку компанії, фінансові фактори, такі як вартість виробництва, ключові регіони та темпи зростання.

Звіт Ocean, провідна компанія зі стратегічного консалтингу та дослідження ринку, у своєму нещодавньому дослідженні оцінила розмір ринку кібербезпеки Індонезії в 1,04 мільярда доларів США в 2022 році. Протягом прогнозованого періоду між 2023 і 2029 роками Report Ocean очікує, що розмір ринку кібербезпеки Індонезії досягне буму. вражаючий CAGR у 24,29%, досягнувши значення 3,83 мільярда доларів США до 2029 року. Зростання кількості випадків кібератак і зростаюча складність цих атак є двома основними факторами розвитку індонезійського ринку кібербезпеки. Уряд і підприємства впроваджують необхідні заходи безпеки, оскільки, за даними Asmag, Індонезія є мішенню номер один для кібератак, одержуючи майже 42 000 атак на день. Це сприяє стрімкому зростанню індонезійського ринку кібербезпеки…

За галузевою вертикаллю ринок кібербезпеки Індонезії сегментований на аерокосмічну та оборонну сферу, уряд, BFSI, IT та телекомунікації, охорону здоров’я, роздрібну торгівлю, виробництво тощо. На сегмент BFSI припадає найвища частка ринку. Зростаюча тенденція до віддаленої роботи, гібридної робочої сили, хмарних програмних платформ і платформ онлайн-платежів піддала сектор BFSI новим кіберзагрозам. Співробітники більше не отримують доступ до даних виключно через мережі та системи, які контролюються компанією. Як

наслідок, індустрія BFSI в Індонезії спостерігає різке зростання попиту на рішення кібербезпеки.

Пандемія COVID-19 відкрила значні можливості для зростання індонезійського ринку кібербезпеки завдяки значному сплеску кіберзагроз і витоку даних. Згідно зі звітом Reuters у вересні 2021 року, Індонезійська картка повідомлень про здоров'я (eHSC) (також відома як програма для тестування та відстеження COVID-19) розкрила особисті дані та стан здоров'я 1,3 мільйона людей через підозрювану помилку в безпеці. Крім того, зростаюча поширеність віддаленої роботи та все більше використання хмарних обчислень і програмного забезпечення також наражають важливі дані організацій на потенційні кіберзагрози. Очікується, що ці фактори сприятимуть інтеграції передових заходів кібербезпеки в Індонезії, сприяючи загальному зростанню ринку…

Основні гравці, що працюють на ринку кібербезпеки Індонезії, включають: Trend Micro Inc., Caulis Inc., Internet Initiative Indonesia, Inc., IBM Corporation, Cisco Systems, Inc., LAC Co. Ltd., SCSK Corporation, NEC Corporation, Spider Labs Ltd., Cybereason Indonesia Corporation, Caulis Inc. і Cybersecurity Cloud, Inc. Для подальшого збільшення своєї частки на ринку ці компанії використовують різні стратегії, зокрема злиття та поглинання, партнерства, спільні підприємства, ліцензійні угоди та запуск нових продуктів.

Поглиблений аналіз звіту надає інформацію про потенціал зростання, майбутні тенденції та ринок кібербезпеки Індонезії. У ньому також висвітлюються фактори, що впливають на прогнози загального розміру ринку. У звіті обіцяють надати останні технологічні тенденції на ринку кібербезпеки Індонезії та статистику галузі, щоб допомогти особам, які приймають рішення, приймати обґрунтовані стратегічні рішення. Крім того, у звіті також аналізуються драйвери зростання, виклики та конкурентна динаміка ринку…» ***(Indonesia Cybersecurity Market Demand And Growth Rate Forecast 2024-2032 // Taiwan News (https://www.taiwannews.com.tw/news/5890097). 14.06.2024).***

***

«Нещодавні вибори в Південній Африці проходили на тлі підвищеної стурбованості щодо кібербезпеки, коли країна зіткнулася зі сплеском цифрових атак, націлених на критичну інфраструктуру та підприємства. Вразливі місця в системі цифрового захисту країни були оголені через порушення в урядових установах, включаючи Виборчу комісію, напередодні виборів.

Реабецве Мотсамаі, менеджер із маркетингу та комунікацій MakwaIT Technologies, заздалегідь попереджав: «Ці атаки, які могли поставити під загрозу конфіденційні дані, як-от особиста інформація чи фінансові записи, підкреслюють вразливість критичної інфраструктури та підкреслюють нагальну потребу в розширеному запобіганні загрозам, оскільки серйозність і очікується ескалація частоти атак».

Ландшафт загроз поширювався за межі державного сектору протягом усього періоду виборів. За даними охоронної фірми Check Point, південноафриканські підприємства продовжували стикатися з у середньому понад 1000 атак на тиждень. Незважаючи на те, що 73% організацій передбачали підривний інцидент з кібербезпекою протягом двох років, лише 7% були належним чином підготовлені до виборів.

Посилаючись на індекс готовності Cisco Cybersecurity Readiness Index за 2024 рік, Мотсамаі зазначив, що кібератаки стають «більш витонченими, поширеними та частими – випереджаючи поточні засоби захисту бізнесу». Її наголос на необхідності для організацій постійно вдосконалювати свої заходи безпеки виявився доречним із розгортанням сезону виборів.

У зв’язку з тим, що вибори відбулися в Південній Африці та заплановані на цей рік у 19 інших африканських країнах, попередження Інтерполу про дві загрози, які швидко поширюються – програмне забезпечення-вимагач і компрометація бізнес-електронної пошти (BEC) – залишалися актуальними протягом усього виборчого процесу.

Програмне забезпечення-вимагач: постійна загроза

Напередодні виборів 78% південноафриканських компаній стали жертвами атак програм-вимагачів, головними цілями яких були Porsche і TransUnion. Ці

атаки, які шифрують життєво важливі дані та вимагають плату за їх оприлюднення, стояли за порушеннями в державних установах.

Що стосується, лише 19% організацій вважали програми-вимагачі значною загрозою в рік виборів. Це самовдоволення викликало занепокоєння, враховуючи, що середня вартість атаки програм-вимагачів оцінювалася в 5,13 мільйона доларів.

Motsamai відстоював багатосторонній підхід до зменшення ризиків програм-вимагачів, включаючи навчання персоналу, впровадження надійної безпеки електронної пошти та кінцевих точок, розгортання вдосконаленого захисту від зловмисного програмного забезпечення та регулярне резервне копіювання критичних даних. Ці заходи виявилися вирішальними під час виборів.

Погрози електронною поштою на основі ШІ під час виборів

За рік, що передував виборам, компрометація бізнес-електронної пошти, складної форми фішингу, зросла майже вдвічі Згідно зі звітом Mimecast про стан безпеки електронної пошти та співпраці за 2024 рік. П’ятдесят сім відсотків південноафриканських компаній стали жертвами цих атак, у тому числі Пасажирське залізничне агентство Південної Африки, яке втратило 30,6 мільйона рандів.

«BEC швидко стає серйозною загрозою, особливо з прогресом у штучному інтелекті, який робить атаки більш витонченими та їх важко виявити», — попередив Мотсамаї. Це передбачення справдилося, оскільки шахраї використовували ШІ, щоб видавати себе за законних контактів протягом сезону виборів, намагаючись обманом змусити компанії здійснювати неавторизовані платежі або перенаправляти кошти.

Для боротьби з цією загрозою Мотсамай порадив бути пильними щодо несподіваних платіжних запитів, рекомендував перевіряти незаплановані або термінові інструкції через надійні контактні канали та застосовувати інструменти автентифікації електронної пошти. Ці запобіжні заходи виявилися цінними в період підвищеного ризику виборів.

Ландшафт кібербезпеки після виборів

Як і очікувалося, ландшафт кіберзагроз у Південній Африці змінився після виборів, коли зловмисники перемістили фокус з політичних планів на фінансові злочини. Вплив варіювався від фінансових втрат і репутаційної шкоди до регулятивних штрафів і, в деяких випадках, збоїв у національних службах.

Висновок Мотсамаї залишився слушним: «Запроваджуючи передові стратегії запобігання загрозам і розвиваючи культуру обізнаності про кібербезпеку, державні та приватні організації можуть зменшити свій ризик».

Оскільки Південна Африка вийшла з виборчого процесу, постійна готовність країни до кібербезпеки залишається надзвичайно важливою для захисту її демократичних інститутів та економічної стабільності перед обличчям постійних цифрових загроз». ***(Brendon Petersen. Cybersecurity Threats Persisted Through South Africa's Elections // Memeburn (https://ventureburn.com/2024/06/cybersecurity-threats-persisted-through-south-africas-elections/). 27.06.2024).***

***

Кіберстрахування

«Вперше Національний центр кібербезпеки Великобританії («NCSC») співпрацював з індустрією кіберстрахування, а саме; Асоціація британських страховиків («ABI»), Британська асоціація страхових брокерів («BIBA») і Міжнародна асоціація андеррайтингу («IUA»), щоб виробити спільне керівництво для організацій, які розглядають можливість сплати викупу. Рекомендації було опубліковано 14 травня 2024 року («Керівництво»).

Завжди гаряче обговорюється питання про те, чи повинні жертви кібератак платити вимоги викупу чи ні. Керівництво не відповідає на цю дискусію, зазначаючи, що це остаточне рішення жертви. Однак Посібник містить дуже необхідні поради для організацій, які розглядають можливість оплати, заповнюючи чітку прогалину в знаннях, що існує з загальнодоступних джерел.

Це сталося після звіту RUSI, опублікованого в липні 2023 року, в якому детально викладені висновки та рекомендації після незалежного дослідження передбачуваної ролі індустрії кіберстрахування в стимулюванні кримінальної екосистеми шляхом покриття виплат викупу. Доповідь RUSI критикувала «чорно-білу позицію» британського уряду щодо виплати викупу.

Критики можуть сказати, що будь-яке керівництво, яке не лобіює проти платежів, матиме ефект дозволу. Однак той факт, що платежі здійснюються і що вони не завжди є незаконними чи незаконними, є джином, якого неможливо помістити назад у свою пляшку. Натомість це сміливе керівництво гарантує, що організації продумають усі відповідні міркування перед здійсненням платежу. Хоча на перший погляд Посібник може здатися переліком міркувань «здорового глузду», часто здоровий глузд втрачає вікно, коли намагаються прийняти складне рішення, засноване на оцінці ризику, серед паніки атаки програм-вимагачів. Роблячи це, Керівництво прагне: (i) допомогти жертвам кібератак мінімізувати збої та вартість інциденту; (ii) зменшити кількість сплачуваних викупів; та (iii) зменшити розмір викупу, який вирішують заплатити жертви.

Цей альянс між NCSC та індустрією кіберстрахування у публікації цього Посібника слід вітати.

Не панікуйте та знайдіть час, щоб дослідити та оцінити свої можливості

У Керівництві наголошується на тому, що заявам і обіцянкам суб'єктів загрози не можна довіряти. Зловмисники чинять тиск на компанії, щоб вони приймали необдумані рішення, до яких потрібно заплатити; дотримання термінів, створюючи враження, що альтернативи відновленню немає, і стверджуючи, що вони публікуватимуть виманені дані в Інтернеті, якщо не буде здійснено оплату. Однак насправді, якщо організація витратила деякий час на дослідження масштабів атаки та перевірку заяв учасників загрози, перш ніж поспішати з будь-яким рішенням, вона може виявити, що:

- існують альтернативні способи відновлення (часткового або повного) – наприклад, за допомогою життєздатних резервних копій або доступу до ключа дешифрування через треті сторони, такі як правоохоронні органи. Крім того, у

Керівництві зазначено, що оплата не гарантує доступу до постраждалих пристроїв і даних, і іноді, особливо для великих організацій зі складними мережами, насправді може бути швидше використовувати резервне копіювання.

- вплив на бізнес, з точки зору операцій, даних і фінансів, може бути меншим, ніж передбачалося спочатку – Посібник заохочує організації розглянути: (i) можливі обхідні шляхи, які можна прийняти для управління збоями; (ii) характер і обсяг скомпрометованих даних і, таким чином, пов'язані з цим ризики для осіб; (iii) витрати на перерву в бізнесі та зусилля по відновленню (включаючи витрати на понаднормову роботу персоналу та зовнішню підтримку), які насправді можуть бути меншими, ніж будь-яка обговорена вимога викупу.

Зверніться до зовнішніх експертів

Посібник рекомендує залучати зовнішніх експертів, таких як постачальники кібербезпеки/реагування на інциденти в IT, консультанти з реагування на порушення та професійні учасники переговорів щодо загроз, щоб надавати підтримку в судовому розслідуванні, консультувати щодо юридичних і нормативних зобов'язань і розвідки про загрози/тактику переговорів відповідно – усе які значно покращують якість прийняття рішень організацією. Посібник спрямовує організації скористатися перевагами групи постачальників, схваленою їхніми кіберстраховиками, і списком рекомендованих NCSC компаній CIR.

Попередження

Керівництво також містить наступні застереження:

- Зловмисники є злочинцями, і їм не можна довіряти - важливо пам'ятати, що оплата викупу не є безпечним способом запобігти публікації викрадених даних - обіцянка кіберзлочинця видалити дані в обмін на оплату не може бути довірою. Це також не спосіб відмовитися від необхідності проведення ретельної оцінки скомпрометованих даних не лише для перевірки тверджень суб'єкта загрози, але й для оцінки ризику даних і розгляду питання про необхідність повідомлення суб'єкта даних відповідно до статті 34 GDPR.

- сплата викупу не відповідає нормативним зобов'язанням організації [2] – як раніше повідомлялося в спільному листі NCSC та ICO до Товариства юристів та

Ради адвокатів, сплата викупу не розглядається як крок, який зменшує потенційну шкоду для суб'єктів даних, і не допоможе організації уникнути регуляторних наслідків або зменшить суму будь-якого штрафу за ICO.

- розглянути законодавчу та нормативну практику щодо платежів – у Керівництві зазначено, що платіж може бути незаконним, наприклад, якщо він здійснюється суб'єкту господарювання чи території зі списку санкцій Великобританії. Він також позначає, що якщо це стосується дочірніх компаній, розташованих в інших юрисдикціях, також може знадобитися врахувати додаткові місцеві закони та правила.

Насамкінець, Посібник рекомендує організаціям повідомляти про інциденти владі Великобританії, включаючи NCSC, і встановлює переваги цього, зокрема нагадує організаціям, що це може призвести до більш сприятливої відповіді регуляторів, наприклад меншого штрафу від ICO.

Коментарі

Посібник не є загальною інструкцією не платити, але він все одно перешкоджає організаціям робити це без належного дослідження всіх інших варіантів та оцінки ризиків. Оплата представлена як абсолютний крайній засіб, і навіть тоді немає жодної гарантії, що вона зможе досягти обіцяних результатів, як стверджує суб'єкт загрози. Керівництво відображає зрілість позиції британського уряду, яку дехто раніше критикував як надто спрощену позицію «не плати».

Це Керівництво має міжнародне значення, і буде цікаво побачити, чи інші юрисдикції офіційно приймуть подібне керівництво.

Мервін Скіт, директор із загальної страхової політики ABI, сказав: «Це спільне керівництво є ще одним позитивним кроком у боротьбі з кіберзлочинністю у Великій Британії, і ми з нетерпінням чекаємо продовження співпраці з NCSC над цією спільною метою». Таким чином, ця спільна точка зору NCSC і індустрії кіберстрахування може бути першою з наступних». ***(Hans Allnutt and Camilla Elliot. Cyber ransom payments - The NCSC and cyber insurance industry unite to fill the guidance void // DAC Beachcroft (https://www.dacbeachcroft.com/en/What-we-think/Cyber-ransom-payments). 10.06.2024).***

***

«У той час як ринок страхування кібернетичної інформації та конфіденційності даних продовжує розвиватися, ескалація кібернетичних загроз у поєднанні з дедалі зростаючими національними та зарубіжними правилами щодо конфіденційності даних і розкриття кіберподій створює проблеми для компаній, які прагнуть отримати достатньо страхування для пом'якшення фінансові ризики кібератак.

За останні 16 місяців було введено низку нових державних і федеральних нормативних актів щодо кібербезпеки для додаткового захисту акціонерів і споживачів. Ці нові правила збільшують витрати та ризик для репутації кожної нової кібератаки. У цій статті досліджуються тенденції ринку кіберстрахування в поточному нормативному ландшафті, щоб допомогти компаніям забезпечити адекватне покриття регуляторних ризиків кіберінцидентів.

Поточний нормативний ландшафт

У 2023 році SEC продемонструвала своє зобов'язання притягувати компанії до відповідальності за ненадання інформації, пов'язаної з кібербезпекою. У березні 2023 року Комісія з цінних паперів і цінних паперів (SEC) подала примусовий позов проти Blackbaud у зв'язку з тим, що вона нібито не розкрила адекватну інформацію щодо атаки програм-вимагачів, яка нібито вплинула на клієнтів компанії.

Після цих примусових дій 15 грудня 2023 року набули чинності нові правила кібербезпеки цінних паперів і бірж США. Ці правила спрямовані на публічні компанії та вимагають відкритого розкриття суттєвих інцидентів кібербезпеки протягом чотирьох робочих днів після виявлення. Нові правила також вимагають від публічних компаній розкривати свою практику управління ризиками кібербезпеки, структури управління та процедури реагування на інциденти у своїх щорічних звітах 10-K.

Ці правила набули чинності після тривалого періоду коментарів, під час якого компанії висловлювали занепокоєння щодо практичних ускладнень,

пов’язаних із коротким періодом розкриття інформації, а також занепокоєння щодо публічного розкриття подробиць про практику кібербезпеки компанії.

Хоча повний вплив цих правил ще не видно, нові вимоги до звітності для публічних компаній уже призвели до розкриття інформації кількома відомими компаніями через документи SEC 8-K, що стосуються кіберінцидентів. Хоча правило вимагає лише розголошення суттєвих інцидентів кібербезпеки, у деяких випадках ці компанії розкривають інформацію через велику обережність.

Наприклад, 19 січня 2024 року компанія Hewlett Packard подала заяву 8-K, яка розкриває кіберінцидент, який стався 12 січня 2024 року, коли підозрюваний суб’єкт національної держави отримав несанкціонований доступ до хмарного середовища електронної пошти HPE.

Компанія окремо зазначила, що компанія ще не дійшла висновку щодо суттєвості порушення, заявивши, що «станом на дату подання цієї заяви інцидент не мав істотного впливу на діяльність Компанії, і Компанія не визначила інцидент має розумну ймовірність суттєвого впливу на фінансовий стан або результати діяльності Компанії». Пізніше компанія підтвердила, що розкрила інформацію, намагаючись відповідати новим правилам SEC.

Кібербезпека, ймовірно, залишиться в центрі уваги SEC у 2024 році з розробкою правил щодо управління ризиками кібербезпеки для брокерів і дилерів.

На державному рівні нормативні акти, що регулюють конфіденційність даних, продовжують займати центральне місце. Хоча Каліфорнія спочатку лідирувала в регулюванні конфіденційності даних із прийняттям Закону Каліфорнії про конфіденційність споживачів (CCPA) і Закону Каліфорнії про права на конфіденційність (CPRA) у 2018 році, нещодавно інші штати приєдналися до цієї категорії, ухваливши комплексні закони про конфіденційність, які застосовуються в усіх галузях і регулюють спосіб збору та зберігання конфіденційної інформації.

Ці правила зазвичай вимагають від компаній інформувати споживачів, якщо вони збирають та/або продають дані, і надають споживачеві можливість «відмовитися» від такої практики. На сьогоднішній день 15 штатів прийняли

всеосяжні закони про конфіденційність даних, і в 2025 році їх, ймовірно, прийме ще більше штатів.

За кордоном, у Сполученому Королівстві, Директива про мережеву та інформаційну безпеку (NIS2) має набути чинності в жовтні 2024 року. Ця постанова є продовженням попередньої Директиви Європейського Союзу з кібербезпеки, яка спрямована на досягнення вищих стандартних рівнів кібербезпеки в Європейському Союзі.

Серед іншого, NIS2 розширює вимоги до кібербезпеки, розширює сферу охоплених організацій і запроваджує суворіші санкції за порушення по всій Європі. NIS2 вимагає, щоб початковий звіт про інцидент кібербезпеки був надісланий компетентному органу протягом 24 годин, а більш детальний звіт про повідомлення – протягом 72 годин.

Так само Закон ЄС про кібернетостійкість, який, як очікується, набуде чинності в третьому кварталі 2024 року, передбачає певні обов'язкові вимоги щодо кібербезпеки для виробників і роздрібних торговців.

Страхове покриття кіберрегуляторних ризиків

Ці регулятивні тенденції додатково ілюструють важливість страхування кібервідповідальності. Незважаючи на те, що після 2023 року ринок страхування дещо пом'якшився, багато учасників галузі повідомили про дещо зниження премій і значне зростання ринку кіберстрахування, покриття регуляторних ризиків загалом стало більш обмеженим через зростання занепокоєння щодо витрат на дотримання нормативних вимог, розслідування, розрахунки та штрафні санкції.

В опитуванні KYND 2024 року, в якому взяли участь понад 100 страхових компаній і брокерів, 11% респондентів визначили регуляторні зміни як провідну рушійну силу продажів кіберстрахування у 2024 році, і ми можемо побачити, що премії за покриття почнуть відображати зростання ризиків, коли ми рухатимемося далі компанія захисту кібербезпеки у 2024 році.

Власники полісів ще багато чого можуть зробити, щоб отримати оптимальне покриття регулятивних ризиків кібербезпеки.

По-перше, компанії можуть краще захистити себе від регуляторних проблем, першочергово визначаючи, як запобігти та зменшити кіберризики та ризики конфіденційності та витрати. Згідно зі звітом IBM Cost of Data Breach Report 2023, середня вартість витоку даних у 2023 році становила 4,45 мільйона доларів. Компанії можуть завчасно захистити себе, проводячи регулярні тренінги для співробітників, регулярні перевірки й оцінки безпеки, а також розробляючи ефективний план реагування на інциденти. Крім того, компанії повинні бути в курсі змін нормативних вимог, щоб переконатися, що вони залишаються відповідними.

Опитування 2024 року під назвою «State of Security – The Race to Harness AI», автором якого є Splunk, компанія з кібербезпеки, повідомляє, що 45% респондентів назвали кращу узгодженість із вимогами відповідності як найкращу область для вдосконалення у 2024 році.

По-друге, компанії повинні ретельно переглянути свою поточну кіберполітику, щоб виявити прогалини та гарантувати, що вони мають покриття для своїх збільшених ризиків унаслідок нормативних правил. У галузі кіберстрахування існує незначна стандартизація, і мова, яка використовується в конкретному полісі, визначатиме обсяг покриття, а також винятки та обмеження. У разі потреби компаніям слід шукати адекватне додаткове покриття.

Наприклад, ствердне покриття незаконного збору даних може бути особливо важливим, враховуючи постійно зростаюче нормативне середовище, що регулює збір даних споживачів. Це може включати покриття збитків, спричинених незаконним збором особистої чи конфіденційної інформації (незалежно від того, чи сприяла подія кібербезпеки такому ймовірному незаконному збору).

Крім того, враховуючи нові вимоги Комісії з цінних паперів та цінних паперів щодо розкриття практики управління ризиками та структур управління, може знадобитися охоплення лише керівників компанії. Деякі політики можуть ствердно охоплювати претензії про невиконання керівниками своїх обов’язків у сфері кібербезпеки.

І, хоча деякі кіберполітики часто охоплюють оцінку штрафів і покарань у розслідуваннях і змагальних провадженнях за участю Федеральної комісії зі зв'язку та Федеральної торгової комісії, вони можуть виключати покриття позовів щодо цінних паперів. Пошук підтвердженого покриття відповідності SEC може бути корисним.

Ми можемо побачити нові схвалення політики, спрямовані на ці ризики, включно з схваленнями, що покривають витрати, пов'язані з оновленими зобов'язаннями Комісії з цінних паперів і бірж США звітувати про кіберінциденти, включаючи юридичні збори за відповідність і вимоги до розкриття інформації, як-от подання 8-К.

Нарешті, враховуючи стислі часові рамки для розкриття суттєвих кібер-інцидентів згідно з новими правилами SEC, компанії повинні мати можливість оперативно реагувати на кібер-події. Водночас деякі поліси кіберстрахування вимагають від страхувальника отримання схвалення, перш ніж залучати будь-якого постачальника чи консультанта з реагування на інциденти. Компанії повинні розглянути питання про отримання попереднього дозволу для постачальників реагування на інциденти та консультантів із питань конфіденційності даних, щоб мінімізувати затримки.

Консультант із страхового покриття може допомогти, проаналізувавши прогалини в страховому полісі, покращивши формулювання полісу та вирішивши претензії щодо страхового покриття, пов'язані з кібернетичними засобами…» ***(Stephanie E. Gee, Courtney C.T. Horrigan, Evan Knott. Cyber and data privacy insurance trends in an era of increased regulation // Reuters (https://www.reuters.com/legal/legalindustry/cyber-data-privacy-insurance-trends-an-era-increased-regulation-2024-06-13/). 13.06.2024).***

***

«Підрозділ компанії General Dynamics, іспанська компанія Santa Barbara Systems, яка займається ремонтом танків Leopard для доставки в Україну, зазнала кібератаки, яка вивела з ладу її веб-сайт, повідомила проросійська хакерська група.

Речник General Dynamics у Німеччині сказав, що оборонний підрядник все ще аналізує причину збою веб-сайту, додавши, що всі його операції в Європі працюють нормально.

Хакерська група NoName у службі обміну повідомленнями Telegram взяла на себе відповідальність за розподілену атаку типу «відмова в обслуговуванні» (DDoS).

DDoS-атаки спрямовують великі обсяги інтернет-трафіку на цільові сервери, щоб вивести їх з офлайн.

«Ми направили наші DDoS-ракети на сайти в русофобській Іспанії», - написала група, яка часто спрямовує такі дії проти країн, які підтримують Україну, у Telegram у вівторок.

Минулого місяця НАТО заявило, що Росія стоїть за посиленням кампанії гібридних атак на компанії та інфраструктуру в державах-членах, звинувачення, яке Росія відкинула як «дезінформацію».

«Santa Barbara» збирає важкі транспортні засоби, такі як танки «Леопард» і артилерійське обладнання для іспанської армії, а також бере участь у модернізації законсервованих іспанських танків «Леопард» для доставки українській армії, повідомляє Міністерство оборони…» ***(Russians Hack Spain Firm Preparing Tanks for Ukraine // news max (https://www.newsmax.com/world/globaltalk/russia-hackers-website/2024/06/05/id/1167536/?utm_source=flipboard&utm_content=FlipboardCanada%2Fmagazine%2FWorld+News). 05.06.2024).***

***

«Провідні охоронні фірми попереджають, що суб'єкти, пов'язані з Росією, включно зі спецслужбами та хактивістами, піддаються високому

ризику здійснення кібератак і кампаній з дезінформації проти організацій, пов'язаних з Олімпіадою в Парижі.

Тривала напруженість між Москвою та європейськими державами, а також рішення Міжнародного олімпійського комітету заборонити Росії брати участь у майбутніх літніх Олімпійських іграх через її вторгнення в Україну у 2022 році є двома основними причинами, які, ймовірно, спричинять сплеск кібератак з боку російських акторів, вважають дослідники. від Insikt Group Recorded Future у звіті у вівторок.

«Москва, ймовірно, бачить значну вигоду від націлювання на майбутні Олімпійські ігри в тій чи іншій формі», – йдеться у звіті, підвищуючи ймовірність того, що група військової розвідки Sandworm і групи хакерів і витоків, такі як Turla, можуть отримати наказ від Кремля діяти.

Діяльність може варіюватися від шпигунських кампаній, націлених на персонал МОК, до зривів трансляції подій і кампаній впливу.

Російські державні хакери зламали попередні Олімпійські ігри, в тому числі. проти спортивних і антидопінгових організацій напередодні літніх Ігор у Токіо в 2020 році

Однією зі стратегій, яку Москва може прийняти, є покладатися на кіберпроксі, такі як групи хактивістів, або звернутися за допомогою до іншої групи національних держав, щоб зберегти правдоподібне заперечення, кажуть дослідники.

Microsoft у понеділок попередила про зловмисну російську кібердіяльність, включаючи операції впливу, спрямовані на очорнення репутації МОК.

Російські групи, які ведуть ці кампанії, включають загрозливих акторів, яких Microsoft відслідковує як Storm-1679 і Storm-1099, або Doppelganger, які почали проводити кампанії з дезінформації минулого жовтня.

Групи вже почали поширювати в Telegram дезінформацію, зосереджену на Олімпійських іграх, використовуючи підроблені аудіо, створені штучним інтелектом, які імітують Тома Круза, і підроблені відео, нібито надійшли від французької телекомпанії France24.

«Центр аналізу загроз Microsoft спостерігав, як старі тактики змішуються зі штучним інтелектом у зловмисній діяльності. Використання зручних комп'ютерних спецефектів і широка маркетингова кампанія, включаючи фальшиві підтвердження від західних ЗМІ та знаменитостей, вказує на значне зростання навичок і зусиль. у порівнянні з більшістю кампаній Influence Operations (IO)», - заявили в компанії.

Російські кампанії з дезінформації поки що були спрямовані на франкомовних людей, але це, ймовірно, зміниться ближче до дати початку конкурсу в липні. За словами Microsoft, російські загрозливі групи, ймовірно, активізують використання генеративного штучного інтелекту та, ймовірно, перейдуть на англійську, німецьку та інші мови, щоб максимізувати видимість і ефективність цих кампаній». ***(Akshaya Asokan. Russian Cyberthreat Looms Over Paris Olympics // Information Security Media Group, Corp. (https://www.databreachtoday.com/russian-cyberthreat-looms-over-paris-olympics-a-25402?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 04.06.2024).***

***

«Принаймні з березня 2023 року суб'єкти, спонсоровані державою Китаю, атакували урядову установу в рамках кампанії кібершпигунства, яку дослідники відслідковують як Багряний палац.

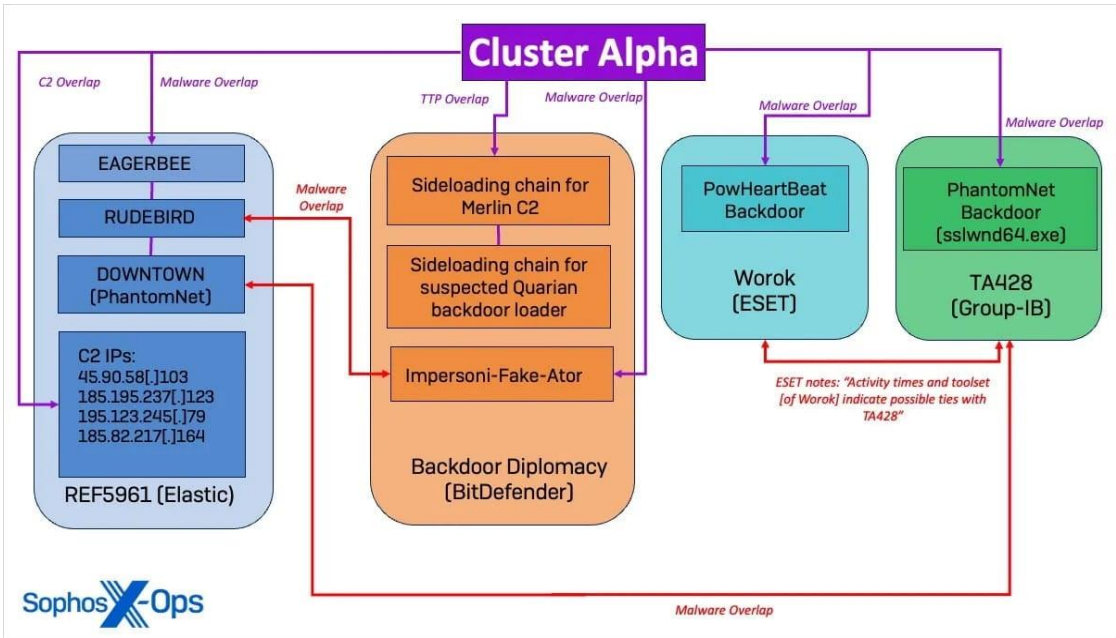
Відповідно до звіту компанії з кібербезпеки Sophos, кампанія спиралася на нові варіанти шкідливого програмного забезпечення та три різні кластери активності, які вказують на скоординовану атаку.

Хоча початковий доступ визначити не вдалося, дослідники спостерігали пов'язану активність, починаючи з початку 2022 року, яка використовувала спеціальне шкідливе програмне забезпечення Nupakage, раніше пов'язане з китайською групою загроз Mustang Panda.

Три кластери діяльності

Sophos виявила три кластери активності, пов’язані з відомими китайськими групами загроз, такими як «BackdoorDiplomacy», «REF5961», «Worok», «TA428» і підгрупа APT41 Earth Longzhi.

Аналітики з високою впевненістю оцінили, що робота цих кластерів централізовано координується в рамках єдиної організації.



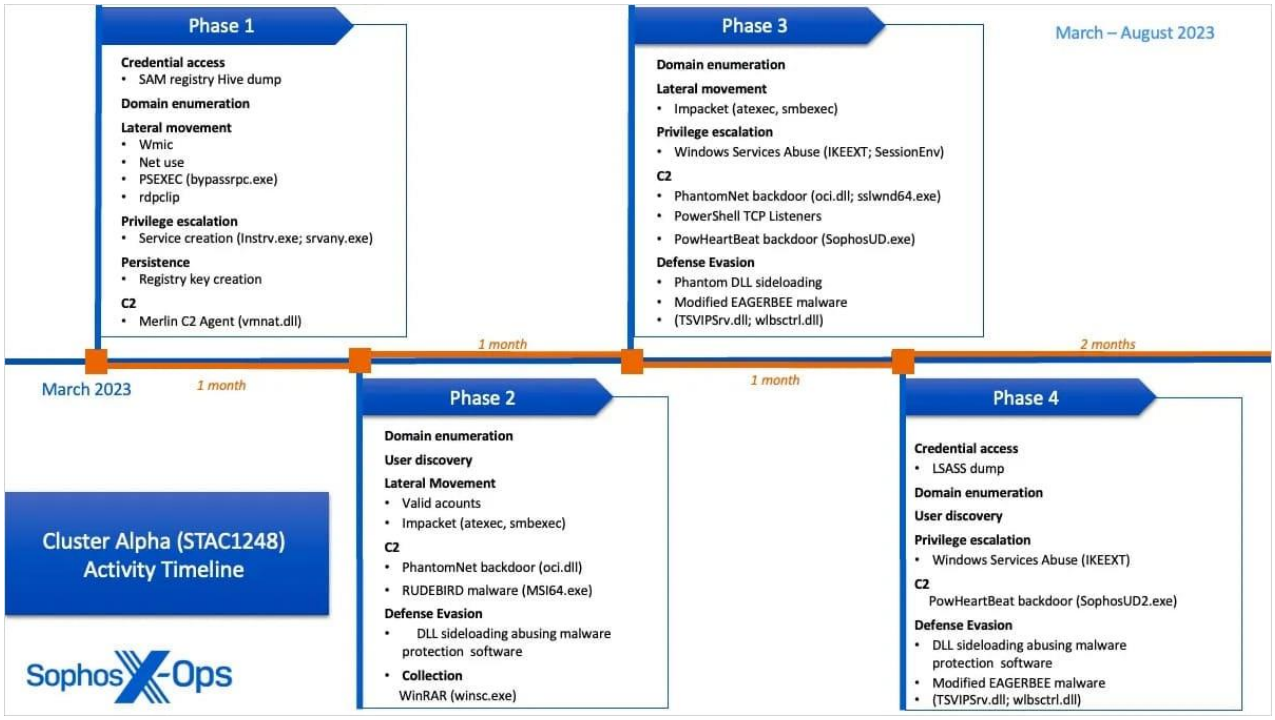
Збігається з відомими суб’єктами загрози

Кластер Alpha (STAC1248): активний з початку березня по серпень 2023 року, він зосереджувався на розгортанні оновлених варіантів зловмисного програмного забезпечення «EAGERBEE», здатних порушити мережевий зв’язок агентств безпеки.

Основною метою було відобразити підмережі серверів і перерахувати облікові записи адміністраторів шляхом проведення розвідки інфраструктури Active Directory.

Діяльність покладалася на кілька постійних каналів командування та контролю (C2), включаючи Merlin Agent, бекдор PhantomNet, зловмисне програмне забезпечення RUDEBIRD і бекдор PowHeartBeat.

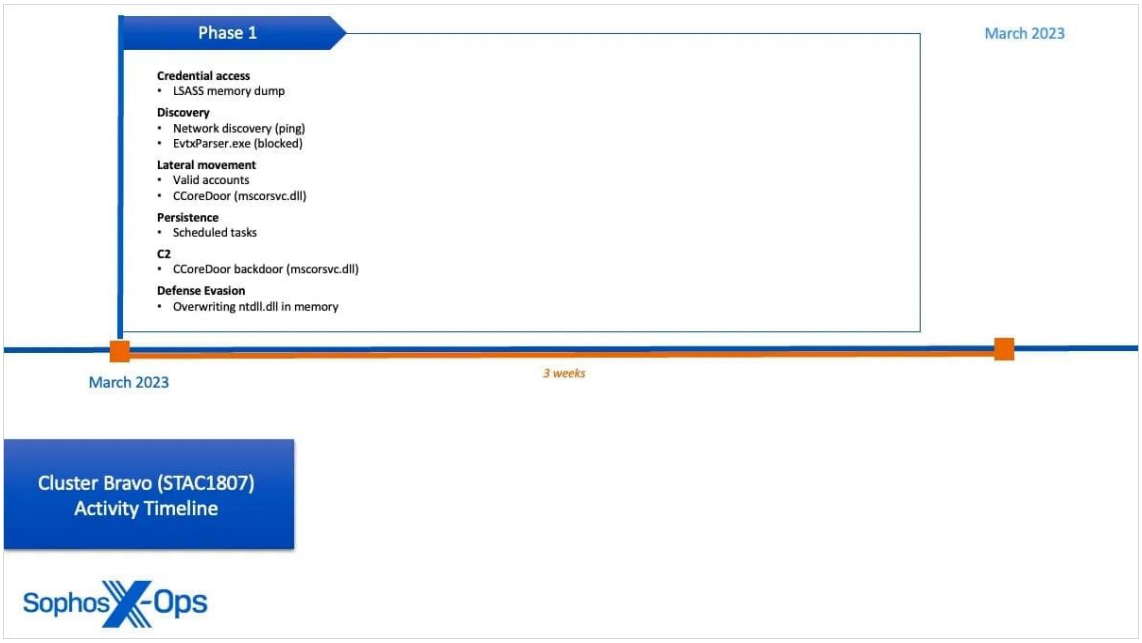
Щоб уникнути виявлення, зловмисник використовував живі двійкові файли (LOLBins) для збереження служби з підвищеними привілеями SYSTEM і здійснив бокове завантаження DLL із вісьмома унікальними DLL, використовуючи служби Windows і законні двійкові файли Microsoft.



Фази активності кластера Альфа

Cluster Bravo (STAC1807): активний лише три тижні в березні 2023 року, він зосереджувався на бічному русі та наполегливості, скидаючи раніше невідомий бекдор під назвою «CCoreDoor» на цільові системи. Бекдор встановив зовнішній зв’язок C2, виконав виявлення та скинув облікові дані.

Актор використовував перейменовані версії підписаних двійкових файлів, які можна завантажувати збоку, щоб приховати бекдорне розгортання та полегшити бічний рух, а також перезаписав ntdll.dll у пам’яті, щоб від’єднати процес агента захисту кінцевих точок Sophos від ядра.

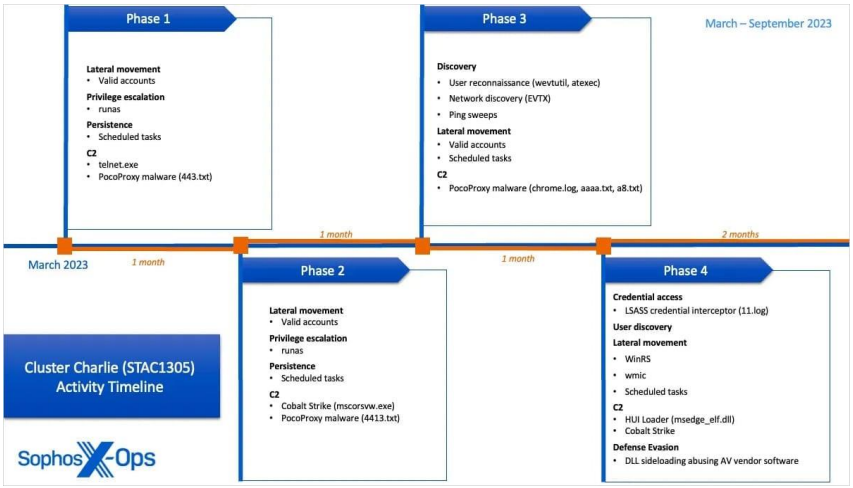


Активність кластера Браво

Кластер «Чарлі» (SCAT1305): активний з березня 2023 року принаймні до квітня 2024 року, він займався постійним керуванням доступом і широкою розвідкою протягом тривалого періоду.

Актор розгорнув кілька зразків раніше не ідентифікованого шкідливого програмного забезпечення під назвою «PocoProxy», яке використовується для постійного зв’язку C2. Вони також використовували завантажувач HUI, щоб вставити Cobalt Strike Beacon у mstsc.exe, хоча ці спроби були заблоковані.

Крім того, зловмисник застосував перехоплювач облікових даних для входу LSASS для захоплення облікових даних на контролерах домену та провів масовий аналіз журналів подій і автоматичний аналіз ping для відображення користувачів і кінцевих точок у мережі.



Огляд діяльності кластера Чарлі

Кампанія Crimson Palace була спрямована на агентство уряду Південно-Східної Азії з метою кібершпигунства.

«Ми з помірною впевненістю оцінюємо, що кілька різних суб'єктів, спонсорованих китайською державою, брали активну участь у цій відомій урядовій організації Південно-Східної Азії принаймні з березня 2022 року», — пояснює Sophos.

«Хоча ми наразі не можемо з високою достовірністю визначити атрибуцію або підтвердити характер зв'язку між цими кластерами, наше поточне дослідження показує, що кластери відображають роботу окремих суб'єктів, яким доручає центральна влада з паралельними цілями в інтересах китайської держави» - Софос.

Загалом три кластери працювали в стандартний китайський робочий час (з 08:00 до 17:00 за центральноєвропейським стандартним часом), розбиваючи період на три частини, які не перетинаються, що свідчить про високий рівень координації.

Комбінована діяльність (вгорі) та ізоляція кластера (внизу)

Sophos виявила, що зловмисна активність різко зросла в деяких випадках, наприклад 12 червня 2023 року, коли в цільовій країні було вихідним. Ймовірно, це призвело до того, що захисники були недостатньо укомплектовані та здійснювали діяльність у той час, коли системи не контролювалися настільки ретельно.

Через відсутність видимості Sophos не зміг визначити початковий доступ, але оцінив, що загрозливий суб’єкт мав доступ до мережі щонайменше з березня 2022 року на основі виявлення шкідливого програмного забезпечення Nupakage, яке зазвичай використовується для викрадання даних.

Достовірне приписування або підтвердження зв’язку між трьома кластерами є складним. Дослідники Sophos вважають, що виявлена діяльність є «роботою окремих акторів, яким центральна влада доручає паралельні цілі в інтересах китайської держави».

Незважаючи на те, що Sophos заблокував імпланти C2 загрозливого актора в серпні 2023 року, і з тих пір активність Cluster Alpha не спостерігалася, дослідники кажуть, що активність Cluster Charlie спостерігалася після кількох тижнів тиші, і супротивник намагався зламати мережу та відновити роботу "на у вищому темпі й у більш ухиляючій манері».

Sophos продовжує відстежувати активність вторгнень у цільову мережу». ***(Bill Toulas. Chinese hacking groups team up in cyber espionage campaign // Bleeping***

Computer® LLC (https://www.bleepingcomputer.com/news/security/chinese-hacking-groups-team-up-in-cyber-espionage-campaign/?utm_source=flipboard&utm_content=waral01%2Fmagazine%2FRumors+Of+War). 05.06.2024).

***

«Данський центр кібербезпеки (CFCS) підвищив оцінку рівня загрози для руйнівних кібератак проти Данії з «низького» до «середнього» через зростання загроз з боку Росії, заявив міністр оборони у вівторок.

Згідно з CFCS, «середній» рівень, або три за п'ятирівневою шкалою, означає наявність одного або кількох суб'єктів, які мають намір і здатність до атак або шкідливої діяльності, але жодних ознак будь-яких конкретних планів такої діяльності.

«Ми все частіше бачимо Росію, яка готова кинути виклик країнам НАТО за допомогою диверсій, впливу на кампанії та кібератак», — заявив на прес-конференції міністр оборони Троелс Лунд Поульсен.

Поульсен заявив, що немає прямої військової загрози для Данії, посилаючись на Службу оборонної розвідки Данії». ***(Denmark raises threat level for destructive cyber attacks to 3 on 5-level scale // yahoo! finance (https://finance.yahoo.com/news/denmark-raises-threat-level-destructive-124252719.html?utm_source=flipboard&utm_content=other). 04.06.2024).***

***

«Голландська військова розвідка заявила в понеділок, що китайське кібершпигунство було більш масштабним, ніж передбачалося спочатку, і спрямоване проти західних урядів і оборонних компаній.

Агентство MIVD заявило, що підтримувана державою китайська хакерська група, яка стояла за хакерською атакою на міністерство оборони Нідерландів у 2023 році, за кілька місяців забрала щонайменше 20 000 жертв по всьому світу, а можливо, і набагато більше.

Посольство Китаю в Гаазі не відразу відповіло на запит про коментар. Пекін постійно заперечує звинувачення в кібершпигунстві та заявляє, що виступає проти всіх форм кібератак.

«Ціль включала десятки західних урядів, міжнародних організацій і численних компаній, що працюють в оборонній промисловості», - йдеться в заяві MVID.

Він закликав організації прийняти принцип «Припустити порушення», згідно з яким передбачається, що успішна цифрова атака вже відбулася або відбудеться незабаром.

У квітні MIVD у своєму щорічному звіті заявив, що китайські шпигуни атакували голландську напівпровідникову, аерокосмічну та морську промисловість, щоб спробувати зміцнити збройні сили Китаю». ***(Dutch intelligence says Chinese cyber espionage goes wider than it suspected // Reuters (https://www.reuters.com/technology/cybersecurity/dutch-intelligence-says-chinese-cyber-espionage-goes-wider-than-it-suspected-2024-06-11/). 11.06.2024).***

***

«У четвер члени Конгресу США вимагали від Microsoft пояснити, як «каскад помилок, яких можна було уникнути», дозволив китайській хакерській групі зламати електронну пошту високопосадовців США.

Президент Microsoft Бред Сміт провів більше трьох годин, відповідаючи на запитання членів Комітету Палати представників з питань внутрішньої безпеки у Вашингтоні. Він запевнив їх, що кібербезпека все глибше вплітається в культуру технологічної компанії.

«Microsoft бере на себе відповідальність за кожну з проблем, згаданих» в дошкульному звіті уряду США про злам, «без жодних сумнівів чи вагань», - сказав Сміт комітету.

Рада з огляду кібербезпеки (CSRB) під керівництвом Міністерства внутрішньої безпеки США провела семимісячне розслідування минулорічного інциденту за участю пов'язаного з Китаєм кібершпигуна Storm-0558.

«Microsoft має величезний вплив як в урядових мережах, так і в мережах критичної інфраструктури», - сказав Сміту на відкритті слухань конгресмен і член комітету Бенні Томпсон.

«Ми всі зацікавлені у швидкому вирішенні питань безпеки, порушених у цьому звіті».

Операція, вперше виявлена Державним департаментом США в червні 2023 року, включала зломи офіційних і особистих поштових скриньок міністра торгівлі Джини Раймондо і посла США в Китаї Ніколаса Бернса.

Microsoft надає послуги хмарних обчислень, такі як Azure або Office360, в яких зберігаються конфіденційні дані та здійснюються бізнес-операції та урядові операції в основних секторах економіки.

У звіті критикується корпоративна культура Microsoft, яка «суперечить... рівню довіри клієнтів до компанії».

Огляд виявив низку операційних і стратегічних рішень, прийнятих Microsoft, які відкрили двері для витоку інформації, включаючи нездатність компанії виявити скомпрометований ноутбук нового співробітника після корпоративного поглинання в 2021 році.

Також було виявлено, що Microsoft не дотримується стандартів безпеки, яких дотримуються конкуруючі хмарні компанії, такі як Google, Amazon та Oracle.

«Рада вважає, що цьому вторгненню можна було запобігти, і воно ніколи не повинно було статися», - йдеться в огляді, який вказує на «каскад помилок Microsoft, яких можна було уникнути, і які дозволили цьому вторгненню досягти успіху».

У звіті також рекомендується, щоб Microsoft розробила та оприлюднила план із зазначенням термінів впровадження масштабних реформ безпеки у всіх своїх продуктах та практиках.

«Справжній виклик полягає в тому, як досягти ефективних довготривалих культурних змін», - сказав Сміт, зазначивши, що в Microsoft працює майже 226 000 співробітників.

Сміт заявив, що в Microsoft працює еквівалент 34 000 інженерів, які працюють повний робочий день над усуненням недоліків у сфері безпеки, і назвав цей проект найбільшим інженерним проектом, присвяченим кібербезпеці, в історії цифрових технологій.

За словами Сміта, в середу рада директорів Microsoft схвалила зміни, які пов'язують досягнення в галузі кібербезпеки з річними бонусами для вищого керівництва та інтегрують їх у щорічний огляд кожного співробітника. Сміт поінформував комітет, що Microsoft щодня виявляє близько 300 мільйонів кібератак на своїх клієнтів, більшість з яких походять з Китаю, Ірану, Кореї, Росії та Кореї, а також операції з вимагання викупу.

«Ми маємо справу з чотирма грізними ворогами - Китаєм, Росією, Північною Кореєю та Іраном, і вони стають кращими», - сказав Сміт.

«Ми повинні очікувати, що вони працюватимуть разом; вони здійснюють атаки з надзвичайною швидкістю».

Сміт додав, що противники неминуче використовуватимуть штучний інтелект для все більш витончених атак, але він також зазначив, що ця технологія вже використовується для посилення кіберзахисту». ***(US congress puts pressure on Microsoft over Cybersecurity // Bol Media Group (https://www.bolnews.com/technology/2024/06/us-congress-puts-pressure-on-microsoft-over-cybersecurity/). 14.06.2024).***

***

«У суботу проросійська хакерська група продовжила атакувати сайти федерального уряду Швейцарії та організацій, залучених до участі у Саміті миру, пише УНН з посиланням на повідомлення швейцарського федерального відомства з кібербезпеки NCSC, швейцарські видання watson та Keystone-SDA.

Деталі

Згідно з повідомленням NCSC, атаки тривали перед початком Саміту миру в Бюргенштоці.

«Сьогодні, у суботу, перед початком конференції високого рівня щодо миру в Україні, перевантажуючі атаки тривають, як і очікувалося. Цілями атак залишаються федеральні сайти та організації, які беруть участь у конференції. Федеральне відомство з кібербезпеки стежить за ситуацією та підтримує контакти з постраждалими організаціями», - зазначили у NCSC.

Ці атаки, вказали у відомстві, «не впливають на безпеку постраждалих або на проведення конференції». «Через DDoS-атаки окремі веб-сайти тимчасово недоступні. Такі атаки не завдають прямої шкоди IT-інфраструктурі», - зазначається у повідомленні.

Відповідальність за атаки несе група під назвою «NoName057(16)», повідомила прессекретар NCSC Гізела Кіпфер інформаційному агентству Keystone-SDA на запит. В результаті атак сайти можуть бути тимчасово недоступні…» ***(Юлія Шрамко. Атаки проросійських хакерів на швейцарські урядові сайти продовжилися у день старту Саміту миру // Інформаційне агентство «Українські Національні Новини» (https://unn.ua/news/ataky-prorosiiskykh-khakeriv-na-shveitsarski-uriadovi-saity-prodovzhylysia-u-den-startu-samitu-myru). 15.06.2024).***

***

«Росія проводить цілеспрямовану недружню діяльність проти країн-союзниць по Альянсу, включаючи акти саботажу, кібернетичні атаки та використання міграції в якості засобу тиску, але така ворожа діяльність не відверне країни НАТО від продовження підтримки України

Про це сьогодні у Брюсселі на підсумковій пре-конференції після завершення дводенної зустрічі міністрів оборони Альянсу заявив генеральний секретар НАТО Єнс Столтенберг.

«Міністри відповіли на триваючу кампанію ворожих дій, які Росія проводить проти союзників. Протягом минулих тижнів ми бачили сплеск випадків саботажу, кібератак, інструменталізації міграції та інших недружніх вчинків зі сторони Росії. Ми будемо спокійними та зваженими у нашій відповіді на російські провокації. У

той же час, ми припинимо російські дії та виставимо рахунок». – сказав Столтенберг.

Він зауважив, що сьогодні міністри оборони НАТО погодили пакет заходів у відповідь на такі російські дії, які країни-союзниці вживатимуть індивідуально та колективно. Це включає посилення обміну розвідувальною інформацією, підвищення рівня захисту критичної інфраструктури, включаючи підводну та кібернетичну. Столтенберг також зазначив, що ці дії передбачають посилені заходи проти оперативних співробітників російських спецслужб.

«Російська кампанія не стримає нас від (продовження – ред.) підтримки України. І ми будемо продовжувати захищати нашу територію та населення проти недружніх дій», - додав керівник НАТО.

Як повідомлялося, сьогодні у Брюсселі завершилася дводенна зустріч міністрів оборони країн НАТО, одним з головних питань якої було продовження підтримки України та посилення координуючої ролі Альянсу у наданні Україні безпекової допомоги». ***(Столтенберг заявив про сплеск гібридних атак РФ проти країн НАТО // Ua-Independent (https://ua-independent.com/home/stoltenberg-zayaviv-pro-splesk-gibridnikh-atak-rf-proti-krajin-nato). 17.06.2024).***

***

«Сьогодні Служба військової розвідки та безпеки Нідерландів (MIVD) попередила, що вплив китайської кампанії кібершпигунства, оприлюдненої на початку цього року, «набагато більший, ніж було відомо раніше».

Як повідомило MIVD у лютому в спільному звіті зі Службою загальної розвідки та безпеки (AIVD), китайські хакери використовували критичну вразливість віддаленого виконання коду FortiOS/FortiProxy (CVE-2022-42475) протягом кількох місяців між 2022 і 2023 роками для розгортання. зловмисне програмне забезпечення на вразливих пристроях безпеки мережі Fortigate.

«Протягом цього так званого періоду «нульового дня» актор заразив лише 14 000 пристроїв. Цілі включають десятки (західних) урядів, міжнародних

організацій і велику кількість компаній оборонної промисловості», – повідомили в MIVD.

Шкідливе програмне забезпечення трояна віддаленого доступу Coathanger (RAT), яке використовувалося в атаках, також було виявлено в мережі міністерства оборони Нідерландів, яка використовується в дослідженнях і розробках (R&D) несекретних проектів. Проте через сегментацію мережі зловмисникам було заблоковано перехід на інші системи.

MIVD виявило, що цей раніше невідомий штам зловмисного програмного забезпечення, який міг вижити після перезавантаження системи та оновлення мікропрограми, був застосований спонсорованою державою китайською хакерською групою в рамках кампанії політичного шпигунства, націленої на Нідерланди та їхніх союзників.

«Це дало державному актору постійний доступ до систем. Навіть якщо жертва встановлює оновлення безпеки з FortiGate, державний актор продовжує зберігати цей доступ», — додали в MIVD.

«Невідомо, у скількох жертв насправді встановлено зловмисне програмне забезпечення. Голландські спецслужби та NCSC вважають ймовірним, що державний актор потенційно може розширити свій доступ до сотень жертв у всьому світі та виконувати додаткові дії, такі як крадіжка даних».

Щонайменше 20 000 систем Fortigate зламано

Починаючи з лютого, нідерландська військова розвідувальна служба виявила, що китайська група загроз отримала доступ до щонайменше 20 000 систем FortiGate по всьому світу в 2022 і 2023 роках протягом декількох місяців, щонайменше за два місяці до того, як Fortinet розкрила вразливість CVE-2022-42475.

MIVD вважає, що китайські хакери все ще мають доступ до багатьох жертв, оскільки зловмисне програмне забезпечення Coathanger важко виявити, оскільки воно перехоплює системні виклики, щоб уникнути виявлення своєї присутності, а також його складно видалити, оскільки воно виживає після оновлення мікропрограми.

CVE-2022-42475 також використовувався як нульовий день для націлювання на державні організації та пов’язані з ними організації, як було оприлюднено Fortinet у січні 2023 року.

Ці атаки багато в чому схожі з іншою китайською хакерською кампанією, яка була націлена на невиправлені пристрої SonicWall Secure Mobile Access (SMA) зі шкідливим програмним забезпеченням для кібершпигунства, розробленим для того, щоб протистояти оновленням мікропрограми». ***(Sergiu Gatlan. Chinese hackers breached 20,000 FortiGate systems worldwide // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/chinese-hackers-breached-20-000-fortigate-systems-worldwide/?utm_source=flipboard&utm_content=zhogfan%2Fmagazine%2FPOLITICS.WAR.LEGAL.RELIGION). 11.06.2024).***

***

«Група хакерів, пов'язана з російською зовнішньою розвідкою, проводила багаторічну, ретельно сплановану кампанію, спрямовану проти французьких дипломатів та посольств, яка поставила під загрозу французькі та європейські зовнішньополітичні інтереси.

Про це йдеться в новому звіті Національного агентства з безпеки інформаційних систем (ANSSI), органу, відповідального за кібербезпеку Франції, передає Укрінформ.

«Члени ANSSI вважають, що звинувачення у діяльності проти французьких дипломатичних установ є доведеними», - підкреслюється в документі.

У ньому описується серія хакерських атак, здійснених групою під назвою «Нобеліум». Хакери використовували схожий спосіб дій: надсилання повідомлень із «шпигунськими» вкладеннями з поштової скриньки, викраденої у її справжнього власника, зазвичай співробітника французької або іноземної дипломатичної місії.

Так, у квітні і травні 2022 року на десятки електронних адрес Міністерства закордонних справ Франції надійшли повідомлення із зараженими вкладеннями, у яких йшлося про закриття посольства України або пропонувалася зустріч з послом

Португалії. У травні 2023 року посольство Франції в Києві разом з іншими європейськими дипустановами отримали листи, в якому пропонувалося виставити на продаж «дипломатичне авто». Цього ж року аналогічними методами хакери намагались «зламати» базу посольства Франції в Румунії.

«Можливості, застосовані для компрометації такої великої кількості електронних поштових скриньок, наполегливість атак, зусилля, докладені до підробки документів, вказують на те, що «Нобеліум» майже напевно діє від імені державного суб'єкта», - доходять висновку експерти.

На їхню думку, ці численні спроби хакерських атак створюють загрозу національній безпеці, а також французьким та європейським дипломатичним інтересам». ***(Французькі дипломати стали мішенню хакерських атак РФ // Укрінформ (https://www.ukrinform.ua/rubric-world/3877442-francuzki-diplomati-stali-misennu-hakerskih-atak-rf.html). 21.06.2024).***

***

«Національний директорат кібербезпеки Румунії (DNSC) задокументував 25 DDoS-атак на румунські вебсайти пов'язаних із Росією хакерських груп протягом 17-21 червня.

Про це йдеться в повідомленні DNSC, яке цитує «Європейська правда».

Кібератаки проросійських хакерів, як зазначається, були націлені на державні установи Румунії та приватні організації у «фінансово-банківському, транспортному та телекомунікаційному секторах».

«Команда Директорату заздалегідь попередила атаковані організації, оскільки про атаки було заздалегідь оголошено на онлайн-платформах чату, які використовувалися зловмисниками, і підтримувала з ними постійний контакт», – додали в DNSC.

Там зазначили, що суттєвих перебоїв у роботі атакованих сайтів не спостерігали, натомість були «короткі періоди недоступності послуг».

DDoS-атаки передбачають генерацію величезного потоку запитів на з'єднання, що може призвести до перебоїв у роботі або виведення з ладу сайтів, на які вони спрямовані.

Зазначимо, що під час кібератак Румунія оголосила про рішення передати Україні свій зенітно-ракетний комплекс Patriot». ***(Олег Павлюк. Проросійські хакери атакували Румунію // Європейська правда (https://www.eurointegration.com.ua/news/2024/06/21/7188672/). 21.06.2024).***

***

Кіберзахист критичної інфраструктури

«Управління кібербезпеки, енергетичної безпеки та реагування на надзвичайні ситуації Міністерства енергетики розробило рекомендації за участю виробників енергетичної автоматизації та промислових систем керування, а також Національної лабораторії Айдахо, яка спеціалізується на дослідженнях у сфері кібербезпеки.

Відділ перераховує 10 напрямків найкращої практики як для постачальників, так і для кінцевих споживачів. Вони включають такі пріоритети, як підтримка процесів управління вразливістю для постачальників, які дотримуються найкращих галузевих практик, а також надання підтримки продуктів, включаючи виправлення безпеки та пом’якшення протягом життєвого циклу транзакції кінцевого користувача.

Для кінцевих користувачів департамент заохочує включати договірні формулювання «тих положень, умов і вимог до тестування, які вплинуть на ваші результати безпеки», а також співпрацювати з постачальниками для повного розуміння та інтеграції відповідних засобів контролю та платформ кібербезпеки.

Сполучені Штати не єдині, хто активізував зусилля, пов’язані з кібербезпекою виробництва — це питання обговорювалося лідерами на саміті G7 в Апулії, Італія, на початку цього місяця. Офіційні особи там зобов’язалися

«продовжити обговорення» того, як підвищити стійкість кібербезпеки в ключових секторах, включно з тим, як покращити безпеку ланцюжка поставок.

«Оскільки нові цифрові технології чистої енергії інтегруються, ми повинні забезпечити їхню кібербезпеку, щоб запобігти руйнуванню або перебоям у роботі послуг», — сказав радник з національної безпеки Джейк Салліван у заяві Білого дому 18 червня. «G7 працюватиме над створенням колективної структури кібербезпеки для операційних технологій як для виробників, так і для операторів».

Кіберзагроза критичному виробництву США зростає. Згідно з даними ФБР, минулого року цей сектор зазнав другого за кількістю кібератак серед галузей промисловості США – 218, поступаючись лише сектору охорони здоров'я. У глобальному масштабі майже половина критично важливих виробників знаходяться під загрозою кібератаки, причому багатьом організаціям бракує видимості в їхніх ширших бізнес-екосистемах, щоб успішно відбити атаку.

Щоб боротися з підвищеним ризиком, адміністрація Байдена виявила підвищений інтерес до посилення безпеки виробництва та ланцюга постачання в США. У листопаді адміністрація створила Раду Білого дому з питань стійкості ланцюга поставок, яка була офіційно оформлена на початку цього місяця виконавчим указом.

На рівні агентства протягом останніх місяців Міністерство енергетики співпрацювало з енергорозподільниками, щоб покращити кібербезпеку. Відділ створив подібні «базові показники » в лютому, спрямовані на підвищення безпеки систем розподілу та розподілених енергоресурсів.

У січні департамент також виділив 30 мільйонів доларів США для фінансування досліджень, розробок і демонстраційних проектів, спрямованих на підвищення кібербезпеки ресурсів чистої енергії». ***(Kate Magill. Manufacturing cybersecurity at heart of new White House guidance // Industry Dive (https://www.constructiondive.com/news/energy-department-cybersecurity-manufacturing-supply-chain-best-practices/719934/). 26.06.2024).***

***

«Атака програми-вимагача на Synnovis, британського постачальника послуг медичної лабораторії, значно порушує обслуговування пацієнтів і послуги тестування в кількох лікарнях NHS та інших закладах охорони здоров'я в Лондоні.

Інцидент у Великій Британії є одним із щонайменше двох серйозних збоїв у секторі охорони здоров'я. У США мережа лікарень Ascension заявила, що досягає регіонального прогресу у відновленні електронних медичних записів та інших критичних IT-систем, які були виведені з ладу внаслідок атаки 8 травня. Тим не менш, EHR не відновлять роботу в лікарнях Ascension у всіх регіонах до середини червня.

Кібератака вразила британську компанію Synnovis у понеділок, і інцидент негативно вплинув на обслуговування пацієнтів у кількох лондонських лікарнях та інших закладах надання медичної допомоги, повідомив у вівторок прес-секретар лондонського регіону NHS England Information Security Media Group.

«Це суттєво вплине на надання послуг у лікарнях Гая та Сент-Томаса, фондах Національної служби охорони здоров'я Королівського коледжу та службах первинної медичної допомоги на південному сході Лондона», — сказав речник. «Ми приносимо вибачення за незручності, які це спричиняє пацієнтам та їхнім родинам».

«Ми терміново працюємо над тим, щоб повністю зрозуміти наслідки інциденту за підтримки урядового Національного центру кібербезпеки та нашої команди з кібероперацій».

Постачальники NHS мають перевірені та перевірені плани безперервності бізнесу для таких випадків, як цей, які включають пропозицію взаємної допомоги, повідомляє NHS.

Деякі заходи з догляду за пацієнтами вже скасовано або перенаправлено іншим постачальникам, оскільки термінова робота є пріоритетною, сказав речник.

«Невідкладна допомога залишається доступною, і пацієнти повинні відвідувати прийоми, якщо не буде повідомлено інше», - сказав речник. «Ми

продовжуватимемо повідомляти місцевим пацієнтам і громадськості про вплив на послуги та про те, як вони можуть продовжувати отримувати необхідну допомогу».

Synnovis у заяві, наданій ISMG, описує себе як патологічне партнерство між Trust NHS Foundation Гая та Сент-Томаса, Trust NHS Hospitals King's College Hospitals, а також SYNLAB, найбільшим постачальником медичних тестів і діагностики в Європі. Synnovis надає послуги NHS, клінічним користувачам та іншим користувачам послуг.

За словами Synnovis, інцидент вплинув на всі IT-системи Synnovis, що призвело до перебоїв у роботі багатьох патологічних служб. «Безпосередній вплив буде на пацієнтів, які користуються послугами NHS у двох лікарнях-партнерах, а також на послуги лікарів загальної практики в районах Бекслі, Грінвіч, Льюішем, Бромлі, Саутворк і Ламбет», — сказав постачальник.

«Поки ще рано, і ми намагаємося зрозуміти, що саме сталося. Робоча група IT-експертів із Synnovis і Національної служби охорони здоров’я працює, щоб повністю оцінити наслідки, які це мало, і вжити необхідних заходів. Ми працюємо тісно співпрацювати з партнерами NHS Trust, щоб мінімізувати вплив на пацієнтів та інших користувачів послуг».

Оновлення Вознесіння

У США компанія Ascension, яка 8 травня зазнала кібератаки, яка порушила роботу клінічних IT-систем у багатьох із 140 її лікарень та інших закладів догляду в 19 штатах, заявила в оновленій заяві у вівторок, що досягає прогресу у відновленні багатьох IT-сервісів. у кількох регіонах, а повне відновлення EHR очікується приблизно через 10 днів.

Доступ до EHR було відновлено в установах у Флориді, штат Алабама, і Остіні, штат Техас, повідомляє Ascension.

«Грунтуючись на тому, що ми дізналися про цей процес на сьогоднішній день, ми працюємо над завершенням відновлення EHR в усьому нашому міністерстві до кінця тижня, що закінчується 14 червня», — сказав Вознесіння.

«Оскільки EHR буде відновлено в усіх наших мережах, клініцисти матимуть доступ до записів пацієнтів, як вони робили до цього інциденту», — сказав Асеншен.

«Хоча це багатообіцяючі події в наших зусиллях з відновлення, наше розслідування цього інциденту продовжується разом із відновленням додаткових систем. Це складний процес, і для його завершення все одно знадобиться час».

Роздрібна торгівля Ascension Rx, доставка додому та спеціалізовані аптеки тепер відкриті та можуть видавати рецепти, повідомила організація. «Це означає, що постачальники медичних послуг можуть передавати рецепти в електронному вигляді та можуть надсилати рецепти в аптеки Ascension Rx для своїх пацієнтів».

Минулого тижня Міжнародний союз офісних і професійних службовців Local 40 у місті Макомб, штат Мічиган, який представляє медсестер, радіологів та інших медичних працівників, які працюють у лікарні Ascension Providence Rochester Hospital, надіслав петицію до керівництва лікарні з вимогою вжити ряд заходів безпеки пацієнтів. на місці, поки EHR та інші клінічні системи не працюють.

Станом на вівторок близько 232 членів профспілок підписали петицію. Діна Карлайл, зареєстрована медсестра, яка працює в лікарні, що не відноситься до Вознесіння, і є президентом місцевої ради персоналу 40 OPEIU RN, розповіла ISMG, що лікарня Ascension Providence Rochester спілкувалася з профспілкою, але вона досі не вжила конкретних заходів безпеки пацієнтів. вимагалося в петиції.

Тривожні тенденції

Атаки на лікарні NHS у Великобританії та установи Ascension у США є одними з останніх хакерських інцидентів, які спричинили серйозні збої в IT у секторі охорони здоров’я.

«Ці атаки найчастіше здійснюються бандами програм-вимагачів, які проживають у Східній Європі, і завжди можливо, що цим групам надає притулок російський уряд», — сказав Шон Добі, головний технолог охоронної фірми Semperis.

«За останній рік угруповання програм-вимагачів LockBit і ALPHV здійснили майже 20% усіх атак програм-вимагачів і отримали понад 1 мільярд доларів у вигляді викупу від жертв», — сказав він.

«Я настійно рекомендую, щоб лікарні працювали на основі підходу «передбачуваного порушення». Це означає не лише відповідь на атаку, але й готовність до швидкого відновлення, якщо системи будуть скомпрометовані», — сказав Добі.

«Актор загрози з достатньою мотивацією та ресурсами знайде спосіб проникнути в більшість лікарень, і тому вони повинні якнайшвидше впроваджувати рішення та методи для виявлення, реагування та стримування порушень».

Оскільки ці напади продовжують зростати, для організацій сектора охорони здоров'я та їхніх основних постачальників дуже важливо вжити заходів для посилення своєї безпеки, сказав Патрік Гарріті, дослідник безпеки в охоронній фірмі VulnCheck.

Це включає швидке оновлення та виправлення систем, які мають уразливості з відомим використанням, сказав він. «Це також означає усунення кінцевих додатків і технологій, що може бути складним у середовищі догляду за пацієнтами через складність таких речей, як медичні пристрої. Однак це не слід використовувати як виправдання», — сказав він.

«Працюючи з постачальниками медичних послуг у Великій Британії та США, я можу підтвердити, що технології, що вийшли з експлуатації, часто широко поширені, оскільки організації охорони здоров'я все ще покладаються на застарілі системи та програми», — сказав Гарріті. Підтримка та тестування плану резервного копіювання та аварійного відновлення, який включає внутрішні сценарії програм-вимагачів і сторонніх постачальників, також є критично важливим, додав він». ***(Marianne Kolbasuk McGee. UK Vendor's Attack Disrupts Care at London NHS Hospitals // Information Security Media Group, Corp. (https://www.databreachtoday.com/uk-vendors-attack-disrupts-care-at-london-nhs-hospitals-a-25410?utm_source=flipboard&utm_content=other). 04.06.2024).***

***

«Лікарні та великі медичні організації все частіше стають головними цілями для кіберзлочинців. У відповідь Департамент охорони здоров'я та соціальних служб (HHS) заснував нову ініціативу в рамках Національного інституту здоров'я (NIH), спрямовану на посилення заходів кібербезпеки для лікарень.

Цю ініціативу під назвою «Універсальне виправлення та відновлення для автономної оборони» (UPGRADE) було запущено 20 травня. Місія UPGRADE полягає в розробці індивідуального та масштабованого набору програмних інструментів, які дозволять IT-командам лікарень ефективно боротися з атаками програм-вимагачів і зменшити час, необхідний для виправлення вразливих продуктів охорони здоров'я, від місяців до кількох днів або тижнів.

Веб-сайт UPGRADE висвітлює мету програми — об'єднати виробників обладнання, експертів з кібербезпеки та IT-персонал лікарень для створення надійного пакету програмного забезпечення, призначеного для підвищення кіберстійкості лікарень. Це оголошення зроблено в критичний час у 2024 році, коли сектор охорони здоров'я стикається з численними атаками програм-вимагачів, які порушують доступ до медичної документації та рятувальних пристроїв. Ці кібератаки не лише загрожують безпеці пацієнтів, але й порушують конфіденційність пацієнтів, розкриваючи захищену інформацію про здоров'я (PHI) та інші конфіденційні дані. Організації охорони здоров'я, які не захищають записи пацієнтів, можуть зазнати значних санкцій згідно з Правилами конфіденційності та безпеки HIPAA.

Майбутній конкурс від NIH збиратиме команди виконавців для подання пропозицій щодо чотирьох технічних напрямків: створення програмної платформи для пом'якшення вразливості, розробка високоякісних цифрових двійників лікарняного обладнання, автоматичне виявлення вразливостей і автоматична розробка спеціальних засобів захисту. NIH опублікувала чернетку оголошення про модуль із запитом на відгук громадськості та планує опублікувати остаточне оголошення про модуль для UPGRADE у червні 2024 року.

Це сталося після того, як заступник радника з національної безпеки Енн Нойбергер заявила, що адміністрація розглядає можливість встановлення мінімальних стандартів кібербезпеки для організацій, які отримують фінансування Medicare і Medicaid, як повідомляв Bloomberg на початку цього місяця. Однак терміни реалізації цих вимог залишаються незрозумілими.

Крім того, у Конгресі сенатор Марк Ворнер (D-VA) запропонував законодавство, яке забороняє виплату авансових платежів або прискорених платежів постачальникам, які не відповідають мінімальним стандартам кібербезпеки, встановленим HHS. Програми прискорених і авансових платежів є ключовим інструментом, який дозволяє постачальникам, платіжні системи яких постраждали від атаки на кібербезпеку, все одно отримувати оплату від Medicare за надані послуги». ***(Amica J. Nesbitt. HHS Pledges $50 million to Empower Hospitals in the Battle Against Cyberattacks // Reed Smith LLP. (https://www.healthindustrywashingtonwatch.com/2024/06/articles/department-of-health-and-human-services/hhs-pledges-50-million-to-empower-hospitals-in-the-battle-against-cyberattacks/#page=1). 03.06.2024).***

***

«Атака на лікарні загальної практики може виявитися прибутковою для кіберзлочинців. Які проблеми кібербезпеки слід планувати?

Зрозуміло, що для хірургічних операцій йти в ногу з останніми практичними системами та технологіями часто може мати менший пріоритет, ніж задоволення потреб пацієнтів.

Однак із зростанням кількості складніших кібератак і невідомими наслідками штучного інтелекту для індустрії нездатність йти в ногу з технологіями та кібербезпекою створює значний ризик.

У кращому випадку хірургічному закладу може пощастити й уникнути будь-яких загроз, але в гіршому — це може стати причиною серйозних порушень даних, довготривалої шкоди репутації та втрати пацієнтів і контрактів.

Більшість лікарень загальної практики, які працюють через Національну службу охорони здоров'я, мають контракт, у якому визначено послуги, які вони повинні надавати. Зазвичай це включає ведення записів і наявність відповідних технологій і систем для проведення практики. Як мінімум, практики зазвичай мають веб-сайт, контактну форму для пацієнтів, телефонні лінії, журнал записів на прийом, мобільний додаток і системи входу пацієнтів.

Але це лише сторона, звернена до громадськості. За лаштунками є програмне забезпечення для керування заробітною платою, системи для допомоги в управлінні фінансами та персоналом, а також інструменти для відстеження поточних поточних витрат.

Обсяг необхідного програмного забезпечення є величезним і вміщуватиме сотні тисяч фрагментів даних.

Оскільки майже всі аспекти цього підтримуються онлайн і мають важливе значення для роботи практики, лікарі загальної практики піддаються шахрайству та кіберзлочинам.

Які і де ризики?

Кіберзлочинці не дотримуються етики щодо того, на кого вони спрямовані, і напади на лікарні загальної практики можуть бути прибутковими. Для практики ця загроза зазвичай відноситься до однієї з двох категорій.

Перше стосується пацієнтів. Злом карток пацієнтів і доступ до інформації, особливо до конфіденційних даних, може завдати величезної шкоди хірургічному відділу, але, на жаль, вигідно для кіберзлочинців.

Друга загроза стосується практики та її персоналу. Існує ймовірність того, що технологія, яка використовується для підтримки роботи практики, як-от системи запису на прийом або програмне забезпечення HR для конфіденційної інформації про персонал, може бути скомпрометована.

Це не тільки створює загрозу для повсякденної роботи бізнесу, але також може завдати значних страждань колегам, які можуть стати жертвами подальших злочинів.

Коли мова заходить про підвищення безпеки, можна зробити три кроки. Це:

1. Подивіться та повторіть кіберзахист.

Керівники та власники практик повинні інформувати колег про потенційні загрози та виклики.

Дії, які потрібно вжити, можуть бути такими простими, як не записувати інформацію про пацієнта в цифровому вигляді за межами офіційних систем або переконатися, що всі дотримуються найкращих практик щодо оновлення паролів і отримують сповіщення про підозрілий трафік електронної пошти.

Також варто врахувати фізичну безпеку, наприклад ключ-карти. Може бути корисним покласти відповідальність на когось, хто буде регулярно перевіряти безпеку та ділитися нагадуваннями з командою.

2. Управління ризиками

Моніторинг і реєстрація інцидентів і невдач може допомогти виявити закономірності або виявити ширші проблеми, які вимагають ближчого вивчення. Кожне порушення має бути належним чином розслідувано, щоб уникнути його повторення. Важливо захистити те, що у вас є, і мати надійний план боротьби з цим, якщо станеться порушення.

Ці плани повинні включати чіткі дії для безперебійної роботи практики, плани ведення пацієнтів, а також план зовнішніх і внутрішніх комунікацій.

3. Зрозумійте, яку підтримку ви маєте та яка додаткова резервна копія вам може знадобитися

Хоча деякі контракти з постачальниками можуть покривати вас від кібератак, інші можуть ні. Подібним чином ваш договір із NHS може охоплювати будь-які пов’язані з NHS дані, що зберігаються в системах NHS, але не може поширюватися на ті самі дані, що використовуються на інших платформах.

Витратьте час, щоб зрозуміти, які ваші зобов’язання щодо захисту даних, які ви використовуєте, і, якщо ви зазнаєте небезпеки, поговоріть зі страховим експертом. Є також доступне страхування кібербезпеки, яке може допомогти забезпечити додатковий рівень підтримки та порад у випадку атаки». ***(Kabir Ahmed. Cyber security – what GP practices need to know to protect themselves //***

Cogora Limited (https://managementinpractice.com/practice-intelligence/cyber-security-what-gp-practices-need-to-know-to-protect-themselves/). 17.06.2024).

***

«Приблизно чверть американців зазнали витоку їхніх медичних карт, а дослідження виявили, що понад 79,6 мільйонів людей були охоплені витоком даних. Приблизно 71% порушень відбуваються через злам постачальника медичних послуг.

Дослідження, проведене американською компанією з кібербезпеки Incogni, разом із даними, опублікованими Міністерством охорони здоров'я та соціальних служб США, детально показало, як з 2020 року постачальники медичних послуг зазнали 1572 порушень, що становить 57,6% усіх американських профілів охорони здоров'я, які були викриті.

У той же час звіт Incogni виявив таку саму закономірність із зареєстрованими атаками програм-вимагачів, встановивши, що з 2020 року приблизно 76,1% атак були спрямовані на постачальників медичних послуг. Дослідження описують найпоширенішу причину злому як хакерські та IT-інциденти, що спричинили 1622 порушення та вплинули на 136,8 мільйона профілів охорони здоров'я.

Найбільшим порушенням, названим у звіті, був злом у 2021 році оптометричної компанії 20/20 Eye Care Network, у результаті якого були зламані дані про охорону здоров'я приблизно 3,3 мільйона американців після того, як ворожі особи отримали доступ до хмарних систем зберігання даних компанії.

Даріус Белєєвас, керівник служби захисту даних Incogni, сказав: «Перехід до електронних систем охорони здоров'я, безсумнівно, приніс численні переваги сектору охорони здоров'я, але він також створив значні ризики. Розголошення конфіденційної інформації про здоров'я може мати руйнівні наслідки для людей, оскільки їхні дані можуть бути використані брокерами даних або навіть злочинцями. Incogni виступає за більш суворі заходи конфіденційності та безпеки для організацій, які керують інформацією пацієнтів.

«Оскільки порушення продовжують порушувати конфіденційність пацієнтів, вони також ставлять під загрозу безпеку пацієнтів і підривають їх довіру до системи охорони здоров'я. Крім того, вони можуть призвести до крадіжки особистих даних, медичного шахрайства та інших форм експлуатації».

Очікується, що ринок кібербезпеки, орієнтований на охорону здоров'я, неухильно зростатиме разом із зростанням кількості атак на заклади охорони здоров'я. Дослідження GlobalData показало, що глобальний ринок кібербезпеки становитиме 334 мільярди доларів до 2030 року, зростаючи на 10% у період між 2022 та 2030 роками. Крім того, окреме дослідження британської компанії з кібербезпеки Sophos показало, що лише 24 % організацій охорони здоров'я змогли запобігти атаці програм-вимагачів до того, як зловмисники зашифрували їхні дані – порівняно з 34% у 2022 році.

Причини кібератак на заклади охорони здоров'я відрізняються різними причинами, але в останні кілька років кібератаки на лікарні та заклади охорони здоров'я використовувалися як інструмент для зриву з боку ворожих держав, таких як Росія.

«Чверть усіх американських медичних записів було порушено» було спочатку створено та опубліковано Medical Device Network, брендом, який належить GlobalData». ***(Joshua Silverwood. Quarter of all American healthcare records have been breached // yahoo! finance (https://finance.yahoo.com/news/quarter-american-healthcare-records-breached-105325526.html?fr=sycsrp_catchall). 27.06.2024).***

***

«Лікарні стають дедалі привабливішими цілями для атак програм-вимагачів через їх повні бази даних пацієнтів, конфіденційну інформацію та взаємозв'язок між системами та обладнанням.

Крім того, погані заходи безпеки зробили лікарні вразливими до кіберзагроз. Під час атаки кіберзлочинці потенційно можуть отримати контроль над цілими

системами лікарень і отримати доступ не лише до інформації про здоров'я пацієнтів, а й до їхніх фінансових і страхових даних.

Це одні з висновків Міжнародного звіту про охорону здоров'я KnowBe4, який досліджує кризу кібербезпеки, яку зараз відчуває сектор охорони здоров'я, зокрема лікарняні групи, у всьому світі.

Африка була регіоном із найвищою середньою кількістю щотижневих кібератак на організацію у 2023 році: кожна 19 організація на континенті зазнавала спроби атаки щотижня.

Незважаючи на те, що сектору охорони здоров'я Південної Африки вдалося уникнути великої атаки з 2020 року, тривожна ескалація атак в інших секторах країни свідчить про те, що це лише питання часу, коли станеться наступна атака, роблячи це питання «коли», а не «якщо», згідно зі звітом.

Лікарні серйозно постраждали від кібератак, які можуть призвести до скорочення обслуговування пацієнтів, втрати доступу до електронних систем і залежності від неповних паперових записів. Це також може призвести до скасування операцій, тестів, призначень, а в деяких випадках навіть до втрати життя.

Деякі висновки зі звіту включають:

* У перші три квартали 2023 року світовий сектор охорони здоров'я зазнавав 1613 кібератак на тиждень, що майже вчетверо перевищує середній показник у світі, і значно збільшився порівняно з тим самим періодом попереднього року.

* За останні три роки в секторі охорони здоров'я спостерігалося різке зростання витрат на кібератаки, причому середня вартість злому сягнула майже 11 мільйонів доларів США, що більш ніж у три рази перевищує середній світовий показник. Це робить охорону здоров'я найдорожчим сектором для кібератак.

* Атаки програм-вимагачів були найпоширенішим видом кібератак на організації охорони здоров'я, на них припадає понад 70% успішних атак за останні два роки.

* Більшість кібератак (від 79% до 91%) у різних секторах починаються з фішингу або тактики соціальної інженерії, які дозволяють кіберзлочинцям отримати доступ до облікових записів або серверів.

* Згідно зі звітом KnowBe4 про фішинг за галузевим порівняльним аналізом за 2024 рік, медичні та фармацевтичні організації є одними з найбільш уразливих до фішингових атак, причому ймовірність стати жертвою фішингового електронного листа для співробітників великих організацій у секторі становить 51,4%. Це означає, що кіберзлочинці мають більше ніж 50/50 шансів успішно фішингувати співробітника в секторі.

«Сектор охорони здоров'я залишається основною мішенню для кіберзлочинців, які прагнуть заробити на життєво-смертельних ситуаціях, з якими стикаються лікарні», — говорить Стю Сьюверман, генеральний директор KnowBe4. «З огляду на те, що дані пацієнтів і критично важливі системи знаходяться в заручниках, багато лікарень відчувають, що їм не залишається іншого вибору, окрім як платити непомірні викупи. Це порочне коло можна розірвати, приділивши пріоритет комплексному навчанню з питань безпеки, щоб розширити можливості співробітників і культивувати позитивну культуру безпеки як надійний захист від фішингу та атак соціальної інженерії».

У звіті розглядається стан кібербезпеки в секторі охорони здоров'я в Північній Америці, Європі, Великобританії, Азіатсько-Тихоокеанському регіоні, Африці та Латинській Америці. Крім того, у ньому також висвітлюються деякі з найбільш плідних глобальних атак програм-вимагачів, які відбулися в період з грудня 2023 року по травень 2024 року, їх наслідки та те, що організації охорони здоров'я можуть зробити, щоб захистити себе від кібератак». ***(Healthcare is in a cybersecurity crisis // IT-ONLINE (https://it-online.co.za/2024/06/27/healthcare-is-in-a-cybersecurity-crisis/). 27.06.2024).***

***

«Усі кол-центри стикаються з загрозами кібербезпеці, оскільки вони обробляють таку інформацію, як номери кредитних карток, медичні записи та особисту історію покупок. Однак кол-центри, які підтримують федеральні агентства, мають додатковий ризик обробки дуже конфіденційної інформації, що робить їх основними цілями для кіберзлочинців.

Найпоширеніші типи загроз кібербезпеці, які ставлять кол-центри під загрозу, включають:

Поширеною проблемою є фішингові атаки, які використовують електронні листи, щоб спонукати людей надати конфіденційну інформацію. Ці атаки часто включають підозрілі посилання або вкладення, які можуть поставити під загрозу безпеку ваших даних і системи. Якщо хакерам це вдасться, вони зможуть отримати доступ до важливих мережевих ресурсів, таких як облікові записи електронної пошти та жорсткі диски.

DoS-атаки або атаки на відмову в обслуговуванні є шкідливими збоями в кол-центрах через перевантаження їх штучним трафіком, наприклад занадто великою кількістю дзвінків або помилковими запитами. Це може спричинити простої та проблеми з роботою, через що системи будуть недоступні для законних користувачів. Наприклад, кол-центри можуть стати мішенями під час протестів, що може перервати обслуговування та зв’язок.

Хакери також можуть знайти слабкі місця та отримати доступ до баз даних колл-центру, поставивши під загрозу безпеку та конфіденційність даних. Потрапивши в систему, вони можуть викрасти або змінити конфіденційну інформацію, потенційно порушивши роботу уряду.

Проблеми внутрішньої безпеки, такі як нагляд або недбалість співробітників, також є загрозою. Людські помилки можуть призвести до витоку даних або системних проблем.

Щоб впоратися з ризиками кібербезпеки, необхідно використовувати різноманітні стратегії та інструменти, такі як безперервне навчання та навчання,

апаратне та програмне забезпечення. Нижче наведено кілька початкових кроків, які повинні зробити адміністратори кол-центру, щоб створити першу лінію захисту від атак на кібербезпеку:

Надійні профілі безпеки: переконайтеся, що ваша електронна пошта має найвищий рівень безпеки, щоб відловлювати та зупиняти спроби фішингу. Це означає використання фільтрів електронної пошти, перевірку посилань і навчання співробітників виявляти фішингові шахрайства. Регулярні сеанси підвищення рівня безпеки можуть допомогти вашій команді швидко розпізнавати спроби фішингу та повідомляти про них.

Проактивний моніторинг і оповіщення: використовуйте системи виявлення та запобігання вторгненням, щоб відловлювати та зупиняти DoS-атаки в реальному часі. Підготуйте плани для швидкого реагування та співпрацюйте з постачальниками послуг, щоб блокувати підозрілий трафік і підтримувати роботу служб. Сегментація мережі та резервування можуть допомогти, розподіляючи вхідний трафік між кількома серверами або центрами обробки даних.

Безперервне навчання та підвищення обізнаності: створіть серед ваших співробітників середовище, яке буде обізнаним і відповідальним у питаннях кібербезпеки, за допомогою постійного навчання та навчання. Заохочуйте співробітників негайно повідомляти про проблеми безпеки та надайте чіткі вказівки щодо вирішення інцидентів. Регулярні тренування з безпеки та симуляції можуть допомогти перевірити готовність і покращити навички реагування.

Контроль доступу та автентифікація. Обов’язково використовуйте суворий контроль доступу та багатофакторну автентифікацію (MFA), щоб захистити конфіденційні дані та забезпечити доступ до систем лише потрібним людям, зменшуючи ризик внутрішніх порушень. Зберігайте свої бази даних у безпеці за допомогою шифрування, керування доступом на основі ролей і регулярних перевірок уразливостей, щоб запобігти несанкціонованому доступу та виявити будь-яку незвичну діяльність. Регулярні аудити безпеки та перевірки відповідності є ключовими для підтримки високих стандартів безпеки.

Відповідність нормативним вимогам. Навіть якщо федеральні кол-центри не повинні безпосередньо дотримуватися таких правил, як Загальний регламент захисту даних (GDPR) або Стандарти безпеки даних індустрії платіжних карток (PCI DSS), вони все одно повинні дотримуватися власних стандартів безпеки, регулярно перевіряючи та оновлюючи, щоб запобігти злом. Суворі заходи безпеки мають вирішальне значення для безперебійної та безпечної роботи навіть без суворих правил.

Федеральні колл-центри стикаються з низкою проблем із постійними загрозами та мінливими ризиками в кібербезпеці. Але використовуючи суворі заходи безпеки, залишаючись обізнаними та дотримуючись внутрішніх процесів, ці кол-центри можуть впоратися з ризиками та залишатися в безпеці. Пріоритет кібербезпеки допомагає захистити конфіденційні дані, забезпечує безперебійну роботу операцій і забезпечує надійне обслуговування мільйонів людей, які залежать від них. Застосування цих стратегій не тільки захищає кол-центри, але й зміцнює довіру та впевненість серед громадськості». ***(Jerry Dotson. Securing your call centers: Best practices for cybersecurity protection // Industry Dive (https://www.cybersecuritydive.com/spons/securing-your-call-centers-best-practices-for-cybersecurity-protection/717175/). 03.06.2024).***

***

«Після юридичного втручання Федерального агентства з кібербезпеки Німеччини Microsoft розкрила додаткову інформацію про заходи шифрування, які вона застосувала для захисту даних своїх клієнтів.

У четвер корпорація Майкрософт опублікувала технічну документацію, в якій детально описано, як компанія розгортає шифрування з подвійним ключем на своїй платформі, включаючи Microsoft 365 і Azure.

«Біла книга описує деякі можливі сценарії загроз, які необхідно взяти до уваги, а також відповідні контрзаходи», — повідомили в блозі німецького офісу Microsoft.

Рішення Microsoft опублікувати звіт було прийнято після того, як Федеральне відомство з інформаційної безпеки (BSI) у травні застосувало пункт у Законі про Федеральне відомство з інформаційної безпеки країни, який вимагає від компаній інформаційних технологій надавати «всю необхідну» інформацію, пов'язану з інцидентами безпеки, коли на запит агентства.

Повідомляється, що BSI подав юридичний позов про розкриття інформації після того, як Microsoft неодноразово не надала належної інформації про свої заходи шифрування на запити агентства. Розслідування BSI пов'язане з розслідуванням інциденту 2023 року, в результаті якого хакери викрали токени Azure Active Directory для атаки на урядові мережі США.

У той час компанія приписувала атаку китайському загрозливому актору, відстежуваному як Storm-0558 або Volt Typhoon. Після того, як Microsoft розкрила факт злому, BSI працює з компанією, щоб перевірити заходи безпеки, зокрема, щоб зрозуміти кроки захисту даних, які використовує компанія від подібних атак Violet Typhoon.

Представник Microsoft у Німеччині повідомив Information Security Media Group, що BSI не подала позов, як широко повідомляли німецькі ЗМІ. Компанія завжди співпрацювала з владою щодо «уточнення документів, коли з'являлися нові або недостатньо представлені вектори загроз», сказав речник.

Представник BSI підтвердив, що агентство не подавало позов проти Microsoft. У четвер агентство закликало користувачів Microsoft у Німеччині розгорнути правильний сервіс шифрування, запропонований компанією, щоб захистити дані своїх клієнтів.

BSI перевіряє Microsoft на тлі посилення критики компанії через недавні гучні збої в системі безпеки. У травні уряд Німеччини заявив, що російські хакери використали невідому вразливість нульового дня в Microsoft Outlook, щоб атакувати членів Соціал-демократичної партії Німеччини.

Перед цим комітет парламенту Німеччини з нагляду за технологіями провів закриту зустріч із керівниками вищої ланки Microsoft після того, як у березні обчислювальний гігант оприлюднив інформацію про те, що російські хакери

зовнішньої розвідки отримали доступ до сховищ вихідного коду та внутрішніх систем.

Нещодавно президент Microsoft Бред Сміт під час слухань у Конгресі США визнав відповідальність за серію збоїв у безпеці, які дозволили російським і китайським державним суб'єктам атакувати державні установи в усьому світі та компанію.

За словами Денніса-Кенджі Кіпкера, професора права IT-безпеки в Міському університеті прикладних наук Бремена на північному заході Німеччини, після цього слухання Microsoft привернула до себе більший політичний інтерес з боку Німеччини.

«Для BSI також зрозуміло, що інформація, надана Microsoft на сьогоднішній день, не тільки абсолютно неадекватна, але також викликає побоювання, що в Microsoft справді існують явні проблеми безпеки. Очевидно, що концепція «безпеки через невідомість», якого Microsoft, очевидно, переслідувала роками, більше не працює і закінчується», - сказав Кіпкер». ***(Akshaya Asokan. German BSI Forces Microsoft to Disclose Security Measures // Information Security Media Group, Corp. (https://www.databreachtoday.com/german-bsi-forces-microsoft-to-disclose-security-measures-a-25553?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 18.06.2024).***

***

Масштабні витоки персональних даних

«Кіберзлочинна організація, відома як USDoD, нібито викрала 2,9 мільярда записів у Флоридського інформаційного брокера National Public Data, який обробляє пошук API для компаній, які запитують перевірку даних.

Базу даних вперше було помічено в Інтернеті в квітні 2024 року за ціною 3,5 мільйона доларів, а пізніше експерти з VX-Underground перевірили її як принаймні напівсправжню.

VX-Underground також вважає, що USDoD планує витік бази даних обсягом близько 300 ГБ, яка в основному містить записи громадян США, але також може містити дані про людей з інших країн, які жили в США, якщо вони не зробили одну просту річ.

USDoD знову витік

Інформація в базі даних містила конфіденційну особисту інформацію, включаючи повні імена, адреси та історію адрес, номери соціального страхування та детальну інформацію про членів родини, включаючи померлих.

Разом з усією невтішною інформацією, наданою VX-Underground, вони надали трохи хороших новин, заявивши, що «база даних НЕ містить інформації від осіб, які користуються службами відмови від даних. Кожен, хто користувався якоюсь послугою відмови від даних, не був присутній».

USDoD була однією з двох кіберзлочинних груп, причетних до витоку кримінальних досьє мільйонів американців на початку цього року, а також до крадіжки 3 ГБ бази даних TransUnion у 2023 році.

Провідний розробник інструментів для видалення зловмисного програмного забезпечення Malwarebytes минулого місяця заявив, що група USDoD прагне замінити BreachForums, який було ліквідовано ФБР у травні, але з тих пір якимось чином повернулося». ***(Benedict Collins. Cache of three billion background check records set to be sold online by cyber criminals // Future US, Inc. (https://www.techradar.com/pro/cache-of-three-billion-background-check-records-set-to-be-sold-online-by-cyber-criminals?utm_source=flipboard&utm_content=other). 04.06.2024).***

***

«Дослідники з кібербезпеки повідомили про ймовірний витік даних за участю щонайменше одного мільйона користувачів Facebook, який з'явився на форумі про порушення даних.

Команда некомерційної організації CyberPeace, що базується в Нью-Делі, стверджує, що 1 00 000 рядків свіжих даних користувачів із Facebook (Meta) з'явилися на форумі про порушення даних.

«Скомпрометовані дані включають повні імена, профілі, електронні адреси, номери телефонів і місцезнаходження», — заявили в CyberPeace.

Розголошення особистих даних може призвести до фішингових атак та інших зловмисних дій проти постраждалих.

Особи загрозливих осіб, відповідальних за це порушення, наразі невідомі.

Facebook (Meta) ще не прокоментувала заяви CyberPeace.

«Триває розслідування, щоб визначити, чи є цей злом роботою досвідченої групи кіберзлочинців, хактивістів або інших зловмисних організацій», — сказали дослідники.

«Facebook (Meta) загрожує потенційній репутаційній шкоді через занепокоєння щодо безпеки даних, що потенційно може вплинути на довіру користувачів», — сказали дослідники.

Передбачуване порушення даних Facebook (Meta) підкреслює постійні виклики, пов'язані з кіберзагрозами в цифровому просторі.

Дослідники заявили, що цей інцидент підкреслює критичну необхідність для організацій постійно покращувати та зміцнювати свої заходи кібербезпеки для захисту даних користувачів і підтримки громадської довіри». ***(Facebook hit with fresh user data leak, claim researchers // AhmedabadMirror (https://www.ahmedabadmirror.com/facebook-hit-with-fresh-user-data-leak-claim-researchers/81868653.html). 10.06.2024).***

***

Кібербезпека та хмарні технології

«Наступного тижня президент Microsoft Бред Сміт дасть свідчення перед Комітетом Палати представників із внутрішньої безпеки щодо «каскаду збоїв» своєї компанії після того, як пов'язані з державою Китаю хакери зламали

понад 500 федеральних хмарних облікових записів у травні минулого року. Під час слухань законодавці почують оновлення щодо нових методів кібербезпеки від керівництва Microsoft і розглянуть, що ще можна зробити, щоб зміцнити компанію проти атак. Те, що, ймовірно, не обговорюватиметься: альтернативи олігополії хмарних сховищ Сполучених Штатів, якщо її противники продовжуватимуть отримувати доступ до критично важливих державних даних у майбутньому.

Розмір і масштабованість дозволяють великим постачальникам хмарних технологій пропонувати урядам послуги та ціни, з якими місцеві конкуренти не можуть зрівнятися. Лише три технічні гіганти США — Google, Amazon і Microsoft — відповідають за зберігання найбільш конфіденційних державних баз даних по всій Америці та Європі. Навіть якщо їхня хмарна архітектура не «прив'язана» до одного постачальника, держави можуть втратити можливість домовитися про вигідні умови через тривалі мегаугоди, реалізація яких є дорогою, а відмова від них ще дорожча.

У Сполучених Штатах, де минулого року федеральні витрати на хмарні обчислення перевищили 19 мільярдів доларів, окремі IT-провайдери відіграють центральну роль у національній кібербезпеці. Лише дві фірми, Microsoft і Amazon, мають право на контракти Міністерства оборони на хмарний хостинг на мільярди доларів на рік, і понад 30 відсотків контрактів Microsoft були укладені без ефективної конкуренції. Примітно, що це менш централізоване середовище, ніж у попередні роки; У 2019 році Microsoft мала отримати майже 10 мільярдів доларів, ексклюзивні контракти на суму перш ніж конкуренти Amazon і Oracle подали до суду за ймовірні порушення федерального законодавства про закупівлі.

Хоча здається дивним, що в США буде так мало постачальників для послуги, яка пропонується протягом майже 20 років, збереження довіри до лідера галузі приносить значні переваги. Під керівництвом такого гіганта, як Microsoft, федеральні агентства мають доступ до розгалуженої мережі послуг, IT-експертів, які працюють за викликом, і брандмауерів кібербезпеки на передньому краї ринку. Взаємодія програмних пакетів означає, що інфраструктура, яка підтримує хмару, вільна від накопичених даних, непотрібного дублювання та інших недоліків.

Великі технологічні фірми також відіграли важливу роль у забезпеченні технічної експертизи, продуктів і фінансових інвестицій, які дозволили агентствам оптимізувати перехід до хмари та запровадити загальносистемні інновації під час кризи.

Однак, якщо щось здається занадто гарним, щоб бути правдою, зазвичай це так. Хоча федеральні знижки від великих постачальників хмарних технологій спочатку є вигідними, річні ставки на хмарний хостинг зростають з часом стрімко та нерівномірно в уряді. Відключатися від однієї екосистеми до іншої непросто, і, згідно з судовими позовами постачальників, антиконкурентна корпоративна практика ще більше ускладнює перехід для федеральних споживачів. Незважаючи на вражаючий масштаб і частку ринку Microsoft, експерти та інсайдери все частіше критикують її нездатність запровадити основні протоколи безпеки — самовдоволення призводить до значних наслідків для національної безпеки, оскільки вона захищає найважливіші оборонні технології та розвідувальні дані американських військових.

Враховуючи ці ризики, нові федеральні заходи спрямовані на покращення ринкової конкуренції та кидають вогонь великим технологіям. Закон SAMOSA, який швидко набув двопартійного імпульсу та очікує на розгляд у Сенаті, був запроваджений для регулювання «необмежених» хмарних угод та інших грабіжницьких корпоративних практик. інфраструктуру. Минулого місяця Комітет Сенату з внутрішньої безпеки та урядових справ ухвалив Закон про багатохмарні інновації та розвиток, який пропонує стандартизувати федеральну хмару. На слуханнях у Палаті представників президент Microsoft Бред Сміт виступить із доповіддю, опублікованою Радою з аналізу кібербезпеки в березні, в якій зазначено, що культура безпеки Microsoft є «неадекватною та потребує перегляду».

Для деяких ці дії доводять, що законодавці нарешті вирішують ключові системні збої, якими довго нехтували. Однак без життєздатної альтернативи наслідки дозволу на втручання будуть не більшими, ніж ляпасом по зап’ястку. Фактично, це може навіть прийти із стимулами; минулого року Міністерство оборони оголосило, що буде допомагати федеральним постачальникам хмарних

технологій покращувати їхні пакети кібербезпеки. Притягнути постачальників хмарних технологій до відповідальності за їхні заявлені обіцянки, перейти до більш надійного партнера чи погрожувати побудувати власну мережу керування хмарами – це не було варіантом, незважаючи на те, що валовий прибуток галузі зріс до понад 50 відсотків у 2024 році.

Субсидуючи надійніші протоколи безпеки замість того, щоб вимагати їх, державні установи прагнуть зберегти давні відносини та підтримувати постійну співпрацю щодо федеральних IT-ініціатив. Незважаючи на внески великих технологічних компаній у державу, їхня головна відповідальність лежить на прибутковості — і якщо федеральні закупівлі стануть збитковими, вони дослідять інші варіанти. Щоб зберегти свою переговорну силу, законодавці повинні робити те саме. Збалансовуючи інтереси акціонерів і безпеку США та їхніх союзників, не повинно виникати сумнівів щодо позиції нашого уряду». ***(Courtney Manning. Shaming Microsoft won't strengthen US cybersecurity. It's time for alternatives // Nexstar Media Inc. (https://thehill.com/opinion/technology/4705671-shaming-microsoft-wont-strengthen-us-cybersecurity-its-time-for-alternatives/?utm_source=flipboard&utm_content=user%2FTheHill). 05.06.2024).***

***

«Злом клієнтів компанії Snowflake, що займається хмарним зберіганням даних, схоже, може перетворитися на одну з найбільших витоків даних за всю історію. Минулого тижня компанія Snowflake, яка дозволяє компаніям зберігати величезні набори даних на своїх серверах, виявила, що злочинні хакери намагалися отримати доступ до облікових записів її клієнтів, використовуючи вкрадені дані для входу. Порушення даних, націлених на Ticketmaster і Santander, були пов'язані з атаками.

За кілька днів після того, як Snowflake вперше заявила про доступ до «обмеженої кількості» облікових записів клієнтів, кіберзлочинці публічно заявили, що продають викрадені дані двох інших великих фірм, і стверджували, що інформацію було взято з облікових записів Snowflake. У той же час TechCrunch

повідомив, що сотні паролів клієнтів Snowflake були знайдені в мережі і доступні кіберзлочинцям.

Серед претензій залишається невизначеність щодо обсягу та масштабу спроби атаки на клієнтів Snowflake, ким можуть бути зловмисники та як працює інструмент атаки під бездушною назвою «rapeflake». Він також підкреслює зростання використання зловмисного програмного забезпечення infostealer за останні роки та підкреслює потребу сторонніх постачальників програмного забезпечення та компаній увімкнути багатофакторну автентифікацію, щоб зменшити ймовірність скомпрометації облікових записів.

Сніжний ком

Значна частина драми про Snowflake наразі розігрується на сумнозвісному ринку кіберзлочинців BreachForums. ФБР захопило форум у середині травня, але швидко з'явилася інша версія, і її власники, хакерська група ShinyHunters, заявили про продаж 560 мільйонів записів від Ticketmaster і 30 мільйонів від Santander. Обидві компанії заявили, що постраждали від витоку даних, причому Ticketmaster безпосередньо пов'язала інцидент зі Snowflake, а Santander заявила, що помітила несанкціонований доступ до однієї зі своїх баз даних, «розміщеної стороннім постачальником». Жодна з компаній не підтвердила розміри порушень.

Останніми днями обліковий запис BreachForums під назвою Sp1d3r опублікував ще дві компанії, чиї дані, як стверджується, пов'язані з інцидентом зі Сніжинкою: автомобільний гігант Advance Auto Parts, від якого Sp1d3r стверджує, що володіє 380 мільйонами даних про клієнтів, і компанія з фінансових послуг LendingTree. і дочірня компанія QuoteWizard, від якої вона стверджує, що має дані, пов'язані з 190 мільйонами людей.

Адреси електронної пошти деяких співробітників Advance Auto Parts і клієнтів, зазначені хакером у зразках даних, виглядають як законні облікові записи; електронні листи WIRED, надіслані на ці адреси, не поверталися і не відхилялися іншим чином. BleepingComputer повідомляє, що перевірив дані клієнтів від Advance Auto Parts.

«Ми знаємо про повідомлення про те, що Advance може бути причетний до інциденту безпеки, пов’язаного зі Snowflake», — сказав WIRED представник компанії Дарріл Карр. «Ми розслідуємо це питання і наразі не маємо додаткової інформації, щоб поділитися. Ми не зазнали жодного впливу на наші операції чи системи».

На момент написання статті ні LendingTree, ні Advance Auto Parts не подали повідомлення про порушення до Комісії з цінних паперів та бірж. Обидві компанії раніше були включені до списку клієнтів Snowflake.

Представник LendingTree підтвердив у заяві для WIRED, що компанія використовує Snowflake «для наших бізнес-операцій» і що компанія була повідомлена про те, що її дочірня компанія QuoteWizard «могла мати дані, які вплинули на цей інцидент». Представник LendingTree каже, що внутрішнє розслідування триває. «Станом на цей час, схоже, що це не вплинуло на інформацію про фінансові рахунки споживача, а також на інформацію материнської організації LendingTree», — сказав речник.

Оскільки Snowflake визнала, що облікові записи були ціллю, вона надала додаткову інформацію про інцидент. Бред Джонс, головний спеціаліст з інформаційної безпеки Snowflake, зазначив у дописі в блозі, що зловмисники використовували дані для входу в облікові записи, які були «куплені або отримані за допомогою зловмисного програмного забезпечення для крадіжки інформації», яке призначене для отримання імен користувачів і паролів із зламаних пристроїв. Схоже, що інцидент є «цільовою кампанією, спрямованою на користувачів з однофакторною автентифікацією», — додав Джонс.

У публікації Джонса сказано, що Snowflake разом із компаніями з кібербезпеки CrowdStrike і Mandiant, яких вона найняла для розслідування інциденту, не знайшли доказів того, що атака була «спричинена скомпрометованими обліковими даними поточного або колишнього персоналу Snowflake». Однак було виявлено, що демо-рахунки одного колишнього співробітника отримали доступ, стверджуючи, що вони не містять конфіденційних даних.

Коли його запитали про можливі порушення даних конкретних компаній, представник Snowflake вказав на заяву Джонса: «Ми не знайшли доказів того, що ця діяльність була спричинена вразливістю, неправильною конфігурацією або порушенням платформи Snowflake». У подальшій заяві компанія пояснила, що вона має на увазі під «порушенням»: «Будь-який з облікових записів наших клієнтів, до яких було отримано доступ у результаті витоку облікових даних, не викликаний … Snowflake», — сказав представник. (Охоронна компанія Hudson Rock заявила, що видалила дослідницьку публікацію, включно з різними неперевіреними заявами про інцидент зі Snowflake, після того як отримала правовий лист від Snowflake).

Агентство з кібербезпеки та безпеки інфраструктури США повідомило про інцидент зі Snowflake, а Центр кібербезпеки Австралії заявив, що йому «відомо про успішні компрометації кількох компаній, які використовують середовища Snowflake».

Незрозуміле походження

Мало відомо про рекламні дані облікового запису Sp1d3r на BreachForums, і неясно, чи отримав ShinyHunters дані, які він продавав, з іншого джерела чи безпосередньо з облікових записів Snowflake жертв — інформація про порушення Ticketmaster і Santander спочатку була опублікована на іншому форумі кіберзлочинності. новим користувачем під назвою SpidermanData.

Обліковий запис Sp1d3r опублікував на BreachForums, що 2 терабайти передбачуваних даних LendingTree і QuoteWizard продаються за 2 мільйони доларів; тоді як 3 ТБ даних, нібито з Advance Auto Parts, коштуватимуть комусь 1,5 мільйона доларів. «Ціна, встановлена загрозою, здається надзвичайно високою для типового списку, опублікованого на BreachForums», — каже Кріс Морган, старший аналітик із розвідки кіберзагроз охоронної фірми ReliaQuest.

Морган каже, що законність Sp1d3r не ясна; однак він зазначає, що є схиляння до підліткової хакерської групи Scattered Spider. «Цікаво, що зображення профілю загрозливого актора взято зі статті, у якій згадується група загроз Scattered Spider, хоча незрозуміло, чи це означає навмисну асоціацію з групою загроз».

Хоча точне джерело ймовірного витоку даних невідоме, інцидент підкреслює, наскільки взаємопов'язаними можуть бути компанії, покладаючись на продукти та послуги сторонніх постачальників. «Я думаю, що багато в чому це просто визнання того, наскільки взаємозалежними є ці служби зараз і як важко контролювати стан безпеки третіх сторін», — сказав WIRED дослідник безпеки Торі Хант, коли вперше з'явилися інциденти.

У рамках відповіді на атаки Snowflake попросила всіх клієнтів переконатися, що вони застосовують багатофакторну автентифікацію для всіх облікових записів і дозволяють трафік лише від авторизованих користувачів або місць. Компанії, які постраждали, також повинні скинути свої облікові дані для входу в Snowflake. Увімкнення багатофакторної автентифікації значно зменшує ймовірність того, що онлайн-акаунти будуть скомпрометовані. Як уже згадувалося, цього тижня TechCrunch повідомив, що він бачив «сотні передбачуваних облікових даних клієнтів Snowflake», отриманих зловмисним програмним забезпеченням для крадіжки інформації з комп'ютерів людей, які мали доступ до облікових записів Snowflake.

В останні роки, коли після пандемії Covid-19 більше людей почали працювати вдома, спостерігалося зростання використання зловмисного програмного забезпечення для викрадання інформації. «Викрадачі інформації стали більш популярними, тому що вони користуються великим попитом і їх досить легко створити», — каже Ян Грей, віце-президент із розвідки охоронної компанії Flashpoint. Було помічено, що хакери копіюють або модифікують існуючі викрадачі інформації та продають їх лише за 10 доларів США за всі дані для входу, файли cookie, файли тощо з одного зараженого пристрою.

«Це зловмисне програмне забезпечення може бути доставлено різними способами та націлено на конфіденційну інформацію, як-от дані браузера (файли cookie та облікові дані), кредитні картки та крипто-гаманці», — каже Грей. «Хакери можуть прочесати журнали в пошуках облікових даних підприємства, щоб зламати облікові записи без дозволу». ***(The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever // Condé Nast (https://www.wired.com/story/snowflake-***

breach-advanced-auto-parts-lendingtree/?utm_source=flipboard&utm_content=rossdonn%2Fmagazine%2FSECURITY). 06.06.2024).

***

Кібербезпека Інтернету речей. Штучний інтелект

«Кібератаки, спричинені штучним інтелектом (ШІ), створюють безпрецедентні ризики для глобальної економіки, ланцюгів поставок і торгівлі. Майбутнє дослідження журналу Risk Analysis досліджує каскадні наслідки кібератак, керованих ШІ.

На відміну від традиційних кібератак, які зазвичай відбуваються вручну або за сценарієм, кібератаки, керовані штучним інтелектом, використовують алгоритми штучного інтелекту та машинного навчання, щоб підвищити свою ефективність, прихованість і адаптивність. Кібератаки, керовані штучним інтелектом, можуть самостійно вивчати та розвивати свою тактику, методи та процедури на основі зворотного зв'язку в реальному часі та змін середовища.

За допомогою симуляційних сценаріїв дослідники виявили потенційні економічні наслідки кібератак, зосередившись на регіонах, які значною мірою залежать від цифрових технологій і взаємопов'язаних ланцюжків поставок. Аналіз виявив значне зниження реального ВВП, торговельних цін і обсягів, а також порушення торговельних шляхів між регіонами. Найбільш уразливими економіками були Китай, США, Великобританія та ЄС – через їх глибоку інтеграцію в глобальні мережі.

Вплив кібератак, керованих штучним інтелектом, на світову торгівлю та економіку є багатогранним і всеосяжним. Відповідно до звіту IBM Cost of a Data Breach Report, у 2021 році середня вартість витоку даних у всьому світі досягла 4,24 мільйона доларів. У звіті Всесвітнього економічного форуму про глобальні

ризики за 2022 рік кіберзагрози є одними з головних ризиків для бізнесу та економіки в усьому світі.

Вплив на ВВП

Результати дослідження показали різний ступінь негативного впливу на реальний ВВП основних регіонів за різних сценаріїв кіберзагроз. Для кіберзагрози низького рівня з обмеженими порушеннями зниження реального ВВП було відносно незначним, коливаючись від 0,02 до 0,25%. У Китаї, Японії та Південній Кореї спостерігалося дещо більше падіння реального ВВП. На ці три економіки припадає близько 20% світової торгівлі, і вони є основними взаємними торговими партнерами з сильною внутрішньогалузевою торгівлею продукцією промисловості.

Що стосується кіберзагрози високого рівня, США, Великобританія, ЄС, Китай, Японія та Індія зіткнулися з більш вираженим скороченням ВВП. Це демонструє посилений згубний вплив кіберзагрози високого рівня, що призводить до більш значних економічних збоїв.

Вплив на торгові ціни

У рамках дослідження всі регіони зазнали погіршення умов торгівлі, тобто їхні експортні ціни зросли менше, ніж ціни на імпорт через кібератаку ШІ. Різке падіння обсягів торгівлі відбулося в країнах із високою залежністю від цифрових технологій і потужними взаємопов’язаними ланцюжками поставок (наприклад, США). Економіки, які більшою мірою залежать від експорту, відчувають кращі умови торгівлі (наприклад, Китай, Японія та Південна Корея) порівняно з іншими економіками, такими як Великобританія, Індія та Росія.

Вплив на торговельні шляхи

У сценарії високої кібератаки основні торговельні партнери, такі як Китай і США, зазнають збоїв у своїх прямих обмінах, пропонуючи альтернативні маршрути та приносячи користь таким країнам-посередникам, як Індія, Японія та країни Північної та Латинської Америки. Експорт Китаю до США різко впав на -24%, а його експорт до Великобританії та ЄС зменшився на -4,5% і -3,2% відповідно.

Наслідки дослідження

Отримані дані підкреслюють нагальну потребу в глобальній зміні парадигми в бік кіберстійкості, щоб пом'якшити далекосяжні наслідки кіберзагроз, спричинених штучним інтелектом, для взаємопов'язаної екосистеми глобальної торгівлі. Дослідження демонструє ефективність профілактичних заходів, таких як адаптивні виробничі системи, різноманітні торговельні партнери та надійна інфраструктура кібербезпеки для пом'якшення несприятливих наслідків кібератак.

«Включення кіберстійкості значно послаблює негативні наслідки, про які повідомлялося, підкреслюючи критичну роль готовності в боротьбі з цифровою війною», — каже дослідник д-р Шериф Елгенді. «Колективні зусилля зі зміцнення інфраструктури кібербезпеки, сприяння міжнародній співпраці в розвідці загроз і створення відкритих і стійких торговельних структур мають вирішальне значення для навігації в підступному лабіринті кібератак, керованих ШІ». ***(AI-Driven Cyberattacks Can Inflict Damage On GDP And Supply Chains For World's Largest Economies // Eurasia Review (https://www.eurasiareview.com/06062024-ai-driven-cyberattacks-can-inflict-damage-on-gdp-and-supply-chains-for-worlds-largest-economies/?utm_source=flipboard&utm_content=EurasiaReview%2Fmagazine%2FEurasia+Review). 06.06.2024).***

***

«…Кілька місяців тому команда дослідників опублікувала статтю, в якій говорилося, що вони змогли використати GPT-4 для автономного зламу одноденних (або N-денних) уразливостей – це вже відомі вади безпеки, але для яких виправлення ще не випущено. Якщо отримати список загальних вразливостей і ризиків (CVE), GPT-4 зміг використати 87% CVE критичного рівня серйозності самостійно.

На цьому тижні та сама група дослідників опублікувала додаткову статтю, в якій говориться, що їм вдалося зламати вразливості нульового дня – вразливості, про які ще не відомо – за допомогою команди автономної великої мовної моделі,

що саморозповсюджується. (LLM) агентів, які використовують метод ієрархічного планування з агентами, що відповідають конкретним завданням (HPTSA).

Замість того, щоб призначати одного агента LLM, який намагається вирішити багато складних завдань, HPTSA використовує «агента планування», який контролює весь процес і запускає кілька «субагентів», які залежать від конкретного завдання. Подібно до начальника та його підлеглих, агент з планування координує роботу з керуючим агентом, який делегує всі зусилля кожного «субагента-експерта», зменшуючи навантаження одного агента на завдання, яке йому може бути важко.

Це техніка, подібна до тієї, яку Cognition Labs використовує зі своєю командою розробників програмного забезпечення Devin AI; він планує роботу, з'ясовує, які працівники їй знадобляться, а потім керує проектом до кінця, створюючи власних «співробітників» спеціалістів для виконання завдань за потреби.

ШІ Командна робота

Під час порівняння з 15 реальними веб-вразливими місцями HPTSA показала, що на 550% ефективніше, ніж один LLM у використанні вразливостей, і змогла зламати 8 із 15 уразливостей нульового дня. Одиночна спроба LLM змогла зламати лише 3 із 15 уразливостей.

Чорний капелюх чи білий капелюх? Існує законне занепокоєння, що ці моделі дозволять користувачам зловмисно атакувати веб-сайти та мережі. Деніел Кан (Daniel Kang), один із дослідників і автор білої книги, зокрема зазначив, що в режимі чат-бота GPT-4 «недостатньо для розуміння можливостей LLM» і не може нічого зламати самостійно.

Це принаймні хороші новини.

Коли я запитав ChatGPT, чи може він використати для мене вразливості нульових днів, він відповів: «Ні, я не в змозі використовувати вразливості нульових днів. Моя мета — надавати інформацію та допомогу в межах етичних і правових норм», і запропонував мені проконсультуватися натомість спеціаліст із кібербезпеки». ***(Joe Salas. GPT-4 autonomously hacks zero-day security flaws with***

53% success rate // New Atlas (https://newatlas.com/technology/gpt4-autonomously-hack-zero-day-security-flaws/?utm_source=flipboard&utm_content=johnspies%2Fmagazine%2FWTF%3F%3F). 08.06.2024).

***

Корпорація Майкрософт у п’ятницю заявила, що внесе серйозні зміни в нещодавно анонсований продукт штучного інтелекту, який покладається на скріншоти екранів користувачів, щоб створити доступний для пошуку журнал минулих дій, крок, який був зроблений після того, як дослідники безпеки послабили критику.

Коли минулого місяця Microsoft анонсувала функцію, яку вона назвала Recall, генеральний директор Сатья Наделла назвав її «фотографічною пам’яттю», яка може «відтворювати моменти з минулого» будь-чого, що робить користувач, використовуючи фірмові моделі штучного інтелекту компанії, які працюють на майбутніх ПК Copilot+.

Дослідники безпеки швидко вказали, що такі скріншоти містять конфіденційну інформацію, включаючи імена користувачів і паролі, але Microsoft заявила, що дані захищені. Видатні експерти з питань безпеки, зокрема Кевін Бомонт, швидко звернули увагу на те, що дані насправді зберігаються у вигляді звичайного тексту, і назвали рішення запустити продукт, який було заплановано на 18 червня, «найдурнішим кроком у сфері кібербезпеки в світі». десятиліття».

Використовувати функцію виявилося досить легко. Алекс Хагенах, дослідник із SIX Group AG, наприклад, створив інструмент під назвою «TotalRecall», який скопіював базу даних і аналізував її на цікаві деталі.

У п’ятницю корпорація Майкрософт оголосила про серію змін у продукті, включно з тим, щоб включити та вимкнути Recall за замовчуванням. Крім того, продукт потребуватиме біометричної реєстрації через продукт компанії Windows Hello, щоб увімкнути його, і підтвердження присутності для перегляду хронології

знімків екрана та пошуку в Recall. Компанія також заявила, що покращить шифрування бази даних Recall.

«Навіть до того, як зробити Recall доступним для клієнтів, ми почули чіткий сигнал про те, що ми можемо спростити людям вибір для ввімкнення Recall на своїх ПК Copilot+ і покращити захист конфіденційності та безпеки», — Паван Давулурі, корпоративний віце-президент Microsoft Windows і пристроїв, йдеться в дописі в блозі в п’ятницю.

Зміни в Recall відбулися після того, як Microsoft пообіцяла надавати пріоритет безпеці в розробці свого продукту після серії гучних порушень безпеки з боку російських і китайських державних хакерів. У звіті Комітету з аналізу кібербезпеки США зроблено висновок, що Microsoft створила корпоративну культуру, яка знецінила безпеку.

Ця доповідь спонукала Наделлу оголосити співробітникам корпорації Майкрософт наказ, наказуючи їм надати пріоритет безпеці її продуктів. «Якщо ви зіткнулися з компромісом між безпекою та іншим пріоритетом, ваша відповідь однозначна: забезпечте безпеку», — написав він у записці для компанії.

Експерти з безпеки вказали на проблеми з безпекою Recall як на доказ того, що Microsoft ще не дотримується цієї обіцянки, і Бомонт заявив у п’ятницю, що деталі того, як впроваджуються зміни, будуть мати значення, припускаючи, що дослідники з безпеки проводять «глибоке занурення в найближчий час». тижнів» щодо претензій Microsoft щодо посилення безпеки». ***(AJ Vicens. Microsoft rolls back ‘dumbest cybersecurity move in a decade’ // CyberScoop (https://cyberscoop.com/microsoft-rolls-back-dumbest-cybersecurity-move-in-a-decade/?utm_source=flipboard&utm_content=other). 07.06.2024).***

***

«Відповідно до звіту компанії з кібербезпеки Deep Instinct, команди з кібербезпеки змінюють свої стратегії, щоб не відставати від нових загроз на основі штучного інтелекту, спрямованих на бізнес.

У звіті Deep Instinct Voice of SecOps було опитано 500 старших експертів з кібербезпеки з компаній із понад 1000 співробітників у США.

У звіті встановлено, що 75% респондентів змінили свою стратегію кібербезпеки за останні 12 місяців для боротьби з кіберзагрозами, створеними на базі ШІ.

Майже всі (97%) опитаних фахівців із безпеки висловили занепокоєння, що їхня організація постраждає від злому через ШІ.

Ще 61% зізналися, що за останні 12 місяців спостерігали збільшення дипфейків. Три чверті (75%) респондентів сказали, що бачили дипфейки, які намагалися видати себе за генерального директора або керівника старшого офісу.

Незважаючи на зростання занепокоєння щодо штучного інтелекту, Deep Instinct виявив, що 41% компаній покладаються на застарілі рішення для виявлення та реагування на кінцеві точки (EDR) для захисту своїх організацій.

EDR відстежують пристрої кінцевих користувачів для виявлення потенційних кіберзагроз. Однак у звіті використання EDR для боротьби зі штучним інтелектом «еквівалентно боротьбі з пожежею з п’ятьма сигналами тривоги за допомогою садового шланга».

Близько 31% респондентів заявили, що планують збільшити свої інвестиції в EDR для боротьби зі штучним інтелектом.

Крім EDR, 42% опитаних фахівців з кібербезпеки заявили, що їхня організація використовує превентивні технології для боротьби з атаками штучного інтелекту, включаючи платформи прогнозної профілактики.

Майже половина (45%) респондентів визнали, що вважають, що їхні роботодавці витрачають даремно свої інвестиції в кібербезпеку.

Інші серйозні проблеми, які висвітлювали фахівці з безпеки, включали відсутність досвіду щодо штучного інтелекту, старіння інфраструктури та систем, а також погану оцінку ризиків.

«Кількість кібератак, спричинених штучним інтелектом, продовжує зростати в геометричній прогресії, і організації більше не можуть захищатися від них, покладаючись на застарілі, реактивні інструменти кібербезпеки, – сказав Лейн

Бесс, генеральний директор Deep Instinct. – Ось мій виклик для керівників інформаційної безпеки, правлінь і команд безпеки: поставте пріоритет у профілактиці, поки не пізно. Глибоке навчання — це єдиний спосіб протистояти цим загрозам на основі штучного інтелекту, передбачаючи та запобігаючи наступній кіберзагрозі до того, як вона станеться, підвищуючи стійкість кібербезпеки та полегшуючи виснаження».

У звіті Deep Instinct також випливає, що генеративний штучний інтелект завдає шкоди фахівцям із безпеки.

Більше половини (53%) опитаних професіоналів сказали, що їхні команди відчувають підвищений тиск у залі засідань, тоді як 56% сказали, що їхній рівень стресу був гіршим, а 66% сказали, що штучний інтелект «викликає відчуття виснаження та стресу».

У звіті було виявлено, що співробітники C-suite стурбовані готовністю свого бізнесу протистояти атакам штучного інтелекту, причому одна третина (33%) стурбована тим, що їм не вистачає необхідної інформації про системи та інструменти штучного інтелекту.

Близько 35% респондентів сказали, що інструменти штучного інтелекту підвищують продуктивність і автоматизують рутинні завдання. Стільки ж сказано, що застосування проактивного підходу до кібербезпеки допомагає зняти стрес, пов’язаний з виконанням ролі». ***(Ben Wodecki. AI Cyber Threats Force 75% of Firms to Change Security Strategies // Informa PLC (https://www.itprotoday.com/vulnerabilities-threats/ai-cyber-threats-force-75-of-firms-to-change-security-strategies). 05.06.2024).***

***

«В епоху, коли кіберзагрози стають дедалі складнішими та поширеними, роль штучного інтелекту (ШІ) у зміцненні захисту кібербезпеки є критичнішою, ніж будь-коли. Здатність штучного інтелекту аналізувати величезні масиви даних, виявляти аномалії та автоматизувати відповіді пропонує потужний набір інструментів для боротьби з цими загрозами, що розвиваються.

Оскільки організації по всьому світу прагнуть захистити свої цифрові активи, піонерські рішення, такі як Strata Copilot від Palo Alto Networks, встановлюють нові стандарти в інтеграції штучного інтелекту в кібербезпеку.

Однією з ключових фігур у розробці революційного Strata Copilot є Сакші Махендру, старший інженер Palo Alto Networks. З моменту приєднання до компанії в липні 2021 року Сакші відіграв важливу роль у кількох проектах, останнім із яких є Strata Copilot, інструмент мережевої безпеки на основі штучного інтелекту, який працює на базі технології Precision AI, щоб забезпечити безперебійне виявлення, миттєве розуміння та керовані дії для швидшого дозвіл.

«Strata Copilot кардинально змінює правила гри. Завдяки інтеграції штучного інтелекту та обробки природної мови ми створили інструмент, який не тільки виявляє та запобігає загрозам, але й допомагає командам безпеки розуміти та ефективно вирішувати проблеми», — пояснив Сакші.

Вплив Strata Copilot на кіберзахист

Strata Copilot є частиною ширшої ініціативи Palo Alto Networks щодо продовження впровадження штучного інтелекту в пропозиції продуктів. Інструмент використовує власну систему Precision AI, яка поєднує машинне навчання, глибоке навчання та генеративний штучний інтелект для забезпечення точних результатів безпеки. Ця система автоматизує виявлення, запобігання та усунення загроз, значно скорочуючи середній час вирішення (MTTR).

«Штучний інтелект — це єдиний спосіб боротьби зі штучним інтелектом. Кіберзловмисники використовують ШІ для масштабування та прискорення атак, і ми повинні використовувати передові системи штучного інтелекту, такі як Precision AI, щоб залишатися попереду», — підкреслив Сакші.

Крім того, Precision AI від Palo Alto Networks надає можливості високої роздільної здатності кіберзахисникам шляхом централізації та аналізу даних за допомогою моделей безпеки. Це допомагає командам безпеки автоматизувати виявлення, запобігання та реагування з провідною в галузі точністю. Більш широкі наслідки Strata Copilot і Precision AI є глибокими, оскільки вони дозволяють

організаціям боротися з загрозами, спричиненими ШІ, спрощувати операції безпеки та захищати інфраструктуру ШІ.

Революція кібербезпеки за допомогою ШІ

Внесок Sakshi виходить за межі розробки продукту. Вона бере активну участь у передових дослідженнях і постійно досліджує нові технології та методології для підвищення кібербезпеки. Її здатність процвітати в динамічному середовищі та випереджати нові загрози робить її ключовим гравцем у сфері кібербезпеки.

«Коли відбувається інцидент безпеки, швидке реагування має вирішальне значення. Однак традиційне реагування на інцидент може бути повільним через ручний збір, аналіз і виправлення даних, що призводить до тривалого впливу та потенційних порушень», — пояснив Сакші. «Інтеграція Generative AI у систему кібербезпеки значно прискорює реагування на інциденти. Це дозволяє системам розуміти запити природною мовою та відповідати на них, роблячи складні завдання більш доступними та швидшими для виконання. Поєднуючи GenAI з розширеним машинним навчанням і глибоким навчанням, ми можемо забезпечувати точні та ефективні дії розуміння для ефективного усунення загроз і вразливостей».

Використання ШІ для боротьби із загрозами, спричиненими ШІ

Оскільки кіберзагрози стають все більш витонченими, потреба в передових рішеннях на основі штучного інтелекту стає гострішою, ніж будь-коли. Хакери використовують штучний інтелект для покращення фішингу, масштабування атак, створення нових векторів атак і виявлення вразливостей. Precision AI від Palo Alto Networks дає можливість організаціям розвиватися до автономної безпеки в режимі реального часу, щоб зупиняти передові загрози, покращувати MTTR і вирішувати операційні проблеми.

«Точний штучний інтелект є наріжним каменем нашого підходу до трансформації кібербезпеки. Він дозволяє нам виявляти приблизно 1,6 мільйона нових унікальних атак щодня, блокуючи близько 8,6 мільярда атак», – зазначив Сакші, повторюючи статистику, наведену генеральним директором компанії під час запуску продукту. «Такий рівень точності й автоматизації має вирішальне значення для того, щоб випереджати супротивників».

Автоматизуючи виснажливі завдання та надаючи корисну інформацію, Strata Copilot і Precision AI не тільки зміцнюють захист кібербезпеки, але й звільняють людські ресурси, щоб зосередитися на більш стратегічних ініціативах. Експертиза Сакші Махендру та його внесок у цю сферу не тільки підвищують ефективність захисту кібербезпеки, але й прокладають шлях до нової ери кібербезпеки, перш за все ШІ.

Національні та глобальні наслідки

Інтеграція штучного інтелекту в кібербезпеку — це не просто технологічний прогрес, а важливий крок у захисті національних і глобальних інтересів. Оскільки кіберзагрози від державних і недержавних суб'єктів зростають у масштабах і витонченості, такі інструменти, як Strata Copilot і Precision AI, стають незамінними. Вони відіграють вирішальну роль у забезпеченні того, щоб як американські, так і глобальні компанії могли захистити свою критично важливу інфраструктуру, конфіденційні дані та інтелектуальну власність від зловмисних дій, тим самим сприяючи загальній національній безпеці та економічній стабільності.

Запроваджуючи інновації в галузі кібербезпеки на основі штучного інтелекту, Сакші Махендру та її команда з Palo Alto Networks встановлюють нові стандарти для галузі, гарантуючи, що організації в усьому світі будуть краще оснащені для протидії кіберзагрозам завтрашнього дня та за його межами». ***(Maria Williams. Harnessing AI for Cyber Defense with Strata Copilot: Insights from Cybersecurity Expert Sakshi Mahendru // Tech Times Inc. (https://www.techtimes.com/amp/articles/305597/20240611/harnessing-ai-for-cyber-defense-with-strata-copilot-insights-from-cybersecurity-expert-sakshi-mahendru.htm). 11.06.2024).***

***

«15 травня 2024 року Міністерство науки, інновацій і технологій (DSIT) опублікувало конкурс на отримання думок щодо кібербезпеки ШІ.

Він зосереджений на ризиках кібербезпеки для моделей і технологій штучного інтелекту (ШІ) на відміну від ризиків безпеки та кібербезпеки, пов'язаних із ШІ, які є ширшими питаннями.

У центрі цього заклику до представлення думок знаходиться пропозиція щодо добровільного Кодексу практики кібербезпеки штучного інтелекту, який, у свою чергу, має створити новий глобальний стандарт для моделей штучного інтелекту.

Тут ми підсумовуємо ключові моменти.

Кіберризики та потреба в безпечному дизайні

DSIT підкреслив, що кібербезпека є ключовою основою безпеки штучного інтелекту, особливо в міру розвитку технологій навколо цього. Це відображає один із п'яти ключових принципів, викладених у Білій книзі щодо регулювання штучного інтелекту Великобританії; Безпека, захист і міцність. Відповідно, уряд Великобританії підкреслив необхідність підтримки розробників і розгортачів систем штучного інтелекту в боротьбі з ризиками кібербезпеки для їхніх систем.

Зокрема, конкурс підкреслив очевидну слабкість внутрішньої інфраструктури багатьох організацій: 47% організацій, які використовують штучний інтелект, не мають жодних конкретних практик або процесів кібербезпеки штучного інтелекту.

Відповідно, передбачуваний підхід до кібербезпеки у Великій Британії є безпечним за проектом, який має захищати підприємства та спільноти від кіберзагроз із самого початку.

Це слід розглядати в контексті Національної кіберстратегії уряду Великобританії вартістю 2,6 мільярда фунтів стерлінгів... Ця стратегія спрямована на захист і популяризацію Великобританії в Інтернеті шляхом створення заходів безпеки для майбутніх технологій, таких як ШІ.

Пропонований добровільний кодекс практики

Як і вище, Call for Views пропонує новий Кодекс кібербезпеки штучного інтелекту відповідно до цього безпечного підходу.

Цей код базується на рекомендаціях NCSC щодо безпечної розробки систем штучного інтелекту, опублікованих у листопаді 2023 року спільно з Агентством

кібербезпеки та безпеки інфраструктури США та іншими міжнародними кіберпартнерами. Рекомендації були спільно підписані агенціями з 18 країн.

Практичний кодекс кібербезпеки штучного інтелекту спрямований на дотримання інноваційного, заснованого на принципах підходу до розробки ШІ, встановленого урядом Великобританії. У ньому викладено 12 принципів забезпечення кібербезпеки систем ШІ.

Це:

Підвищення обізнаності персоналу щодо загроз і ризиків;

Спроектуйте свою систему для безпеки, а також функціональності та продуктивності;

Моделювати загрози вашій системі;

Переконайтеся, що рішення щодо взаємодії з користувачем ґрунтуються на ризиках, пов’язаних зі штучним інтелектом;

Визначайте, відстежуйте та захищайте свої активи;

Захистіть свою інфраструктуру;

Захистіть свій ланцюг поставок;

Документуйте свої дані, моделі та підказки;

Провести відповідне тестування та оцінку;

Комунікація та процеси, пов'язані з кінцевими користувачами;

Підтримуйте регулярні оновлення безпеки для моделі та систем ШІ; і

Слідкуйте за поведінкою вашої системи.

Кожен із цих принципів по-різному застосовується до розробників, системних операторів і контролерів даних моделей ШІ. У Принципах пояснюється, як зацікавлені сторони в ланцюжку постачання штучного інтелекту можуть вжити практичних заходів для захисту своїх користувачів.

Запропоновані глобальні стандарти

У свою чергу, цей Кодекс призначений для розробки Глобального стандарту для моделей ШІ.

Кібербезпека штучного інтелекту стає все більш важливим питанням на глобальному рівні, а також аспектом, який конкретно розглядається в статті 15 Закону ЄС про штучний інтелект.

У рамках цього конкурсу DSIT наголошує на необхідності глобального підходу для забезпечення узгодженості технічних стандартів і базових вимог до кібербезпеки, а також зміцнення позиції Великобританії як світового лідера в розробці кібербезпеки для глобальних технологій.

Відповідно, DSIT підкреслив, що продовжуватиме участь у багатосторонніх ініціативах для продовження цього діалогу, таких як G7, G20, OECD та ООН.

Наступні кроки

9 серпня 2024 року закінчується конкурс на отримання думок, який передбачає надання відгуків щодо двостороннього Кодексу практики та наміру розробити глобальний стандарт. Відповідно, він вітає зворотній зв'язок від індустрії та органів стандартизації на глобальному рівні.

Зацікавленим сторонам у ланцюжку постачання штучного інтелекту пропонується надавати конкретні відгуки про втручання та рекомендувати інші варіанти політики.

Протягом 12-тижневого періоду перегляду DSIT організовуватиме семінари з галузевими організаціями та зустрічатиметься з міжнародними колегами для просування їхньої роботи. Крім того, компанія продовжить брати участь у британських і міжнародних конференціях, щоб представити свій підхід у всьому світі.

Після отримання відгуків DSIT опублікує огляд ключових тем і окреслить майбутній напрямок розвитку кібербезпеки ШІ. DSIT також почне розглядати розробку глобального стандарту, якщо це буде підтримано». ***(Victoria McCarron. Government Seeks Views on Cyber Security of AI: Call for Evidence // Burges Salmon LLP (https://blog.burges-salmon.com/post/102j8so/government-seeks-views-on-cyber-security-of-ai-call-for-evidence). 04.06.2024).***

***

«EDPS опублікував сьогодні свої рекомендації щодо генеративного штучного інтелекту та персональних даних для інституцій, органів, офісів та агенцій ЄС (EUI). Рекомендації спрямовані на те, щоб допомогти EUI виконувати зобов'язання щодо захисту даних, викладені в Регламенті (ЄС) 2018/1725, під час використання або розробки генеративних інструментів ШІ…

Щоб забезпечити їх практичне застосування EUI, у настановах наголошується на основних принципах захисту даних у поєднанні з конкретними прикладами, щоб допомогти передбачити ризики, виклики та можливості генеративних систем та інструментів ШІ.

Таким чином, керівні принципи зосереджені на ряді важливих тем, включаючи поради щодо того, як EUI можуть визначити, чи передбачає використання таких інструментів обробку даних окремих осіб; коли проводити оцінку впливу на захист даних; та інші важливі рекомендації.

EDPS видає ці вказівки в рамках своєї ролі незалежного органу із захисту даних EUI, щоб вони відповідали чинному законодавству ЄС про захист даних, зокрема Регламенту (ЄС) 2018/1725. EDPS не випустив ці вказівки в рамках своєї ролі наглядача ШІ EUI відповідно до Закону ЄС про штучний інтелект, для якого готується окрема стратегія». ***(EDPS Guidelines on generative AI: embracing opportunities, protecting people // European Data Protection Supervisor (https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-guidelines-generative-ai-embracing-opportunities-protecting-people_en?mkt_tok=MTM4LUVaTS0wNDIAAAGTfgW_WQWtCl6NE6oIcGvCGgXEtsr9s8OxbOzf_CqDcXYfozNzPDUdxTN1r6Sw9khtf520Ec27j2RwHt-6nlzgckl0rMcFlabbir8qK9ZUsg_w). 03.06.2024).***

***

«Поява генеративного штучного інтелекту та його, здавалося б, нескінченних можливостей також супроводжувалася безліччю складних загроз. І оскільки організації переходять до дедалі складніших цифрових середовищ і намагаються аналізувати експоненційне зростання даних безпеки,

рішення SIEM розвиваються, щоб використовувати потужність генеративного ШІ. Проте, враховуючи потенційні ризики, багато компаній застрягли над питанням: впроваджувати чи не впроваджувати генеративний ШІ?

Щоб відповісти на це запитання, нам потрібно розглянути кілька факторів.

ЕВОЛЮЦІЯ SIEM

Щоб візуалізувати, як могло б виглядати майбутнє з генеративним штучним інтелектом, нам потрібно здійснити швидку подорож у минуле. У відповідь на зростання мережевого трафіку SIEM вперше з'явився на сцені на початку 2000-х років. Це був перший випадок, коли спеціалісти з безпеки об'єднали інформацію та управління подіями в одній комплексній стратегії. Щоб не відставати від мінливого ландшафту, SIEM еволюціонував, щоб задовольнити потребу в інструменті для виявлення справжніх загроз у режимі реального часу. Збір і сортування тисяч сповіщень безпеки, створених іншими інструментами безпеки — брандмауерам, антивірусним програмним забезпеченням і системами виявлення вторгнень (IDS), — було революційним.

Машинне навчання (ML) уже давно використовується в інструментах безпеки, спочатку в інструментах захисту від зловмисного програмного забезпечення та в ширшому виявленні аномалій для наших мереж і користувачів. Потужне виявлення аномалій було наріжним каменем еволюції SIEM, але це також означало, що в сучасних середовищах SIEM став більше схожим на фабрику сповіщень, ніж на корисний інструмент. Ви отримуєте сповіщення: «визначено подію». Зовсім інша справа, як ви на це реагуєте. Ця відповідальність лежить на професіоналах безпеки, яких не вистачає. Тепер ми намагаємося подолати цей розрив за допомогою сучасної аналітики безпеки та генеративного ШІ.

ДЕФЕКТ НАВИЧОК: ВРАЗЛИВІСТЬ КІБЕРБЕЗПЕКИ

Дефіцит робочої сили з кібербезпеки зріс до рекордного рівня – трохи менше 4 мільйонів, незважаючи на те, що загальна кількість робочої сили з кібербезпеки у світі зросла майже на 10% за останній рік. Кількість фахівців з кібербезпеки просто не може встигати за зростаючим попитом на їхні навички.

Причини дефіциту багатошарові. Існуючі фахівці з кібербезпеки стикаються зі складнішими робочими навантаженнями, меншими командами та нижчими бюджетами в поєднанні з дедалі небезпечнішими загрозами та складнішими нормативними протоколами та протоколами відповідності. Менші бюджети також суттєво впливають на здатність команд залучати нових учасників до кібербезпеки та будувати свою організаційну структуру. Крім того, існує хибне уявлення про те, що спеціалісти-практики повинні мати технічну освіту, хоча це не завжди так. Це відлякує людей, які походять з різних і нетрадиційних джерел, але можуть стати першокласними аналітиками безпеки.

За допомогою генеративного ШІ організації можуть допомогти подолати дефіцит робочої сили, стикаючись із загрозами, що розвиваються. Завдяки поєднанню можливостей генеративної обробки даних штучного інтелекту з власними даними, які обслуговуються потужною пошуковою системою за допомогою доповненої генерації пошуку (RAG), вам більше не потрібні спеціальні знання предметної області для виконання певних критично важливих для бізнесу завдань — штучний інтелект робить це за вас.

Зрештою, генеративний розмовний пошук на основі штучного інтелекту означає, що команди безпеки можуть охопити різноманітність, яка виявилася їх сильною стороною. Завдяки доступу до технічних знань і можливостей через генеративний штучний інтелект ширше коло професіоналів раптово може взяти на себе роль у сфері кібербезпеки.

ЯК ГЕНЕРАТИВНИЙ ШІ МОЖЕ ПРАЦЮВАТИ НА ВАШУ КОМАНДУ З КІБЕРБЕЗПЕКИ

Ви не можете захистити те, чого не бачите. У сучасних розподілених середовищах обсяги даних продовжують збільшуватися. Тому відсутність видимості між потоками є найбільшою проблемою, з якою стикаються професіонали з безпеки. Хоча уніфікована платформа даних є життєво важливою для вирішення цієї проблеми, генеративний штучний інтелект у поєднанні з технологією пошуку змінює спосіб взаємодії IT, кібербезпеки та бізнес-користувачів зі своїми даними через різні канали.

Generative AI надає організаціям можливості розмовного пошуку. У контексті безпеки ця можливість може допомогти покращити видимість, аналітику та швидкість відповіді. Незалежно від того, автоматизований для фонової аналітики чи використовується як сховище знань із можливістю пошуку, генеративний ШІ, доповнений власними даними, є потужним інструментом для різноманітних випадків використання безпеки.

Ось як генеративний ШІ може працювати в кібербезпеці:

Примножувач сили: Generative AI діє як примножувач сили існуючих професіоналів з кібербезпеки, роблячи його більш доступним для молодших аналітиків за допомогою природної мови. Інші аналітики можуть легко отримати доступ до знань аналітиків за допомогою природної мови, а не коду чи математики.

Синтез даних: Generative AI може синтезувати та аналізувати величезні обсяги даних про загрози, компенсуючи обмежену кількість аналітиків загроз.

Покращена здатність виявлення: моделі можуть значно покращити виявлення аномальної поведінки в процесах, а не лише для одного користувача чи пристрою.

Прогнозний аналіз для проактивного захисту: Generative AI може краще передбачати та виявляти потенційні вразливості безпеки, пропонуючи рішення ще до того, як спеціалісти навіть дізнаються про загрози.

Автоматизоване звітування: Generative AI може надавати автоматичний зворотний зв’язок і навчання для кожного, гарантуючи, що сьогоднішні дані та ідеї можна використовувати в майбутньому.

Не можна недооцінювати силу пошуку природної мови для підвищення стійкості безпеки. Повернемося до поширеної дилеми безпеки: спрацьовує сповіщення та виявляється подія — що далі? У цьому сценарії фахівець із безпеки за допомогою генеративного штучного інтелекту може попросити помічника штучного інтелекту отримати відповідну інформацію, передові практики та рекомендовані дії для наступних кроків. Отримавши відповідь із комплексного контексту, який включає як загальнодоступні, так і приватні дані, пов’язані з проблемою, практики можуть скоротити час для відповіді та вирішення.

ПРОБЛЕМИ ВИКОРИСТАННЯ ГЕНЕРАТИВНОГО ШІ ДЛЯ КІБЕРБЕЗПЕКИ

Хоча генеративний штучний інтелект є потужним інструментом, він також має свої труднощі. Однією з проблем використання генеративного ШІ для кібербезпеки є ймовірність галюцинацій. Як практики можуть бути впевнені, що результати, створені ШІ, є фактичними та актуальними? RAG є одним із рішень. Доданий контекст може призвести до меншої кількості помилок. Однак навіть це не є ідеальним рішенням.

Вам все одно потрібна людина, щоб поставити правильні запитання. Хоча генеративний штучний інтелект обіцяє допомогти зменшити розрив у навичках і дефіцит персоналу, ви не можете видалити людей із циклу. Повністю функціонуючий процес виявлення, розслідування та реагування на загрози (TDIR) уже повинен існувати, щоб генеративний ШІ доповнював його. Штучний інтелект — це не заміна центру безпеки, а помічник — прискорювач.

МАЙБУТНЄ ГЕНЕРАТИВНОГО ШІ В КІБЕРБЕЗПЕЦІ

У звіті Elastic Global Threat Report виявлено, що з переходом підприємств на хмарне середовище зловмисники користуються перевагами неправильної конфігурації, слабкого контролю доступу, незахищених облікових даних і відсутності принципу найменших привілеїв (PoLP). Швидкість і прикриття, з якими пересуваються загрозливі особи, також зростають. З нинішньою нестачею фахівців з кібербезпеки генеративний штучний інтелект виступатиме як чаша терезів. За умови належного впровадження та використання фахівцями з кібербезпеки генеративний штучний інтелект може протистояти перевагам атак зловмисників.

Як такий, генеративний штучний інтелект, безсумнівно, формує майбутнє робочої сили з кібербезпеки та кібербезпеки, як ми її знаємо. Технологія переосмислює набори навичок і ролі в командах з кібербезпеки на майбутнє. Можливість виконувати більше технічної роботи тепер доступна для користувачів, які ще не мають цих навичок.

Отже, чи варто впроваджувати генеративний ШІ у вашій організації? З моєї точки зору, так, ви повинні розглянути це. Озброєння ваших аналітиків

інструментами для боротьби з дефіцитом навичок і захисту від безмежної загрози буде дуже важливим для захисту вашої організації, оскільки ця сфера продовжує розвиватися». ***(Mandy Andress. Generative AI for cybersecurity: Is it right for your organization? // Mansueto Ventures, LLC (https://www.fastcompany.com/91125893/generative-ai-for-cybersecurity-is-it-right-for-your-organization?utm_source=flipboard&utm_content=jscotta%2Fmagazine%2FAI%2C+ML%2C+LLM). 17.06.2024).***

***

«Штучний інтелект і хмарні обчислення можуть здатися складною комбінацією, але ці дві технології вже давно присутні в нашому повсякденному житті. Коли ми просимо Alexa встановити 15-хвилинний таймер приготування їжі, використовуємо Карти Google, щоб знайти новий маршрут навколо пробки, або нещодавно просимо ChatGPT написати нам хитру формулу Excel, ми покладаємося на безперебійну взаємодію між ШІ і хмара. Але штучний інтелект також інтегрується в хмару набагато більш просунутими та критично важливими способами, приносячи як великі переваги, так і ризики.

Прискорене відстеження даних: наша все більша залежність від ШІ та хмари

Сьогодні організації в таких галузях, як електронна комерція, банківська справа та виробництво, використовують комбінацію ШІ-хмари для автоматизації власних виробничих процесів і розшифровки конфіденційних наборів даних. Такі великі технологічні гравці, як Google, використовують його для покращення операцій за допомогою прогнозної аналітики та виявлення аномалій. Навіть охорона здоров’я стає залежною від штучного інтелекту та хмарних технологій — дослідники використовують штучний інтелект, щоб переглядати мільйони хмарних фармацевтичних паперів, щоб виявляти закономірності та розкривати новаторські біомедичні зв’язки, що може призвести до відкриттів рятівних для життя ліків.

Простіше кажучи, хмарні обчислення, керовані ШІ, каскадують у багатьох аспектах бізнесу та життя. Але в міру того, як наша залежність від нього зростає, а його доступність і потужність зростають, зростають і методи, які використовують кіберзлочинці для його використання. Технологія штучного інтелекту надає хакерам нові способи застати нас зненацька — від складних фішингових електронних листів до підроблених відео. Давайте дослідимо ці зростаючі ризики та те, як ваш бізнес може захистити себе.

ШІ підвищує рівень загроз

За оцінками, до 2025 року витрати від кіберзлочинності сягнуть приблизно 10,5 трильйонів доларів США на рік, що на 300 відсотків більше, ніж у 2015 році. Національний центр кібербезпеки вже попередив, що зловмисне використання штучного інтелекту сприятиме розповсюдженню загроз у 2024 році. У середовищі, де штучний інтелект стає все більш озброєним і забезпечує постійно розвиваються «оновлення» хакерських інструментів, не дивно, що витрати на інформаційну безпеку та управління ризиками досяг 188,1 мільярда доларів у 2023 році.

Це нове, надзвичайно складне середовище загроз здебільшого пов’язане з наддосконалими можливостями ШІ. Найбільш очевидні шкідливі тактики – це ті, які покладаються на створення тексту для атак соціальної інженерії. Але це не тільки фішинг, але й потенційна загроза швидкого розповсюдження шкідливих програм. Зловмисники можуть використовувати штучний інтелект для виявлення вразливостей у хмарі та створення зловмисного програмного забезпечення для їх використання. Він може виявляти слабкі місця та використовувати недоліки безпеки набагато швидше, ніж можуть зреагувати IT-команди. Він навіть може створювати складне шкідливе програмне забезпечення, яке вчиться уникати виявлення, що робить майже неможливим антивірусного програмного забезпечення. боротьбу з традиційним захистом

Навчання та інфраструктура повинні йти в ногу з розвитком

Враховуючи ці ризики, велика відповідальність керівників компаній у 2024 році полягає в тому, щоб забезпечити навчання співробітників тому, як розпізнавати «контрольні ознаки» атаки з підтримкою ШІ. Останні знання про

новітні тактики допоможуть запобігти непоміченому проникненню зловмисного програмного забезпечення та програм-вимагачів крізь тріщини.

Але навчання – це лише частина головоломки. Компанії також повинні забезпечити безпеку та простоту своїх хмарних операцій. Кроки включають:

1. Впровадження сильного управління контролем доступу, яке дотримується принципу найменших привілеїв. Це означає надання всім користувачам або програмам мінімального необхідного рівня доступу з багатофакторною автентифікацією, необхідною на кожному рівні.

2. Шифрування всіх даних у стані спокою та під час передачі. Це допоможе неавторизованим особам отримати доступ до конфіденційної інформації та розшифрувати її. Водночас ключі шифрування, які розшифровують дані, слід регулярно змінювати та надійно зберігати.

3. Регулярна оцінка вразливостей. Такі інструменти, як тестування на проникнення, дозволять компаніям моделювати атаки в реальному світі, які допомагають висвітлити слабкі місця в їхній хмарній інфраструктурі, які потім можна усунути.

4. Прийняття хмарної стратегії. Компанії, які працюють у хмарі, повинні переконатися, що вони використовують лише методи безпеки та технології, які спеціально розроблені для хмарних середовищ, допомагаючи усунути будь-які застарілі прогалини та створити безпеку в додатках із самого початку.

Боротьба ШІ з ШІ

Однак лише зміцнення хмарної інфраструктури вже недостатньо для захисту її даних. Оскільки кіберзлочинці нарощують використання штучного інтелекту в різних напрямках атак, підприємства повинні робити те саме. Використовуючи штучний інтелект для виявлення загроз і виявлення «нестандартної» поведінки та моделей, компанії можуть бути на крок попереду злочинців, краще захищаючи свій периметр безпеки.

AI може особливо допомогти захистити дані в гібридних хмарних середовищах. Він може виявляти тіньові дані та шукати аномалії доступу до даних, миттєво сповіщаючи IT-групи про потенційні загрози. Штучний інтелект може

аналізувати та перевіряти спроби входу за допомогою даних про поведінку, надаючи доступ користувачам, які поводяться нормально, і позначаючи або навіть блокуючи тих, хто діє ненормально або підозріло.

AI може навіть виконувати аналіз загроз у реальному часі та аналіз ризиків після дії. Тоді IT-лідери можуть налаштувати автоматичне реагування на інциденти, що пришвидшить запобігання атакам і розслідування для водонепроникної кібербезпеки. Крім того, штучний інтелект також відіграє певну роль в автоматизації багатьох стандартних і трудомістких процесів безпеки, знижуючи ризик людської помилки та підвищуючи ефективність персоналу.

Розблокування повної впевненості у вашій хмарі

Нещодавно Сполучене Королівство та США підписали знакову угоду про спільну роботу над тестуванням передового ШІ та оцінкою його загроз. Це перша двостороння угода такого роду, яка підкреслює, наскільки серйозно дві найпотужніші країни світу сприймають цю нову технологію. Тому підприємства теж повинні.

Оскільки компанії виділяють більше ресурсів у хмару, ми всі повинні використовувати найпередовіші доступні технології для її захисту. Безпека на основі штучного інтелекту — це найшвидший, найбільш адаптивний і найінтелектуальніший інструмент, який у нас під рукою. І щоб бути впевненим, що у вашому арсеналі є правильні щити штучного інтелекту, варто співпрацювати з експертом із корпоративного програмного забезпечення та постачальником хмарних порад. Таким чином ви отримаєте доступ до вбудованого чи додаткового захисту AI, який захищатиме ваш бізнес протягом наступної великої технологічної революції». ***(Ravi Bindra. Navigating the cloud risks in the growing AI threat landscape // Future US, Inc. (https://www.techradar.com/pro/navigating-the-cloud-risks-in-the-growing-ai-threat-landscape?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 17.06.2024).***

***

«Check Point Software, провідний постачальник хмарних платформ кібербезпеки на основі штучного інтелекту, опублікував звіт, у якому підтверджується, що понад 97% команд безпеки зараз використовують інструменти на основі штучного інтелекту (ШІ) як частину своєї стратегії кіберзахисту.

Дослідження, проведене у співпраці з британською дослідницькою компанією Vanson Bourne, вказує на те, що інструменти штучного інтелекту розгортаються різними способами, включаючи підвищення рівня реагування на інциденти, покращення захисту від шкідливого програмного забезпечення та зменшення випадків втрати даних.

Лес Вільямсон, керуючий директор ANZ у Check Point Software Technologies, підкреслив важливість ШІ в сучасних стратегіях кібербезпеки. «Штучний інтелект дозволяє командам безпеки набагато швидше реагувати на загрози та нейтралізувати зловмисників до того, як вони зможуть завдати шкоди чи збою», — сказав Вільямсон.

Дослідження виявило, що значна кількість організацій використовують передові інструменти Generative AI (GenAI), щоб зменшити ручну роботу та мінімізувати хибно-позитивні позначки. В Азіатсько-Тихоокеанському регіоні майже кожна друга організація вважає, що GenAI може оптимізувати операції безпеки та оптимізувати розподіл ресурсів. Ця частка є найвищою в трьох глобальних регіонах, охоплених дослідженням: Північній Америці, Європі та Азіатсько-Тихоокеанському регіоні.

Учасники опитування визначили кілька ключових переваг інструментів GenAI. Понад 50% вказали на головну перевагу краще розуміння поведінки користувачів і аномалій. Інші переваги включали підвищену точність подій безпеки (понад 45%), швидший аналіз подій безпеки (понад 42%) і покращене виявлення та запобігання загрозам (понад 35%).

«Дослідження показує, що інструменти GenAI вже дають значні переваги як групам безпеки, так і їхнім користувачам», — сказав Вільямсон. «Завдяки

продовженню швидкого розвитку цих інструментів переваги з часом лише збільшуватимуться».

Незважаючи на переваги, опитування також виявило постійну прогалину в навичках у командах безпеки: 89% організацій повідомили про брак кваліфікованого персоналу. Конкуренція за таланти залишається гострою, і 98% респондентів підтвердили, що нестача навичок впливає на ефективність їхніх операцій безпеки, причому 40% описують цей вплив як сильний.

Вільямсон визнав проблеми, пов’язані з нестачею навичок, особливо тому, що кіберзлочинці також використовують інструменти ШІ для посилення своїх атак. «Прогалина в навичках серйозно перешкоджає тому, наскільки ефективно організації можуть зібрати правильний захист від штучного інтелекту та загальної кіберзлочинності», — сказав він. Він додав, що багато організацій все частіше звертаються до інструментів GenAI, щоб подолати цю прогалину шляхом автоматизації виснажливих, трудомістких завдань, що дозволяє членам команди зосередитися на діяльності, що додає більше вартості.

Незважаючи на багатообіцяючу роль GenAI у кібербезпеці, респонденти опитування вказали на проблеми, пов’язані з підтримкою моделей штучного інтелекту в актуальному стані та відповідністю нормам щодо даних. «GenAI допоможе трансформувати організації, оскільки постачальники послуг кібербезпеки інтегрують у свої пропозиції більше інтелектуальних засобів», — підсумував Вільямсон. «Використання можливостей GenAI прокладе шлях до більш безпечного та стійкого цифрового майбутнього». ***(Sean Mitchell. 97% of cyber security teams using AI tools, says report // TechDay (https://securitybrief.co.nz/story/97-of-cyber-security-teams-using-ai-tools-says-report). 11.06.2024).***

***

«Кібербезпека завжди була головним пріоритетом для бізнесу, але для багатьох малих і середніх підприємств (МСП) вартість і складність впровадження надійних заходів безпеки можуть бути величезними. Увійдіть у

штучний інтелект – кардинальний крок у сфері кібербезпеки. Штучний інтелект змінює спосіб розробки та розгортання рішень безпеки, роблячи їх більш доступними та доступними для організацій будь-якого розміру. Ці технологічні інновації рухають прогрес.

Одним із ключових аспектів технологічних інновацій є їх визнання та відзначення. Нагорода Global Recognition Awards відзначила ці інновації своїми технологічними нагородами, відзначаючи їх глибокий вплив на безпеку, ефективність і продуктивність. На чолі з генеральним директором Джетро Спарксом цього року конкурс Global Recognition Awards отримав заявки з понад 50 країн, що свідчить про зростання їхнього впливу та престижу. «Наша місія — демократизувати доступ до престижних нагород», — заявляє Спаркс. «Прогресивні технології усунули географічні бар'єри та спростили процес номінації, дозволивши нам визнавати найкращих і найяскравіших».

Розуміння ШІ в кібербезпеці

Традиційні заходи кібербезпеки ґрунтувалися на ручному моніторингу, системах виявлення на основі сигнатур і реактивних підходах. Ці методи вимагали багато часу та не відставали від кібератак, що розвивалися. Поява штучного інтелекту запровадила проактивні та адаптивні рішення безпеки, які можуть передбачати та зменшувати ризики в реальному часі.

ШІ в кібербезпеці включає алгоритми машинного навчання, поведінкову аналітику та прогнозну аналітику. Ці технології виявляють аномалії, визначають закономірності та передбачають загрози ще до їх виникнення. Рішення безпеки на основі штучного інтелекту пропонують швидше виявлення загроз, підвищену точність і здатність обробляти величезні обсяги даних, що вкрай важливо для компаній, які прагнуть захистити свої цифрові активи економічно ефективно.

Економічні рішення безпеки

Однією з найважливіших переваг штучного інтелекту в кібербезпеці є його потенціал щодо зниження витрат. Традиційні заходи безпеки часто вимагають значних інвестицій у кваліфікований персонал, програмне та апаратне

забезпечення. ШІ може автоматизувати більшість процесів, зменшуючи потребу у великих групах безпеки та дорогій інфраструктурі.

Численні компанії повідомили про значну економію коштів після впровадження рішень безпеки на основі ШІ. Наприклад, телекомунікаційна компанія зі списку Fortune 500 використовувала Snorkel Flow для класифікації зашифрованих мережевих потоків даних, подолавши такі проблеми, як повільне, шумне та дороге ручне маркування даних. Цей підхід, керований штучним інтелектом, досяг вищої точності та підвищення ефективності роботи завдяки автоматизації маркування даних і адаптації до динамічних умов мережі.

Масштабованість безпеки, керованої ШІ

Багато інструментів безпеки на основі штучного інтелекту доступні як хмарні служби, що робить їх доступнішими та доступнішими для компаній будь-якого розміру. Ці інструменти можна збільшувати або зменшувати залежно від конкретних потреб бізнесу, гарантуючи, що навіть невеликі підприємства зможуть скористатися передовими засобами безпеки.

Такі компанії, як CrowdStrike і Darktrace, пропонують масштабовані платформи безпеки на основі штучного інтелекту, які можна налаштувати відповідно до потреб бізнесу. Ці платформи забезпечують комплексне покриття безпеки, від захисту кінцевих точок до моніторингу мережі.

Покращене виявлення загроз і реагування

Штучний інтелект у сфері кібербезпеки дуже ефективний у виявленні та усуненні загроз, коли вони виникають у реальному часі. Звичайні методи безпеки зазвичай залежать від виявлення на основі сигнатур, яке обмежується розпізнаванням уже ідентифікованих загроз. Штучний інтелект використовує поведінковий аналіз і машинне навчання для виявлення незвичайних моделей і потенційних загроз, навіть тих, яких раніше не було.

Системи, керовані штучним інтелектом, можуть автоматично реагувати на загрози, мінімізуючи час між виявленням і пом’якшенням. Це швидке реагування є життєво важливим для запобігання витоку даних і мінімізації збитків. Такі інструменти, як QRadar від IBM і Cortex XDR від Palo Alto Networks,

використовують штучний інтелект, щоб забезпечити розширені можливості виявлення загроз і реагування, аналізуючи величезні обсяги даних у режимі реального часу для нейтралізації загроз.

Автоматизація та ефективність

ШІ може автоматизувати багато звичайних завдань безпеки, звільняючи команди з кібербезпеки зосередитися на складніших питаннях. Така автоматизація підвищує ефективність і зменшує ймовірність людської помилки, що є суттєвим фактором порушень безпеки. Завдяки автоматизації таких завдань, як моніторинг і реагування на інциденти, ШІ дозволяє групам безпеки працювати ефективніше, що призводить до економії коштів і покращення результатів безпеки.

Capital One впровадив систему безпеки на основі штучного інтелекту, яка значно підвищила ефективність роботи. Їхні моделі ML допомогли скоротити час вирішення проблем із мобільними додатками до 50%.

Персоналізовані рішення безпеки

AI пропонує можливість створювати персоналізовані рішення безпеки, адаптовані до конкретних потреб бізнесу. Ця настройка є особливо корисною для малих і середніх підприємств, які часто мають унікальні вимоги до безпеки. ШІ може аналізувати бізнес-операції та виявляти потенційні ризики безпеці, дозволяючи розробляти індивідуальні заходи безпеки. Цей підхід гарантує, що підприємства отримають необхідний захист, не платячи за непотрібні функції.

Як великі, так і малі компанії успішно впровадили рішення безпеки на основі ШІ, адаптовані до їхніх конкретних потреб. Наприклад, Best Buy реалізувала систему кібербезпеки NVIDIA на основі штучного інтелекту, щоб підвищити точність виявлення фішингу до 96% і зменшити помилкові спрацьовування.

Аналітика безпеки на основі ШІ

Аналітика безпеки є критично важливим компонентом сучасних стратегій кібербезпеки. AI покращує аналітику безпеки, надаючи глибше розуміння потенційних загроз і вразливостей. Інструменти на основі штучного інтелекту, такі як Splunk і LogRhythm, аналізують дані безпеки та надають корисну інформацію, визначаючи закономірності та тенденції, які традиційні методи можуть пропустити.

Виклики та обмеження

Хоча ШІ пропонує багато переваг, він не позбавлений і проблем. Потенційні підводні камені включають ризик надмірної залежності від штучного інтелекту, потребу в постійних оновленнях і ймовірність того, що системи штучного інтелекту стануть мішенню для кіберзлочинців. Щоб пом'якшити ці ризики, компанії повинні поєднувати ШІ з традиційними заходами безпеки. Регулярні оновлення та моніторинг є важливими для забезпечення ефективності рішень безпеки на основі ШІ.

У міру розвитку кіберзагроз системи ШІ повинні адаптуватися. Компанії повинні бути в курсі останніх розробок у сфері штучного інтелекту та кібербезпеки, щоб забезпечити ефективність своїх систем.

Штучний інтелект демократизує кібербезпеку, роблячи передові рішення безпеки більш доступними та доступними для компаній будь-якого розміру. Штучний інтелект пропонує численні переваги, які допомагають компаніям захистити свої цифрові активи: від зниження витрат до покращення виявлення загроз і реагування на них. Незважаючи на те, що проблеми залишаються, майбутнє штучного інтелекту в кібербезпеці виглядає багатообіцяючим, і очікується, що постійний прогрес покращить заходи безпеки». ***(David Balaban. How AI Is Making Cybersecurity Solutions More Accessible // Forbes (https://www.forbes.com/sites/davidbalaban/2024/06/27/how-ai-is-making-cybersecurity-solutions-more-accessible/). 27.06.2024).***

***

«Гонконзький наглядовий орган з інформаційної безпеки використовує штучний інтелект (ШІ) для посилення своїх можливостей виявлення загроз, оскільки зафіксував 31-відсоткове збільшення інцидентів кібербезпеки в першій половині року.

Координаційний центр команди реагування на комп'ютерні надзвичайні ситуації Гонконгу (HKCERT) у вівторок заявив, що з травня він тестує мовні

моделі штучного інтелекту, щоб допомогти виявити фішингові веб-сайти та покращити свої системи оповіщення про ризики.

HKCERT обробив 5161 інцидент кібербезпеки в першій половині 2024 року, що на 31 відсоток більше порівняно з 3950 у другій половині минулого року, повідомила група, що фінансується урядом.

Причиною зростання стало зростання кількості інцидентів фішингу на 59%, під час яких організація виявила рекордні 18 000 шкідливих URL-адрес.

Алекс Чан Чун-ман, генеральний менеджер відділу цифрової трансформації HKCERT, сказав, що зросла кількість хакерів, які використовують передові інструменти, включаючи створені штучним інтелектом глибокі фейки та шкідливі програми, які важче виявити.

«Ми бачимо, як хакери стають більш просунутими та витонченими», — сказав Чан.

Починаючи з травня, сторожовий орган заявив, що використовує велику мовну модель штучного інтелекту для перегляду доменних імен веб-сайтів, щоб виявити потенційні фішингові сайти, про які потім можна повідомити або видалити.

Лише в травні інструмент штучного інтелекту зміг проаналізувати понад 3,7 мільйона веб-сайтів, збільшивши можливості сторожової обробки більш ніж у тисячу разів.

Інструмент успішно виявив фішингові веб-сайти, які імітують популярний японський сайт електронної комерції Rakuten і соціальні медіа-платформи, такі як WhatsApp і Facebook.

Крім того, штучний інтелект також використовувався для покращення системи оповіщення про кібербезпеку HKCERT.

Інструмент штучного інтелекту аналізуватиме дані про загрози, зібрані HKCERT, на предмет тенденцій фішингу, зловмисного програмного забезпечення та атак ботнетів, характерних для Гонконгу.

Потім він може генерувати сповіщення безпеки для веб-сайту сторожової організації після оцінки персоналом.

Чан сказав, що це підвищило ефективність аналізу розвідувальних даних на 80 відсотків.

«Для аналізу загроз вам потрібно проаналізувати багато даних», — сказав Чан. «Якщо ми використовуємо штучний інтелект… ми можемо видавати більш точні сповіщення для [мешканців] Гонконгу».

Оголошення було зроблено лише через день після того, як поліція оголосила, що отримала понад 18 000 повідомлень про кібер-атаки в першому кварталі цього року.

Ряд резонансних витоків даних на початку цього року, в яких були задіяні як приватні компанії, так і державні департаменти, поновили заклики до міста посилити зусилля з кібербезпеки.

Раніше цього місяця стало відомо, що 41 житель втратив 12 мільйонів гонконгських доларів (1,54 мільйона доларів США) через шахрайство зловмисного програмного забезпечення, запущене підозрюваним синдикатом із Малайзії.

Менш ніж за тиждень на початку травня було виявлено, що особисті дані понад 130 000 людей були виточені в результаті окремих порушень, які стосувалися Департаменту протипожежної служби, Реєстру компаній і Департаменту електричних і механічних послуг.

Послідовні витоки даних спонукали Офіс головного інформаційного директора уряду – вищий урядовий підрозділ інформаційних технологій – попросити всі бюро та департаменти переглянути свою комп’ютерну безпеку.

Ювелірна мережа Luk Fook Holdings і Гонконгський технологічний коледж також стали жертвами кібератак пізніше того ж місяця.

IT-експерти звернулися до уряду з проханням розробити політику централізації захисту кібербезпеки для всіх департаментів і асоційованих організацій, намагаючись зменшити ризик нових порушень.

Виконавчий директор Джон Лі Ка-Чіу оголосив у своїй програмній промові на 2023 рік, що цього року уряд запровадить нове законодавство для посилення захисту кібербезпеки критичної інфраструктури». ***(Connor Mycroft. Hong Kong cybersecurity watchdog turns to AI tools as incidents rise 31% in 6 months // South***

China Morning Post Publishers Ltd. (https://www.scmp.com/news/hong-kong/law-and-crime/article/3268016/hong-kong-cybersecurity-watchdog-turns-ai-tools-incidents-rise-31-6-months). 25.06.2024).

***

«Офіційні особи випустили попередження для всіх користувачів iPhone і Android після зростання експлойтів «нульового кліку».

На відміну від звичайних форм зловмисного програмного забезпечення, атаки з нульовим кліком є досить складними й не вимагають від жертв натискання підозрілих посилань.

Натомість кіберзлочинці можуть зламати систему вашого телефону та встановити шкідливе програмне забезпечення, просто використовуючи недоліки в системі.

Вони можуть зробити це, використовуючи лазівки для перевірки даних і часто користуючись додатками для обміну повідомленнями або голосовими викликами, відповідно до компанії з кібербезпеки Kaspersky.

Використовуючи ці програми, зловмисники можуть впроваджувати код через файли зображень, запити автентифікації, вкладення електронної пошти та навіть маніпулювати відкритими URL-адресами.

У зв’язку зі стрімкою популярністю смартфонів і різноманітних у соціальних мережах додатків користувачів iPhone та Android попереджають бути уважними.

Оскільки ці атаки зростають, Агентство національної безпеки (АНБ) детально розробило спосіб, за допомогою якого потенційні жертви можуть запобігти спробам нульового кліку, і методи, які вони можуть використовувати для захисту своїх даних.

Нещодавно АНБ оприлюднило цю інформацію в рамках всеосяжного звіту під назвою «Найкращі практики мобільних пристроїв».

«Загрози для мобільних пристроїв стають все більш поширеними, масштаби та складність зростають», — пише агентство.

«Користувачі мобільних пристроїв хочуть повною мірою скористатися функціями, доступними на цих пристроях, але багато функцій забезпечують зручність і можливості, але жертвують безпекою».

Двосторінковий документ консультує користувачів техніки щодо різних заходів безпеки, включаючи спосіб перезавантаження.

NSA заявляє, що вимкніть і знову ввімкніть свій мобільний пристрій, щоб запобігти доступу хакерів до вашої конфіденційної інформації.

Повне перезавантаження телефону призведе до закриття всіх програм, виходу з облікових записів у соціальних мережах, а відкриті URL-адреси неможливо використовувати.

Крім того, ця проста тактика також пом’якшить будь-які загрозливі фішингові атаки.

У цьому типі експлойту хакери намагаються викрасти інформацію, наприклад облікові дані для входу, за допомогою методів соціальної інженерії.

За даними CrowdStrike, у цих спробах злочинці часто спонукають жертв натискати на шкідливі посилання та завантажувати вкладення.

Крім поради користувачам Apple і Android щотижня перезавантажувати свої пристрої, АНБ детально розробило ще кілька методів запобігання шахрайству без натискання.

Агентство радить вимикати Bluetooth, коли ви ним не користуєтеся, і уникати підключення до загальнодоступних мереж Wi-Fi.

Користувачі мобільних телефонів також повинні використовувати надійний шестизначний PIN-код і розглянути можливість використання біометричних даних, таких як автентифікація обличчя або розблокування відбитків пальців.

Користувачам також рекомендується відмовитися від громадських USB-зарядних станцій і вимкнути служби визначення місцезнаходження, коли вони не використовуються.

У документі NSA також зазначено, що користувачі повинні часто оновлювати свої пристрої за допомогою новітніх технологій, оскільки хакерам легше маневрувати зі старим програмним забезпеченням.

Хоча ця нова порада не є на 100 відсотків ефективною, агентство заявило, що вона повинна створювати перешкоди для різноманітних зловмисних дій.

Крім того, Федеральна комісія зі зв'язку (FCC) раніше застерігала користувачів мобільних телефонів від демонтажу налаштувань безпеки.

«Зміни заводських налаштувань вашого телефону, джейлбрейк або рутування вашого телефону підривають вбудовані функції безпеки, які пропонують ваші бездротові служби та смартфон, і водночас роблять його більш вразливим до атак», — написали вони». ***(Ella Scott. Urgent warning to all iPhone and Android users after millions of devices targeted by secret cyberattack // LADbible Group (https://www.uniladtech.com/apple/iphone/iphone-android-user-warning-zero-click-hack-prevention-270035-20240604?utm_source=flipboard&utm_content=UNILADTech%2Fmagazine%2FUNILAD+Tech). 05.06.2024).***

***

«Австралійська компанія з видобутку рідкоземельних елементів Northern Minerals заявила, що кіберзлочинці викрали конфіденційні корпоративні секрети з її систем незабаром після того, як уряд змусив кількох китайських інвесторів продати свої частки в компанії.

Гірничодобувний гігант, який володіє багатим корисними копалинами проектом Browns Range у Західній Австралії, повідомив у повідомленні на фондовій біржі у вівторок, що він дізнався про інцидент із кібербезпекою наприкінці березня та звернувся до Австралійського центру кібербезпеки, Офісу комісара з інформації Австралії. і зовнішніх консультантів з кібербезпеки для розслідування інциденту.

«Вилучені дані включали корпоративну, операційну та фінансову інформацію, а також деякі деталі, що стосуються нинішнього та колишнього

персоналу, а також деяку інформацію про акціонерів. Процес сповіщення відповідних постраждалих осіб триває та триває», — заявили в Northern Minerals. Компанія заявила, що інцидент не мав суттєвого впливу на її роботу чи системи в цілому.

«Деякі з викрадених даних тепер опубліковано в дарк-мережі», – додала компанія.

Компанія Northern Minerals розкопує проект Browns Range на північному краю пустелі Танамі, яка багата на диспрозій і тербій – рідкісні мінерали, необхідні для виробництва високоефективних магнітів для електромобілів, вітряних турбін і оборонних установок. Зараз Китай володіє та видобуває 99% світових запасів диспрозію.

Оголошення гірничодобувного гіганта надійшло через день після того, як казначей Австралії Джим Чалмерс наказав п’ятьом інвесторам, пов’язаним з Китаєм, відмовитися від своїх акцій компанії. Інвестори - Yuxiao Fund Pte Ltd, Black Stone Resources Limited, Indian Ocean International Shipping and Service Company Limited, Сімей Лю і Сі Ван - наразі володіють 613 мільйонами акцій, що становить 10,4% випущеного капіталу Northern Minerals.

Представник Міністерства фінансів заявив, що це рішення захищає національні інтереси країни та забезпечує дотримання її рамок іноземних інвестицій. «Австралія має надійну та недискримінаційну систему іноземних інвестицій і, якщо буде потрібно, вживатиме подальших заходів для захисту наших національних інтересів у цьому питанні», — додав речник.

Група програм-вимагачів BianLian у вівторок зазначила Northern Minerals як жертву на своєму темному веб-порталі. Група стверджує, що викрала корпоративну інформацію на суму 1,65 гігабайт із систем компанії, включаючи оперативні дані, стратегічні дані та дані про геологічні та гірничі дослідження.

Група стверджувала, що викрадені дані також включали фінансову інформацію Northern Minerals, дані про дослідження конкурентів, акціонерів і потенційних інвесторів, корпоративні архіви електронної пошти та особисті дані співробітників.

За даними Агентства з кібербезпеки та безпеки інфраструктури США, група програм-вимагачів BianLian з червня 2022 року націлилася на сектори критичної інфраструктури США та Австралії, і її основною метою є вимагання грошей.

Група використовує скомпрометовані протоколи віддаленого робочого столу, щоб отримати початковий доступ, а потім використовує інструменти з відкритим кодом і сценарії командного рядка для виявлення та збору облікових даних і викрадає дані жертви за допомогою протоколу передачі файлів - Rclone або Mega.

CISA повідомила, що група спочатку застосовувала подвійне вимагання, шифруючи системи жертв після викрадання їхніх даних, але нещодавно перейшла на здирництво на основі викрадання, яке залишає системи жертв недоторканими. Нещодавня зміна тактики групи узгоджується із заявою Northern Minerals про те, що інцидент не вплинув на її ширші системи чи операції.

Хоча CISA не включала BianLian до списку національних державних акторів, компанія з кібербезпеки Resecurity у грудні виявила «значний зв'язок» між BianLian та двома іншими групами програм-вимагачів, які відстежуються як White Rabbit і Mario. Відстежуючи спільну операцію трьох груп проти компаній фінансових послуг у Сінгапурі, дослідники відстежили більшість їхніх IP-адрес у Китаї». ***(Jayant Chakravarti. Australian Mining Giant Confirms BianLian Ransomware Attack // Information Security Media Group, Corp. (https://www.databreachtoday.com/australian-mining-giant-confirms-bianlian-ransomware-attack-a-25414?utm_source=flipboard&utm_content=other). 05.06.2024).***

***

«Актор дарк-мережі повідомив про злам малайзійської Railway Assets Corporation (RAC). Метою злому даних RAC стала ключова структура Міністерства транспорту Малайзії. Зловмисник «billy100» здійснив це порушення та опублікував свої звинувачення на платформі BreachForums.

Порушення даних RAC, яке було оприлюднено на темному веб-форумі, стосується кадрових записів, які нібито були розкриті та пов'язані з Railway Assets Corporation (RAC).

За даними billy100, у скомпрометованій базі даних є 481 рядок документів. Як доказ, зловмисник надав зразки файлів CSV «users_id» і «detail», які включали хешовані паролі, адреси електронної пошти та імена користувачів.

Порушення даних RAC нібито розкриває конфіденційну інформацію

Корпорація залізничних активів (RAC), заснована відповідно до Закону про залізниці 1991 року, є федеральною статутною організацією, завданням якої є підтримка залізничної інфраструктури Малайзії. З моменту свого заснування в 1992 році RAC відіграє важливу роль у виведенні залізничної галузі країни на рівень інших провідних країн. Оскільки корпорація відповідає за управління та зростання залізничних активів, це дуже важливо.

Конфіденційні дані співробітників нібито приховані в базі даних RAC, яка виявила порушення даних. Однією з розкритих деталей є інформація про декілька аспектів кадрового діловодства. Викрадені дані складаються з двох основних файлів: users_id.csv, який містить важливу інформацію користувача, як-от ідентифікатори, імена, електронні адреси, паролі тощо, і detail.csv, який містить додаткову докладну інформацію про співробітника, наприклад особисті ідентифікатори, відомості про відділ, зарплату та дати народження.

Розслідування та кібератаки на залізничному секторі

Запити про втрату даних RAC і потенційну причетність банди програм-вимагачів надіслали організації The Cyber Express. Однак на момент написання цієї статті офіційної відповіді чи заяви не було зроблено, тому звинувачення щодо витоку даних RAC залишаються необґрунтованими.

Залізниці, будучи важливою інфраструктурою в епоху цифрових технологій, стають дедалі вразливішими до кіберзагроз, які ставлять під загрозу як їх щоденну роботу, так і громадську безпеку. Атаки на міжнародні залізничні мережі останнім часом привернули увагу до необхідності посилення захисту кібербезпеки. Уразливості, викликані застарілими системами, незахищеними мережами та пристроями Інтернету речей, підвищують ризики.

Залізничні оператори повинні надати пріоритет видимості активів, запровадити надійну автентифікацію, шифрувати мережі зв’язку та зберігати запас

актуальних виправлень і оновлень для посилення безпеки. забезпечити, щоб співробітники проходили комплексне навчання з кібербезпеки Важливо також. Щоб і в майбутньому транспорт був надійним і безпечним, кібербезпека повинна бути повністю інтегрована в роботу залізниці». ***(Ashish Khaitan. Malaysia's Railway Assets Corporation (RAC) Faces Alleged Data Breach // The Cyber Express (https://thecyberexpress.com/malaysias-rac-data-breach/?utm_source=flipboard&utm_content=TheCyberExpress%2Fmagazine%2FThe+Cyber+Express+by+Cyble). 06.06.2024).***

***

«Витоки даних викликають усе більше занепокоєння в сучасному цифровому середовищі, впливаючи на організації будь-якого розміру та в різних галузях. Що стосується програм-вимагачів і порушень безпеки, жодна організація не звільнена від загрози. Насправді, згідно зі звітом PT Security у 2022 році, найчастіше жертвами кібератак є державні установи (22% від загальної кількості атак на організації), промислові компанії (9%), IT-компанії (8%) та фінансові установи (7%).

У глобальному масштабі Азіатсько-Тихоокеанський регіон виділявся як основна ціль, на яку припало 31% кібератак у всьому світі. Нещодавні зломи, як-от інцидент з одним із трьох провідних брокерів В'єтнаму, відновлення якого зайняло сім днів і вплинуло на мільйони клієнтів, або злам даних понад 34 мільйонів власників індонезійських паспортів хакером, відомим як Бьорка, — підкреслюють критичну важливість надійної кібербезпеки для захисту цілісності даних і захисту конфіденційності користувачів.

У відповідь на такі загрози я настійно рекомендую організаціям дотримуватись NIST Cybersecurity Framework, у якій описано п'ять основних функцій (ідентифікація, захист, виявлення, реагування та відновлення), щоб підвищити свою стійкість проти нових загроз.

• Ідентифікація: ця функція передбачає визначення потенційних ризиків кібербезпеки, а також розуміння того, що потребує захисту, коли йдеться про

системи, активи та дані. Дотримуючись цієї функції, організації можуть краще зрозуміти стан своєї кібербезпеки, уразливості та потенційні ризики, тим самим підвищуючи загальну безпеку.

• Захист: функція захисту передбачає впровадження заходів безпеки для захисту конфіденційних активів і даних. За допомогою такої функції, як Protect, організації можуть завчасно оцінити та впровадити заходи безпеки для захисту своїх критично важливих активів і даних, зменшуючи ймовірність успішних кібератак.

• Виявлення: ця функція зосереджена на розробці та впровадженні можливостей для виявлення несанкціонованого доступу або підозрілих дій у реальному часі. Завдяки активному моніторингу мереж і систем на наявність підозрілих дій або аномалій організації можуть своєчасно виявляти потенційні загрози та реагувати на них, мінімізуючи вплив порушень безпеки.

• Реагувати: функція реагування передбачає розробку планів і вжиття відповідних заходів для відновлення після інцидентів кібербезпеки. Це гарантує, що організації мають заздалегідь визначені стратегії реагування та процедури для пом’якшення впливу порушень безпеки та швидкого відновлення роботи.

• Відновлення: функція відновлення зосереджена на відновленні постраждалих систем і даних після інциденту кібербезпеки. Він підкреслює важливість стійкості та навчання на основі інцидентів кібербезпеки. Шляхом оперативного відновлення після порушень безпеки та аналізу даних після інцидентів організації можуть виявити слабкі місця в інфраструктурі та процесах безпеки, що дозволить їм посилити захист і краще підготуватися до майбутніх загроз.

Крім того, для подальшої обробки кіберінцидентів і ефективного відновлення роботи після атаки компаніям необхідно розробити ретельні та ефективні плани аварійного відновлення (DRP) і плани безперервності бізнесу (BCP).

Ці плани побудовані на основі процесів комплексного аналізу впливу на бізнес (BIA), які визначають важливість кожної бізнес-діяльності, оцінюють вплив збоїв на кожному етапі та визначають часові вимоги для відновлення роботи.

Результати BIA служать вхідними даними для розробки DRP, визначення пріоритетів інфраструктурних ресурсів, необхідних технологій, персоналу для моніторингу, резервування та встановлення пріоритетів, а також встановлення процедур аварійного відновлення для заміни основних систем, які постраждали від інцидентів.

Згідно з аналізом BIA, окрім DRP, який відіграє основну роль через те, що більшість бізнес-операцій сьогодні значною мірою залежить від технологічного середовища, компаніям також необхідно розробити BCP як комплексний план відновлення критично важливих бізнес-операцій. Цей план включає організацію робочої сили, місць, інструментів, процедур і технологій. Мета полягає в тому, щоб якомога швидше відновити основні послуги до комплексних за будь-якого сценарію інциденту.

Нарешті, виходячи з досліджень Стенфордського університету, може бути несподіванкою те, що приголомшливі 88% кібератак пов’язані з людською помилкою або поведінкою. Ця статистика підкреслює важливість людського фактора у визначенні ефективності заходів кібербезпеки. Щоб створити міцну основу в основі вашої комплексної системи безпеки, я раджу організаціям дотримуватися цих чотирьох ініціатив:

1. Зобов’язання керівництва: забезпечте підтримку на найвищому рівні та прихильність ініціативам у сфері кібербезпеки, зокрема розподіл ресурсів і визначення пріоритетів у сфері кібербезпеки.

2. Навчання співробітників. Проводьте регулярні тренінги з кібербезпеки та програми підвищення обізнаності для співробітників на всіх рівнях, щоб покращити їхнє розуміння ризиків безпеки та найкращих практик.

3. Встановлення чітких політик і процедур: розробка та впровадження політик і процедур кібербезпеки гарантує, що працівники розуміють свої обов’язки та наслідки невиконання. Це включає вказівки щодо обробки даних, контролю доступу та звітування про інциденти.

4. Сприяння культурі пильності: заохочуйте співробітників залишатися пильними та негайно повідомляти про будь-які підозрілі дії чи інциденти безпеки.

Створення каналів для звітування та надання стимулів для активної участі може допомогти виявити та пом'якшити потенційні загрози на ранніх стадіях». ***(Hung Cuong LE. Strengthening Cybersecurity Resilience For Organizations In The Asia-Pacific Region: A Comprehensive Approach // Forbes (https://www.forbes.com/sites/forbestechcouncil/2024/06/04/strengthening-cybersecurity-resilience-for-organizations-in-the-asia-pacific-region-a-comprehensive-approach/?utm_source=flipboard&utm_content=forbes%2Fmagazine%2FInnovation&sh=77cb18fc6e30). 04.06.2024).***

***

«Фінансово мотивований хакер стверджує, що викрав понад 34 гігабайти даних, що належать сінгапурській телекомунікаційній компанії Absolute Telecom PTE Ltd.

Information Security Media Group не змогла відразу перевірити законність даних. Зразок даних, схоже, включає внутрішні дані, такі як дані для входу, паролі та інформація про підписників.

Хакер під назвою GhostR стверджує, що має доступ до даних компанії, включаючи корпоративні дані, бухгалтерію, продажі, клієнтів, повну інформацію про кредитну картку та записи дзвінків.

Absolute Telecom, зареєстрована в Сінгапурі, надає підприємствам послуги голосового дзвінка, включаючи SIP-транкінг, рішення Enterprise PBX, Ribbon Enterprise Products і Telco grade IVR. Компанія не відразу відповіла на запит про коментар.

На кримінальному форумі під назвою BreachForums було сказано про витоки даних. GhostR минулого тижня ймовірно викрав дані в австралійської логістичної компанії Victorian Freight Specialists.

BreachForums, англомовний кримінальний форум, нещодавно став мішенню для захоплення ФБР. Однак адміністраторам сайту вдалося відновити роботу конфіскованого домену після того, як реєстратор із Гонконгу відновив їхній

обліковий запис, що дозволило їм відновити контроль перед переходом до іншого реєстратора.

Відтоді на сайті зберігаються дані про резонансні зломи, включно з TicketMaster та іспанським транснаціональним банком Santander.

GhostR нещодавно став відомим, погрожуючи оприлюднити записи, викрадені з World-Check, бази даних, яку банки та установи використовують для боротьби з фінансовими злочинами та застосування санкцій.

Актор загрози опублікував електронну таблицю з іменами членів королівської родини по всьому світу, показуючи точну інформацію.

GhostR також опублікував електронні таблиці зі списком ідентифікованих терористів, які також, здається, стосуються реальних людей. Жодна з електронних таблиць не містить контактної інформації чи інших конфіденційних даних, крім дати народження». ***(Prajeet Nair. Hackers Claim They Breached Telecom Firm in Singapore // Information Security Media Group, Corp. (https://www.databreachtoday.com/hackers-claim-they-breached-telecom-firm-in-singapore-a-25461?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology). 09.06.2024).***

***

«У зв'язку зі зростанням кількості випадків кіберзалякування в соціальних мережах та на інших онлайн-платформах генеральний директор Управління з кібербезпеки Гани д-р Альберт Антві-Боасяко повідомив, що Управління з кібербезпеки розробляє структуру, яка боротиметься з поведінкою студентів в Інтернеті та відстежуватиме її. захистити їх від загроз кібербезпеці.

У зверненні, виголошеному від його імені на семінарі з питань кібербезпеки, організованому деканом у справах студентів Технічного університету Такораді (TTU) у співпраці з Комітетом у справах студентів, д-р Антві-Боасяко сказав, що це

стало необхідним через нещодавно зареєстровані випадки, отже, структура є це стало можливим завдяки прийнятим законам про кібербезпеку та захист даних.

«Шляхом поєднання положень Закону про кібербезпеку 2020 року (Закон 1038) і Закону про захист даних 2012 року (Закон 843) 2020 року Управління кібербезпеки розробляє всеохоплюючу структуру для вирішення проблем поведінки та наслідків роботи студентів в Інтернеті діяльності. Ця структура охоплюватиме інформаційні кампанії, освітні програми та рекомендації щодо відповідальної поведінки в Інтернеті», – запевнив він.

Тому д-р Антві-Босіако заохочував студентів TTU та інших старших шкіл, які брали участь у семінарі з кібербезпеки, створювати хорошу онлайн-репутацію, яка відображає їхні цінності.

«Усе, що ви публікуєте, публікуєте або використовуєте в Інтернеті, залишає слід, до якого можуть отримати доступ працівники приймальної комісії університету, маркетингові компанії, рекрутери, посольства тощо. Цей цифровий слід може мати далекосяжні негативні чи позитивні наслідки, які можуть вплинути на особисте та професійне життя студента, як-от пропозиції стипендій або спричинення виключення з університету через поведінку в Інтернеті. Студенти також можуть зіткнутися з негайними наслідками, такими як кіберзалякування, переслідування в Інтернеті, онлайн-шахрайство, сексуальне здирство, шантаж або репутаційна шкода», – закликав він.

Директор із забезпечення якості та навчального планування TTU, інженер. Професор Ебенезер Боак’є, який представляв віце-канцлера TTU на заході, порадив студентам, особливо студентам з комп’ютерних наук та інформаційних технологій, ознайомитися з Законом про кібербезпеку та його наслідками для їхньої майбутньої кар’єри.

«Як студенти цього престижного навчального закладу, ви є майбутніми лідерами та новаторами в галузі технологій. Ви повинні розуміти наслідки цього Закону та важливість кібербезпеки в нашому повсякденному житті. Незалежно від того, чи вивчаєте ви інформатику, інформаційні технології чи будь-яку іншу

суміжну галузь, ви, безсумнівно, зіткнетеся з проблемами, пов'язаними з кібербезпекою, у своїй майбутній кар'єрі», – підбадьорив він.

Він зазначив, що TTU має сувору політику щодо кіберзлочинів і порушень у соціальних мережах, і видав суворе попередження про серйозні наслідки для студентів, визнаних винними в таких порушеннях.

«Університет займає рішучу позицію проти будь-якої форми неправомірної поведінки, особливо коли йдеться про зловживання технологіями та платформами соціальних мереж. Будь-який студент, якого визнають винним у таких порушеннях, зазнає суворих дисциплінарних стягнень, зокрема виключення з університету... Подумайте, перш ніж публікувати публікацію, і пам'ятайте, що ваші дії в Інтернеті можуть мати реальні наслідки. Давайте всі прагнути створити позитивну та безпечну онлайн-спільноту для нашого університету», – попередив він.

Декан зі студентських справ TTU, професор Брюс Амарті-молодший, обґрунтовуючи захід, вказав на збільшення випадків кіберзалякування, сексуального здирства та поширення відвертого контенту, які ставлять під загрозу безпеку та благополуччя студентів і загрожують Репутація навчального закладу змусила деканат підвищити обізнаність щодо правильного використання технологій.

«Ми прагнемо дати можливість нашим студентам приймати обґрунтовані рішення, захищати їхню конфіденційність і дотримуватися етичних стандартів під час взаємодії в Інтернеті. Ми віримо, що, підвищуючи обізнаність і сприяючи відповідальному використанню технологій, ми можемо створити безпечнішу та більш шанобливу онлайн-спільноту для всіх», – сказав він.

Доктор ACP Френсіс Ціді, який є заступником регіонального начальника поліції Заходу, у вичерпній презентації згадав деякі основні ознаки того, що є кіберзлочинністю.

ін зазначив, що люди, яких викриють у таких діях, як хакерство, кіберпереслідування та вимагання дітей, можуть зіткнутися із серйозними санкціями, такими як штрафи до 5000 Gh¢ або отримати 5-10 років ув'язнення.

Він порадив учасникам піклуватися про безпеку та повідомляти про випадки агресивних дій.

«Кожен має знати про особисту безпеку. Якщо ваша фотографія циркулює в повітрі, ви повинні звинувачувати себе, принаймні у вас є закон, який вас захищає. Тож, якщо ви зіткнулися з цим, повідомте нам. Нам потрібна велика сенсибілізація", - порадив він.

Управління у справах студентів Технічного університету Такораді обіцяє регулярно організовувати семінари з кібербезпеки для вирішення нових кіберзагроз для студентів». ***(Akwasi Agyei Annim. Cybersecurity Authority to monitor students' online behavior // CitiNewsroom.com (https://citinewsroom.com/2024/06/cybersecurity-authority-to-monitor-students-online-behaviour/). 09.06.2024).***

***

«У неділю польський спортивний канал TVP Sport зазнав кібератаки з IP-адрес у Польщі, що на деякий час перервало трансляцію матчу Польща-Нідерланди, перш ніж послуги були відновлені.

У неділю польський спортивний канал TVP Sport зазнав кібератаки. Про це повідомляє PAP, передає УНН.

Деталі

Як повідомляє TVP Info у соціальних мережах, неділю о 15:00 польське телебачення стало жертвою хакерської атаки під час трансляції матчу.

Через атаку вболівальники не змогли побачити початок трансляції матчу Польща-Нідерланди в Інтернеті.

За інформацією, атаку здійснили з IP-адрес у Польщі.

IT-служби швидко відновили роботу.

Відтак, на початку другої половини матчу доступ до сайту було відновлено.

Крім того, директор TVP Sport Якуб Квятковський на сайті X вибачився перед вболівальниками за незручності». ***(Юлія Котвицька. Польський спортивний телеканал TVP Sport зазнав кібератаки // Інформаційне агентство***

«Українські Національні Новини» (https://unn.ua/news/polskyi-sportyvnyi-telekanal-tvp-sport-zaznav-kiberataky). 17.06.2024).

***

«Наприкінці травня 2024 року Федеральне бюро розслідувань США здійснило арешт у справі, яку воно описало щодо чогось «вирваного зі сценарію».

Операція знищила ботнет, який заразив мільйони комп'ютерів шкідливим програмним забезпеченням у майже 200 країнах. Продаж доступу до цієї мережі сприяв злочинам, зокрема фінансовим шахрайствам на мільярди доларів, крадіжці особистих даних, погрозам вибуху та доступу до матеріалів щодо експлуатації дітей по всьому світу.

Передбачуваний оператор використовував виручені кошти для купівлі швидкісних автомобілів, розкішних годинників і нерухомості в багатьох країнах.

Сервіс, відомий як «911 S5», вважається найбільшим у світі прикладом ботнету. І це відбувається, оскільки частка веб-трафіку, спричиненого шкідливими ботами, зростає з року в рік.

Що таке ботнет?

Ботнети створюються, коли кіберзлочинці використовують шкідливі віруси, які називаються троянами, щоб порушити безпеку комп'ютерів користувачів і навіть підключених пристроїв Інтернету речей (IoT).

Це зловмисне програмне забезпечення може бути приховано у зараженому вкладенні електронної пошти або за посиланням, яке користувача обманом змусили відкрити. У випадку з 911 S5 домашні IP-адреси були скомпрометовані, коли користувачі завантажували піратське програмне забезпечення або програми віртуальної приватної мережі, які потім завантажували шкідливі програми на їхні пристрої.

Потім злочинці беруть під контроль заражені машини та організовують їх у мережу ботів, також відому як «армія зомбі», якою вони можуть дистанційно керувати. Власники зазвичай не знають про те, що відбувається.

Майже половина всього глобального трафіку пов’язана з діяльністю ботів, причому третина загального трафіку пов’язана зі зловмисною програмою, згідно зі щорічним звітом Bad Bot Report від компанії з кібербезпеки Imperva.

Для чого використовуються ботнети?

Ботнети можуть використовуватися хакерами та організованими злочинцями для здійснення незаконної діяльності в Інтернеті. Наприклад, запуск атак на відмову в обслуговуванні – спроба перевантажити веб-сайт або мережу, щоб погіршити їх продуктивність або зробити його недоступним – або надсилання фішингової атаки з метою викрадення облікових даних для крадіжки особистих даних.

За допомогою 911 S5 злочинці купували доступ до служби, а потім використовували захоплені комп’ютери, щоб приховати свою особу під час скоєння злочину.

За даними ФБР, це нібито включало орієнтування на програми допомоги пандемії та подання сотень тисяч шахрайських заяв на страхування від безробіття. Шахрайство призвело до шахрайських збитків на суму понад 5,9 мільярда доларів.

Інші тенденції кіберзлочинності

Кіберзлочинність зростає. За прогнозами, у найближчі п’ять років глобальні збитки від кіберзлочинності становитимуть майже 14 трильйонів доларів.

У останньому звіті Всесвітнього економічного форуму про глобальні ризики кібербезпека входить до п’яти найбільших ризиків, з якими зараз стикається світ.

За даними Microsoft, одними з найпопулярніших кіберзагроз є спроби викрадення паролів, програми-вимагачі – тип шкідливого програмного забезпечення, яке блокує доступ до файлів або пристроїв, доки не буде сплачено викуп, а також спроби фішингу, зокрема компрометація бізнес-електронної пошти, коли шахрай намагається обдурити керівника чи розпорядника бюджету з метою переказу коштів або розкриття конфіденційної інформації.

У звіті Форуму про глобальні ризики говориться, що нові інструменти та можливості, такі як генеративний штучний інтелект, зроблять кіберзлочинність менш ризикованою та дешевою, а також відкриють нові ринки для злочинців.

Наприклад, фішингові атаки тепер можна легко перекладати на мови меншин за допомогою ШІ.

Протягом наступних років, як ідеться у звіті, більш складні засоби кіберзахисту перемістять цілі до менш безпечної інфраструктури та систем і людей, які мають меншу цифрову грамотність.

Що робиться з кіберзлочинністю?

«Чого вони не показують у фільмах, — сказав речник Бюро промисловості та безпеки Міністерства торгівлі США щодо справи 911 S5, — так це копіткої роботи внутрішніх і міжнародних правоохоронних органів, тісно співпрацюючи з промисловістю. партнерів, щоб зруйнувати таку нахабну схему».

Тим не менш, світ зіткнувся з великим розривом у кібернавичках, у всьому світі бракує майже 4 мільйонів кіберпрофесіоналів. Проблеми, зокрема відсутність чітких кар'єрних шляхів, застаріле навчання та дорогі сертифікати, є одними з перешкод, які заважають людям продовжувати професійну кар'єру в сфері кібербезпеки.

Всесвітнього економічного форуму Центр кібербезпеки працює над стимулюванням державно-приватних дій для пошуку рішень для таких проблем. Шлях вперед, як йдеться в останній Глобальній перспективі кібербезпеки, «вимагає стратегічного мислення, узгоджених дій і непохитної відданості кіберстійкості». ***(David Elliott. FBI takes down army of 'zombie' computers. Here what to know // World Economic Forum (https://www.weforum.org/agenda/2024/06/botnet-cybercrime-zombie-computers/?utm_source=flipboard&utm_content=mhartley2012%2Fmagazine%2FCYBER%3A+Privacy%2C+Crime%2C+%26+Security). 19.06.2024).***

***

«Кібератаки, здається, нищівніші, ніж будь-коли, і компаніям-мішеням потрібно ще більше часу для їх усунення.

Остання атака, яка привернула широку увагу, продовжує цю тенденцію: триваючий кіберінцидент у CDK Global, чиє програмне забезпечення автосалони

використовують для керування всім, від планування до записів, руйнує дилерські центри вже кілька днів, і кінця не видно.

У травні кібератака на Ascension, некомерційну мережу в Сент-Луїсі, яка включає 140 лікарень у 19 штатах, змусила систему перенаправити машини швидкої допомоги з кількох лікарень. На повне вирішення проблеми знадобився майже місяць.

А в лютому атака програми-вимагача на Change Healthcare, дочірню компанію гіганта охорони здоров'я UnitedHealth Group, спричинила збої в виставленні рахунків в аптеках по всьому США та загрожувала вивести з ладу деяких постачальників медичних послуг.

Експерти кажуть, що хакери стають все більш досвідченими і можуть довше ховатися в системах організації непоміченими. Ці хакери атакують компанії в стилі ланцюжка поставок, знищуючи цілі галузі, щоб отримати більше грошей. А певні галузі, які часто використовують застарілі системи, як-от охорона здоров'я, стають ще легшими мішенями.

«Ми навіть не можемо порівняти те, що відбувалося десять років тому, з тим, що відбувається сьогодні», — сказав CNN Дрор Лівер, співзасновник компанії з кібербезпеки Coro. «(Хакери) беруть участь у грі, щоб отримати набагато більші прибутки, ніж вони були раніше».

Чому хаки набагато руйнівніші

За словами Лівера, хакери не тільки більш досвідчені, але й більш терплячі.

Хакери на деякий час ховаються в структурі організації та пересуваються через цю структуру, впливаючи на численні частини системи. Вони чекають, доки настане відповідний час для нападу. І чим довше хакери чекають, тим більша шкода.

«Коли (хакери) вмикають і виконують атаку, це справді завдає шкоди організації, яка потім приносить їм більше доходу», — сказав Лівер.

Експерти, з якими спілкувався CNN, сказали, що важко відразу отримати конкретні подробиці окремих кібератак. По-перше, компанії хочуть захистити репутацію свого бренду від потенційних судових розглядів. Крім того, організації

можуть не захотіти розкривати конкретні деталі атаки до завершення розслідування, кажуть експерти, у випадку, якщо є якісь імітатори.

Ерік Нунан, генеральний директор постачальника кібербезпеки CyberSheath, сказав, що атаки програм-вимагачів зазвичай проникають через такі шляхи, як фішинговий електронний лист. Ці порушення можуть залишатися непоміченими протягом кількох днів або навіть тижнів, оскільки хакер рухається вбік.

Фактичне розгортання програм-вимагачів часто відбувається швидко та широко, сказав Нунан. Більшість жертв дізнаються, що їх зламали, коли вони втрачають доступ до важливих файлів або отримують цифрові повідомлення про викуп.

«Програмне забезпечення-вимагач — це цифровий еквівалент самовільного захоплення будинку. Початковий вхід залишається непоміченим, дозволяючи сквотерам зайняти та контролювати власність, і до того моменту, як власники будинків помічають, що є проблема, процес відновлення контролю та власності є руйнівним і дорогим», – сказав Нунан.

У той час як у минулому компанії використовували менше взаємопов’язаних систем, перехід до хмари та використання сторонніх систем — незважаючи на те, що вони допомагають у щоденних бізнес-операціях — створюють складні системи, які більш сприйнятливі до масових хакерів.

«Це також створює щось на зразок яблучка і допомагає зловмисникам зосередити свої зусилля на конкретних типах інфраструктури або конкретних хмарних платформах», — сказав Нунан.

А хакери націлені на організації, які обслуговують ланцюг постачання галузей. Наприклад, атакуючи програмне забезпечення CDK, хакери змогли зупинити галузь дилерів автомобілів. Великі мережі лікарень Change і Ascension не змогли забезпечити належну допомогу своїм численним відділенням. Це дає хакерам можливість вимагати все більші суми грошей, сказав Джон Дваєр, директор з досліджень безпеки в Binary Defense, фірмі з рішень для кібербезпеки.

Незважаючи на те, що хакери мають більше важелів впливу, успіх у сплаті викупу та швидкому одужанні є невловимими, вважають експерти.

«Ніколи не було написано про компанію, яка успішно заплатила викуп, а потім швидко відновила свої системи», — сказав Нунан.

Охорона здоров'я – легка мішень

Нунан сказав, що проблема не в тому, що хакери обов'язково стають все більш просунутими, а в тому, що багатьом організаціям бракує сучасних, актуальних систем. Більшість організацій не проводять вправ з реагування на інциденти, тому відновлення після масових хакерів займає більше часу.

«Більшість нашої критично важливої інфраструктури значно відстає в тому, щоб бути готовими до розпізнавання кіберзагроз, коли вони з'являються, але, що важливіше, відновлюватися від них», — сказав Нунан.

У звіті ФБР було встановлено, що зловмисники зловмисників найбільше націлювалися на охорону здоров'я та сектор громадського здоров'я, за якими йдуть важливі виробництва та державні установи.

Оскільки системи стають все більш взаємопов'язаними, бізнес може зробити дуже багато, щоб підтримувати свою кібербезпеку, особливо якщо покладатися на сторонні системи, як це роблять автосалони з CDK.

«Автосалони не займаються кібербезпекою, тому вони насправді не справляються із завданням захисту такого типу системи. Це залежить від постачальника», – сказав Кліфф Штайнхауер, директор із інформаційної безпеки та залучення National Cybersecurity Alliance.

Штайнхауер також сказав, що це постійна гра в «кішки-мишки».

«Щоразу, коли ми щось виправляємо, хакер все ще може це зламати. І вони мають бути праві лише один раз, ми маємо бути праві кожного разу», – сказав Штайнгауер.

Напади на лікарні зросли. Медсестра, яка працює в лікарні Ascension Providence Rochester Hospital поблизу Детройта, штат Мічиган, раніше повідомила CNN, що атака програм-вимагачів на мережі «ставить під загрозу життя пацієнтів», оскільки медичні працівники змушені вдаватися до паперових карток із завантаженням пацієнтів, яких потрібно прийняти. дбати про.

Інші кажуть, що охорона здоров'я піддається мішенню через застарілі технології цієї галузі, – сказав у релізі Стівен МакКеон, засновник і генеральний директор програмних компаній MacguyverTech і MacNerd. Ця технологія допомагає пацієнтам вимагати поповнення ліків за рецептом, переглядати результати аналізів і записуватися на прийом, але також є більш сприйнятливою до хакерів.

CNN звернувся до Ascension and Change за коментарем.

Як запобігти тривалим зупинкам

Дваєр сказав, що компанії можуть краще працювати, використовуючи досвід сторонніх розробників, оскільки багато команд внутрішньої безпеки досить малі. Найкращі приклади використовують внутрішню команду, яка є експертом із внутрішніх систем організації, і наймають сторонніх постачальників кібербезпеки для збільшення їх розміру.

За словами Лівера, організації також можуть запроваджувати системи, які можуть контролювати безпеку всього їхнього бізнесу.

Інші кажуть, що для публічних компаній повинні бути обов'язкові мінімальні вимоги до кібербезпеки. За словами Нунана, ці мінімальні стандарти слід розглядати як ремені безпеки та подушки безпеки — вони не запобіжать нещасним випадкам, але краще підготують компанії.

«Є багато компаній, що займаються програмним забезпеченням, виробників критично важливих деталей або частин ланцюга постачання, про які американці ніколи не чули, — про ці компанії, програми та програмне забезпечення або частини, які вони виробляють, поки вони не стають доступними. Є багато інших CDK, — сказав Нунан». ***(Ramishah Maruf. The auto dealers outage has been hamstringing car dealerships for days. Experts say that's the new normal for cyberattacks // yahoo! finance (https://finance.yahoo.com/news/auto-dealers-outage-hamstringing-car-100043354.html?fr=sycsrp_catchall). 27.06.2024).***

***

«Лише минулого тижня Управління морської промисловості (Marina) підтвердило кібератаку, яка скомпрометувала чотири його веб-системи, які обробляють реєстрацію суден і документи моряків.

Крім того, цього місяця значний витік даних у Maxicare Philippines, пов'язаний з хакером «OPCODE-90», розкрив конфіденційну інформацію понад 1000 великих компаній, включаючи ABS-CBN і Accenture. Це було зроблено шляхом націлювання на Lab@Home, стороннього постачальника запитів на лабораторні дослідження.

У травні хакери зламали дві системи Національної поліції Філіппін, які зберігають конфіденційні дані про ліцензії на вогнепальну зброю. Це порушення викликало занепокоєння щодо безпеки даних правоохоронних органів. У відповідь на ймовірний витік даних PNP призупинив усі онлайн-сервіси на невизначений термін для оцінки та розслідування інциденту, зберігаючи при цьому оперативні послуги в регіональних офісах і Camp Crame.

Це найновіші випадки, але сталося ще незліченну кількість, незалежно від того, чи було про них повідомлено, чи вони розглянуті. Кіберзлочинці використовують уразливості в цифровому середовищі Філіппін для фінансового шахрайства, атак програм-вимагачів і витоку даних, націлюючись як на окремих осіб, так і на організації.

Таким чином, неправильно думати про кібербезпеку лише тоді, коли є такі повідомлення про порушення в якійсь комп'ютерній системі.

Прагнення Філіппін до цифрової трансформації для підтримки економічного зростання та інклюзії заслуговує похвали. Технології пропонують численні можливості для прогресу, якщо ми їх добре використовуємо та використовуємо стратегічно.

Ось чому адміністрація Маркоса-молодшого інвестує в способи збільшення інвестицій у комунікаційну інфраструктуру, а також працює над підвищенням кваліфікації людей, щоб дозволити більшій кількості філіппінців повноцінно брати участь у цифровій економіці. Крім того, технології ближче інтегрують нас до решти світової економіки.

Але є зворотний бік технології, яка може завдати великої шкоди тим, хто її використовує, від споживачів до державних установ і критично важливої інфраструктури, яка живить суспільства. І саме тому цифрова безпека має розглядатися як така ж важлива, як і цифрова трансформація.

Кібербезпека є проблемою, яка стосується як національної, так і економічної безпеки, особливо тому, що вона може виходити за кордон і впливати на людей, де б вони не були.

Філіппіни, враховуючи своє унікальне положення в Індо-Тихоокеанському регіоні та вирішальне становище в геополітиці, опиняються в центрі різноманітних зовнішніх загроз кібербезпеці, головним чином спричинених державними акторами та кіберзлочинцями. Ці спонсоровані державою загрози, особливо з боку таких країн, як Китай із розвиненими кібер-можливостями, несуть значні ризики, включаючи шпигунство, крадіжку інтелектуальної власності та порушення критичної інфраструктури.

У той же час люди повинні усвідомлювати, що вони є об’єктами впливу суб’єктів впливу, і повинні мати можливість відрізнити доброякісну діяльність від злоякісної. Кожен користувач повинен знати та розуміти ризики, які це становить для нього самого, суспільства та країни.

Як тоді уряд має діяти у забезпеченні кібербезпеки, навіть якщо ми просуваємося до того, щоб стати більш цифровою нацією та економікою?

Усвідомлюючи необхідність вирішення цих нових викликів безпеці в кіберсфері, прес-секретар Збройних сил Філіппін (AFP) Франсел Таборлупа нещодавно заявив, що їхній департамент адаптується, щоб йти в ногу з мінливими загрозами. Ці зусилля охоплюють широкий спектр операційних областей, причому кібер тепер інтегровано як четверту область поряд із землею, повітрям і морем.

Критична інфраструктура, включаючи порти, енергетику та телекомунікації, потребує надійних заходів кібербезпеки. Без надійної позиції кібербезпеки цифрові технології можуть наражати націю на руйнівні кібератаки на її економічну та національну оборону.

Основи політики національної безпеки на 2023-2028 рр. підкреслюють кіберінформаційну та когнітивну безпеку як життєво важливі компоненти національної безпеки, спрямовані на загальну кіберстійкість. Нещодавно підписаний Національний план кібербезпеки окреслює кілька ключових ініціатив і програм, спрямованих на посилення стану кібербезпеки країни, зокрема проти зовнішніх загроз. Одним із основних компонентів є створення Національного оперативного центру кібербезпеки, який слугуватиме централізованим центром моніторингу, виявлення та реагування на кіберзагрози. Цей центр має на меті покращити здатність країни справлятися з кіберінцидентами в режимі реального часу.

План також підкреслює важливість державно-приватного партнерства, заохочуючи співпрацю між урядовими установами та суб'єктами приватного сектору для розробки єдиної системи кібербезпеки. Це включає ініціативи, які сприяють обміну інформацією та спільним зусиллям у боротьбі з кіберзагрозами. План також зосереджується на розбудові потенціалу та підвищенні кваліфікації, пропонуючи стипендії та навчальні програми для вирішення проблеми нестачі кваліфікованих фахівців з кібербезпеки.

Неможливо переоцінити центральну роль участі приватного сектора в кібербезпеці. Приватний сектор повинен інвестувати в передові технології кібербезпеки, впроваджувати суворі протоколи безпеки та показувати приклад у найкращих практиках захисту своїх даних і мереж. Вони повинні брати участь у державно-приватних партнерствах, обмінюватися розвідувальною інформацією про загрози та проводити спільні навчання з державними установами для розробки надійних планів реагування на інциденти.

Дійсно, багатогранний і багатогалузевий підхід є ключовим. Необхідно посилити міжнародне співробітництво для захисту Філіппін від цих зовнішніх кіберзагроз. Ефективна відповідь включає вдосконалення політики кібербезпеки, інвестиції в передові технології безпеки та сприяння співпраці з глобальними партнерами для обміну інформацією про загрози та передовим досвідом.

Кібербезпека є предметом спільної турботи та спільної відповідальності як приватного, так і державного секторів, а також внутрішніх і міжнародних гравців, оскільки вона має потенціал вплинути на регіональну стабільність, безпеку та процвітання — загалом на наш спосіб життя, який ми знаємо це». ***(Victor Andres C. Manhit. Cybersecurity entails cooperation at every level // BusinessWorld Publishing (https://www.bworldonline.com/opinion/2024/06/26/604005/cybersecurity-entails-cooperation-at-every-level/). 26.06.2024).***

***

«Нові загрози зловмисного програмного забезпечення зростають швидше, ніж будь-коли, і під загрозою знаходяться всі види бізнесу, стверджується в новому звіті BlackBerry.

Виходячи з початкової телеметрії компанії за перший квартал 2024 року, кількість атак, заснованих на нових варіантах шкідливого програмного забезпечення, зросла на 40% за хвилину. Іншими словами, в середньому 7500 унікальних варіантів зловмисного програмного забезпечення націлювалися на клієнтів BlackBerry щодня (5,2 на хвилину).

Комерційні підприємства також стають дедалі мішенню. Більше третини (36%) усіх загроз були спрямовані на комерційні підприємства (роздрібна торгівля, виробництво, автомобільна промисловість і професійні послуги), що на 3% більше, ніж у попередньому звітному періоді. Тим не менш, було сказано, що в цьому секторі спостерігався 10% стрибок випадків нового шкідливого програмного забезпечення, оскільки суб'єкти загрози ставали все більш досконалими.

Високомотивовані хакери

Незважаючи на те, що викрадення реєстраційної інформації за допомогою соціальної інженерії та використання доступу для розгортання зловмисного програмного забезпечення, безумовно, є популярним методом серед злочинців, вони також все частіше використовують уразливості програмного забезпечення. За словами BlackBerry, це особливо вірно для інфокрадиків і операторів програм-вимагачів.

Нарешті, діяльність правоохоронних органів, хоч і заслуговує похвали, навряд чи залишає пляму на загальному ландшафті кібербезпеки. LockBit, Hunters International і 8Base продовжують активно сіяти хаос у галузях, незважаючи на всі зусилля поліції, щоб утримати ці загрози.

Ісмаель Валенсуела, віце-президент із дослідження загроз і розвідки BlackBerry, сказав, що зловмисники мають «високу мотивацію» або вкрасти гроші у своїх жертв, або просто спостерігати, як горить світ. «У рік, коли понад 50 країн проводять вибори, геополітична напруженість досягає найвищого рівня, і кожна нація незабаром буде зосереджена на Олімпійських іграх, ландшафт загроз може здатися приголомшливим для навігації».

Іншими словами, цього року ми можемо очікувати ще більше дезінформації та кампаній із глибокого фейку. Вторгнення Росії в Україну, війна Ізраїлю та ХАМАС та вибори залишаться ключовими елементами хакерських кампаній у майбутньому». ***(Sead Fadilpašić. New malware threats are rising faster than ever — and all kinds of businesses are at risk // Future US, Inc. (https://www.techradar.com/pro/security/new-malware-threats-are-rising-faster-than-ever-and-all-kinds-of-businesses-are-at-risk). 27.06.2024).***

***

«Унаслідок кількох кібератак, яких Японське космічне агентство (JAXA) зазнало з минулого року, міг статися витік даних.

Як передає Укрінформ, про це повідомляє Kyodo News із посиланням на заяву уряду Японії.

Генеральний секретар Кабінету міністрів Японії Йошімаса Хаяші заявив на пресконференції, що JAXA разом зі спеціалізованими організаціями розслідує кібератаки, щоб визначити їх вплив.

У агентстві запевнили, що мережа, до якої отримали доступ зловмисники, не містила «чутливої інформації», пов’язаної з роботою ракет, супутників та національною безпекою.

Міністр науки Моріяма Масахіто також твердить, що «немає великого занепокоєння» у зв'язку із кібератаками.

За даними джерел Kyodo News, кібератаки, ймовірно, були скоєні пов'язаними з Китаєм хакерами. Вони могли переглянути велику кількість файлів, у тому числі інформацію про зовнішні компанії та організації, які мають угоди про нерозголошення із JAXA, додали джерела.

Також повідомляється, що сервер, який хакери атакували у червні 2023 року, містив персональні дані співробітників космічного агентства, і вони могли бути використані для отримання доступу до секретних документів. Зловмисники, вочевидь, скористалися вразливістю у віртуальній приватній мережі, через яку можна підключитися до внутрішньої системи агентства.

За словами джерела, цьогоріч JAXA зазнало кількох кібератак. Агентство також було об'єктом кібернападів у 2016-му та 2017 роках. Як вважається, їх учинили пов'язані з Китаєм хакери з метою крадіжки даних». ***(Японське космічне агентство з минулого року зазнало кількох кібератак // Укрінформ (https://www.ukrinform.ua/rubric-ato/3877547-aponske-kosmicne-agentstvo-z-minulogo-roku-zaznalo-kilkoh-kiberatak.html). 22.06.2024).***

***

Діяльність хакерів та хакерські угруповування

«Аналітики зі сфери кібербезпеки спостерігають зростання кількості хакерських атак. Збитки від їхніх дій можуть перевершити торішні показники, оскільки тільки за травень 2024 року зловмисники викрали $575 млн. Про це пише incrypted з посиланням на дані PeckShield.

Хакери мають усі шанси «поліпшити» свої результати, вважають експерти. Збитки за I квартал 2024 року зросли на 42% порівняно з аналогічним періодом минулого року. При цьому травневі показники підскочили на 666% при зіставленні з квітнем.

На думку CEO платформи криптографічного ризику та аналітики Merkle Science Мріганки Паттнаіка, кіберзлочинці адаптуються під нові реалії. Вони змінюють методи злому та обирають як цілі найбільш вразливі компанії та гаманці користувачів.

Експерт підкреслив, що все частіше хакери відмовляються від пошуку вразливостей у смартконтрактах. Замість цього вони зосередили увагу на фішингових атаках і викраденні приватних ключів. Такий метод простіший у плані реалізації, а також вимагає менш тривалої підготовки, вважає Паттнаїк.

«Хоча вразливості смартконтрактів залишаються проблемою, хакери дедалі частіше націлюються на царини за їхніми межами, на кшталт витоку приватних ключів. Ці методи призвели до значних втрат», — заявив CEO Merkle Science.

За даними платформи, мережеві зловмисники тривалий період часу дистанціюються від злому смартконтрактів. Збитки від цього типу атак ще у 2023 році скоротилися на 92% порівняно з 2022 роком. З позначки в $2,6 млрд показник знизився до рівня в $179 млн.

В останні місяці ця тенденція посилюється, а головною проблемою став саме витік приватних ключів, заявили в Merkle Science.

Підвищена активність хакерів також пов’язана з «бичачими настроями» на ринку цифрових активів, зазначають аналітики. Збільшення вартості криптовалют і різних альткоїнів призвело до зростання потенційної вигоди в разі успішної атаки, вважають експерти». ***(У травні хакери вкрали $575 млн і збільшили збитки від кібератак на 666% — аналітики // ТОВ "МінфінМедіа" (https://minfin.com.ua/ua/2024/06/10/128700063/). 10.06.2024).***

***

Вірусне та інше шкідливе програмне забезпечення

«Ось ще одна несподівана новина про ізраїльського розробника шкідливого програмного забезпечення NSO Group та його привілейованих клієнтів. Дослідники Citizen Lab виявили ще більше телефонів, заражених

флагманським шкідливим програмним забезпеченням Pegasus від NSO. І знову під загрозою опинилися журналісти, критики, дисиденти та лідери опозиції.

Останнє розслідування виявило ще сім російськомовних і білоруськомовних членів громадянського суспільства та журналістів, які проживають за межами Білорусі та Росії, які стали мішенню та/або були інфіковані шпигунським програмним забезпеченням Pegasus. Багато з них публічно критикували російський уряд, зокрема, вторгнення Росії в Україну. Ці особи, більшість з яких наразі живуть у вигнанні, зіткнулися з інтенсивними погрозами з боку російських та/або білоруських служб державної безпеки.

Незважаючи на те, що компанія перебуває на межі банкрутства, програмне забезпечення, яке вона продала різним авторитарним лідерам і автократам, все ще існує. І воно все ще може бути використане для переслідування людей, які не подобаються цим жадібним до влади урядам.

Який може бути сенс заражати телефони дисидентів, журналістів і критиків зловмисним програмним забезпеченням, яке розглядається як засіб проти жорстоких злочинів і міжнародного тероризму? Підприємства, яким NSO продав, неодноразово давали зрозуміти, що вони витрачатимуть мільйони на програмне забезпечення лише з метою участі в дрібних операціях помсти. Це тому, що уряди, які контролюють це шпигунське програмне забезпечення, надто тонкошкірі, щоб мати справу зі звичайними недоліками роботи в державному бізнесі: критикою, незгодою та підйомом лідерів опозиції, які відстоюють усе, за що не відстоюють ці уряди.

Хоча помста може бути дрібною, результати далеко не тривіальні. Перетворення телефону на активний пристрій відстеження, який також дозволяє урядам підслуховувати розмови та перехоплювати комунікації, означає, що набагато легше знайти людей, яких ви хочете змусити замовкнути. Як зазначає Citizen Lab, помста проти критиків Путіна та його східноєвропейських друзів є суворою, починаючи від заборони на в’їзд до арештів. І завжди існує ймовірність

того, що оперативники просто спробують убити критиків — те, що російські оперативники робили неодноразово.

Хоча ця новина не дивує, вона допомагає зберегти ім’я NSO у новинах. Чим довше це триває, тим менше шансів, що він зможе знову залишитися поза увагою та продовжувати працювати як завжди.

Він також надає ще один набір спростувань численним захистам NSO своїх продуктів, тактики продажу та вибору клієнтів. Коли вперше стався витік цілей зловмисного програмного забезпечення NSO, компанія заявила, що список фальшивий. І навіть якщо це був список цілей, він був лише списком потенційних цілей, а не показом того, як клієнти розгортали його продукти.

Цей список був повний журналістів, критиків, дисидентів, лідерів опозиції, релігійних лідерів, захисників прав людини та юристів, залучених до судових процесів проти урядів. Група NSO стверджувала, що цей список нічого не означає. Це був лише список, і його не можна було прив’язувати до NSO, її клієнтів чи людей, на яких цільовими є її клієнти.

Буквально все, що було виявлено після того витоку, показало протилежне: клієнти NSO прямо чи опосередковано (просячи інші уряди виконати їх брудну роботу) націлені саме на тих людей, які містяться в цьому списку. Зловмисне програмне забезпечення NSO стверджує, що це потужний інструмент, який дозволяє урядам відслідковувати небезпечних злочинців і міжнародних терористів, а також це лише спосіб для урядів змусити замовкнути критиків, усунути незручні людські перешкоди та іншим чином переконатися, що наратив залишається тільки для них. Стримуючий ефект цих дій очевидний.

NSO не може стверджувати, що має чисті руки. Хоча це правда, він не може запобігти клієнтам від зловмисного розгортання свого шкідливого програмного забезпечення, він міг відмовити в продажу відомим порушникам прав людини. це не новина На даний момент. Перші повідомлення про продажі NSO злочинцям, таким як уряд Саудівської Аравії, з’явилися більше півдесятка років тому.

Це не те, що багато урядових НСО, яким нещодавно продано, почали брати участь у масових порушеннях прав людини. Кожен із цих сумнівних клієнтів був у бізнесі гноблення роками, якщо не протягом усього свого існування.

NSO нікуди подітися, доки тривають ці розслідування та така звітність. Поки світло залишається достатньо яскравим, тіні будуть занадто малі, щоб у них сховатися. Тож, хоча ці останні новини можуть бути більш однаковими, вони все одно важливі». ***(Tim Cushing. NSO Malware Discovered On The Phones Of Critics Of Putin And His Allies // Techdirt (https://www.techdirt.com/2024/06/04/nso-malware-discovered-on-the-phones-of-critics-of-putin-and-his-allies/?utm_source=flipboard&utm_content=Techdirt%2Fmagazine%2FTechdirt). 04.06.2024).***

***

«Наші статті про зловмисне програмне забезпечення зазвичай стосуються Android або Windows, але користувачам Apple час від часу доводиться мати справу зі зловмисним програмним забезпеченням. Наприклад, команда з кібербезпеки Moonlock Lab нещодавно виявила різновид зловмисного програмного забезпечення для macOS, яке може легко уникнути виявлення.

Як пояснюють дослідники, ланцюг зараження починається, коли користувач Mac відвідує сайт у пошуках піратського програмного забезпечення. На сайті вони можуть завантажити файл під назвою CleanMyMacCrack.dmg, вважаючи, що файл є зламаною версією програми очищення Mac CleanMyMac. Після запуску файлу DMG на комп’ютері виконується файл Mach-O, який завантажує AppleScript, здатний викрасти конфіденційну інформацію з Mac.

Ось усе, що зловмисне програмне забезпечення може зробити після зараження комп’ютера macOS:

- Збирає та зберігає ім’я користувача власника Mac
- Створює тимчасові каталоги для зберігання вкрадених даних перед викраденням

- Витягує історію веб-перегляду, файли cookie, збережені паролі тощо з браузерів
- Визначає та отримує доступ до загальних каталогів, що містять гаманці криптовалюти
- Копіює дані брелоків macOS, дані Apple Notes і файли cookie з Safari
- Збирає загальну інформацію про користувача, відомості про систему та метадані
- Передає всі викрадені дані зловмисникам

Moonlock стверджує, що зловмисне програмне забезпечення macOS, схоже, пов'язане з відомим російськомовним загрозником Rodrigo4. Повідомляється, що хакер був помічений на підпільному форумі XSS, який вербував інших хакерів, щоб допомогти розповсюдити його викрадач за допомогою маніпуляцій SEO та реклами…». ***(Jacob Siegal. Dangerous macOS malware steals browser data and cryptocurrency // BGR Media, LLC. (https://bgr.com/tech/dangerous-macos-malware-steals-browser-data-and-cryptocurrency/). 05.06.2024).***

***

«Дослідники з кібербезпеки виявили оновлену версію шкідливого програмного забезпечення під назвою ValleyRAT, яке поширюється в рамках нової кампанії.

«В останній версії ValleyRAT представлено нові команди, такі як створення скріншотів, фільтрація процесів, примусове завершення роботи та очищення журналів подій Windows», — повідомили дослідники Zscaler ThreatLabz Мухаммед Ірфан В. А. і Маніша Рамчаран Праджапаті.

ValleyRAT був раніше задокументований QiAnXin і Proofpoint у 2023 році у зв'язку з фішинговою кампанією, націленою на китайськомовних користувачів і японські організації, які поширювали різні сімейства зловмисного програмного забезпечення, наприклад Purple Fox і варіант трояна Gh0st RAT, відомий як Sainbox RAT (він же FatalRAT).

Вважається, що зловмисне програмне забезпечення є роботою китайського загрозливого актора, який може похвалитися можливостями збирання конфіденційної інформації та скидання додаткових корисних даних на скомпрометовані хости.

Відправною точкою є завантажувач, який використовує файловий сервер HTTP (HFS) для отримання файлу під назвою «NTUSER.DXM», декодованого для вилучення файлу DLL, відповідального за завантаження «client.exe» з того самого сервера.

Розшифрована бібліотека DLL також призначена для виявлення та припинення дії рішень для захисту від зловмисного програмного забезпечення від Qihoo 360 і WinRAR, намагаючись уникнути аналізу, після чого завантажувач переходить до отримання ще трьох файлів – «WINWORD2013.EXE», «wwlib.dll» і «xig.ppt» – із сервера HFS.

Далі зловмисне програмне забезпечення запускає «WINWORD2013.EXE», законний виконуваний файл, пов’язаний із Microsoft Word, використовуючи його для завантаження «wwlib.dll», який, у свою чергу, встановлює постійність у системі та завантажує «xig.ppt» у пам’ять.

«Звідси розшифрований «xig.ppt» продовжує процес виконання як механізм для розшифровки та введення шелл-коду в svchost.exe», — сказали дослідники. «Зловмисне програмне забезпечення створює svchost.exe як призупинений процес, виділяє пам’ять у процесі та записує туди шелл-код».

Зі свого боку, код оболонки містить необхідну конфігурацію для зв’язку з сервером керування (C2) і завантаження корисного навантаження ValleyRAT у формі файлу DLL.

«ValleyRAT використовує складний багатоетапний процес для зараження системи кінцевим корисним навантаженням, яке виконує більшість зловмисних операцій», — сказали дослідники. «Цей поетапний підхід у поєднанні з боковим завантаженням DLL, ймовірно, призначений для кращого уникнення рішень безпеки на основі хоста, таких як EDR та антивірусні програми».

Ця подія сталася після того, як лабораторії Fortinet FortiGuard Labs виявили фішингову кампанію, спрямовану на іспаномовних людей за допомогою оновленої версії кейлоггера та викрадача інформації під назвою Agent Tesla.

Ланцюжок атак використовує вкладення файлів Microsoft Excel Add-Ins (XLA), які використовують відомі недоліки безпеки (CVE-2017-0199 і CVE-2017-11882), щоб ініціювати виконання коду JavaScript, який завантажує сценарій PowerShell, розроблений щоб запустити завантажувач, щоб отримати Agent Tesla з віддаленого сервера.

«Цей варіант збирає облікові дані та контакти електронної пошти з пристрою жертви, програмне забезпечення, з якого він збирає дані, і основну інформацію про пристрій жертви», — сказав дослідник безпеки Сяопен Чжан. «Агент Tesla також може збирати контакти електронної пошти жертви, якщо вона використовує Thunderbird як клієнт електронної пошти». ***(China-Linked ValleyRAT Malware Resurfaces with Advanced Data Theft Tactics // The Hacker News (https://thehackernews.com/2024/06/china-linked-valleyrat-malware.html). 11.06.2024).***

***

«Експерти з кібербезпеки ідентифікували новий тип шкідливого програмного забезпечення під назвою «Noodle RAT», яке китайськомовні хакерські групи використовують для націлювання на сервери Linux.

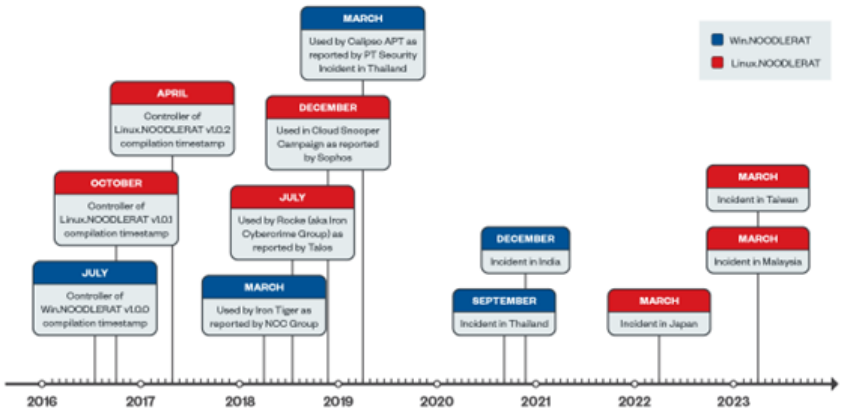
Хоча це зловмисне програмне забезпечення активно з 2016 року, воно лише нещодавно було належним чином класифіковано, що проливає світло на його широке використання як у шпигунстві, так і в кіберзлочинності.

Поява Noodle RAT

Noodle RAT, також відомий як ANGRYREBEL або Nood RAT, — це бекдорне зловмисне програмне забезпечення з версіями як для Windows (Win.NOODLERAT), так і для Linux (Linux.NOODLERAT).

TrendMicro Відповідно до блогу, незважаючи на його довгу історію, його часто неправильно класифікували як варіанти інших шкідливих програм, таких як Gh0st RAT або Rekoobe.

Однак нещодавні дослідження підтвердили, що Noodle RAT є окремим сімейством шкідливих програм.



Noodle RAT Timeline

Графік розробки та розгортання Noodle RAT такий:

Липень 2016: скомпільовано v1.0.0 для Win.NOODLERAT.

Грудень 2016: скомпільовано v1.0.1 для Linux.NOODLERAT.

Квітень 2017 р.: оновлено v1.0.1 для Linux.NOODLERAT.

Кілька звітів задокументували атаки за участю Noodle RAT з 2018 року, але його часто помилково ідентифікували як інші сімейства шкідливих програм…

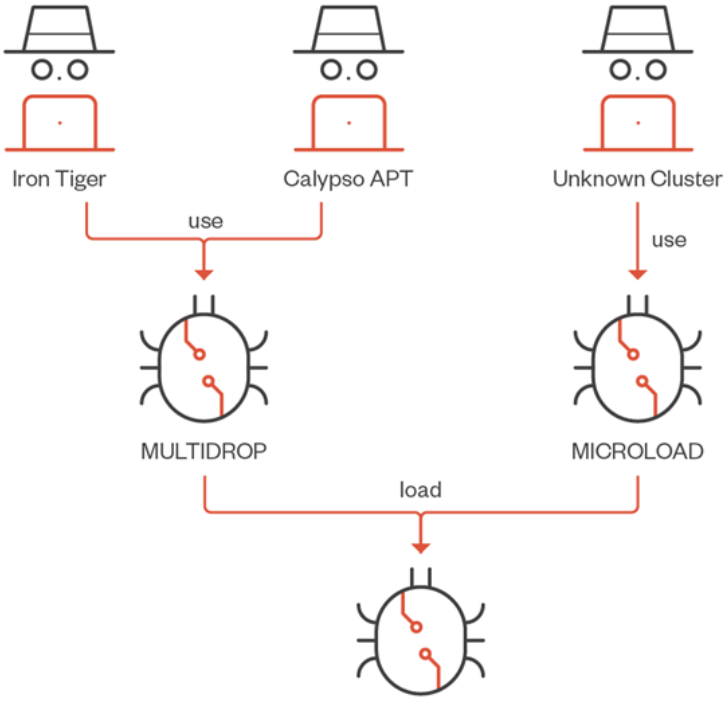
Зокрема, з 2020 року шпигунські кампанії з використанням Noodle RAT були націлені на такі країни, як Таїланд, Індія, Японія, Малайзія та Тайвань.

Технічні деталі Noodle RAT

Win.NOODLERAT

Win.NOODLERAT — це модульний бекдор, сформований у оперативній пам’яті за допомогою шелл-коду. Його використовували такі групи, як Iron Tiger і Calypso APT. Його можливості включають:

- Завантаження та завантаження файлів
- Запуск додаткових модулів у пам'яті
- Робота як TCP проксі



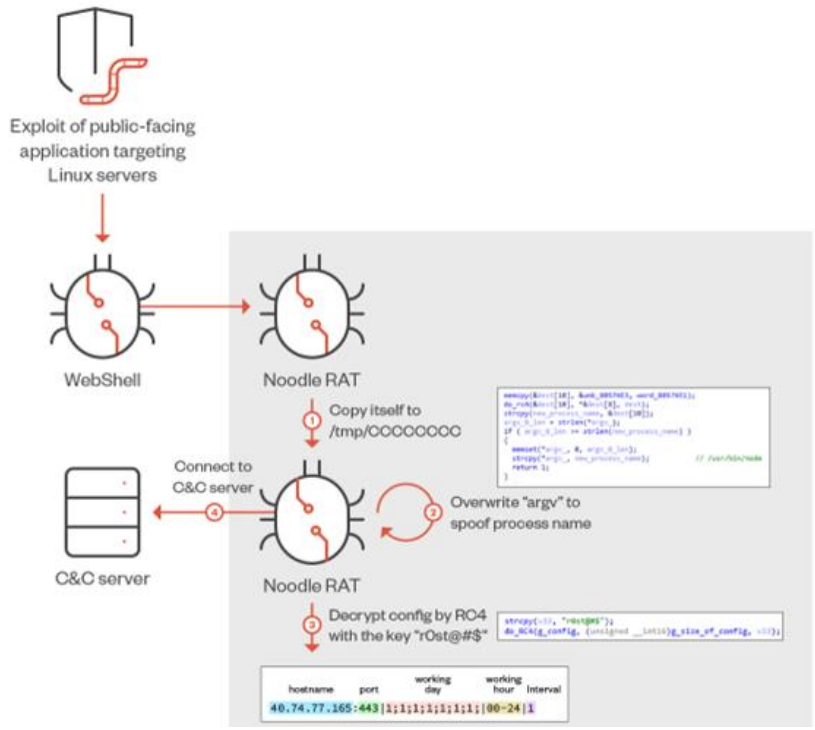
Відносини Win.NOODLERAT з групами загроз

Зловмисне програмне забезпечення використовує такі завантажувачі, як MULTIDROP і MICROLOAD для встановлення, і використовує складні алгоритми шифрування для зв'язку C&C.

Linux.NOODLERAT

Linux.NOODLERAT, ELF-версія Noodle RAT, використовувалася такими групами, як Rocke (Iron Cybercrime Group) і Cloud Snooper Campaign. Його можливості включають:

- Зворотна оболонка
- Завантаження та завантаження файлів
- Планування виконання
- SOCKS тунелювання



Спостережений потік виконання Linux.NOODLERAT

Зловмисне програмне забезпечення зазвичай розгортається як додаткове корисне навантаження експлойту проти загальнодоступних програм і використовує складні алгоритми шифрування для зв'язку C&C.

Команди бекдора

І Win.NOODLERAT, і Linux.NOODLERAT реалізують різні команди бекдору. У наведеній нижче таблиці підсумовано деякі з цих команд:

Дії	Тип 0x03A2 (Win)	Тип 0x132A (Win)	Тип 0x03A2 (Linux)	Тип 0x23F8 (Linux)
Успішно авторизовано	0x03A2	0x132A	0x03A2	0x23F8
Завантажте файл на C&C сервер	0x390A	0x590A	0x3	0x3
Рекурсивний список каталогів	0x390A	0x590A	0x3	0x3
Завантажте файл із C&C сервера	0x390A	0x590A	0x3	0x3

Дії	Тип 0x03A2 (Win)	Тип 0x132A (Win)	Тип 0x03A2 (Linux)	Тип 0x23F8 (Linux)
Розпочати зворотний сеанс оболонки	N/A	N/A	0x1	0x1

Подібності з іншими шкідливими програмами

Noodle RAT має певну схожість із Gh0st RAT і Rekoobe, але досить відмінний, щоб класифікувати його як нове сімейство шкідливих програм…

Наприклад, хоча він використовує деякі плагіни від Gh0st RAT, основний бекдор-код відрізняється. Подібним чином Linux.NOODLERAT поділяє певний код із Rekoobe v2018, але решта його коду унікальна.

Останні дані виявили панелі керування та конструктори для Noodle RAT, що вказує на складну екосистему зловмисного програмного забезпечення.

Панель керування для Linux.NOODLERAT під назвою «NoodLinux v1.0.1» підтримує TCP і HTTP для протоколу C&C і вимагає пароля для відкриття.

Конструктори для Linux.NOODLERAT, версії v1.0.1 і v1.0.2, допомагають створювати спеціальні конфігурації для зловмисного програмного забезпечення…

Noodle RAT роками неправильно класифікували та недооцінювали.

Це нове розуміння його можливостей і використання підкреслює необхідність пильності в кібербезпеці, особливо для систем Linux/Unix.

Оскільки використання публічних програм зростає, Noodle RAT залишається потужним інструментом для учасників загроз, тому фахівцям із кібербезпеки важливо бути в курсі та бути готовими». ***(Divya. Chinese Hackers using New Noodle RAT to Attack Linux Servers // GBHackers (https://gbhackers.com/noodle-rat-to-attack-linux-servers/). 11.06.2024).***

***

«Пов'язане з ХАМАС угруповання Arid Viper використовує шпигунське програмне забезпечення AridSpy для Android ще з 2022 року. Тепер дослідники вперше надали повний аналіз раніше загадкових пізніх стадій розвитку цього шкідливого програмного забезпечення.

Виявляється, AridSpy поширюється через троянські програми обміну повідомленнями, повідомляють дослідники з ESET, які нещодавно опублікували новий звіт про кампанії AridSpy.

«Новим у цих кампаніях є те, що AridSpy був перетворений на багатоступеневий троян, з додатковим корисним навантаженням, яке завантажується з командно-контрольного сервера за допомогою початкового троянського додатку», - йдеться у звіті.

Згідно зі звітом, дослідники проаналізували п’ять окремих зусиль AridSpy, спрямованих на користувачів Android у Єгипті та Палестині. AridSpy часто ховається в програмах із законними функціями, що ускладнює його виявлення. У цьому випадку жертви в Палестині були націлені на рекламу шкідливого додатка, який видавався за Палестинський реєстр громадян, повідомили в ESET. У Єгипті шпигунське програмне забезпечення на першому етапі було приховано в додатку під назвою LapizaChat, а також у оголошеннях про шахрайські вакансії. Програми доступні для завантаження зі сторонніх сайтів, контрольованих зловмисниками, а не з Google Play.

Після початку другого етапу викрадання даних аналіз показав, що група загроз здатна збирати низку даних, включаючи місцезнаходження пристрою, список контактів, журнали викликів, текстові повідомлення, мініатюри фотографій, дані буфера обміну, сповіщення, мініатюри відеозаписів, а також як надання кіберзлочинцям можливості записувати аудіо, робити фотографії тощо.

Попередній аналіз показав, що AridSpy використовувався у 2022 році для націлювання на Чемпіонат світу з футболу, який проходив у Катарі, серед інших кампаній на Близькому Сході, йдеться у звіті.

ESET попереджає, що спеціалізовані сайти все ще проводять принаймні три шпигунські кампанії AridSpy.

«На момент публікації три з п’яти виявлених кампаній все ще активні; кампанії використовували спеціалізовані веб-сайти для розповсюдження шкідливих додатків, що видають себе за NortirChat, LapizaChat і ReblyChat... оголошення про роботу... і додатки Палестинського цивільного реєстру», - йдеться в повідомленні.

Arid Viper, ймовірно, також підтримуватиме та покращуватиме код AridSpy з часом.

«Звичайно, корисне навантаження другого етапу містить останні оновлення та зміни шкідливого коду, які можна перенести в інші поточні кампанії», — зазначили дослідники. «Ця інформація свідчить про те, що AridSpy обслуговується і може отримувати оновлення або зміни функцій». ***(Hamas Hackers Sling Stealthy Spyware Across Egypt, Palestine // Informa PLC (https://www.darkreading.com/cyberattacks-data-breaches/hamas-hackers-stealthy-spyware-egypt-palestine?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 17.06.2024).***

***

«Нещодавно виявлена шкідлива програма Linux під назвою «DISGOMOJI» використовує новий підхід до використання емодзі для виконання команд на заражених пристроях під час атак на урядові установи в Індії.

Зловмисне програмне забезпечення було виявлено компанією з кібербезпеки Volexity, яка вважає, що воно пов’язане з пакистанським загрозником, відомим як «UTA0137».

«У 2024 році Volexity виявив кампанію кібершпигунства, яку розгорнув підозрюваний пакистанський загрозливий актор, якого Volexity зараз відстежує під псевдонімом UTA0137», — пояснює Volexity.

«Volexity з високою впевненістю оцінює, що UTA0137 має цілі, пов’язані зі шпигунством, і пов’язаний з цільовими урядовими організаціями в Індії. На основі аналізу Volexity, кампанії UTA0137 виявилися успішними», – продовжують дослідники.

Зловмисне програмне забезпечення схоже на багато інших бекдорів/ботнетів, що використовуються в різних атаках, дозволяючи суб’єктам загрози виконувати

команди, робити знімки екрана, викрадати файли, розгортати додаткові корисні навантаження та шукати файли.

Однак використання Discord і emojis як платформи керування та управління (C2) виділяє зловмисне програмне забезпечення серед інших і може дозволити йому обійти програмне забезпечення безпеки, яке шукає текстові команди.

Дискорд і емодзі як C2

За даними Volexity, зловмисне програмне забезпечення було виявлено після того, як дослідники помітили виконуваний файл ELF, запакований UPX, у ZIP-архіві, який, ймовірно, поширювався через фішингові електронні листи.

Volexity вважає, що зловмисне програмне забезпечення націлене на спеціальний дистрибутив Linux під назвою BOSS, який індійські урядові установи використовують як робочий стіл. Однак зловмисне програмне забезпечення можна так само легко використовувати для атак на інші дистрибутиви Linux.

Після виконання зловмисне програмне забезпечення завантажить і відобразить PDF-приманку, яка є формою бенефіціара з Фонду забезпечення офіцерів оборонної служби Індії на випадок смерті офіцера.

Однак у фоновому режимі буде завантажено додаткові корисні дані, зокрема шкідливе програмне забезпечення DISGOMOJI та сценарій оболонки під назвою «uevent_seqnum.sh», який використовується для пошуку USB-накопичувачів і викрадення даних з них.

Коли DISGOMOJI запускається, зловмисне програмне забезпечення вилучає системну інформацію з машини, включаючи IP-адресу, ім’я користувача, ім’я хоста, операційну систему та поточний робочий каталог, які надсилаються назад зловмисникам.

Щоб контролювати зловмисне програмне забезпечення, зловмисники використовують проект управління та керування з відкритим кодом discord-c2, який використовує Discord та емодзі для зв’язку із зараженими пристроями та виконання команд.

Зловмисне програмне забезпечення з’єднається з сервером Discord, яким керує зловмисник, і чекатиме, доки зловмисники введуть емодзі в канал.

Дев’ять емодзі використовуються для представлення команд для виконання на зараженому пристрої, які перераховані нижче.

Emoji	Emoji Name	Command Description
🏃	Man Running	Execute a command on the victim’s device. This command receives an argument, which is the command to execute.
📸	Camera with Flash	Take a screenshot of the victim’s screen and upload it to the command channel as an attachment.
👇	Backhand Index Pointing Down	Download files from the victim’s device and upload them to the command channel as attachments. This command receives one argument, which is the path of the file.
☝️	Index Pointing Up	Upload a file to the victim’s device. The file to upload is attached along with this emoji.
👉	Backhand Index Pointing Right	Upload a file from the victim’s device to Oshi (`oshi[.]at`), a remote file-storage service. This command receives an argument, which is the name of the file to upload.
👈	Backhand Index Pointing Left	Upload a file from the victim’s device to `transfer[.]sh`, a remote file-sharing service. This command receives an argument, which is the name of the file to upload.
🔥	Fire	Find and send all files matching a pre-defined extension list that are present on the victim’s device. Files with the following extensions are exfiltrated: CSV, DOC, ISO, JPG, ODP, ODS, ODT, PDF, PPT, RAR, SQL, TAR, XLS, ZIP
🦊	Fox	Zip all Firefox profiles on the victim’s device. These files can be retrieved by the attacker at a later time.
💀	Skull	Terminate the malware process using `os.Exit()`.

Зловмисне програмне забезпечення підтримує постійність на пристрої Linux за допомогою команди @reboot cron для запуску зловмисного програмного забезпечення під час завантаження.

Volexity каже, що вони виявили додаткові версії, які використовували інші механізми збереження для DISGOMOJI та сценарій крадіжки даних USB, включаючи записи автозапуску XDG.

Після того, як пристрій зламано, зловмисники використовують свій доступ, щоб поширюватися вбік, викрадати дані та намагатися викрасти додаткові облікові дані цільових користувачів.

Хоча емодзі можуть здатися «милою» новинкою для зловмисного програмного забезпечення, вони можуть дозволити йому обійти виявлення програмним забезпеченням безпеки, яке зазвичай шукає команди зловмисного програмного забезпечення на основі рядків, що робить цей підхід цікавим». ***(Lawrence Abrams. New Linux malware is controlled through emojis sent from Discord // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/new-linux-malware-is-controlled-through-emojis-sent-from-discord/?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology). 15.06.2024).***

***

Програми-вимагачі

«Минулого року активність програм-вимагачів різко зросла, оскільки зловмисники почали використовувати законні інструменти віддаленого доступу, щоб зламати корпоративні мережі, йдеться у звіті Mandiant у понеділок.

Минулого року на сайтах витоку даних було 4520 публікацій, що на 75% більше, ніж у 2022 році. Групи загроз використовують сайти витоку даних, щоб робити претензії та посилювати тиск на ймовірних жертв. За словами Mandiant, у третьому кварталі кількість публікацій зросла до понад 1300, встановивши квартальний рекорд. У другому кварталі фірма відстежила понад 1200 публікацій на сайтах витоку даних.

У 2023 році Mandiant провела на 20% більше розслідувань за участю програм-вимагачів, ніж у попередньому році, що підтверджує нові докази зростання кількості атак. «Незначне зниження вимагань у 2022 році було аномалією», — заявили в дослідницькій компанії.

Висновки Mandiant підкреслюють колективну неспроможність галузі зменшити атаки програм-вимагачів і значну шкоду, яку вони завдають підприємствам і людям.

Минулого року Mandiant провела рекордну кількість розслідувань інцидентів із програмним забезпеченням-вимагачем, оскільки зафіксувала найбільшу кількість публікацій на сайтах з витоком даних з тих пір, як у 2020 році почала відстежувати сайти, що ганьблять. Минулого року ймовірні організації-жертви сайтів з витоком даних охоплювали понад 110 країн.

Майже 3 з 5 атак програм-вимагачів, які Mandiant спостерігав минулого року, включали підтверджену або підозрювану крадіжку даних.

Згідно з дослідженням Mandiant, більшість первинних векторів доступу для атак програм-вимагачів у 2023 році включали вкрадені облікові дані або використані вразливості в публічній інфраструктурі.

«У майже 40% інцидентів, у яких було виявлено початковий вектор доступу, суб'єкти загрози використовували скомпрометовані легітимні облікові дані, щоб отримати доступ до середовищ жертви, або шляхом використання вкрадених облікових даних, або шляхом грубої атаки», — йдеться у звіті дослідників Mandiant. «Переважна більшість цих інцидентів стосувалася автентифікації в корпоративній інфраструктурі VPN жертви»

За даними Mandiant, використані вразливості спричинили майже 30% атак програм-вимагачів минулого року проти 24% у 2022 році.

«Зростаюча залежність від законних інструментів, яка спостерігається, ймовірно, відображає зусилля зловмисників приховати свої операції від механізмів виявлення та скоротити час і ресурси, необхідні для розробки та підтримки спеціальних інструментів», — йдеться у звіті. «Подібним чином, хоча ми все ще постійно розглядаємо використання вразливостей як популярний метод отримання початкового доступу до середовища жертви, суб'єкти загроз частіше покладалися на відомі вразливості». ***(Matt Kapko. CVE exploits, stolen credentials fueled ransomware surge in 2023 // Industry Dive***

(https://www.cybersecuritydive.com/news/exploits-credentials-fuel-ransomware-surge/717943/?utm_source=flipboard&utm_content=other). 04.06.2024).

***

«Програмне забезпечення-вимагач використовується хакерами для зловживання даними жертв, блокуючи їх до сплати викупу.

Цей метод кібератаки є вигідним, оскільки він використовує переваги близькості та життєздатності даних для окремих осіб і компаній, тож у них немає іншого вибору, як платити за швидку віддачу.

Вторгнення почалося з електронного листа, що містив роздвоєний варіант IcedID, який наголошував на доставці корисного навантаження.

Отримавши початковий доступ, зловмисник встановив на комп'ютер ScreenConnect для віддаленого керування, неправомірно використовував маяки Cobalt Strike і розгорнув CSharp Streamer RAT, щоб отримати облікові дані та пересуватися в межах контролерів домену та серверів.

Під час фази ідентифікації конфіденційну інформацію поміщали в «confucius_cpp», спеціальну програму, rclone якої показувала вилучення…

Протягом восьми днів вони виконували систематичне розгортання інсталяторів ScreenConnect на хостах за допомогою WMI, перш ніж нарешті завантажити програмне забезпечення-вимагач ALPHV після видалення резервних копій.

Розгортання програм-вимагачів ALPHV

Шкідлива електронна пошта зі спамом, яка обманом спонукала здобич завантажити та розархівувати папку з readme і Visual Basic Script (VBS), слугувала початковим вектором доступу.

Активація VBS запустила вбудовану обфусцовану DLL завантажувача IcedID, яка відкинула та запустила інше корисне навантаження DLL IcedID, завершивши ланцюжок зараження, йдеться у звіті DFIR.

Це узгоджується з відомою зловмисною діяльністю, де той самий метод використовувався для розповсюдження форка IcedID, який займається розгортанням корисного навантаження замість банківської діяльності.

Зловмисник розгорнув інструменти віддаленого доступу ScreenConnect за допомогою замаскованих інсталяційних програм, які працювали через сеанси wmiexec і RDP.

Для отримання маяків Cobalt Strike було використано кілька методів, зокрема bitsadmin, certutil і PowerShell.

CSharp Streamer RAT підтримував постійність через заплановані завдання в дампі облікових даних LSASS, боковому переміщенні та зв'язку C2.

IcedID забезпечив свою постійність за допомогою запланованих завдань, а ScreenConnect став постійним під час перезавантаження.

Під час бокового переміщення до winlogon.exe та rundll32.exe спостерігалося впровадження процесу. Перейменовані інсталятори були видалені актором.

Ключові дії включали дамп облікових даних LSASS, який перевірявся за допомогою аналізу пам'яті, а dcsync виконувався від плацдарму до контролера домену для збору облікових даних.

Після цього зловмисник виконав початкове розпізнавання за допомогою власних утиліт Windows, запущених через IcedID, а потім використав ScreenConnect для додаткових розвідувальних команд.

SoftPerfect netscan для сканування мережі проводився в різні дні, націлюючись на діапазони IP-адрес плюс порти резервних копій RPC, SMB, RDP і Veeam.

Потім інсталятори ScreenConnect були скопійовані через SMB і розгорнуті за допомогою wmiexec.py для отримання дистанційного керування. Зловмисник широко використовував RDP для бокового переміщення, включаючи проксі через CSharp Streamer.

До викрадання спеціальний інструмент під назвою confucius_cpp перераховував системи за запитом LDAP, отримував доступ до спільних ресурсів

на основі ключових слів і стискав конфіденційну інформацію. Також зловмисник відкрив документи за допомогою інсталяції Firefox.

Зловмисник використовував кілька інструментів під час вторгнення:

- IcedID для початкового доступу до зв'язку з modalefastnow[.]com
- Маяки Cobalt Strike через хости, що підключаються до відстежуваної інфраструктури C2
- CSharp Streamer RAT на 109.236.80.191 використовує WebSockets через обертові порти
- Інструменти віддаленого доступу ScreenConnect, розгорнуті через перейменовані двійкові файли, що виконуються через wmiexec.py

Тоді як Firefox використовувався для попереднього перегляду документів і завантаження rclone, який виконувався через сценарій VBS для викрадання даних.

Остаточним корисним навантаженням було програмне забезпечення-вимагач ALPHV, розміщене на сервері резервного копіювання, а потім розгорнуте на хостах через хсору та виконання, ініційоване WMI, після видалення резервних копій.

Записка про викуп із посиланням на Twitter групи була залишена після шифрування…» ***(Tushar Subhra Dutta. ALPHV Ransomware Deployment Started With RDP Access And ScreenConnect Installations // GBHackers (https://gbhackers.com/alphv-ransomware-rdp-screenconnect-deployment/). 10.06.2024).***

***

«Програми-вимагачі та інші загрози безпеці даних продовжують зростати, оскільки обсяги даних зростають експоненціально. Експерти рекомендують багатогранну стратегію безпеки, і технологія LTO може відіграти ключову роль у масштабуванні швидкого, доступного, високоємного офлайн-сховища для останньої лінії захисту.

Обсяги даних продовжують збільшуватися експоненціально, без жодних ознак сповільнення. Наприклад, IDC прогнозує, що обсяг комерційних даних у сховищі зросте до 12,8 ZB до 2026 року. Щоб дивитися фільми розміром 12,8 ZB у

форматі 780p HD, вам потрібно буде сидіти перед телевізором понад 154 мільйони років.

Захист цих постійно зростаючих обсягів даних є пріоритетним завданням, і хоча існує багато різних типів загроз кібербезпеці корпоративних даних, програми-вимагачі домінують у цій галузі. Програми-вимагачі спричинили майже чверть (24%) випадків витоку даних у звіті Verizon Data Breach Investigations Report за 2023 рік, а у звіті Sophos State of Ransomware 2023 встановлено, що дві третини опитаних компаній зазнали атаки програм-вимагачів.

Клаус Торп Дженсен, колишній технічний директор і керівник відділу архітектури в CVS Health and Aetna, погодився, що програми-вимагачі викликають найбільше занепокоєння. «На вершині діаграми ризиків кібербезпеки знаходяться атаки програм-вимагачів. Стратегії кібербезпеки мають перейти від захисту даних до більш цілісного підходу до безперервності бізнесу. …У сучасному середовищі часто неможливо встановити 100% захист, але ми можемо гарантувати, що якщо і коли щось станеться, у нас є чіткий шлях і підхід до швидкого відновлення».

Експерти розбираються щодо найкращого підходу до безпеки

Існує загальна згода з тим, що, хоча сучасні стратегії кібербезпеки є критичними, вони не можуть повністю захистити дані від програм-вимагачів та інших видів атак. Проте ведуться дискусії щодо найкращого підходу до захисту цих даних.

за останні п’ять років нульова довіра значною мірою закріпилася, і це не дарма. За словами Річа Геймана, керівника штучного інтелекту Tier4.ai, «Нульова довіра діє за принципом «ніколи не довіряй, завжди перевіряй», — каже Гейман. «Йдеться про те, щоб припустити найгірше та перевірити це. Це різкий контраст з іншими парадигмами безпеки, такими як Defense in Depth, які є більш спекулятивними. Суть нульової довіри полягає в перевірці. Тож, хоча моя відповідь — нульова довіра, [це] я відстоюю не лише концепцію, а спосіб мислення. Я думаю, ви повинні підтвердити свої припущення, свою технологію, свою політику, своїх людей і свої процеси».

У подібному ключі Рохіт Гай, генеральний директор RSA, наголошує на необхідності захисту та захисту особистих даних. «Ідентифікація завжди була найбільш успішно атакуваною ціллю в інфраструктурі організації», — зазначає Гай. «І хоча організації досягли великих успіхів у впровадженні багатофакторної автентифікації, нещодавні витоки даних показали, що суб'єкти загроз пристосовуються до нових можливостей кібербезпеки та знаходять способи обійти MFA. Організації будуть настільки безпечними, наскільки захищені їхні особи».

Обґрунтування багатогранного підходу

Але існує широкий консенсус, що ані відсутність довіри, ані контроль ідентифікації не можуть повністю захистити дані організації. Як наслідок, Джин Де Ліберо, керівник Digital Mindshare LLC, рекомендує включити нульову довіру разом зі штучним інтелектом та іншими технологіями. «По-перше, використання системи безпеки на основі штучного інтелекту дозволяє розширене прогнозне виявлення загроз і автоматичне реагування, використовуючи штучний інтелект, щоб випереджати кіберзагрози», — говорить Де Ліберо. «По-друге, реалізація архітектури нульової довіри передбачає обов'язкову перевірку кожного запиту на доступ, різко мінімізуючи поверхню атаки. Нарешті, використання сітчастої архітектури кібербезпеки дозволяє бездоганно працювати разом між різними рішеннями кібербезпеки, покращуючи загальний механізм захисту. Разом ці стратегії забезпечують підприємство всебічною системою захисту, підтримуючи стратегічні пріоритети керівників технологій і маркетингу щодо захисту даних їхніх організацій».

Брайан Томас, IT-директор DivergentCIO, робить цей підхід на крок далі, стверджуючи про «все більш складний і динамічний ландшафт кібербезпеки». Це вимагає багатогранного підходу, який поєднує в собі передові технології та проактивні стратегії. Що включає архітектуру нульової довіри, розширене виявлення загроз, шифрування, аудит безпеки, оцінку технологічних ризиків і навчання з питань кібербезпеки, і, звичайно, регулярне аварійне відновлення/планування безперервності бізнесу».

Сантьяго Мартін-Романі, який є віце-президентом із технологічних послуг у різних компаніях, повторив Томаса та Де Ліберо щодо важливості багатогранної стратегії кібербезпеки. «У 2024 році та далі, — каже Мартін-Романі, — багаторівневий підхід до кібербезпеки є життєво важливим. впровадження багатофакторної автентифікації (MFA) зменшить спроби зламу облікового запису на 90% Згідно зі звітом Microsoft. Доступ до мережі без довіри (ZTNA) може ще більше посилити контроль доступу. Регулярні перевірки безпеки в поєднанні з навчанням працівників кібергігієні мають вирішальне значення для обізнаності користувачів. А також використання технологій шифрування даних із розміром ринку, який, як очікується, досягне 180 мільярдів доларів до 2025 року».

Нарешті, Вілл Лассаль, IT-директор JLS Technology USA, вказує на важливість підготовки не лише засобів кіберзахисту для запобігання успішній атаці, але й впровадження надійного плану пом'якшення та відновлення збитків від неминучого успішного злому. «Замість того, щоб зосереджуватися виключно на профілактиці, — каже Лассаль, — організації повинні прийняти мислення стійкості. Це передбачає підготовку до неминучих порушень і визнання того, що кожна система має вразливі місця. Стійкість виходить за рамки оборони та включає надійні стратегії для сценаріїв після злому. Кіберстійкість охоплює два критичні аспекти:

Безперервний захист: посилення операцій проти постійних атак для забезпечення безперервності бізнесу в «нормальних» умовах кібервійни.

Стратегія після злому: розробка адаптивних планів, які виходять за рамки відновлення, визнаючи динамічне цифрове поле битви, на якому розвиваються загрози».

Введіть LTO: остання лінія захисту, перевірена часом

Резервне копіювання та відновлення є важливою частиною цієї стратегії після злому, яку часто називають останньою лінією захисту. Але IT-спеціалістам може бути важко ефективно масштабувати ці системи, щоб захистити обсяги даних, що швидко збільшуються, без шкоди для продуктивності та надійності. Традиційні системи можуть зіткнутися зі значними вузькими місцями та обмеженнями.

LTO (Linear Tape-Open) — це добре запроваджена технологія зберігання даних на магнітній стрічці, яка вперше була запущена в 2000 році, і продовжує мати актуальні програми для довгострокового архівування, резервного копіювання даних, передачі даних великої ємності та автономного зберігання, особливо з оновленнями які були зроблені для нього протягом останнього десятиліття. Сюди входять такі функції, як одноразове записування, багаторазове читання (WORM), апаратне шифрування, лінійна стрічкова файлова система (LTFS), що дозволяє розділяти дані, кілька методів цифрового кодування та методи стиснення даних без втрат. LTO-9 може зберігати 18 ТБ нестиснутих даних (45 ТБ зі стисненням 2,5:1) на одному картриджі зі швидкістю передачі даних до 400 МБ/с (1000 МБ/с 2,5:1 стиснення).

Найкраща новина? Картридж LTO-9 коштує всього близько 100 доларів.

Технологія LTO забезпечує масштабоване, доступне за ціною засіб високої щільності для отримання офлайн-сховища для даних, які можна швидко відновити. Це не повне вирішення ширших проблем з програмами-вимагачами та безпекою даних, але воно може відігравати важливу та незамінну роль у багатогранному захисті…» ***(Jeff Miller. Cybersecurity strategies for protecting data against ransomware and other threats // IDG Communications, Inc. (https://www.cio.com/article/2497144/cybersecurity-strategies-for-protecting-data-against-ransomware-and-other-threats.html). 24.06.2024).***

***

Фішингові атаки

«Дослідники з кібербезпеки розкрили деталі триваючої фішингової кампанії, яка використовує приманки на тему найму та роботи для створення бекдору на базі Windows під назвою WARMCOOKIE.

«WARMCOOKIE, схоже, є початковим бекдор-інструментом, який використовується для розвідки мереж жертв і розгортання додаткових корисних навантажень», — сказав дослідник Elastic Security Labs Даніель Степаніч у новому

аналізі. «Кожен зразок скомпільовано із жорстко закодованою IP-адресою [командування та керування] та ключем RC4».

Бекдор має можливості знімати відбитки пальців на заражених машинах, робити знімки екрана та видаляти інші шкідливі програми. Компанія відстежує діяльність під назвою REF6127.

Ланцюги атак, які спостерігалися з кінця квітня, включають використання електронних повідомлень, нібито від таких кадрових фірм, як Hays, Michael Page і PageGroup, які закликають одержувачів натиснути вбудоване посилання, щоб переглянути деталі про вакансію.

Користувачам, які в кінцевому підсумку перейшли за посиланням, буде запропоновано завантажити документ, виконавши завдання CAPTCHA, після чого файл JavaScript («Update_23_04_2024_5689382.js») видаляється.

«Цей обфускований сценарій запускає PowerShell, запускаючи перше завдання для завантаження WARMCOOKIE», — сказав Еластик. «Сценарій PowerShell зловживає Background Intelligent Transfer Service (BITS), щоб завантажити WARMCOOKIE».

Вирішальним компонентом кампанії є використання скомпрометованої інфраструктури для розміщення початкової фішингової URL-адреси, яка потім використовується для перенаправлення жертв на відповідну цільову сторінку.

DLL Windows, WARMCOOKIE, виконує двоетапний процес, який дозволяє встановити постійність за допомогою запланованого завдання та запустити основну функціональність, але не раніше, ніж виконується серія перевірок антианалізу, щоб обійти виявлення.

Бекдор призначений для отримання інформації про заражений хост у спосіб, подібний до артефакту, який використовувався у зв’язку з попередньою кампанією під кодовою назвою Resident, яка була націлена на виробничі, комерційні та медичні організації.

Він також підтримує команди для читання та запису файлів, виконання команд за допомогою cmd.exe, отримання списку встановлених програм і створення знімків екрана.

«WARMCOOKIE — нещодавно відкритий бекдор, який набирає популярності та використовується в кампаніях, орієнтованих на користувачів у всьому світі», — сказав Еластік.

Розкриття сталося після того, як Trustwave SpiderLabs детально описала складну фішингову кампанію, яка використовує приманки, пов'язані з рахунками-фактурами, і використовує переваги функції пошуку Windows, вбудованої в HTML-код, для розгортання шкідливого програмного забезпечення.

Повідомлення електронної пошти містять ZIP-архів, що містить файл HTML, який використовує застарілий обробник протоколу URI «пошуку» Windows для відображення файлу ярлика (LNK), розміщеного на віддаленому сервері в Провіднику Windows, створюючи враження, що це локальний результат пошуку.

«Цей файл LNK вказує на пакетний сценарій (BAT), розміщений на тому самому сервері, який, клацаючи користувачем, потенційно може викликати додаткові зловмисні операції», — повідомили в Trustwave, додавши, що не можуть отримати пакетний сценарій через те, що сервер не відповідає.

Варто зазначити, що зловживання search-ms: і search: як вектором поширення зловмисного програмного забезпечення було задокументовано Trellix у липні 2023 року.

«Хоча ця атака не використовує автоматичне встановлення шкідливого програмного забезпечення, вона вимагає від користувачів взаємодії з різними підказками та клацаннями», – заявили в компанії. «Однак ця техніка спритно приховує справжні наміри зловмисника, використовуючи довіру користувачів до знайомих інтерфейсів і звичайних дій, таких як відкриття вкладень електронної пошти». ***(New Phishing Campaign Deploys WARMCOOKIE Backdoor Targeting Job Seekers // The Hacker News (https://thehackernews.com/2024/06/new-phishing-campaign-deploys.html). 12.06.2024).***

***

«Дослідники з кібербезпеки помітили фішингову атаку, яка розповсюджувала зловмисне програмне забезпечення More_eggs, маскуючи його під резюме, метод, спочатку виявлений більше двох років тому.

Атака, яка була невдалою, була спрямована на неназвану компанію в індустрії промислових послуг у травні 2024 року, повідомила минулого тижня канадська фірма з кібербезпеки eSentire.

«Зокрема, цільовою особою був рекрутер, якого зловмисник ввів в оману, щоб подумати, що вони претенденти на роботу, і заманив їх на свій веб-сайт для завантаження завантажувача», — йдеться в повідомленні.

More_eggs, який вважається роботою загрозливого актора, відомого як Golden Chickens (він же Venom Spider), є модульним бекдором, який здатний збирати конфіденційну інформацію. Він пропонується іншим злочинцям за моделлю шкідливого програмного забезпечення як послуги (MaaS).

Минулого року eSentire викрила реальні особи двох осіб – Чака з Монреаля та Джека, – які, як кажуть, керували операцією.

Останній ланцюжок атак передбачає, що зловмисники відповідають на оголошення про роботу в LinkedIn посиланням на підроблений сайт для завантаження резюме, що призводить до завантаження шкідливого файлу Windows Shortcut (LNK).

Варто зазначити, що попередня активність More_eggs була націлена на професіоналів у LinkedIn із пропозиціями про роботу зі зброєю, щоб обманом змусити їх завантажити зловмисне програмне забезпечення.

«Перехід за тією самою URL-адресою через кілька днів призводить до отримання резюме користувача у звичайному HTML-коді без вказівок на переспрямування чи завантаження», — зазначив eSentire.

Потім файл LNK використовується для отримання шкідливої DLL за допомогою законної програми Microsoft під назвою ie4uinit.exe, після чого бібліотека виконується за допомогою regsvr32.exe для встановлення стійкості, збору даних про заражений хост і видалення додаткових корисних даних, включаючи на основі JavaScript Бекдор More_eggs.

«Кампанії More_eggs все ще активні, і їх оператори продовжують використовувати тактику соціальної інженерії, наприклад, видавати себе за претендентів на роботу, які хочуть подати заявку на певну посаду, і заманювати жертв (зокрема рекрутерів) завантажити їхнє шкідливе програмне забезпечення», — сказав eSentire.

«Крім того, такі кампанії, як more_eggs, які використовують пропозицію MaaS, здаються рідкісними та вибірковими порівняно з типовими мережами розповсюдження спаму».

Ця подія сталася після того, як фірма з кібербезпеки також оприлюднила подробиці кампанії завантажень, яка використовує підроблені веб-сайти для інструменту активації Windows KMSPico для розповсюдження Vidar Stealer.

«Сайт kmspico[.]ws розміщено за Cloudflare Turnstile і вимагає введення людиною (введення коду) для завантаження остаточного ZIP-пакета», — зазначив eSentire. «Ці кроки є незвичайними для легітимної сторінки завантаження програми та виконуються, щоб приховати сторінку та остаточне корисне навантаження від автоматизованих веб-сканерів».

Trustwave SpiderLabs повідомила минулого тижня, що подібні кампанії соціальної інженерії також створюють схожі сайти, які імітують законне програмне забезпечення, наприклад Advanced IP Scanner, для розгортання Cobalt Strike.

Це також слідує за появою нового фішингового набору під назвою V3B, який використовувався для виділення банківських клієнтів у Європейському Союзі з метою викрадення облікових даних і одноразових паролів (OTP).

Набір, який пропонується за 130-450 доларів США на місяць через модель Phishing-as-a-Service (PhaaS) у темній мережі та спеціальний канал Telegram, зазначається, що активний з березня 2023 року. Він розроблений для підтримки понад 54 банків. розташовані в Австрії, Бельгії, Фінляндії, Франції, Німеччині, Греції, Ірландії, Італії, Люксембурзі та Нідерландах.

Найважливішим аспектом V3B є те, що він містить налаштовані та локалізовані шаблони для імітації різних процесів автентифікації та перевірки, поширених у системах онлайн-банкінгу та електронної комерції в регіоні.

Він також має розширені можливості для взаємодії з жертвами в режимі реального часу та отримання їхніх кодів OTP і PhotoTAN, а також для здійснення атаки з використанням QR-коду для входу (так званий QRLJacking) на такі служби, як WhatsApp, які дозволяють входити за допомогою QR-кодів.

«Відтоді вони створили клієнтську базу, зосереджену на європейських фінансових установах», — повідомили в Resecurity. «Наразі за оцінками сотні кіберзлочинців використовують цей набір для шахрайства, залишаючи жертви з порожніми банківськими рахунками». ***(More_eggs Malware Disguised as Resumes Targets Recruiters in Phishing Attack // The Hacker News (https://thehackernews.com/2024/06/moreeggs-malware-disguised-as-resumes.html). 10.06.2024).***

***

«Дослідники з кібербезпеки розкрили нові подробиці про загрозливого актора Sticky Werewolf, який нещодавно розширив свої кампанії кібератак, включивши організації в Росії та Білорусі.

Недавні фішингові атаки були спрямовані на фармацевтичну компанію, російський науково-дослідний інститут мікробіології та вакцин, а також на авіаційний сектор. Відповідно до звіту Morphisec минулого тижня, ці атаки знаменують розширення попереднього фокусу групи на урядових організаціях.

«У попередніх кампаніях ланцюг зараження починався з фішингових електронних листів, які містили посилання для завантаження шкідливих файлів із таких платформ, як gofile.io», — сказав дослідник безпеки Арнольд Осіпов. «Ця остання кампанія використовувала архівні файли, що містять файли LNK, які вказували на корисне навантаження, що зберігається на серверах WebDAV».

Sticky Werewolf приєднується до низки інших загроз, спрямованих на Росію та Білорусь, зокрема Cloud Werewolf (також відомий як Inception і Cloud Atlas), Quartz Wolf (також відомий як RedCurl) і Scaly Wolf. Вперше задокументовано BI.ZONE в жовтні 2023 року, вважається, що Sticky Werewolf був активним принаймні з квітня 2023 року…

Попередні атаки, задокументовані компанією з кібербезпеки, включали фішингові електронні листи з посиланнями на зловмисне корисне навантаження, що призвело до розгортання трояна віддаленого доступу NetWire (RAT). Інфраструктура, що підтримує NetWire, була демонтована на початку минулого року після операції правоохоронних органів.

Новий ланцюжок атак, спостережуваний Morphisec, передбачає прикріплення до архіву RAR. Після розпакування цей архів містить два файли LNK і PDF-документ-приманку, який нібито є запрошенням на відеоконференцію. Він закликає одержувачів натиснути на файли LNK, щоб отримати доступ до порядку денного зустрічі та списку розсилки електронною поштою.

Відкриття будь-якого файлу LNK запускає виконання двійкового файлу, розміщеного на сервері WebDAV, що призводить до запуску обфускованого пакетного сценарію Windows. Цей сценарій розроблено для запуску сценарію AutoIt, який остаточно вводить остаточне корисне навантаження, минаючи програмне забезпечення безпеки та спроби аналізу.

«Цей виконуваний файл є саморозпаковуючим архівом NSIS, який є частиною раніше відомого шифрувальника під назвою CypherIT», — сказав Осипов. «Хоча оригінальний шифрувальник CypherIT більше не продається, поточний виконуваний файл є варіантом, який спостерігається на кількох хакерських форумах».

Кампанія спрямована на розповсюдження товарних RAT і зловмисних програм для викрадання інформації, таких як Rhadamanthys і Ozone RAT.

«Хоча остаточних доказів конкретного національного походження групи Sticky Werewolf немає, геополітичний контекст свідчить про можливі зв’язки з проукраїнською групою кібершпигунства або хактивістами. Однак ця атрибуція залишається невизначеною», – сказав Осипов.

Ця подія сталася після того, як BI.ZONE виявив інший кластер активності під кодовою назвою Sapphire Werewolf, який був пов’язаний із понад 300 атаками на російську освіту, виробництво, IT, оборону та аерокосмічний сектор. ці кіберзломи

Повідомлялося про за допомогою Amethyst, відгалуження популярного SapphireStealer з відкритим кодом.

У березні 2024 року російська компанія також виявила Fluffy Wolf і Mysterious Werewolf кластери. Ці кластери використовували приманки для фішингу для розповсюдження Remote Utilities, майнера XMRig, WarZone RAT і спеціально розробленого бекдора під назвою RingSpy…

«Бекдор RingSpy дозволяє зловмиснику віддалено виконувати команди, отримувати їх результати та завантажувати файли з мережевих ресурсів», — зазначається у звіті. «Сервер керування бекдором — це бот Telegram».

Sticky Werewolf продовжує розширювати свої цілі для кібератак у Росії та Білорусі. Організації повинні залишатися пильними та посилювати заходи кібербезпеки». ***(Abdul Rehman. Sticky Werewolf Expands Cyber Attack Targets in Russia and Belarus // Cloudways Ltd. (https://www.cloudways.com/blog/sticky-werewolf-cyber-attack/). 10.06.2024).***

***

«Дослідники з кібербезпеки пролили світло на нову фішингову кампанію, яка, як було визначено, націлена на людей у Пакистані за допомогою спеціального бекдору.

Securonix назвала PHANTOM#SPIKE, невідомі загрози, що стоять за цією діяльністю, використали фішингові документи військового характеру, щоб активувати послідовність зараження.

«Хоча сьогодні існує багато методів, які використовуються для розгортання зловмисного програмного забезпечення, зловмисники використовували ZIP-файли із захищеним паролем архівом корисного навантаження, який містився всередині», — заявили дослідники Ден Юзвик, Тім Пек і Олег Колесніков у звіті, який поділили з The Hacker News.

Кампанія відрізняється відсутністю складності та використанням простих корисних навантажень для досягнення віддаленого доступу до цільових машин.

Повідомлення електронної пошти містять ZIP-архів, який нібито є протоколом зустрічі, пов’язаної з Міжнародним військово-технічним форумом «Армія 2024», законним заходом, організованим Міністерством оборони Російської Федерації. Його планують провести в Москві в середині серпня 2024 року.

У ZIP-файлі міститься файл Microsoft Compiled HTML Help (CHM) і прихований виконуваний файл («RuntimeIndexer.exe»), перший з яких, коли відкривається, відображає протокол зустрічі, а також кілька зображень, але непомітно працює пакетний двійковий файл, як тільки користувач клацне будь-де на документі.

Виконуваний файл призначений для роботи як бекдор, який встановлює з’єднання з віддаленим сервером через TCP, щоб отримати команди, які згодом виконуються на скомпрометованому хості…

Окрім передачі системної інформації, він виконує команди через cmd.exe, збирає вихідні дані операції та передає їх назад на сервер. Це включає в себе запуск таких команд, як systeminfo, tasklist, curl для отримання загальнодоступної IP-адреси за допомогою ip-api[.]com, і schtasks для налаштування постійності.

«Цей бекдор по суті функціонує як троян віддаленого доступу (RAT) на основі командного рядка, який надає зловмиснику постійний, прихований і безпечний доступ до зараженої системи», — сказали дослідники.

«Можливість виконувати команди віддалено та передавати результати назад на сервер C2 дозволяє зловмиснику контролювати заражену систему, викрадати конфіденційну інформацію або виконувати додаткові шкідливі програми». ***(Military-themed Email Scam Spreads Malware to Infect Pakistani Users // The Hacker News (https://thehackernews.com/2024/06/military-themed-emails-used-to-spread.html). 21.06.2024).***

***

«Двадцять два громадянина Китаю визнали себе винними у скоєнні кіберзлочинів у Замбії.

Вони серед 77 підозрюваних, які були заарештовані у квітні у зв'язку з тим, що влада назвала «складним інтернет-шахрайським синдикатом».

Напад на керовану Китаєм компанію в столиці Лусаці стався після тривожного зростання випадків інтернет-шахрайства в країні, націлених на людей у всьому світі.

Місцеві ЗМІ повідомляють, що вирок громадянам Китаю буде винесено в п'ятницю.

У квітні Комісія з боротьби з наркотиками (DEC) повідомила, що у квітні почастішали випадки, коли замбійці втрачають гроші зі своїх мобільних і банківських рахунків через схеми відмивання грошей, які поширюються на інші іноземні країни.

Люди в таких країнах, як Сінгапур, Перу, Об’єднані Арабські Емірати (ОАЕ) та інших країнах Африки, також стали об’єктами онлайн-шахрайства, заявила влада Замбії.

Десятки молодих замбійців також були заарештовані після того, як нібито були завербовані агентами колл-центру для шахрайства, включаючи інтернет-шахрайство та онлайн-шахрайство, DEC повідомила під час арештів.

Після судового розгляду, який тривав кілька тижнів, 22 громадянина Китаю, включно з однією жінкою, визнали себе винними за трьома пунктами звинувачення: введення в оману, пов’язане з використанням комп’ютера, злочини, пов’язані з ідентифікацією, і незаконна експлуатація мережі або служби.

22 осіб разом із громадянином Камеруну були звинувачені в маніпулюванні особистими даними людей в Інтернеті з метою обману.

Обвинувачені обіймають різні посади в керованій Китаєм Golden Top Support Services, компанії, яка потрапила в центр рейду.

Компанія, розташована в Ромі, елітному передмісті Лусаки, поки не коментує звинувачення.

Лі Сяньліня, якого вважають директором компанії, звинуватили в експлуатації мережі без ліцензії від влади Замбії.

У вівторок державний прокурор звернувся до суду з проханням надати більш детальну інформацію про висунуті обвинувачення.

Громадянам Замбії було висунуто звинувачення в квітні та відпущено під заставу, щоб вони могли допомогти владі в розслідуванні.

Влада заявила, що причетним замбійцям було доручено «вступити в оманливі розмови з нічого не підозрюючими мобільними користувачами на різних платформах, таких як WhatsApp, Telegram, чати та інші, використовуючи сценарії діалогів».

Серед вилученого обладнання були пристрої, що дозволяють абонентам маскувати своє місцезнаходження, і тисячі SIM-карт.

Під час рейду було виявлено 11 SIM-боксів - це пристрої, які можуть направляти дзвінки через справжні телефонні мережі.

Більше 13 000 SIM-карт, як місцевих, так і іноземних, також було конфісковано, що демонструє «масштаб операції», згідно з DEC.

Під час рейду було конфісковано дві одиниці вогнепальної зброї та близько 78 патронів, а також вилучено два автомобілі, що належали громадянину Китаю, пов’язаному з бізнесом». ***(Wycliffe Muia. Chinese nationals ran cybercrime syndicate from Zambia // BBC (https://www.bbc.com/news/articles/c999dyxenx0o?utm_source=flipboard&utm_content=BBCNews%2Fmagazine%2FWorld). 05.06.2024).***

***

«Влада Іспанії заарештувала 22-річного хлопця, якого вважають відомою фігурою хакерської групи Scattered Spider, яка за останні два роки атакувала сотні організацій.

Групу підозрюють у відповідальності за атаку, яка поставила на коліна MGM Resorts у 2023 році, а також за резонансні зломи в Twilio, LastPass, Gitlab, Apple, Walmart тощо.

15 червня іспанські ЗМІ повідомили, що місцева влада за сприяння ФБР заарештувала хакера в Пальма-де-Майорка під час спроби сісти на рейс до Італії.

Murcia Today повідомила, що, за даними поліції Пальми, на момент арешту підозрюваний контролював біткоїни на суму 27 мільйонів доларів.

Джерела, знайомі з розслідуванням, повідомили KrebsOnSecurity, що підозрюваним був 22-річний житель Данді, Шотландія, на ім'я Тайлер Бьюкенен. Відомий хакер, Б’юкенен потрапив під номер 64 у 100 найдосконаліших майстрів заміни SIM-карт згідно з телеграм-каналом, присвяченим шахрайству.

Згідно з темним веб-монітором vx-underground, вважається, що Бьюкенен був «ключовим компонентом» атаки програм-вимагачів MGM Resorts і пов’язаний з кількома іншими найвідомішими атаками групи.

Це другий великий арешт, спрямований на групу Scattered Spider у 2024 році після того, як іншого видатного члена, Майкла Ноа Урбана, заарештували в січні та звинуватили в крадіжці понад 800 000 доларів США в криптовалюті щонайменше у п’яти різних жертв у період із серпня 2022 року до березня 2023 року.

І Б’юкенен, і Урбан належать до вікового діапазону 19-22 років, який зазвичай пов’язаний із філіями групи Scattered Spider, яка вважається компонентом більшої глобальної хакерської мережі, відомої як «Спільнота» або «Com».

Com добре відомий тим, що приймає хакерів з різних організацій, які потім хваляться різними атаками, які вони здійснили, і методами соціальної інженерії, які вони при цьому використовували.

Подвоєні зусилля, щоб знищити Scattered Spider, показують результати

У травні 2024 року ФБР оголосило про придушення організації, а дослідники повідомили, що група стоїть за кампанією атак на страхові компанії з квітня.

Відтоді два резонансних арешти Урбана, а тепер і Б’юкенена, свідчать про досягнення певного успіху у своїх починаннях. Але експерти не думають, що це

означатиме кінець зловмисній діяльності групи, і нові лідери чекають свого часу, щоб заповнити порожнечу.

У розмові з ITPro Джаввад Малік, провідний захисник безпеки в KnowBe4, сказав, що він очікує, що колектив продовжить працювати, незважаючи на втрату двох ключових фігурантів за короткий проміжок часу.

«Арешт видатної особи, безсумнівно, є перемогою для правоохоронних органів і завдає удару по діяльності угруповання, але навряд чи означає кінець зловмисної діяльності Scattered Spider. Організації кіберзлочинців, подібно до міфічної гідри, мають тенденцію проростати нові голови, коли одну відрізають». — пояснив він.

«Кіберзлочинці часто характеризуються дифузною та децентралізованою структурою. Арешт Б'юкенена, безсумнівно, порушить операції, але відсутність єдиного ватажка часто означає, що хтось інший готовий вирватися в порожнечу. Це робить такі групи стійкими до збоїв.

Малік також зазначив, що члени таких груп, як Scattered Spider, як правило, мають довготривалі зв'язки в ширшій спільноті кіберзлочинців і зможуть об'єднати знання та ресурси, щоб продовжувати вчиняти атаки.

«Техніки та інструменти, якими користуються ці угруповання, наприклад обмін SIM-картками, часто широко поширені серед кіберзлочинців. Ці знання не зникають після арешту кількох осіб. Навчальні посібники, форуми та темні веб-майданчики гарантують, що ці методи можуть увічнити та вдосконалити інші», – сказав він.

«Члени таких груп, як Scattered Spider, часто є частиною більш широких кіберспільнот. Навіть за ключових арештів колективні знання та ресурси, доступні іншим учасникам, означають, що операції можуть тривати».

Таким чином, Малік передбачив, що хоча ми можемо очікувати, що група повернеться після періоду зниження активності, поки вони реорганізують свою діяльність.

«У короткостроковій перспективі ми можемо очікувати певного зриву. Арешти змусять Розсіяного Павука перегрупуватися та реорганізуватися.

Можливо, буде тимчасове скорочення їх діяльності, оскільки нове керівництво бере кермо та переглядає свої стратегії». ***(Solomon Klappholz. Alleged Scattered Spider ringleader taken down in Spain after law enforcement crackdown // Future US, Inc. (https://www.itpro.com/security/cyber-crime/alleged-scattered-spider-ringleader-taken-down-in-spain-after-law-enforcement-crackdown?utm_source=flipboard&utm_content=ITPro2019%2Fmagazine%2FNews). 17.06.2024).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Наразі хакери використовують уразливості в трьох дуже популярних плагінах WordPress, включаючи WP Meta SEO, WP Statistics і LiteSpeed Cache, за даними дослідників безпеки.

Будучи однією з найпопулярніших платформ веб-контенту у світі, WordPress завжди в центрі уваги, особливо через плагіни. Як і будь-яке програмне забезпечення, плагіни можуть мати вразливості, і в більшості випадків, особливо у важливих, розробники швидко виправляють проблеми безпеки.

На жаль, наявність виправлення вразливості не означає розгортання цього виправлення. Власники веб-сайтів іноді затримують установку останніх виправлень, а це саме те, на що звертають увагу хакери, коли шукають жертв.

Дослідники з безпеки з Fastly виявили, що три вразливості високого ступеня серйозності, CVE-2024-2194, CVE-2023-6961 і CVE-2023-40000, наразі є ціллю концентрованої атаки. Усі ці вразливості дуже нові, але вже є доступні виправлення, які виправляють проблеми,

«Ці вразливості містяться в різних плагінах WordPress і є схильними до неавтентифікованих атак із збереженим міжсайтовим сценарієм (XSS) через

неналежну обробку вхідних даних і вихідних даних, що дає змогу зловмисникам вводити шкідливі сценарії», — пояснили дослідники.

«Корисне навантаження атаки, яке ми спостерігаємо, спрямоване на ці вразливості, вводить тег сценарію, який вказує на обфускований файл JavaScript, розміщений у зовнішньому домені».

Роль сценарію проста: допомагати зловмисникам створювати нові облікові записи адміністраторів, впроваджувати бекдори на веб-сайти та допомагати злочинцям контролювати заражені веб-сайти.

Впливає на плагін WP Statistics (версія 14.5 і раніше), плагін WP Meta SEO (версія 4.5.12 і раніше) і плагін LiteSpeed Cache (версія 5.7.0.1 і раніше). Веб-сайти, які використовують ці плагіни, нараховуються мільйонами, і значна частина використовує вразливі старіші версії.

Веб-адміністраторам рекомендується оновити всі плагіни до останніх версій і видалити будь-які папки, які могли бути створені старішими ітераціями плагінів. Звичайно, аудит прав користувачів та інші подібні проблеми також бажані разом із перевіркою всіх файлів на наявність ін’єктованого коду». ***(Silviu STAHIE. Hackers Are Targeting Millions of WordPress-Based Websites Through Known Vulnerabilities // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/hackers-are-targeting-millions-of-wordpress-based-websites-through-known-vulnerabilities/?utm_source=flipboard&utm_content=other%2F). 04.06.2024).***

***

«Великі технологічні компанії, такі як Apple, зазвичай використовують програми винагород за безпеку, щоб заохотити дослідників і хакерів знаходити вразливості та повідомляти про них, а не продавати їх зловмисникам, часто державам, які можуть ними скористатися.

«Ми знайшли вразливості нульового дня, нульового кліку, передали всю інформацію в Apple і виконали корисну роботу», — сказав Дмитро Галов, керівник російського дослідницького центру «Лабораторії Касперського», російському

інформаційному агентству RTVI. «По суті, ми повідомили їм про вразливість, за яку вони повинні заплатити винагороду за баг».

Галов навіть запропонував Касперському пожертвувати винагороду на благодійність, але Apple відхилила це, пославшись на внутрішню політику без пояснень. Нерідкі випадки, коли дослідницькі фірми жертвують винагороди від великих компаній на благодійність. Дехто сприймає це як розширення своїх етичних зобов'язань, але це, безсумнівно, сприяє позитивній репутації в середовищі безпеки.

«З огляду на те, скільки інформації ми їм надали і наскільки активно ми це робили, незрозуміло, чому вони прийняли таке рішення».

У 2023 році Касперський публічно оприлюднив передбачувану дуже складну шпигунську кампанію, коли виявив аномалії в десятках iPhone у своїй мережі. Її назвали Operation Trigulation, яка стала найскладнішою атакою на iOS, яку будь-коли створювали.

Атака використовувала серію з чотирьох уразливостей нульового дня, об'єднаних разом, щоб створити експлойт без кліків. Це дозволяло зловмисникам підвищувати привілеї та виконувати віддалений код на скомпрометованих iPhone. Користувачі навіть не підозрюють, що їх пристрій заражений, оскільки шкідливе програмне забезпечення передає конфіденційні дані, включаючи записи з мікрофона, фотографії та геолокацію, на сервери, контрольовані зловмисником.

Касперський не тільки виявив кампанію, але й його дослідницька лабораторія реверсивно спроектувала одну з уразливостей у ланцюжку атак, відстежувану як CVE-2023-38606. Вони виявили, що ядро в основі операційної системи iOS використовувалося для виконання довільного коду та підвищення привілеїв користувачів. Apple була повідомлена, і незабаром компанія випустила екстрені патчі безпеки, посилаючись на команду Kaspersky, яка виявила недолік.

Відповідно до програми Apple Security Bounty Program винагорода за виявлення таких вразливостей може досягати 1 мільйона доларів. Вкрай важливо зберегти цю винагороду, оскільки неповідомлені нульові дні iOS можуть продаватися значно на північ від мільйона доларів у куточках темної мережі.

Незважаючи на те, що Kaspersky є багатонаціональною компанією, її було засновано та розташовано в Росії, країні, до якої Сполучені Штати ввели жорсткі санкції через війну в Україні. Це може серйозно обмежити фінансові операції між американськими компаніями та компаніями в регіоні.

Крім того, згідно з умовами Apple Security Bounty, «нагороди Apple Security Bounty не можуть бути виплачені вам, якщо ви перебуваєте в будь-якій країні, на яку поширюється ембарго США, або внесені до списку спеціально визначених громадян Міністерства фінансів США, списку заборонених осіб Міністерства торгівлі США або Entity List або будь-які інші обмежені партійні списки»…» ***(Arin Waichulis. Security Bite: Apple refused to pay bounty to Kaspersky for uncovering vulnerability part of 'Operation Triangulation' // 9to5 (https://9to5mac.com/2024/06/09/security-bite-apple-refused-to-pay-bounty-to-kaspersky-for-uncovering-vulnerability-part-of-operation-triangulation/?utm_source=flipboard&utm_content=user%2F9to5mac). 09.06.2024).***

***

«Група ізраїльських дослідників вивчила безпеку маркетплейсу Visual Studio Code і зуміла «заразити» понад 100 організацій, троянізувавши копію популярної теми «Dracula Official» для включення ризикованого коду. Подальше дослідження ринку VSCode виявило тисячі розширень з мільйонами інсталяцій.

Visual Studio Code (VSCode) - це редактор вихідного коду, опублікований Microsoft, який використовується багатьма професійними розробниками програмного забезпечення по всьому світу.

Microsoft також управляє ринком розширень для IDE, який називається Visual Studio Code Marketplace, що пропонує доповнення, які розширюють функціональність програми та надають більше можливостей для налаштування.

Попередні звіти висвітлювали прогалини в безпеці VSCode, що дозволяло уособлювати себе за розширенням і видавцем, а також розширення, які викрадають

маркери автентифікації розробника. Були також знахідки в дикій природі, які підтверджено як шкідливі.

Типосквотинг на тему Дракули

Для свого недавнього експерименту дослідники Аміт Ассараф, Ітай Крук та Ідан Дардікман створили розширення, яке друкує тему «Dracula Official» — популярну колірну схему для різноманітних програм, яку встановлено понад 7 мільйонів на VSCode Marketplace.

Dracula використовується великою кількістю розробників завдяки його візуально привабливому темному режиму з висококонтрастною кольоровою палітрою, яка приємна для очей і допомагає зменшити навантаження на очі під час тривалих сеансів кодування.

Фальшиве розширення, яке використовувалося в дослідженні, було названо «Darcula», і дослідники навіть зареєстрували відповідний домен на «darculatheme.com». Цей домен використовувався, щоб стати перевіреним видавцем на VSCode Marketplace, що додало довіри до підробленого розширення…

Їхнє розширення використовує фактичний код із законної теми Darcula, але також містить доданий сценарій, який збирає системну інформацію, включаючи ім’я хоста, кількість встановлених розширень, ім’я домену пристрою та платформу операційної системи, і надсилає її на віддалений сервер через Запит HTTPS POST…

Дослідники відзначають, що інструменти виявлення та реагування кінцевих точок (EDR) не позначають шкідливий код, оскільки VSCode ставиться поблажливо через те, що він є системою розробки та тестування.

«На жаль, традиційні інструменти безпеки кінцевих точок (EDR) не виявляють цю активність (як ми продемонстрували приклади RCE для вибраних організацій під час процесу відповідального розкриття інформації), VSCode створено для читання багатьох файлів і виконання багатьох команд і створення дочірніх процесів., тому EDR не можуть зрозуміти, чи є діяльність із VSCode законною діяльністю розробника чи шкідливим розширенням». - Аміт Ассараф

Розширення швидко набуло популярності, його помилково встановили кілька цінних цілей, у тому числі публічна компанія з ринковою капіталізацією 483

мільярди доларів США, великі охоронні компанії та національна мережа судових органів.

Дослідники вирішили не розголошувати назви постраждалих компаній.

Оскільки в експерименті не було зловмисного наміру, аналітики лише зібрали ідентифікаційну інформацію та включили розголошення в розширення Read Me, ліцензію та код…

Статус VSCode Marketplace

Після успішного експерименту дослідники вирішили зануритися в ландшафт загроз VSCode Marketplace, використовуючи спеціальний інструмент під назвою ExtensionTotal, який вони розробили, щоб знайти високоризикові розширення, розпакувати їх і ретельно перевірити підозрілі фрагменти коду.

Завдяки цьому процесу вони виявили наступне:

1283 з відомим шкідливим кодом (229 мільйонів встановлень).

8161 спілкуються із жорстко закодованими IP-адресами.

1452 запущені невідомі виконувані файли.

2304, які використовують репозиторій Github іншого видавця, що вказує на те, що вони копіюють.

Нижче наведено приклад коду, знайденого в зловмисному розширенні Visual Studio Code Marketplace, яке відкриває зворотну оболонку для сервера кіберзлочинця…

Відсутність у Microsoft суворого контролю та механізмів перевірки коду на VSCode Marketplace дозволяє зловмисникам здійснювати шалені зловживання платформою, що погіршується, оскільки платформа використовується все частіше.

«Як ви можете судити з цифр, існує безліч розширень, які створюють ризики для організацій на ринку Visual Studio Code», — попередили дослідники.

«Розширення VSCode — це зловживана й викрита вертикаль атак із нульовою видимістю, сильним впливом і високим ризиком. Ця проблема становить пряму загрозу для організацій і заслуговує на увагу спільноти безпеки».

Усі шкідливі розширення, виявлені дослідниками, були відповідально повідомлені в Microsoft для видалення. Однак на момент написання цього

переважна більшість залишається доступною для завантаження через VSCode Marketplace.

Дослідники планують опублікувати свій інструмент ExtensionTotal разом із детальною інформацією про його робочі можливості наступного тижня, випустивши його як безкоштовний інструмент, який допоможе розробникам сканувати своє середовище на наявність потенційних загроз.

BleepingComputer зв’язався з Microsoft, щоб запитати, чи планують вони переглянути безпеку Visual Studio Marketplace і запровадити додаткові заходи, які ускладнять друкарські помилки та видавання себе за іншу особу, але ми не отримали відповіді до моменту публікації». ***(Bill Toulas. Malicious VSCode extensions with millions of installs discovered // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/malicious-vscode-extensions-with-millions-of-installs-discovered/). 09.06.2024).***

***

«Дослідники з кібербезпеки виявили нову вразливість у PHP, яка може дозволити хакерам віддалено запускати шкідливий код.

Уразливість відстежується як CVE-2'24-4577 і описується як уразливість ін'єкції аргументів CGI. На момент публікації він не мав оцінки серйозності, але ми знаємо, що він впливає на всі версії PHP, встановлені в операційній системі Windows, і його було введено, коли команда намагалася виправити інший недолік.

Як пояснили дослідники з DEVCORE, уразливість була представлена під час встановлення виправлень CVE-2012-1823: «Під час впровадження PHP команда не помітила функцію Best-Fit для перетворення кодування в операційній системі Windows», — пояснили вони. «Це недогляд дозволяє неавтентифікованим зловмисникам обійти попередній захист CVE-2012-1823 за допомогою певних послідовностей символів. Довільний код може бути виконаний на віддалених серверах PHP за допомогою атаки з ін’єкцією аргументів».

З тих пір було доступно виправлення, і найперші виправлені версії включають 8.3.8, 8.2.20 і 8.1.29. Користувачам рекомендується негайно застосувати

патч, оскільки є докази того, що зловмисники сканують Інтернет на пошук вразливих кінцевих точок.

Як повідомляє The Hacker News, Shadowserver Foundation вже бачив, як хакери досліджують кінцеві точки на наявність уразливості: «Увага! Ми бачимо кілька IP-адрес, які тестують PHP/PHP-CGI CVE-2024-4577 (вразливість до введення аргументів) проти наших датчиків honeypot, починаючи з сьогоднішнього дня, 7 червня», – заявила некомерційна організація на X. «Уразливість впливає на роботу PHP у Windows».

Крім того, DEVCORE заявив, що всі інсталяції XAMPP у Windows є вразливими за замовчуванням, коли вони налаштовані на використання мов для традиційної китайської, спрощеної китайської чи японської мов. Таким чином, адміністратори повинні замінити застарілий PHP CGI на щось на зразок Mod-PHP, FastCGI або PHP-FPM:

«Ця вразливість неймовірно проста, але це також робить її цікавою», — сказали дослідники. «Хто б міг подумати, що патч, який перевірявся та підтверджувався безпечним протягом останніх 12 років, можна обійти через незначну функцію Windows?» ***(Sead Fadilpašić. PHP code could be easily exploited to let hackers target Windows servers // Future US, Inc. (https://www.techradar.com/pro/security/php-code-could-be-easily-exploited-to-let-hackers-target-windows-servers). 10.06.2024).***

***

«Розповсюджувачі зловмисного програмного забезпечення використовують інсталятори MSI, оскільки ОС Windows уже довіряє їм працювати з правами адміністратора в обхід засобів безпеки.

З цієї причини файли MSI є зручним засобом розповсюдження програм-вимагачів, шпигунських програм та іншого шкідливого програмного забезпечення, яке можна видати за встановлення справжнього програмного забезпечення.

Дослідники кібербезпеки з Intezer нещодавно виявили, що зловмисне програмне забезпечення SSLoad використовує інсталятори MSI, щоб запустити ланцюжок доставки.

Зловмисне програмне забезпечення SSLoad використовує інсталятор MSI

Проникнення в систему, збір інформації та доставка корисного навантаження – це деякі з операцій, у яких бере участь SSLoad, тихе шкідливе програмне забезпечення…

Активна кампанія з використанням SSLoad нещодавно включала документ Word-приманку, що містив SSLoad DLL, який виконував Cobalt Strike, і фішинговий електронний лист, що веде до підробленої сторінки Azure, яка завантажила сценарій JavaScript, а також програму встановлення MSI для завантаження корисного навантаження SSLoad.

З квітня 2024 року SSLoad націлюється на жертв, і його численні методи доставки натякають на те, що він використовується для цілей MaaS, отже, показуючи, наскільки він може бути універсальним.

Дослідники. проаналізували інсталятор MSI, який ініціює ланцюжок доставки з кількома завантажувачами, зрештою розгортаючи остаточне корисне навантаження SSLoad.

Перший PhantomLoader — це 32-бітна C/C++ DLL, яка використовує методи самозміни та дешифрування XOR для злому наступного етапу завантажувача.

Цей другий завантажувач завантажує корисне навантаження SSLoad, 32-бітну Rust DLL. SSLoad розшифровує URL-адресу каналу Telegram, яка використовується як мертва точка для отримання адреси командно-контрольного сервера.

Декодер C2 розшифровує адресу C2 та агента користувача та надсилає запит HTTP GET для завантаження наступного етапу корисного навантаження з сервера C2.

Цей варіант SSLoad використовує спеціальний метод для розшифровки рядків за допомогою алгоритму RC4. Кожен рядок зашифровано власним окремим ключем, який зберігається поруч із ним.

Ключ виводиться з перших 6 і останніх 7 байтів закодованого блоку. Після обчислення довжини зашифрованого рядка він декодується за допомогою Base64 і розшифровується за допомогою RC4 за допомогою похідного ключа, вилучаючи URL-адресу каналу Telegram.

Корисне навантаження — це ще один файл Rust, який створює м'ютекс для антианалізу, перевіряє налагодження, динамічно завантажує бібліотеки DLL і отримує постійні ключі XOR за допомогою арифметичних операцій для унікального декодування рядків.

Окрім цього, він використовує RtlGenRandom для унікального іменування папок, динамічно розв'язує виклики бібліотеки шляхом хешування імен модулів і функцій і використовує загальні методи зловмисного програмного забезпечення, як-от маніпулювання PEB для уникнення.

Відбиток JSON надсилається на C2 за допомогою HTTP POST, і Load робить HTTP-запит, що містить ідентифікатор хоста.

Клієнт перевіряє доступні завдання, надсилаючи запит на публікацію з унікальним ідентифікатором хоста SSLoad.

Залежно від доступності завдання C2 відповідає зашифрованою структурою завдання у форматі RC4 і base64 із командою (лише «exe» наразі використовується для завантаження корисних даних) і аргументами.

Він також демонструє, наскільки складним він може бути, як показано в його використанні завантажувача Rust, який складається з динамічного розшифровки рядків і нового завантажувача, який містить механізм захисту від помилок.

Для ефективної боротьби з такими складними кампаніями зловмисного програмного забезпечення потрібен постійний моніторинг і вдосконалене виявлення загроз». ***(Tushar Subhra Dutta. SSLoad Malware Employs MSI Installer To Kick-Start Delivery Chain // GBHackers (https://gbhackers.com/ssload-malware-msi-installer/). 11.06.2024).***

***

«Експерти з кібербезпеки спостерігають тривожне збільшення використання вразливостей нульового дня, особливо проти мережевих пристроїв. Ця тенденція продовжує посилюватися у 2024 році, створюючи значні проблеми, сказав Крістіан Бік, старший директор відділу аналітики загроз у Rapid7. Більше 60% уразливостей, проаналізованих Rapid7 в мережі і Пристрої безпеки у 2023 році використовувалися як нульові дні, сказав він, посилаючись на нещодавній щорічний звіт розвідки Rapid7.

Бік сказав, що високі викупи дозволяють суб'єктам загроз купувати експлойти нульового дня, збільшуючи потенційну шкоду. «Ми дозволяємо суб'єктам загроз купувати нульові дні, і це лякає», — сказав він. Організації повинні запровадити надійні механізми виявлення, враховуючи відсутність традиційних заходів безпеки на мережевих пристроях.

«Ці пристрої повинні захищати наші мережі, але ви не можете встановити на них AV-клієнт, або EDR-клієнт, або запитати у пристроїв якісь химерні журнали про те, що відбувається на самому пристрої», — сказав Бік. «Вони були призначені лише для того, щоб не допустити злих хлопців і дозволити трафіку правильно входити та виходити. Ця відсутність видимості є величезною проблемою».

У цьому відеоінтерв'ю з Information Security Media Group на Infosecurity Europe 2024 Бік обговорив:

Сплеск експлойтів нульового дня, націлених на мережеві пристрої;

Тенденції програм-вимагачів і роль високих викупних платежів у фінансуванні покупок нульового дня;

Необхідність покращення стратегій виявлення та реагування.

Бік має більш ніж 20-річний досвід керівництва дослідженнями кібербезпеки, збору розвідувальних даних і аналізу даних. У Rapid7 він проводить стратегічні дослідження зі збору даних про загрози та винаходу нових методів дослідження». ***(Mathew J. Schwartz. Zero-Day Exploits and Ransomware Trends for 2024 // Information Security Media Group, Corp. (https://www.cuinfosecurity.com/zero-day-exploits-ransomware-trends-for-2024-a-25535). 17.06.2024).***

***

«Представник уряду Великої Британії у вівторок розхвалив потенціал процесора, розробленого для запобігання кібератакам на основі пам'яті, навіть визнавши комерційні перешкоди для його широкого впровадження.

Згідно з документом дослідників CHERI 2021 року, розроблений за підтримки урядів Великобританії та США, Capability Hardware Enhanced RISC Instructions (скорочено CHERI) забезпечує «точний захист пам'яті та масштабоване програмне забезпечення».

«Замість того, щоб дозволити користувачеві програмного забезпечення знайти способи уникнути атаки, CHERI намагається зменшити площу атаки», — сказав Джон Гудакр, директор ініціативи Digital Security by Design уряду Великобританії, під час основної доповіді на Infosec Europe

«Ідея така: якщо ми змінимо спосіб доступу комп'ютера до пам'яті, тоді ми виправимо мільярди й мільярди людей, які повинні нести відповідальність за своє програмне забезпечення», — сказав він. Однією з поширених цифр є те, що приблизно 7 із 10 кібератак пов'язані з проблемами безпеки пам'яті.

Численні уряди закликають IT-індустрію вжити заходів для припинення атак на пам'ять, включаючи перехід від мов програмування C/C++ до безпечних для пам'яті мов, таких як Rust.

Перехід промисловості на CHERI не вимагав би перепрограмування цілих бібліотек коду, щоб вони були безпечними для пам'яті, сказав Пітер Нойман, комп'ютерний науковець, який є головним розробником архітектури.

CHERI «заважає вам виконувати будь-що, що не входить до стеку [програмного забезпечення]», — сказав він Information Security Media Group у короткому інтерв'ю. За його словами, CHERI контролює створення покажчиків пам'яті програмним забезпеченням, дотримуючись обмежень і авторизованого використання. Існуючі бібліотеки C дійсно потребують перекомпіляції, щоб

функціонувати на архітектурі, сказав він, але наявні перетворення показують, що лише близько 2% коду потрібно змінити.

Нойманн також сказав, що назва архітектури є дещо неправильним - хоча вперше вона була розроблена для архітектури RISC, дослідники протестували реалізації x86. "Це боляче, але це працює", - сказав він.

Незважаючи на переваги чіпа, Goodacre сказав відвідувачам конференції, що ключовою проблемою є комерційне розширення проекту, що вимагає від компаній оновлення існуючої операційної системи та програмного забезпечення. Британський виробник напівпровідників Arm на початку 2022 року зробив демонстраційні плати з використанням архітектури CHERI.

«Ми отримуємо багато позитивних відгуків», — сказав Річард Ґрізентвейт, головний архітектор і співробітник Arm, парламентському комітету Великобританії у квітні. «Люди шукають, як це можна комерційно розгорнути, але на даний момент ми не на цьому етапі».

Основною перешкодою, як заявила Microsoft у дописі в блозі 2022 року, є вимога перекомпіляції. «Ніхто не хоче модифікувати свій код (потенційно інвазивними способами) для підтримки архітектури без промислової тяги, і ніхто не хоче поставляти [архітектуру набору інструкцій] без програмного забезпечення».

Німецька компанія з розробки процесорів Codasip є єдиною компанією, яка пропонує комерційне рішення CHERI. Він почав ліцензувати чіпи RSIC-V з CHERI у жовтні». ***(Akshaya Asokan. UK Official Touts CHERI for Memory-Safe Computing // Information Security Media Group, Corp. (https://www.databreachtoday.com/uk-official-touts-cheri-for-memory-safe-computing-a-25421?utm_source=flipboard&utm_content=other). 05.06.2024).***

***

«Програми VPN для Android підвищують конфіденційність і безпеку в Інтернеті, оскільки дані підключення зашифровані, що унеможливлює доступ хакерів або інших сторін до даних зв’язку.

Вони також допомагають розблокувати регіонально-обмежений вміст через приховування IP-адреси, підтримують анонімність в Інтернеті та захищають безпечну інформацію ще більше під час використання незахищеного Wi-Fi.

Дослідник кібербезпеки Саймон Мільяно з Top10VPN нещодавно виявив, що у безкоштовних VPN для Android виникають збої шифрування.

Помилки шифрування безкоштовних VPN

У цьому дослідженні розглядаються проблеми конфіденційності та безпеки безкоштовних додатків VPN, підбадьорені зростаючою тенденцією обмежень Інтернету, встановлених урядом у всьому світі, і подальшим зверненням до віртуальних приватних мереж (VPN)…

З 2018 року загальна кількість установок 100 найпопулярніших безкоштовних VPN для Android різко зросла з 260 мільйонів до понад 2,5 мільярдів.

Це поглиблене дослідження оцінило ризики конфіденційності та безпеки, пов’язані зі 100 найпопулярнішими безкоштовними програмами Android VPN, які зібрали понад 2,5 мільярда загальних установок через зростання глобального попиту.

Тестуючи кожну програму на окремих пристроях, використовуючи різні інструменти в ізольованому середовищі, дослідження виявило шокуючі недоліки в шифруванні, витоку даних і функціях, що порушують конфіденційність, у кодах цих програм.

Найважливіше те, що було виявлено, що більшість із них відкрито ділилися особистою інформацією користувачів безпосередньо з такими фірмами, як «Яндекс» і «Bytedance», що, отже, демонструє протиріччя між обслуговуванням людей без стягнення з них плати та захистом справжньої мети конфіденційності VPN.

Для тих, хто не може дозволити собі платити за VPN, можна знайти хороші безкоштовні, провівши ретельне дослідження. Однак доступні платні варіанти більш надійні.

Тести виявили тривожні недоліки шифрування та витік даних серед усіх 100 безкоштовних програм VPN.

11 зазнали повномасштабних збоїв у процесі шифрування, трохи більше третини застосували неадекватну форму шифрування, і лише деякі використовували найкращі алгоритми хешування або TLS 1.3.

Це сталося через 88 витоків інформації, у тому числі 83, які розкривали запити D N S, і 79, які не тунелювали весь трафік. Більше половини цих програм страждали від нестабільності з'єднання.

Комплексне дослідження вразливостей конфіденційності та безпеки користувачів, проведене за допомогою аналізу трафіку Wireshark в унікальному тестовому середовищі, виявило такі численні вразливості.

Нижче ми згадали назви цих 11 VPN:

- Інжектор HTTP
- Phone Guardian VPN
- Приватний VPN
- Топ VPN
- PotatoVPN
- Swift VPN
- Приватний VPN-браузер Tenta
- Maple VPN
- GoFly VPN
- Захищений браузер AVG
- VPN Сатоші

Було виявлено, що 11 програм взагалі не мають шифрування, що, як наслідок, викриває діяльність веб-переглядача.

Багато з цих витоків даних були широко поширеними, 83 з них викликали витік DNS-запитів і лише 79 могли тунелювати весь трафік.

Крім того, багато досліджених програм (96) містили код, який потенційно впливає на конфіденційність, але деякі мали відстеження місцезнаходження першої сторони разом із дозволами.

Більше занепокоєння викликали ті, у яких було 12 додатків, включаючи сторонній код відстеження точного місцезнаходження та дозволи; деякі навіть відстежують у фоновому режимі.

Основними причинами серйозних проблем із конфіденційністю були такі SDK, як ByteDance, Yandex і Facebook, вбудовані в популярні програми.

Загалом протягом цього тестового періоду 71 програма поділилися особистою інформацією, поки їх VPN ще працював». ***(Tushar Subhra Dutta. Free Android VPNs Suffering Encryption Failures, New Report // GBHackers (https://gbhackers.com/free-android-vpns-encryption-failures/). 10.06.2024).***

***

«Argus Cyber Security співпрацює з Microsoft для створення наскрізної платформи наступного покоління для автомобільної та мобільної безпеки.

Платформа Argus Vehicle Security Platform складається з двох інтегрованих рішень, які поєднують портфоліо автомобільної кібербезпеки Argus із надійною розробкою програмного забезпечення та продуктами безпеки від Microsoft, однієї з найбільш інноваційних технологічних компаній у світі та лідера GenAI.

В останні роки виробники транспортних засобів усвідомили важливість програмно-визначених транспортних засобів (SDV) та інтеграції заходів безпеки на ранніх етапах процесу розробки. Цей підхід до безпеки «зрушення вліво» дозволяє розробникам автомобільного програмного забезпечення підвищити загальну якість і безпеку своїх продуктів, водночас прискоривши час виходу на ринок і зменшивши витрати на розробку.

Платформа безпеки Argus Vehicle Security Platform наступного покоління використовує принципи «зрушення вліво», щоб допомогти виробникам оригінального обладнання та постачальникам рівня 1 вирішити складні проблеми в розробці та захисті підключених програмно-визначених транспортних засобів (SDV), а також забезпечити керування даними та відповідність. Він складається з двох інтегрованих рішень, розроблених для того, щоб допомогти автовиробникам

забезпечити майбутнє мобільності: Automotive Shift-Left Security і Automotive Security Lifecycle Management.

«Бачення Microsoft у поєднанні з досвідом Argus у сфері кібербезпеки автомобілів і пропозиціями продуктів допоможуть прискорити трансформацію циклу розробки автомобільного програмного забезпечення», — сказав Ран Іш-Шалом, віце-президент із продуктів і стратегії Argus. «Ця співпраця зосереджена на розробці нових передових платформ безпеки та розробки, щоб відповідати зростаючим вимогам автовиробників щодо безпеки, управління даними та відповідності вимогам у найближчі роки».

«Поєднуючи досвід Argus Cyber Security у захисті підключених транспортних засобів із можливостями Microsoft Azure AI, новими методологіями розробки програмного забезпечення та ланцюжками інструментів, а також широким портфоліо продуктів кібербезпеки, ми маємо унікальну можливість прискорити інновації безпеки «зсув ліворуч» у всьому автомобільному секторі», - сказав Домінік Ві, корпоративний віце-президент з виробництва та мобільності Microsoft. «Це співробітництво призведе до створення нових інструментів кібербезпеки на основі ШІ, які принесуть користь як водіям, так і автовиробникам».

Рішення «Automotive Shift-Left Security» покращує нещодавно запущену платформу Argus DevSecOps для розробки автомобільного програмного забезпечення на Microsoft Azure шляхом інтеграції передових інструментів розробки програмного забезпечення від Microsoft, включаючи Microsoft Threat Modeling Tool і Microsoft Azure OpenAI Service.

Це рішення використовує Azure OpenAI Service, щоб перенести потужність генеративного штучного інтелекту в автомобільні програми для DevSecOps із масштабом і безпекою Azure. Крім того, відкрита конструкція платформи дозволяє легко інтегрувати її з іншими інструментами, якщо це необхідно, щоб захистити транспортні засоби протягом усього терміну служби.

Друге рішення, відоме як «Automotive Security Lifecycle Management», об’єднує продукт Argus XDR для виявлення загроз і реагування на них для автомобільної промисловості на Azure з надійними операціями безпеки та

інструментами управління від Microsoft, зокрема Microsoft Sentinel, Defender for Cloud, Defender Threat Intelligence та Azure OpenAI. Сервіс. Інтегроване рішення надає автовиробникам комплексне управління безпекою на всіх трьох етапах життєвого циклу автомобіля». ***(Argus Cyber Security and Microsoft partner to secure automotive fleets throughout the vehicle lifecycle // Help Net Security (https://www.helpnetsecurity.com/2024/06/17/argus-cyber-security-microsoft-collaboration/). 17.06.2024).***

***

«У п'ятницю компанія з кібербезпеки Kaspersky заперечила, що є загрозою безпеці після того, як Міністерство торгівлі США заборонило використання її програмного забезпечення в Сполучених Штатах.

Московська компанія, генеральний директор якої Євген Касперський проживає в Росії, заявила, що це рішення не вплине на її здатність продавати та просувати свої продукти кібербезпеки та навчання в США.

Касперський сказав, що уряд обґрунтував своє рішення «геополітичним кліматом і теоретичними проблемами», а не незалежною перевіркою наявності ризику.

Уряд каже, що зв'язки Касперського з Росією означають, що компанія становить «невиправданий або неприйнятний ризик для національної безпеки США або безпеки».

Департамент заявив, що розглянув заперечення Касперського проти початкових висновків розслідування про те, чи становлять продукти або послуги загрозу, і визнав рішення про заборону його програмного забезпечення «добре обґрунтованим».

Окрім зобов'язань компанії дотримуватися російських законів, її програмне забезпечення можна використовувати для ідентифікації конфіденційних даних громадян США та надання їх уряду Росії, повідомило Міністерство торгівлі». ***(Cybersecurity Firm Kaspersky Denies It is a Hazard // Bridge News LLC***

(https://www.newsnetmedia.com/story/50932726/cybersecurity-firm-kaspersky-denies-it-is-a-hazard). 21.06.2024).

***

«Фонд Dfinity представив нову платформу на базі Інтернет-комп'ютерного протоколу (ICP), призначену для заміни традиційних засобів кібербезпеки.

Згідно з прес-релізом, поширеним Cointelegraph, платформа, яка отримала назву Utopia, є приватною безсерверною хмарною інфраструктурою, розробленою для державних установ і корпоративних організацій.

Утопія вирішує проблеми

Згідно з прес-релізом, Utopia виступає за нестримні, захищені від втручання, відкриті платформи незалежної автономії.

Utopia забезпечить безпечну роботу штучного інтелекту (AI), дозволить нативне управління цифровими активами та «дозволить урядам досягти суверенітету».

Домінік Вільямс, засновник і головний науковий співробітник Dfinity Foundation, детально розповів про мету платформи в прес-релізі. Він сказав:

«UTOPIA переосмислює обчислення, вирішуючи найбільші виклики IT нашого часу: кібербезпека, стійкість, IT-продуктивність і суверенітет».

Державний суверенітет

Dfinity Utopia має на меті допомогти урядам досягти суверенітету за допомогою штучного інтелекту, але нещодавня відсутність вказівок щодо цифрових активів свідчить про те, що уряди можуть бути не готові або не бажають повністю прийняти цю технологію.

Регуляторна невизначеність, продемонстрована в березні Комісією з цінних паперів і бірж США (SEC) і Комісією з торгівлі товарними ф'ючерсами (CFTC), свідчить про цю перешкоду для урядового впровадження.

У прес-релізі Вільямс представляє Утопію як рішення для державного суверенітету:

«Уряди обережно ставляться до хмарних сервісів, оскільки вони повинні надавати їм конфіденційні дані. UTOPIA пропонує рішення, яке дозволяє їм керувати приватними суверенними хмарами наступного покоління на апаратному забезпеченні рідної країни, яке має кардинальні властивості безпеки».

Зростання загроз кібербезпеці

У прес-релізі наголошується на зростанні загроз кібербезпеці, включаючи атаки програм-вимагачів на лікарні Лондона, які включають майже 400 гігабайт особистих даних пацієнтів.

Відповідно до публікації в блозі IT Governance, у 2024 році 9478 публічно оприлюднених порушень даних розкрили 35,9 мільярда записів, найбільше вплинувши на оборону, комунальні та фінансові послуги.

Utopia прагне протистояти зростанню кіберзагроз шляхом створення «великомасштабних корпоративних обчислень», здатних блокувати «несанкціонований доступ, зміни функціональності, витік даних і встановлення програм-вимагачів». ***(Josh O'Sullivan. Dfinity announces new ICP-powered platform to tackle cybersecurity // Cointelegraph (https://cointelegraph.com/news/dfinity-icp-powered-cybersecurity-platform-launch). 27.06.2024).***

***

«Лідери в галузі кібербезпеки борються зі складністю, дублюванням і сліпими плямами, які виникають через використання багатьох постачальників і інструментів кібербезпеки. Багато продуктів, які пропонують постачальники засобів кібербезпеки, мають можливості, що збігаються, що полегшує виникнення неправильних конфігурацій і ускладнює виявлення прогалин у безпеці. Консолідація продуктів кібербезпеки зменшує цю складність шляхом оптимізації кількості продуктів та їх взаємодії, таким чином підвищуючи ефективність результатів безпеки.

Організації консолідують рішення безпеки з різних причин, наприклад, нижча загальна вартість володіння за рахунок кращої ефективності, покращення стану безпеки за рахунок кращої інтеграції та охоплення засобів контролю або

простота закупівель. Організації, як правило, консолідуються там, де вони можуть дозволити собі усунути найкращі в своєму класі функціональні можливості без істотного зниження ефективності.

Лідери кібербезпеки можуть використовувати наступні три стратегії для досягнення консолідації платформи кібербезпеки.

1. Визначте бажані результати безпеки

Повідомлення мети є таким же важливим, як і виконання вправи на консолідацію. Часто IT-директори та інші керівники бізнесу та технологій пов'язують проект консолідації зі скороченням бюджету. Хоча зниження загальної вартості володіння може виявитися бажаним побічним продуктом цієї роботи, більшість IT-директорів очікують збільшення бюджету на кібербезпеку.

Натомість керівники кібербезпеки повинні консолідуватися для спрощення. Захищений доступ через межу служби безпечного доступу або покращене виявлення через ізольовані технології за допомогою розширеного виявлення та реагування є двома основними проектами консолідації.

2. Оцініть постачальників та інструменти

Керівники кібербезпеки повинні оцінити продукти, які вони зараз використовують, і такі фактори, як функціональні можливості, які вони пропонують, тривалість контракту, поточні витрати та зусилля на підтримку. Потім вони повинні визначити аспекти та можливості, які є важливими в їхній організації. Керівники кібербезпеки також повинні оцінити альтернативні пропозиції щодо конкретних можливостей — деякі продукти, які наразі не використовуються, можуть бути вже доступні з існуючими схемами ліцензування.

Важливо зібрати результати з усіх можливих сфер і зацікавлених сторін. Коли керівники кібербезпеки оцінюють продукти, вони можуть не враховувати важливі можливості, які не відразу видно. Певний продукт може пропонувати, наприклад, досвід керування користувачем або адміністратором або набір існуючих можливостей, які може бути важко замінити; він може запропонувати послугу, за допомогою якої користувач може зв'язатися з постійними експертами постачальника, щоб отримати вказівки з конкретних тем. Знову ж таки,

консолідація — це не лише вправа з економії коштів — вправа з оцінювання має охоплювати ці тонкощі.

Особливо слід оцінити, наскільки складно видалити продукт або наскільки легко його інтегрувати. Часто успішне підтвердження концепції з єдиним хмарним екземпляром продукту, який є перспективним, але його важко розгорнути, призводить до того, що цей продукт ніколи не буде розгорнутий ширше. Під час наступного поновлення його буде видалено через обмежене використання

3. Проаналізуйте результати та визначте проекти

Після визначення поточних і потенційних інструментів кібербезпеки та постачальників їх результати можна проаналізувати. Керівники кібербезпеки повинні визначити обов'язкові продукти, які можуть бути продуктами, які містять унікальні функції або які було б проблематично видалити.

Керівники кібербезпеки також повинні визначити, для яких можливостей у них є декілька продуктів. Можуть існувати продукти від стратегічних постачальників, які можна додати або підтримувати, а також ті, які можна видалити. Подібні міркування можуть допомогти визначити найбільш реалістичні проекти, які слід спочатку розпочати та реалізувати.

Консолідація буде легшою в більш зрілих технологічних областях. І хоча галузь може бути готова до консолідації, не кожна організація досягне такого рівня зрілості. Зазвичай організації консолідуються, коли мають кілька автономних компонентів, які можна консолідувати на платформі, замість того, щоб додавати абсолютно нові функції як частину платформи.

Після того як лідери кібербезпеки визначили та розпочали проект консолідації, вони повинні пам'ятати, що консолідація не є кінцевою вправою. Необхідно враховувати потенційні наступні проекти консолідації та їх сумісність. Лідери з кібербезпеки можуть переконатися, що компоненти, які вони замінюють, мають автономні продукти, які можуть взаємодіяти — наприклад, відкриваючи інтерфейси програмування додатків — з іншими продуктами та постачальниками в майбутньому». ***(Dionisio Zumerle. 3 Actions to Achieve Cybersecurity Consolidation // TechnologyAdvice (https://www.techrepublic.com/article/gartner-cybersecurity-consolidation/). 21.06.2024).***