**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

№ 2 (лютий)

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.– №2 (лютий) . – 253 с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л. Литвинова, С. Дорогих. Дизайн обкладинки С. Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

ЗМІСТ

Стан кібербезпеки в Україні 4
Національна система кібербезпеки 8
Кібервійна проти України 9
Міжнародне співробітництво у галузі кібербезпеки 18
Світові тенденції в галузі кібербезпеки 19
Сполучені Штати Америки та Канада 81
Країни ЄС та Великобританія 93
Австралія та Нова Зеландія 110
Китай 125
Інші країни 126
Кібервійни та протидія зовнішній кібернетичній агресії 133
Створення та функціонування кібервійськ 151
Кіберзахист критичної інфраструктури 152
Кіберзахист закладів охорони здоров'я 160
Захист персональних даних та соціальні мережі 163
Масштабні витоки персональних даних 168
Кібербезпека Інтернету речей. Штучний інтелект 172
Кіберзлочинність та кібертероризм 191
Діяльність хакерів та хакерські угруповування 213
Вірусне та інше шкідливе програмне забезпечення 215
Фішингові атаки 236
Операції правоохоронних органів та судові справи проти кіберзлочинців . 241
Технічні аспекти кібербезпеки 248
Виявлені вразливості технічних засобів та програмного забезпечення 248

«Понад 2000 комп'ютерів в Україні заражені шкідливим програмним забезпеченням DirtyMoe, попереджає РСМД України (CERT-UA).

«У рамках детального вивчення кіберзагрози було проведено дослідження отриманих зразків шкідливих програм, встановлено особливості функціонування серверної інфраструктури управління та виявлено понад 2000 уражених комп’ютерів в українському сегменті CERT-UA в Інтернеті», – йдеться в пораді щодо безпеки.

Червоподібне розповсюдження на скомпрометованих системах

Цей різновид шкідливого програмного забезпечення, вперше помічений у 2016 році, дозволяє зловмисникам здійснювати DDoS-атаки та криптозлом на зламаних пристроях. Експерти з безпеки відзначили, що зловмисне програмне забезпечення може використовувати відомі недоліки безпеки, щоб поширюватися на скомпрометовані системи у формі хробака.

«DIRTYMOE має функціональні можливості для саморозповсюдження шляхом вибору даних автентифікації та/або використання ряду вразливостей як по відношенню до комп’ютерів, розташованих у локальній комп’ютерній мережі, так і комп’ютерів на основі списку IP-адрес, який формується за окремим алгоритмом залежно від на «зовнішніх» IP-адресах ураженого об’єкта», – пояснюють дослідники.

Поєднується з іншими шкідливими програмами для доставки

Історично DirtyMoe використовував штам зловмисного програмного забезпечення під назвою Purple Fox, щоб досягти цільових пристроїв. Що ще гірше, Purple Fox має можливості руткітів, що дозволяє зловмисникам уникнути виявлення та ускладнює видалення.

Іноді зловмисники маскують його під фальшиві інсталятори MSI, такі як Discord, Telegram або інше популярне програмне забезпечення.

Початковий вектор все ще невідомий

Дослідники приписали зловмисну кампанію суб’єктам загрози UAC-0027 і ще не виявили початковий вектор доступу. CERT-UA рекомендує ізолювати

вразливі пристрої, наприклад ті, що працюють із застарілими операційними системами, віртуально чи фізично, а також запроваджувати фільтрацію як для вхідного, так і для вихідного трафіку.

Консультація CERT-UA містить вичерпні технічні відомості про зловмисне програмне забезпечення, індикатори компрометації та розширений список IP-адрес проміжних вузлів керування, пов'язаних із DirtyMoe.

Захист від DirtyMoe та інших шкідливих програм

Спеціалізоване програмне забезпечення безпеки, таке як Bitdefender Ultimate Security, може захистити вас від цифрових загроз, таких як DirtyMoe. Він включає в себе надійні модулі виявлення та захисту, які можуть захистити віруси, руткіти, трояни, хробаки, експлойти нульового дня, шпигунське програмне забезпечення, програми-вимагачі та інші електронні загрози». ***(Vlad CONSTANTINESCU. DirtyMoe Cryptojacking and DDoS Malware Infects Thousands of Ukrainian Computers // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/dirtymoe-cryptojacking-and-ddos-malware-infects-thousands-of-ukrainian-computers/?utm_source=flipboard&utm_content=other%2F). 05.02.2024).***

***

«На Київському міжнародному форумі з кібербезпеки, президент «Київстар» Олександр Комаров повідомив, що після кібератаки компанія змінила «архітектуру того, як компанія побудована всередині».

Компанія перейде на мікросегментацію, як приклад цієї нової системи Комаров назвав білінгову систему, яка знаходилася в окремому домені, тому не постраждала під час хакерської атаки.

Також президент «Київстар» зазначив, що хакерська атака на компанію мала два вектори. Перший вектор був направлений на віртуальну інфраструктуру, другий вектор був направлений на фізичну інфраструктуру.

Перший вектор виявився ефективним на 90%. Другий вектор вийшов менш ефективним, тому що компанія почала досить швидко реагувати, вимкнула всю інфраструктуру та через конфлікт двох атак, тобто одна атака не дала розвиватися іншій». ***(Артем Житкевич. Що змінилося в компанії "Київстар" після***

кібератаки // ГО "Бізтех Медіа" (https://speka.media/shho-zminilosya-v-kompaniyi-kiyivstar-pislya-kiberataki-9dne65). 07.02.2024).

***

«Міністерство оборони України набуває компетентності у галузі кібербезпеки та планує своїми силами розробляти сервіси кіберзахисту для власних систем.

Про це повідомила Катерина Черногоренко, заступниця Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації.

За словами Катерини Черногоренко, це допоможе Міністерству оборони роботи комплексну оцінку рівня захищеності різних систем в структурі Міноборони від кібератак.

Задля забезпечення кібербезпеки Міністерство оборони вже створили Центр кібербезпеки, який 24/7 моніторить системи міністерства та співпрацює з відповідними центрами ЗСУ.

Також Міноборони вважає, що законопроєкт, який дозволить міністерству використовувати іноземні ЦОД задля зберігання даних є надзвичайно важливим». ***(Артем Житкевич. Міноборони України планує самостійно розробляти засоби кібербезпеки для своїх систем // ГО "Бізтех Медіа" (https://speka.media/minoboroni-ukrayini-v7yl03). 08.02.2024).***

***

«Про звільнення директора з кібербезпеки «Київстару» Юрія Прокопенка стало відомо 14 лютого з повідомлення Forbes. Видання пише, що припущення про його звільнення з’явилося ще у січні. Проте, тоді в «Київстар» спростували повідомлення про його можливе звільнення.

Останній робочий день директора з інформаційної безпеки «Київстару» був 31 січня. Звільнення було за згодою обох сторін, повідомив Прокопенко у коментарі Forbes. Тоді ж він змінив статус у соцмережі Linkedin, де вказав, що відкритий до нових пропозицій про роботу. Прокопенко переконує, що звільнення не пов'язано з кібератакою.

«Люди на нашій посаді інколи вигорають», – каже він.

При звільненні компанія, за його словами, не пропонувала йому іншу посаду. Пресслужба компанії повідомила, що «Прокопенко ухвалив рішення продовжити кар'єру за межами компанії».

За словами Прокопенка, з професії йти він не планує — розглядає аналогічні посади в інших великих компаніях і хоче зайнятися вивченням впливу штучного інтелекту на кібербезпеку, квантових обчислень і використання цих технологій у безпілотних системах.

Нагадаємо, у вересні 2023 року Київстар підтвердив надійність систем управління інформаційної безпеки компанії. Національний телеком-оператор успішно пройшов аудит у липні 2023 р. за сертифікацією міжнародного стандарту ISO/IEC 27001:2013.

«За останні роки Київстар багато інвестував у розвиток функції кібербезпеки, щоб відповідати кращим міжнародним стандартам та практикам. Це важливо як для захищеності самої компанії, так і для того, щоб гарантувати надійність та захищеність інформаційних систем клієнтам і партнерам. Щобільше, від початку повномасштабного військового вторгнення ми вдались до серйозних додаткових заходів для гарантування кібербезпеки», заявив тоді Юрій Прокопенко.

А вже 12 грудня, близько шостої ранку в мережі компанії «Київстар» стався масштабний збій. Фактично всі сервіси оператора перестали працювати. Як повідомляв Інформатор, російські хакери перебували всередині системи оператора «Київстар» принаймні з травня 2023 року. Повний доступ зловмисники отримали вже у листопаді. Більш того, росіяни могли вкрасти особисту інформацію абонентів.

Служба безпеки допомогла «Київстару» відновити інфраструктуру та відбитися від наступних кібератак. Схожий інцидент стався рік тому з неназваним оператором зв'язку, однак катастрофи тоді вдалось уникнути. Про це в інтерв'ю Reuters розповів еачальник управління кібербезпеки СБУ Ілля Вітюк». ***(Директор із кібербезпеки Київстар звільнився: в чому причина // Informator***

(https://fin.informator.ua/uk/direktor-iz-kiberbezpeki-kijivstar-zvilnivsya-v-chomu-prichina-2). 15.02.2024).

***

Національна система кібербезпеки

«Відтепер в Україні діятиме новий покращений проект з кібербезпеки BRAMA (БРАМА)

БРАМА - це синергія громадян, приватного та державного секторів у протидії дезінформації та незаконному контенту в інформаційному просторі.

Наші цілі:

Знищення російських осередків в Інтернеті

Зменшення рівня булінгу та цькування в мережі

Протидія наркотикам та шахрайству

Навчання та тренінги з кібергігієни

Просвіта населення щодо інформаційної гігієни

Залучення та мотивація громадян до активної громадянської позиції

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

Що ми пропонуємо учасникам:

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

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

отримати поради щодо медіа та кіберграмотності;

бути поінформованим про небезпечні схеми шахрайств, які ширяться мережею;

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

Станом на січень 2024 року учасниками спільноти заблоковано понад 26 тисяч джерел поширення неприйнятного контенту. Як видно із статистики – роботи ще багато і ми потребуємо допомоги нових небайдужих і активних учасників…» ***(Кіберполіція запрошує долучитись до соціального проєкту BRAMA // Укрінформ (https://www.ukrinform.ua/rubric-society/3830501-kiberpolicia-zaprosue-dolucitis-do-socialnogo-proektu-brama.html). 22.02.2024).***

***

Кібервійна проти України

«Команди цифрової трансформації впродовж чотирьох років втілили низку проектів у сфері кіберзахисту. Про це CDTO та регіональні лідери розповіли під час Міжнародного форуму з кібербезпеки «Стійкість під час кібервійни».

«Кібербезпека — один з ключових напрямів роботи CDTO. Протягом 4 років у регіонах реалізували понад 20 проектів у сфері кіберзахисту. Зокрема, у 2023 році в Полтавській області провели перші регіональні командно-штабні навчання (ТТХ), у Волинській — перші кібер змагання у форматі CTF, а на Черкащині запровадили систему «Безпечна школа». У світлі непередбачуваних загроз кібербезпеки, особливо в умовах війни, важливо розуміти, що захист вимагає поєднання трьох основних складників: людей, процесів та технологій. Наш досвід показує, що навчання й розвиток навичок кібергігієни — вирішальні в боротьбі із загрозами», — зазначив керівник регіональної цифрової трансформації Міністерства цифрової трансформації України Ігор Панченко.

Крім того, під час панельних виступів CDTO та цифрові лідери поділилися планами та розповіли про пріоритетні напрями подальшої роботи. Вони також звернули увагу на кіберзагрози, перед якими вони постали та які превентивні дії застосовують зараз.

Наприклад, Дніпропетровщина має власний центр обробки даних, який забезпечує кіберзахист основних інформаційних ресурсів. CDTO Дніпропетровщини Іван Начовний розповів, що обласна військова адміністрація

(ОВА) проводить навчання для працівників у цій сфері. Зокрема, курс з кіберзахисту для громад та професіоналів у співпраці з компанією Yalantis.

Серед планів Київської ОВА — аудит безпеки в межах співпраці з проектом USAID «Кібербезпека критичної інфраструктури». За словами Андрія Братуся, CDTO Київської ОВА, у планах також провести фахові навчання з кібербезпеки для системних адміністраторів громад Київщини.

У пріоритетах Львівської міської ради — впровадження інструментів для швидкого відновлення IT-інфраструктури та всіх сервісів у разі кібератаки. Водночас начальниця управління інформаційних технологій Львівської міської ради Олена Гунько зауважила, що критично важливим елементом для кіберзахисту є кваліфіковані люди. З кожним роком таких спеціалістів дедалі складніше залучати та втримувати. Зокрема, через конкуренцію за кадри у сфері інформаційних технологій.

На Рівненщині для захисту інформаційних систем установ та закладів розгорнули системи захисту трафіку на входах. Це дало змогу знизити кількість кіберінцидентів, які пов’язані з фішингом та цілеспрямованими атаками кіберзлочинців. Олександр Терещенко, радник голови Рівненської ОВА з питань цифровізації, розповів про плани розширення системи захисту на 64 громади, структурні підрозділи, комунальні заклади та підприємства, а також створення «Регіонального центру забезпечення кіберзахисту».

Серед основних напрямів роботи Миколаївської міської ради — фізична безпека активного та пасивного мережевого обладнання, безпека та стійкість передавання даних і вразливість систем з «білою» IP-адресою. Начальник відділу стандартизації та впровадження електронного урядування Миколаївської міської ради Дмитро Канарський під час Міжнародного форуму з кібербезпеки поділився планами міста на 2024 рік. Зокрема, завданням стане розвиток муніципальної мультисервісної мережі та затвердження нормативно-правової бази, а також навчання й сертифікація посадових осіб.

Нагадаємо, впродовж чотирьох років CDTO успішно впровадили понад 210 унікальних міжгалузевих проектів. Серед них — проекти з кібербезпеки…»

(Стійкість під час кібервійни: які проекти з кібербезпеки втілюють українські регіони // Кабінет Міністрів України (https://www.kmu.gov.ua/news/stiikist-pid-chas-kiberviiny-iaki-proiekty-z-kiberbezpeky-vtiliuiut-ukrainski-rehiony). 14.02.2024).

***

«Розвиток системи підготовки фахівців та професійної сертифікації кадрів в галузі безпеки інформації та кіберзахисту — актуальне завдання для посилення кіберстійкості України. Про це, виступаючи на Київському міжнародному форумі з кібербезпеки, сказав заступник голови Держспецзв'язку Олександр Потій.

Він підкреслив, що повномасштабному вторгненню росії в Україну передували кібератаки на державні, банківські та інші установи, критичну інфраструктуру. Наша країна фактично стала майданчиком російських кібероперацій та набула значного досвіду протидії ворожим атакам у кіберпросторі. Однак, враховуючи тенденції до збільшення таких атак, в Україні відчутний дефіцит кваліфікованих кадрів у сфері кібербезпеки. Одним із базових шляхів розв'язання цієї задачі, є необхідність створення системи професійної підготовки та сертифікації кадрів відповідно до професійних стандартів.

«До 2021 року, в Україні були лише дві професії в галузі кібербезпеки, цього було критично мало для того, щоб відповідати сучасним реаліям інформаційного протиборства у кіберпросторі. Саме тому Держспецзв'язку формує Національну рамку кваліфікації з кібербезпеки України, відтак протягом 2021-2023 років було внесено до державного класифікатора професій – 27 сучасних професій. Також, протягом 2023-2024 року, робочими групами при Держспецзв'язку розроблено 21 відповідний професійний стандарт. Це завдання було виконано, враховуючи потреби ринку праці у сфері інформаційних технологій та їх безпеки», — зазначив заступник голови Держспецзв'язку Олександр Потій.

Формування власної Національної рамки кваліфікації України у сфері кібербезпеки, є складною державною задачею, яка потребує негайних організаційно-правових дій всіх ланок виконавчої влади та всього суспільства в цілому.

Розробка та впровадження Національної рамки кваліфікації у сфері кібербезпеки проводиться Держспецзв'язку у п'ять етапів:

на першому етапі реалізації – у 2022-2023 році до класифікатора професій ДК – 003: 2010 внесені 27 нових професій у сфері кібербезпеки;

другий етап – підготовка професійних стандартів – на січень 2024 року, країна вже має 21 професійний стандарт у сфері кібербезпеки;

третій етап – створення кваліфікаційних центрів, які підтверджуватимуть фаховий рівень у відповідності професійній кваліфікації;

четвертий етап – імплементація професійних стандартів до освітніх програм підготовки студентів у закладах вищої освіти;

п'ятий етап – формування Національної рамки кваліфікацій у сфері кібербезпеки, а саме: розробка та імплементація в суспільство, безпосередньо самої рамки кваліфікацій з урахуванням сформованих професійних категорій (класифікації організаційної структури, що мають загальні основні професійні функції у сфері кібербезпеки), професійних площин та відповідних їм кваліфікацій, компетентностей тощо.

Система професійної стандартизації та Національна рамка кваліфікацій у сфері кібербезпеки розробляється на основі імплементації рамок кваліфікацій Cybersecurity Workforce Framework USA (NICE NIST 800-801) та Європейської рамки навичок з кібербезпеки (European Cybersecurity Skills Framework/ECSF ENISA). Національна рамка кваліфікацій у сфері кібербезпеки України повинна враховувати вимоги ринку праці до компетентностей працівників, а також бути нормою, яка гармонізує чинне законодавство сфери вищої освіти й соціально-трудових відносин, сприяти національному та міжнародному визнанню кваліфікацій, здобутих в Україні, налагоджувати ефективну взаємодію всіх напрямів розвитку суспільства». ***(Ставка на освіту: Україна посилює стійкість у кіберпросторі через професійну підготовку // Державна служба спеціального зв'язку та захисту інформації України (https://cip.gov.ua/ua/news/stavka-na-osvitu-ukrayina-posilyuye-stiikist-u-kiberprostori-cherez-profesiinu-pidgotovku). 12.02.2024).***

***

«Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA, яка діє при Держспецзв’язку, за минулий рік опрацювала 2543 кіберінциденти, що на 15,9% більше ніж за 2022 рік, коли Україна стикнулася з величезною кількістю атак у зв'язку з повномасштабною російською агресією проти нашої держави.

Найбільше зловмисники атакують уряд та урядові організації, місцеві органи влади та сектор безпеки та оборони, комерційні організації, енергетичний сектор, телекомунікації та багато інших установ.

Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису та компрометація системи.

Метою зловмисників є розвідувальні операції, довготривале шпигунство, знищення даних та інформаційних систем. Кількість ворожих атак продовжує збільшуватися.

«Інтенсивність атак за час повномасштабного вторгнення залишається високою і цього року. Тільки за січень нами опрацьовано 400 кіберінцидентів, 9 з яких – критичного та високого рівня. Кількість кібероперацій проти України збільшується і це можна пов'язати з тим, що військові хакери рф почали активно залучати до атак хакерські кримінальні групи та комерційні компанії», – розповідає заступник начальника Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA Євген Бриксін.

Фахівці CERT-UA припускають, що ризик поширення зловмисниками масових розсилок у І кварталі 2024 року залишається підвищеним. Значна кількість таких розсилок може свідчити про низький рівень успішних заражень. Кількість фішингових атак, як завжди, залишиться на високому рівні». ***(Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти // Державна служба спеціального зв'язку та захисту інформації України (https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti). 08.02.2024).***

***

«У кіберпросторі України росію цікавлять місця скупчення особового складу, зберігання озброєння, військової техніки, зокрема від іноземних партнерів, та критична інфраструктура.

Про це повідомив Іван Павленко, начальник Головного управління радіоелектронної та кіберборотьби ЗСУ.

Крім того, рф постійно намагається отримати документи, які містять військові плани або чутливу для нашої національної безпеки інформації.

Такі самі цілі є основними і для українських кіберсил. Особливу увагу наші кіберфахівці приділяють логістично-транспортній системі росії, щоб розуміти можливості армії рф на кожному напрямку ведення бойових дій.

Головною метою України Іван Павленко називає створення кіберсил для здійснення кіберрозвідки та кіберзахисту в умовах кібервійни». ***(Артем Житкевич. Які основні цілі кібератак на Україну // ГО "Бізтех Медіа" (https://speka.media/yaki-osnovni-cili-kiberatak-v-ukrayini-pk4m3x). 07.02.2024).***

***

«Дослідники кібербезпеки виявили нову операцію впливу, націлену на Україну, яка використовує спам для поширення дезінформації, пов'язаної з війною.

Словацька компанія з кібербезпеки ESET пов'язала цю діяльність із загрозливими суб'єктами, пов'язаними з Росією, яка також виявила фішингову кампанію, спрямовану проти української оборонної компанії в жовтні 2023 року та агентства Європейського Союзу в листопаді 2023 року з метою отримання облікових даних для входу в Microsoft. використання підроблених цільових сторінок.

Операція Texonto, під якою була кодова назва всієї кампанії, не була приписана конкретному учаснику загрози, хоча деякі її елементи, зокрема фішингові атаки, збігаються з COLDRIVER, яка має історію збирання облікових даних через фальшивий вхід. сторінки.

Операція з дезінформації проходила у дві хвилі в листопаді та грудні 2023 року, причому електронні листи містили вкладення у форматі PDF і вміст, пов’язаний з перебоями в опаленні, нестачею ліків і нестачею їжі.

Листопадова хвиля охопила не менше кількох сотень одержувачів в Україні, зокрема уряд, енергетичні компанії та приватних осіб. Наразі невідомо, як був створений цільовий список.

«Цікаво відзначити, що електронний лист було надіслано з домену, замаскованого під Міністерство аграрної політики та продовольства України, в той час як його зміст стосується дефіциту ліків, а в PDF-файлі неправомірно використовується логотип Міністерства охорони здоров'я України», - йдеться в повідомленні ESET, яке було передано The Hacker News.

«Це, можливо, помилка зловмисників або, принаймні, свідчить про те, що вони не подбали про всі деталі».

Друга кампанія з дезінформації електронною поштою, яка розпочалася 25 грудня 2023 року, примітна тим, що вона поширилася за межі України, щоб охопити україномовних людей в інших європейських країнах. Усі повідомлення були написані українською мовою та надіслані різним цілям – від українського уряду до італійського виробника взуття.

Ці повідомлення, хоч і бажали одержувачам щасливого святкового сезону, також мали більш похмурий тон, доходячи до того, що вони пропонували ампутувати одну свою руку чи ногу, щоб уникнути військового розгортання. «Пара хвилин болю, але потім щасливе життя!», – йдеться в електронному листі.

ESET повідомила, що один із доменів, який використовувався для розповсюдження фішингових листів у грудні 2023 року, infonotification[.]com, починаючи з 7 січня 2024 року також розсилав сотні спам-повідомлень, перенаправляючи потенційних жертв на підроблений веб-сайт канадської аптеки.

Точно незрозуміло, чому цей сервер електронної пошти було перепрофільовано для розповсюдження аптечного шахрайства, але є підозри, що зловмисники вирішили монетизувати свою інфраструктуру для отримання

фінансової вигоди після того, як зрозуміли, що їхні домени були виявлені захисниками.

«Операція Texonto демонструє ще одне використання технологій для спроби вплинути на війну», – заявили в компанії.

Ця подія сталася після того, як компанія Meta у своєму щоквартальному звіті про загрози суперництва заявила, що ліквідувала три мережі з Китаю, М'янми та України на своїх платформах, які вели скоординовану неавтентичну поведінку (CIB).

Хоча жодна з мереж не була з Росії, аналітична компанія Graphika заявила, що обсяг публікацій російських державних ЗМІ знизився на 55% порівняно з довоєнним рівнем, а залученість впала на 94% порівняно з дворічною давниною.

«З початку війни російські державні ЗМІ зосередилися на неполітичному інформаційно-розважальному контенті та саморекламі про Росію», — йдеться в повідомленні. «Це може відображати більш широкі зусилля поза платформою, щоб задовольнити внутрішню російську аудиторію після того, як кілька західних країн заблокували торгові точки у 2022 році».

Операція впливу з Росією націлена на Німеччину

Doppelganger, агресивна і наполеглива прокремлівська мережа, відома поширенням антиукраїнської пропаганди і дезінформації, націлювала німецьку аудиторію на контент, що критикує правлячу урядову коаліцію і її підтримку України, згідно зі спільним звітом, опублікованим SentinelOne і ClearSky. Ця діяльність збігається з діяльністю, раніше викритою організаціями «Мета» та «Recorded Future» у минулому році.

Кампанія інформаційної війни, яка отримала назву Doppelganger NG, використовує мережу облікових записів X (раніше Twitter), які діляться «вмістом сторонніх веб-сайтів, вміст яких узгоджується з цілями пропаганди Doppelganger, а також із сайтів, створених самим Doppelganger», – сказав дослідник безпеки Александар Міленкоскі .

Крім того, було виявлено зв'язки між Doppelganger NG та російською групою кібершпигунства APT28 на основі схожості тексту та фрагментів HTML-коду,

знайдених у кампанії, і набору фішингових атак, спрямованих на викрадення облікових даних, введених потенційними жертвами на підроблених сторінках, що імітують такі служби електронної пошти. UKR.NET та Yahoo!

«Передача викрадених даних здійснюється за допомогою раніше скомпрометованих пристроїв Ubiquiti», — зазначила Група реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) у липні 2023 року. Минулого тижня уряд США заявив, що порушив роботу мережі маршрутизаторів Ubiquiti, яка була використовується APT28 для приховування своєї зловмисної діяльності». ***(Russian Hackers Target Ukraine with Disinformation and Credential-Harvesting Attacks // The Hacker News (https://thehackernews.com/2024/02/russian-hackers-target-ukraine-with.html). 21.02.2024).***

***

«Російські хакери здійснили атаку на низку відомих українських медіа, фахівці вже досліджують цей інцидент.

Про це Державна служба спеціального зв'язку та захисту інформації України повідомила у Telegram.

Повідомляється, що до урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, уже звернулися представники видань Liga.net, «Українська правда», «Апостроф» і «Телеграф».

У разі підозри на хакерську атаку CERT-UA закликає одразу звертатися до фахівців команди.

Так, 18 лютого видання LIGA.net заявило, що невідомі зламали його сайт й опублікували там фейкову новину про нібито «розгром» елітних підрозділів Збройних сил України в Авдіївці Донецької області.

«Українська правда» поінформувала про злам її акаунту в соцмережі X. На сторінці видання теж з'явився фейк про «розгром» елітних підрозділів ЗСУ в Авдіївці.

Російські хакери готуються до масштабної кібератаки проти України

Проросійська хакерська група NoName05716 оголосила про плани здійснити масштабну кібератаку на український уряд.

Про це повідомляє The Guardian.

Хакерська група стверджує, що готується атакувати український уряд за допомогою інших хакерських груп 22C, Skillnet, CyberDragon, Federal Legion, People's Cyber Army і Phoenix.

Кібератаки стали предметом занепокоєння українських чиновників від самого початку війни, а контактна група з оборони України сформувала ІТ-коаліцію з 12 країн». ***(Олексій Грушевський. Російські хакери здійснили кібератаку на медіа України — Держспецзв'язку // Online.ua (https://news.online.ua/rosiiski-xakeri-zdiisnili-kiberataku-na-media-ukrayini-derzspeczviazku-873433/). 18.02.2024).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Національне агентство з кібербезпеки та Національний інститут інновацій у сфері кібербезпеки Cybercor були започатковані на першому в цьому році заході – Форумі кібербезпеки Молдови. Інституції відіграватимуть важливу роль у запобіганні та боротьбі з кіберзагрозами.

Форум урочисто відкрили прем’єр-міністр Дорін Речан та віце-прем’єр-міністр, міністр економічного розвитку та цифровізації Думітру Алайба. Чиновники підкреслили, що кібербезпека є пріоритетом для Молдови, повідомили в урядовому департаменті комунікації.

«Тепер, коли ми оцифрували майже всі послуги з Молдови, кібербезпека стає досить важливим аспектом. Настав час для всіх нас, як для працівників державного сектору, так і для підприємців, і для працівників приватного сектору, і як для громадян, щоб приділяти все більше уваги цьому аспекту та все більше і більше інвестувати в кібербезпеку», — сказав прем’єр-міністр Дорін Речан.

Дві нові інституції, запущені на Форумі кібербезпеки Молдови, зосередять свою роботу на забезпеченні безпечного цифрового середовища, захисті критичної інфраструктури держави та суспільства від кібератак, а також на гарантуванні високого рівня безпеки інформаційних мереж. і системи державних і приватних установ.

Захід організовано Міністерством економічного розвитку та цифровізації у партнерстві з Міністерством закордонних справ, Технічним університетом Молдови та Tekwill за підтримки Агентства США з міжнародного розвитку, Швеції, Великої Британії та Місії партнерства Європейського Союзу в Молдова та Академія електронного урядування». ***(Moldovan PM says time is ripe to invest more in cyber security // I.P. MOLDPRES A.I.S. (https://www.moldpres.md/en/news/2024/02/09/24000920). 09.02.2024).***

***

Світові тенденції в галузі кібербезпеки

«На думку фахівців InfoSec, які хотіли б бачити більше реальних прикладів боротьби з інцидентами, вища освіта все ще надто відірвана від повсякденної реальності кібербезпеки.

Під час опитування понад 1000 професіоналів з кібербезпеки в усьому світі половина заявили, що доступність курсів з кібербезпеки чи інформаційної безпеки у формальній вищій освіті є або поганою, або дуже поганою: це число підскочило до 83% для професіоналів із досвідом від двох до п’яти років.

Частково проблема полягає в тому, що індустрія технологій розвивається швидко, але кібербезпека розвивається ще швидше. Він обумовлений не ритмом випуску продуктів, а відкриттям нових методів злому та недоліків нульового дня.

«Я вважаю, що сьогодні ми не маємо достатньо освіти з кібербезпеки, щоб хтось міг справді досягти успіху в цій галузі. Я вважаю, що одна з проблем — і це стосується не лише кібербезпеки, але й технологічного сектора в цілому — полягає в тому, що сучасні технології розвиваються настільки швидко, що те, що є актуальним і актуальним сьогодні, старіє і перетворюється на «спадщину» два роки», — сказав IT-директор з банку в Бразилії, цитований дослідженням.

Трохи більше чверті (30%) фахівців у сфері безпеки сказали, що доступність курсів з кібербезпеки та InfoSec у вищих навчальних закладах є хорошою або дуже хорошою. У Європі лише 20% респондентів вважали, що це так.

Дослідження, проведене на замовлення Kaspersky, показало, що майже 40% працівників сказали, що їхні інструктори та вчителі не мали реального досвіду роботи в галузі.

«Було складно знайти викладачів, які поєднували б теоретичні знання з практичними», — цитує слова директора відділу кібербезпеки в США.

Курси з кібербезпеки зосереджені на теоретичних, а не практичних питаннях

Багато респондентів негативно ставилися до теоретичних знань, які вони отримали на своїх курсах, особливо на початку кар'єри. Працівники на пізнішому етапі своєї кар'єри, здавалося, більше цінували теоретичне обґрунтування.

Менше половини респондентів сказали, що програма їх коледжу чи університету запропонувала їм практичний досвід реальних сценаріїв кібербезпеки у вигляді живих проектів. «Для вирішення реальних інцидентів безпеки потрібен інший набір навичок, ніж лише теоретичні знання», — сказав один американський спеціаліст із кібербезпеки, цитований у звіті.

«У всьому світі хронічно не вистачає експертів з кібербезпеки, і є ознаки того, що освіта може бути винуватцем цієї проблеми», — йдеться у звіті.

«Освітнім програмам з кібербезпеки часто важко йти в ногу з останніми розробками через швидку еволюцію природи кіберзагроз, які випереджають оновлення навчальних програм», — додали в ньому.

Інша частина проблеми полягає в тому, що не завжди є чітко визначені кар'єрні шляхи в сфері безпеки, особливо за межами великих організацій.

Дослідження навичок кібербезпеки, проведене урядом Великої Британії, опубліковане минулого року, показало, що хоча близько половини працівників раніше працювали в цьому секторі, близько третини були прийняті на роботу, не пов'язану з безпекою, а решта починали кар'єру. У багатьох випадках кібербезпека – це те, що додається до наявної ролі, наприклад, поряд із відповідальністю за інфраструктуру чи операції.

Дослідження Kaspersky виявило, що більшість компаній не вимагають від кандидатів кваліфікації інформаційної безпеки на посади початкового рівня.

Понад три чверті тих, хто має від двох до п’яти років досвіду, не вивчали інформаційні технології чи комп’ютерні науки в коледжах чи університетах і вже встигли впоратися з ними.

Натомість працівники кібербезпеки мають низку кваліфікацій, починаючи з інженерії (36%), інформаційних технологій (21%), інформатики (15%), управління бізнесом (13%), природничих наук (10%), математики (3%), та інші. Лише 43% нинішніх фахівців з кібербезпеки мали інформаційну безпеку як частину офіційної навчальної програми.

Можливо, не дивно, що для того, щоб йти в ногу з досягненнями галузі, багато експертів з кібербезпеки повинні пройти подальше навчання. Майже половина опитаних професіоналів (46%) пройшли додаткові курси кібернавчання пізніше у своїй кар’єрі, оскільки вони виявили, що вирішення реальних інцидентів безпеки вимагає іншого набору навичок, ніж лише теоретичні знання.

У звіті говориться, що багато респондентів стверджують, що вони зацікавилися кібербезпекою або знайшли кращі можливості в цій галузі та сприйняли це як органічний розвиток кар’єри в секторі.

«Я вважаю це захоплюючим, оскільки передбачає постійне навчання та адаптацію до нових загроз, технологій і технологій, що розвиваються», — сказав один із респондентів, лідер із кібербезпеки та технологій у Північній Америці. «Здебільшого особистий інтерес спонукав мене прийняти цю роль».

Професія кібербезпеки швидко змінюється

Професор Деніел Прінс, професор кібербезпеки в рамках науки про безпеку та захист Ланкастерського університету, сказав, що професія InfoSec все ще розвивається, і лише за останні 10 років університети Великобританії почали випускати студентів за програмами кібербезпеки.

Але академічна освіта не полягає в навчанні людини виконувати конкретне завдання з певним типом продукту, сказав він.

«Основна увага приділяється розвитку людей, здатних критично мислити про складні проблеми, які породжує кібербезпека, і ґрунтувати це мислення на наукових доказах», — сказав він ITPro. «Зрештою, технології, програмне

забезпечення, продукти постійно розвиваються та розвиваються, але основні концепції та фундаментальні навички залишаються важливими».

За його словами, академічне навчання спрямоване на підтримку розвитку добре обізнаних, глибоко кваліфікованих, критично мислячих людей, які розуміють основні концепції кібербезпеки та можуть адаптуватися до складних ситуацій кібербезпеки.

«Академічній установі ніколи не вдасться підготувати ідеального працівника кібербезпеки, оскільки існує так багато різних комбінацій типів компаній, типів ролей, технологічних платформ, послуг і клієнтів».

Прінс сказав, що практичний досвід є важливим і сказав, що в університетських програмах MSc і MBA використовуються практичні вправи та вправи під керівництвом викликів. «Ключовою річчю в цих типах «практичних» вправ є як поєднання використання технологій та обладнання, так і розуміння та вивчення того, як вони реагують як частина команди, як вони працюють над вирішенням проблем, наскільки добре вони презентують старші люди», - сказав він

Клар Россо, генеральний директор членської асоціації кібербезпеки ISC2, сказав ITPro, що професіонали з безпеки повинні скористатися всіма можливостями навчання без відриву від роботи та наставництва, доступними для них, а також курсами професійного розвитку та програмами сертифікації, орієнтованими на їхні поточні ролі та кар'єрні амбіції.

Россо сказав, що зміни вже відбуваються в університетах по всьому світу, і зростає бажання включити вимоги до практичного досвіду в програми отримання дипломів або узгодити ступені з визнаними галузевими програмами сертифікації.

Громадські коледжі та історично чорношкірі коледжі та університети в США досягають успіху в цьому, додав Россо.

«Дослідження показали, що громадські коледжі не тільки прагнуть обслуговувати більш різноманітне населення, усуваючи нинішню нестачу різноманітності в індустрії кібербезпеки, але вони також часто пропонують можливості для практичного навчання, даючи студентам фактичні повсякденні навички, необхідні їм для досягнення успіху», – сказав Россо.

«Чотирирічні дипломи стають все менш і менш вимогою для найму фахівців з кібербезпеки, тому ми сподіваємося, що цінність громадських коледжів є головною для початківців кібер-практиків». ***(Steve Ranger. Does a cyber security degree help in the real world? Industry professionals have mixed feelings on whether they're useful // Future US, Inc. (https://www.itpro.com/business/careers-and-training/does-a-cyber-security-degree-help-in-the-real-world-industry-professionals-have-mixed-feelings-on-whether-theyre-useful). 09.02.2024).***

***

«… За останні кілька десятиліть кібербезпека суттєво розвинулась у міру того, як технології розвинулися та стали більш інтегрованими в наше повсякденне життя. Там, де кіберзагрози колись обмежувалися хакерством і зловмисним програмним забезпеченням, цифровий ландшафт розширив вразливі місця через постійний світ із постійним зв'язком. Персональні пристрої, хмарні сервіси, Інтернет речей тощо створили нескінченну кількість нових точок входу для зловмисників. У результаті підхід, орієнтований на користувача, зосереджений на профілактиці через інтуїтивно зрозумілий дизайн, став вирішальним. Взаємодія з користувачем та дизайн інтерфейсу зараз відіграють визначальну роль у сучасному кіберзахисті. Віддаючи пріоритет зручності використання та обізнаності, безпеку можна посилити зсередини за допомогою поінформованих, освічених користувачів.

UI/UX у кібербезпеці: зміна парадигми

Програми сертифікації кібербезпеки дедалі більше визнають важливість досвіду користувача та дизайну інтерфейсу в стратегіях кіберзахисту. Відбулася зміна парадигми в тому, як організації підходять до кібербезпеки, переходячи від єдиної уваги до технічного контролю до визнання центральної ролі користувачів. Віддаючи перевагу зручності використання, розумінню та обізнаності за допомогою дизайну інтерфейсу, спеціалісти з безпеки можуть допомогти користувачам зробити кращий вибір і вжити відповідних запобіжних заходів. Коли користувачі відчувають себе наповненими завдяки інтуїтивно зрозумілому, корисному UX, вони, швидше за все, дотримуватимуться протоколів, які

посилюють загальну кіберстійкість. Цей переосмислений підхід розглядає користувачів не лише як слабке місце, а й як найважливіших союзників, які можуть підвищити безпеку за умови ефективного керівництва.

Людський фактор: розуміння поведінки користувачів

Розуміння людської поведінки та прийняття рішень є ключовим для розробки ефективних рішень безпеки, зосереджених навколо користувачів. Користувачі не завжди роблять цілком раціональний вибір і можуть ризикувати або ігнорувати попередження через звичку, терміновість або незнання. Традиційні підходи до кібербезпеки часто не враховують людський фактор і те, що користувачі неминуче допускають помилки.

Однак завдяки глибшому розумінню когнітивних упереджень, емоційних реакцій і поширених помилок можна створити інтерфейси, які спрямовуватимуть користувачів до безпечної поведінки та уникнення вразливостей. Наприклад, спонукання, попередження та відгуки можуть бути розроблені на основі принципів поведінкової психології, щоб заохочувати дотримання найкращих практик безпеки. Дані про те, як фактичні користувачі взаємодіють, також дають зрозуміти, щоб відповідним чином адаптувати UX. Цей підхід, орієнтований на людину, визнає, що користувачам потрібен підтримуючий, корисний дизайн, щоб доповнити їхні цифрові навички та зробити безпеку інтуїтивно зрозумілою частиною їхньої діяльності в Інтернеті.

Розробка інтуїтивно зрозумілих інтерфейсів для безпечної взаємодії

Коли інтерфейси інтуїтивно зрозумілі та прості у використанні, вони дозволяють користувачам безперешкодно застосовувати безпечну поведінку. Розробка з урахуванням зручності використання та розуміння допомагає уникнути вразливості, що виникає через плутанину чи розчарування. Інтерфейси повинні чітко передавати найкращі методи безпеки та попередження за допомогою простої мови без жаргону, адаптованої для різних рівнів навичок. Візуальні підказки, вказівки з урахуванням контексту та відгуки допомагають користувачам зрозуміти, чому певні дії можуть бути ризикованими.

Процеси автентифікації можна оптимізувати за допомогою менеджерів паролів або біометричного входу, щоб зменшити залежність від слабких облікових даних, які повторно використовуються. Налаштування та елементи керування організовано логічно, щоб користувачі могли легко отримати доступ і змінити параметри конфіденційності та безпеки. Потенційні загрози вирішуються завчасно, спонукаючи запускати оновлення, періодично змінювати паролі та остерігатися підозрілих посилань і вкладень. Інтуїтивно зрозумілий UX робить цифрову безпеку легкою частиною онлайн-діяльності.

Поінформованість про загрози в режимі реального часу через інтуїтивно зрозумілі інформаційні панелі

Використовуючи прості для розуміння інформаційні панелі, користувачі можуть у режимі реального часу стежити за потенційними загрозами на своїх онлайн-акаунтах і пристроях. При інтуїтивно зрозумілому дизайні інформаційні панелі дають змогу користувачам бачити стан безпеки мережі.

Ось ключові моменти для визначення загроз у реальному часі за допомогою інтуїтивно зрозумілих інформаційних панелей:

Настроювані віджети: інформаційні панелі дозволяють користувачам додавати відповідні віджети, що відображають активність облікового запису, розташування пристроїв, спроби входу тощо, щоб вони могли налаштувати перегляд важливої інформації безпеки.

Швидкий огляд показників: зведені показники, як-от кілька входів у систему цього місяця або пристрої, підключені зараз, дозволяють користувачам негайно оцінити стан безпеки мережі, не копаючись у вкладених меню.

Проста візуалізація: діаграми, карти та кольорове кодування допомагають користувачам інтуїтивно розуміти складні дані безпеки, такі як географічне розташування спроб входу в систему або шаблони аномальної активності.

Попереджувальні сповіщення: миттєві сповіщення про нові входи, невдалі входи чи інші нерегулярні події привертають увагу до потенційних проблем у режимі реального часу, щоб користувачі могли швидко усунути загрози.

Фільтри деталізації: фільтри дозволяють користувачам виділяти конкретні часові проміжки, типи пристроїв або деталі облікового запису, якщо це необхідно для детальнішого аналізу подій сповіщень або історії активності.

Порівняння контрольних показників: порівняння показників із середніми значеннями аналогів або контрольними показниками особистої історії допомагає користувачам виявити ненормальні моделі використання, які вказують на компрометацію облікового запису або підозрілу внутрішню мережеву активність.

Збалансування безпеки та зручності використання: проблеми та рішення

Хоча першочергове значення має зручність використання та розуміння користувачем, баланс між ними та ефективними функціями безпеки створює проблеми. Суворі протоколи можуть розчаровувати користувачів і призводити до обхідних шляхів, але слабкий захист створює вразливі місця. Розробка інтуїтивно зрозумілих інтерфейсів, які бездоганно вбудовують безпеку, вимагає нюансів рішень. Багатофакторна автентифікація забезпечує надійний захист, але додаткові кроки можуть розчарувати деяких. Сповіщення мають чітко розрізняти справжні загрози та помилкові тривоги. Індивідуальне налаштування дозволяє індивідуальне пошиття, але складні варіанти можуть заплутати інших. Встановлення правильної рівноваги вимагає ретельного дослідження користувачів і тестування різних підходів для оптимізації як результатів безпеки, так і загального досвіду.

Майбутні тенденції: інновації в UI/UX для кібербезпеки

Оскільки технологія швидко розвивається, інтерфейс користувача та дизайн досвіду для кібербезпеки також повинні продовжувати інновації. Такі області, як шоу доповненої та віртуальної реальності, обіцяють занурити користувачів в інтерактивне моделювання навчання безпеки. Біометрична автентифікація за допомогою відбитків пальців, розпізнавання обличчя або відбитків голосу може ще більше спростити процеси входу. Розширені алгоритми машинного навчання можуть ще більше персоналізувати попередження про загрози на основі індивідуальної поведінки в Інтернеті та нових ризиків. Ambient UX, що відображає статус безпеки через підключені домашні пристрої, забезпечує легкий доступ до даних. Інтеграція блокчейну може автоматизувати згоду на обмін даними для

збереження конфіденційності. Майбутнє кіберзахисту значною мірою покладатиметься на винахідливий UI/UX, щоб забезпечити безпечні можливості людей у все більш цифровому світі.

Висновок

У міру того як ландшафт загроз розвивається разом із новими технологіями, кібербезпека також має адаптуватися. Підхід, орієнтований на користувача, зосереджений на запобіганні за допомогою інтуїтивно зрозумілого UX, став першочерговим у сучасних оборонних стратегіях. Якщо інтерфейси розроблені з урахуванням зручності використання, розуміння та обізнаності, вони можуть посилити безпеку зсередини, надаючи можливості освіченим та поінформованим користувачам. Заглядаючи вперед, продовження інновацій у UI/UX буде критично важливим для того, щоб люди могли безпечно орієнтуватися в постійно підключеному цифровому світі. Пріоритет користувальницького досвіду допоможе переосмислити кібербезпеку як спільне зусилля професіоналів із безпеки та зацікавлених, проактивних людей». ***(Cybersecurity Redefined: The Role of UI/UX in Modern Threat Mitigation // Indiapost Media Pvt Ltd (https://indiapost.com/cybersecurity-redefined-the-role-of-ui-ux-in-modern-threat-mitigation/). 13.02.2024).***

***

«За останні кілька десятиліть світ технологічно розвинувся. Оскільки розвиток технологій продовжує впроваджувати інновації, спрощувати й автоматизувати щоденні повсякденні завдання, він також породив зростаючу стурбованість щодо конфіденційності, витоку даних і потенційних ризиків для безпеки. Кібербезпека — це технологічний термін для вирішення таких проблем безпеки та захисту систем і мереж від цифрових атак.

Підприємства тепер приділяють більше уваги найму кваліфікованого IT-персоналу або підписанню договору з авторитетною IT-компанією. Такі найми та співпраця можуть допомогти їм керувати вразливістю та безпекою своєї системи та захистити свої дані від будь-якого несанкціонованого доступу. Немає сумніву, що такий попит на кібербезпеку має вирішальне значення, оскільки кіберзагрози

продовжують розвиватися та становлять невиправну загрозу конфіденційним даним. Нижче ми визначили деякі нові кіберзагрози, на які вам слід звернути увагу.

1. Генеративний ШІ з обох сторін

Оскільки штучний інтелект швидко розвивається, можна передбачити більше розумних атак на основі ШІ. ШІ досягає безпрецедентного рівня складності, наприклад глибока фейкова соціальна інженерія, щоб уникнути виявлення.

Однак цю технологію також можна використовувати для максимального використання потенціалу оборонних заходів. Виявлення аномалій у режимі реального часу на основі штучного інтелекту, автоматичні механізми реагування на інциденти та адаптивна автентифікація можуть бути використані для підвищення нашої здатності виявляти, уникати та боротися з кіберзагрозами. На цьому полі битви кібер-зловмисників і захисників штучний інтелект є потужним інструментом, який може використовувати кожен, хто зрозуміє, як використати його, щоб отримати максимальний потенціал.

2. Вразливість Хмари

Оскільки все більше організацій встановлюють свої сервери та завантажують свої дані в хмару, безпеку потрібно оцінювати на підвищеній основі. Хмарні служби використовують інтерфейси та API (інтерфейси прикладного програмування) для взаємодії з іншими користувачами та службами. Якщо ці інтерфейси не захищені належним чином, вони можуть служити точкою входу для зловмисників, щоб скористатися ними та отримати несанкціонований доступ.

Незважаючи на те, що такі компанії, як Google і Microsoft, запровадили комплексні заходи безпеки, все одно користувачі – обмін ресурсами, встановлення шкідливого програмного забезпечення та внутрішні загрози – можуть викликати занепокоєння щодо конфіденційності даних, незважаючи на додаткові рівні безпеки.

3. Культура віддаленої роботи

Культура роботи вдома широко поширена після того, як пандемія COVID-19 ізолювала світ. Навіть після того, як SOP були скасовані через зменшення випадків, віддалена робота переважала як зручне рішення для працівників і роботодавців.

Однак відсутність безпеки викликає занепокоєння багатьох. Користувачі обмінюються даними з неналежним чином захищених пристроїв і мереж, призначених для простоти та зручності, а не для безпечних операцій і транзакцій.

В офісі реалізовано належне використання брандмауерів, і можна довірити ІТ-команді практикувати адекватні заходи безпеки, такі як безпека мережі, захист кінцевої точки та регулярні перевірки безпеки, щоб уникнути кіберзагроз.

Відсутність міжмережевих екранів і стандартів безпеки у віддаленому робочому середовищі є сигналом тривоги для організацій, щоб включити належні інструменти безпеки та розширені канали зв'язку для підтримки безпечного робочого середовища за межами традиційного офісу.

Кінцева виноска

Поки існує людство, безпека, ймовірно, залишатиметься проблемою, як у фізичному середовищі, так і в Інтернеті. Хоча фізичні заходи безпеки є більш відчутними та можуть бути добре зрозумілі освіченій дорослій людині, кібербезпека вимагає конкретних знань про певну тему.

Усвідомлення найдрібніших деталей і дій, які можуть призвести до серйозніших проблем, має вирішальне значення, і лише людина, яка володіє знаннями та навичками, розробленими в кібердоміні, може ефективно з ними впоратися.

Тим не менш, певні заходи, як-от недопущення несанкціонованого доступу третіх сторін до ваших даних, впровадження методів шифрування для захисту ваших даних і застосування брандмауерів для моніторингу та контролю вхідних і вихідних даних тощо, можуть бути основними кроками для запобігання крадіжці даних або кібератаки, більш активні та старанні підходи можуть бути використані на вищих рівнях, щоб забезпечити загальну безпеку вашої конфіденційної інформації». ***(Emerging Cybersecurity Trends You Should Be Aware Of // Digital Information World (https://www.digitalinformationworld.com/2024/02/emerging-cybersecurity-trends-you.html). 14.02.2024).***

***

«Згідно з новим дослідженням JumpCloud, витрати на кібербезпеку скоротяться на 41% МСП протягом наступного року в умовах складного економічного середовища.

Майже три чверті (72%) IT-адміністраторів, опитаних у США, Великобританії та Індії, погодилися, що будь-які скорочення їхніх бюджетів на безпеку підвищать організаційний ризик.

МСП в Індії, швидше за все, зазнають скорочення кібербезпеки (58%). Далі йдуть США (40%) і Великобританія (25%).

Ризик скорочення бюджету виникає, незважаючи на те, що респонденти вважають безпеку найбільшою проблемою для IT (56%).

Більше половини (56%) IT-адміністраторів також сказали, що вони більше стурбовані безпекою своєї організації, ніж шість місяців тому.

Крім того, було значне занепокоєння щодо впливу ШІ на кібербезпеку. Майже дві третини (62%) погодилися, що ШІ випереджає здатність їхньої організації захищати від загроз в цілому.

Трьома найбільшими загрозами кібербезпеці, з якими стикаються МСП, є мережеві атаки (40%), використання вразливостей програмного забезпечення (34%) і програми-вимагачі (29%).

Раджат Бхаргава, генеральний директор JumpCloud, зазначив: «Хоча штучний інтелект є модним словом, яке захоплює заголовки, безпека залишається головною проблемою для IT-команд, враховуючи дедалі складніші зовнішні загрози та зростаючий нормативний тиск».

У звіті Sage за жовтень 2023 року було виявлено, що 48% малих і середніх підприємств зазнали принаймні одного кіберінциденту у 2023 році.

Біометрична автентифікація зростає серед малих і середніх підприємств

У звіті встановлено, що дві третини (66%) малих і середніх підприємств вимагають використання біометричних даних для аутентифікації співробітників. За даними JumpCloud, це суттєве зростання порівняно з 55% у квітні 2023 року.

Схоже, що зростаюче поширення біометрії зумовлене насамперед міркуваннями безпеки.

Майже дві третини (60%) погодилися, що впровадження біометрії посилить безпеку їхньої організації, тоді як біометрія вважалася найбезпечнішим методом автентифікації (33%). Далі йдуть одноразові паролі (25%) і додаток для перевірки (23%).

Однак 83% IT-адміністраторів повідомили, що їхня організація використовує автентифікацію лише за паролем принаймні для деяких IT-ресурсів. Це незважаючи на те, що 28% визнали, що автентифікація лише за паролем недостатня для захисту ресурсів їхньої організації.

Значною проблемою для респондентів є баланс між безпекою та зручністю для персоналу. Понад дві третини (67%) сказали, що додаткові заходи безпеки зазвичай означають більш громіздкий досвід.

Використання єдиного входу (SSO) є одним із способів, за допомогою якого IT-команди намагаються збалансувати безпеку та досвід: 87% використовують цей метод автентифікації для деяких ресурсів.

Британські МСП найменш готові до кібератак

У звіті встановлено, що МСП Великобританії менш готові до кібератак, ніж їхні колеги в США та Індії:

62% малих і середніх підприємств Великобританії пропонують офіційне навчання з кібербезпеки, на відміну від 72,5% у США та 74% в Індії

78% малих і середніх підприємств Великобританії мають IT-безпеку персоналу проти 87% у США та 94% в Індії

65% малих і середніх підприємств Великобританії фінансово готові відновитися після кібератаки проти 75% у США та 80% в Індії

72% малих і середніх підприємств Великобританії мають план кібербезпеки порівняно з 82% у США та 87,5% в Індії». ***(James Coker. Cybersecurity Spending Expected to be Slashed in 41% of SMEs // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/cyber-spending-slashed-smes/). 14.02.2024).***

***

«Міжнародний консорціум із сертифікації безпеки інформаційних систем та IBM об'єдналися 12 лютого, щоб запустити професійний сертифікат спеціаліста з кібербезпеки IBM та ISC2, який можна отримати за допомогою безкоштовного чотиримісячного навчального курсу для початківців. IBM обрала ISC2 для розробки програми сертифікації, яка готує потенційних спеціалістів з кібербезпеки до кар'єри спеціаліста з кібербезпеки.

Сертифікати IBM та ISC2 забезпечують навчання з кібербезпеки та підтвердження навичок

Професійний сертифікат спеціаліста з кібербезпеки IBM та ISC2 складається з доменів сертифікаційного навчання ISC2 Certified in Cybersecurity, а саме:

Принципи безпеки.

Реагування на інцидент.

Безперервність бізнесу та аварійне відновлення.

Концепції контролю доступу.

Безпека мережі та операції безпеки.

Після завершення сертифікаційної програми з 12 курсів учасники отримають значок IBM Digital Skills Badge, який свідчить про кваліфікацію потенційним роботодавцям. Учасників заохочують до подальшого розвитку своїх навичок, зареєструвавшись як кандидати ISC2 і пройшовши безкоштовний тест ISC2 Certified in Cybersecurity, який допоможе підтвердити свої навички в резюме або під час співбесіди. Понад 360 000 людей у всьому світі пройшли сертифікаційне навчання Certified in Cybersecurity.

Вакансії в сфері кібербезпеки залишаються високим попитом

«Кіберробоча сила терміново потребує кваліфікованих фахівців. Це партнерство дає можливість професіоналам-початківцям продемонструвати технічну майстерність і створити міцну основу навичок, допомагаючи людям вступити в двері роботодавців і розпочати свою кар'єру», — сказав генеральний директор ISC2 Клар Россо в прес- релізі.

Згідно з дослідженням ISC2, у 2023 році розрив між пропозицією та попитом на фахівців з кібербезпеки досяг 4 мільйонів людей. За даними ISC2, робоча сила

має зрости на 73%, щоб ефективно покривати всі потенційно вразливі активи організацій.

«Для IBM і Coursera визнання цінності нашої сертифікації CC є надзвичайно обнадійливим і сприяє прогресу в усуненні розриву кадрів у сфері кібербезпеки», — сказав Россо.

«З огляду на постійно зростаючі загрози для критично важливих систем і світову залежність від технологій, попит на фахівців з кібербезпеки вищий, ніж будь-коли», — сказав директор IBM Skills Network і технічний директор Леон Кацнельсон у прес-релізі. «Ми раді співпрацювати з ISC2 і Coursera в досягненні нашої спільної мети — надати майбутнім професіоналам з кібербезпеки важливі навички для успіху в цій затребуваній професії».

За даними Міністерства праці США в жовтні 2023 року, аналітик з інформаційної безпеки належить до IT-вакансії, яка буде користуватися великим попитом протягом десятиліття з 2022 по 2032 рік.

Як відкриття дверей для молодших спеціалістів приносить користь організаціям і індустрії кібербезпеки

Для організацій подібні програми сертифікації пропонують простий шлях до перенавчання або перенавчання співробітників для внутрішніх посад, якщо це необхідно. Оскільки програмне забезпечення-вимагач все ще використовується, а генеративний штучний інтелект, який потенційно дозволить зловмисникам навчати моделі на основі вкрадених даних у майбутньому, попит на спеціалістів із кібербезпеки, ймовірно, лише зросте.

«Однією з найпоширеніших проблем у сфері кібербезпеки, що постає перед організаціями в усьому світі, є можливість визначити кандидатів початкового та молодшого рівня з потрібними навичками та здібностями, щоб навчатися та розвиватися на роботі», — сказав Россо в електронному листі TechRepublic.

«У той же час ті, хто бажає розпочати кар’єру, не можуть продемонструвати своє розуміння концепцій кібербезпеки та привернути увагу менеджерів з найму… [Сертифікація є] безпрограшною перевагою для роботодавців, майбутніх співробітників і ширшої галузі кібербезпеки», – сказав Россо». ***(Megan Crouse.***

IBM, ISC2 Offer Free Cybersecurity Certificate // TechnologyAdvice (https://www.techrepublic.com/article/cybersecurity-training-ibm-isc2/). 13.02.2024).

***

«Ландшафт кібербезпеки у фінансових послугах зазнає швидких змін. Кіберзлочинці використовують передові технології та методології, роблячи традиційні засоби безпеки застарілими. Проблеми ускладнюються для громадських банків, які повинні захищати конфіденційні фінансові дані від такого ж рівня складних загроз, як і великі установи, але часто з більш обмеженими ресурсами.

Краєвид загроз FinServ #

Останні тенденції свідчать про тривожне зростання складних кібератак. Зараз кіберзлочинці застосовують передові методи, такі як технології глибокої підробки та атаки на основі штучного інтелекту, через що банкам стає все важче розрізняти законну діяльність від зловмисної. Ці зміни вимагають переходу до більш складних та адаптивних заходів кібербезпеки. Візьмемо, наприклад, цю статистику галузі.

Фінансові компанії повідомляють про 703 спроби кібератак на тиждень.

У середньому 270 атак (з несанкціонованим доступом до даних, додатків, мереж або пристроїв) сталися у фінансових службах, що на 31% більше, ніж у попередньому році.

У середньому підприємствам фінансових послуг потрібно в середньому 233 дні, щоб виявити та локалізувати порушення даних.

43% керівників вищої ланки банків не вірять, що їхній банк достатньо обладнаний для захисту даних клієнтів, конфіденційності та активів у разі кібератаки.

Середня вартість витоку даних у сфері фінансових послуг становить 5,72 мільйона доларів США за інцидент.

Спонсоровані державою кібератаки також становлять унікальну загрозу для фінансового сектора. Ці атаки часто є дуже складними та добре фінансованими, спрямованими на дестабілізацію фінансових систем або викрадення конфіденційної економічної інформації. Громадські банки повинні бути готові захищатися від цих

загроз високого рівня, які вимагають іншого підходу, ніж звичайна кіберзлочинна діяльність.

Так само останнім часом спостерігається тривожна тенденція, коли основні постачальники послуг, що обслуговують малі та середні банки, такі як FIS, Fiserv і Jack Henry, стають основними цілями для кібератак. Націлювання на цих постачальників послуг дозволяє суб'єктам загрози розширити свою мережу та зробити свої спроби ефективнішими, оскільки компрометація одного постачальника послуг потенційно може надати доступ до кількох невеликих банків. Це підкреслює критичну важливість сильного управління постачальниками. Громадські банки повинні бути готові захищатися від цих загроз високого рівня, які вимагають іншого підходу, ніж звичайна кіберзлочинна діяльність.

Щоб подолати загрози, з якими стикається галузь FinServ, можна вжити профілактичні заходи. Такі компанії, як ArmorPoint, проводять безкоштовні семінари з кібербезпеки, на яких досвідчені експерти з кібербезпеки виявляють конкретні прогалини в безпеці та дають рекомендації щодо пом'якшення цих ризиків.

5 головних викликів кібербезпеці FinServ і як їх подолати #

1. Розширені стратегії хмарної безпеки #

Хмарні обчислення з численними перевагами масштабованості, гнучкості та економічності все частіше застосовуються фінансовими установами. Однак ця зміна створює певні проблеми безпеки, які можуть бути складними для вирішення. Складність хмарної безпеки зумовлена необхідністю захисту даних у різноманітних та динамічних середовищах. У хмарі дані часто переміщуються між різними службами та географічно, що робить традиційні підходи безпеки на основі периметра менш ефективними. Крім того, модель спільної відповідальності в хмарних обчисленнях може призвести до неоднозначності ролей безпеки та обов'язків між постачальником хмарних послуг і банком.

Щоб вирішити ці виклики, банки повинні прийняти передові хмарні стратегії безпеки. Це передбачає впровадження комплексного шифрування даних для захисту даних у стані спокою та передачі, а також надійних систем керування

ідентифікацією та доступом для контролю того, хто може отримати доступ до яких даних і за яких умов. Моделі безпеки з нульовою довірою, де довіра ніколи не передбачається, а перевірка потрібна від усіх, хто намагається отримати доступ до ресурсів у мережі, стають все більш життєво важливими. Розуміння нюансів різних хмарних середовищ — загальнодоступних, приватних і гібридних — також має ключове значення для ефективного адаптування заходів безпеки.

2. Програмне забезпечення-вимагач: поза основним захистом #

Атаки програм-вимагачів у фінансовому секторі стають дедалі витонченішими, використовуючи такі тактики, як «Програми-вимагачі як послуга» (RaaS), спрямовані на установи. Еволюція програм-вимагачів у поєднанні з високою цінністю фінансових даних робить ці установи особливо вразливими. Традиційні стратегії захисту часто є неадекватними перед обличчям таких складних загроз, які можуть обійти стандартні заходи безпеки та зашифрувати важливі дані, спричиняючи збої в роботі та фінансові втрати.

Банки повинні запровадити багаторівневу стратегію захисту від програм-вимагачів. Сюди входять розширені системи аналізу загроз, які можуть надавати інформацію про нові загрози та вразливості в реальному часі. Регулярні перевірки безпеки мають вирішальне значення для виявлення та усунення потенційних вразливостей в інфраструктурі кібербезпеки банку. Крім того, команди проактивного пошуку загроз можуть відігравати важливу роль у виявленні та нейтралізації загроз до їх реалізації, забезпечуючи додатковий рівень захисту від атак програм-вимагачів.

3. Комплексне управління ризиками постачальника #

Фінансові установи все більше покладаються на сторонніх постачальників для цілого ряду послуг, від хмарних обчислень до управління відносинами з клієнтами. Кожна взаємодія з постачальником створює потенційні ризики для кібербезпеки, оскільки постачальники можуть мати доступ до конфіденційних банківських даних або керувати ними. Управління цими ризиками ускладнюється різними позиціями безпеки та практикою різних постачальників, що ускладнює

забезпечення узгоджених стандартів безпеки для всіх відносин із третіми сторонами.

Ефективне управління ризиками постачальника виходить за рамки початкової оцінки безпеки та вимагає постійного моніторингу та оцінки практики безпеки постачальника. Регулярні перевірки безпеки постачальників є важливими, щоб переконатися, що вони дотримуються узгоджених стандартів безпеки та практики. Інтеграція управління ризиками постачальників у загальну стратегію кібербезпеки банку забезпечує єдиний підхід до безпеки, зменшуючи ймовірність порушень безпеки, пов’язаних із постачальниками.

4. Відповідність нормативним вимогам: навігація складним ландшафтом #

Регуляторний ландшафт кібербезпеки у фінансовому секторі є складним і постійно розвивається. Від банків вимагається дотримуватись широкого спектру міжнародних, національних і регіональних нормативних актів, кожен з яких має власний набір вимог і штрафів за їх невиконання. Орієнтуватися в цьому складному ландшафті складно, оскільки банки повинні постійно адаптувати свої стратегії кібербезпеки, щоб відповідати цим змінним вимогам.

Щоб ефективно орієнтуватися в цьому ландшафті, громадські банки повинні розвинути глибоке розуміння відповідних нормативних актів, таких як GBLA, PCI DSS, SOX тощо. Для цього потрібно створити спеціальну команду з контролю відповідності або навіть залучити віртуального директора з інформаційної безпеки (vCISO), відповідального за те, щоб бути в курсі нормативних змін і гарантувати, що практика кібербезпеки банку відповідає цим вимогам. Регулярне навчання та програми підвищення обізнаності для всього персоналу також мають вирішальне значення для забезпечення повного розуміння та дотримання вимог відповідності.

5. Подолання розриву талантів у сфері кібербезпеки #

Дефіцит кадрів у сфері кібербезпеки створює серйозну проблему для фінансових установ. Природа кіберзагроз, що швидко розвивається, потребує кваліфікованих фахівців, які володіють останніми технологіями та стратегіями. Однак на ринку існує дефіцит таких професіоналів, що ускладнює для банків

наймання та утримання талантів, необхідних для ефективного управління ризиками кібербезпеки.

Банки повинні прийняти творчі рішення, щоб подолати цю прогалину в талантах. Розробка програм внутрішнього навчання може допомогти підвищити кваліфікацію наявного персоналу, щоб зробити його здатним виконувати складніші завдання з кібербезпеки. Співпраця з навчальними закладами для розробки індивідуальних навчальних програм з кібербезпеки може допомогти створити групу кваліфікованих фахівців. Крім того, використання штучного інтелекту та автоматизації для звичайних завдань безпеки може звільнити людські ресурси для більш складних і стратегічних завдань кібербезпеки, оптимізуючи використання наявних талантів.

Крім того, ще одна життєздатна стратегія для усунення нестачі талантів – аутсорсинг. Фінансові установи можуть розглянути можливість аутсорсингу спеціалістів з безпеки, співпрацюючи зі спеціалізованими фірмами для надання експертних послуг із кібербезпеки. Цей підхід дозволяє банкам отримати доступ до пулу досвідчених професіоналів, які можуть відстежувати, виявляти та ефективно реагувати на загрози безпеці. Крім того, передача аутсорсингу інформації на рівні керівника, наприклад віртуального директора з інформаційної безпеки (vCISO), може забезпечити стратегічне керівництво та управління для зміцнення загальної позиції кібербезпеки банку. Завдяки аутсорсингу конкретних потреб у кадрах банки можуть ефективніше подолати дефіцит кадрів, зосереджуючись на досконалості кібербезпеки.

Три кроки до впровадження надійної системи кібербезпеки #

Інтегрований підхід до кібербезпеки є обов’язковим для ефективного управління цими різними викликами. Це передбачає створення цілісної структури, яка поєднує в собі передові технологічні рішення, ретельні політики та процедури, регулярну оцінку ризиків, безперервний моніторинг і проактивне планування реагування на інциденти.

Крок 1: Стратегічне узгодження та планування

Наріжним каменем успішної програми кібербезпеки є її стратегічне узгодження та планування. Цей важливий перший крок передбачає встановлення чітких цілей кібербезпеки, які тісно пов’язані з бізнес-цілями організації. Інтеграція засобів контролю безпеки в організаційну стратегію має важливе значення, гарантуючи, що кожен аспект бізнесу підкріплюється надійними заходами безпеки. Ефективна стратегія також включає створення системи пріоритезації ризиків, яка є важливою для виявлення та зосередження на найбільш критичних загрозах. Крім того, розробка архітектури безпеки, адаптованої до конкретних потреб і профілю ризику організації, є надзвичайно важливою. Ця архітектура має бути динамічною, розвиватися разом із мінливим ландшафтом загроз кібербезпеці та вимогами бізнесу.

Крок 2: Дія, орієнтована на ризик, і розгортання #

Друга фаза розробки програми кібербезпеки зосереджена навколо дій, орієнтованих на ризик, і розгортання. Це передбачає створення ефективної командної структури, спрямованої на ретельне впровадження стратегії кібербезпеки. Ключовим компонентом цього етапу є розгортання необхідних інструментів і технологій, які втілюють стратегічний план у життя. Перетворення стратегій високого рівня на дієві практичні кроки має важливе значення для ефективного виконання. Стратегічний розподіл ресурсів, особливо в областях з вищими передбачуваними ризиками, гарантує пріоритетність і посилення критичних аспектів мережі. Крім того, неможливо переоцінити важливість постійного моніторингу та управління системами безпеки, оскільки вони є життєво важливими для підтримки ефективності заходів безпеки та для швидкого усунення нових загроз.

Крок 3: Постійне повторне калібрування та оптимізація #

На завершальному етапі фокус зміщується на постійне повторне калібрування та оптимізацію програми кібербезпеки. Ця фаза вимагає підтримки підзвітності на всіх рівнях організації та підвищення можливостей реагування на інциденти для забезпечення швидкої та ефективної реакції на загрози.

Культивування культури, яка обізнана з кібербезпекою, через освіту співробітників і зацікавлених сторін про найкращі методи безпеки та ризики, формує основу цього етапу. Регулярні оцінки та прозоре інформування ключових зацікавлених сторін про ефективність програми мають вирішальне значення для створення середовища постійного вдосконалення. Стратегії кібербезпеки повинні постійно переглядатися та вдосконалюватися на основі поточних оцінок. Цей адаптивний підхід гарантує, що заходи кібербезпеки залишаються ефективними та актуальними, узгоджуючи їх із бізнес-середовищем, що постійно змінюється, і мінливим ландшафтом кіберзагроз.

Підготовка до нових тенденцій і майбутніх загроз #

Майбутнє кібербезпеки у фінансовому секторі, ймовірно, буде сформоване новими технологіями та розвитком ландшафту загроз.

ШІ та машинне навчання в кібербезпеці #

Інтеграція штучного інтелекту та машинного навчання в інструменти кібербезпеки призведе до революції у виявленні загроз і реагуванні на них. Ці технології можуть аналізувати величезні масиви даних, щоб ідентифікувати шаблони, що вказують на кіберзагрози, пропонуючи рівень швидкості та ефективності, недосяжний для аналітиків.

Роль блокчейну в підвищенні безпеки #

Технологія блокчейн може запропонувати розширені функції безпеки для фінансових транзакцій і цілісності даних. Його децентралізований і незмінний характер робить його привабливим варіантом для захисту записів транзакцій і запобігання шахрайству.

Кіберзагрози постійно розвиваються; громадські банки повинні залишатися пильними та активними у своїх зусиллях щодо кібербезпеки. Застосування комплексних інтегрованих стратегій кібербезпеки, зосередження на кіберстійкості та підготовка до майбутніх технологічних досягнень є ключовими для захисту від різноманітних та складних загроз у кібернетичному середовищі. Випереджаючи ці виклики, фінансові установи можуть забезпечити безпеку та безперервність своїх операцій, зберігаючи довіру та впевненість своїх клієнтів». ***(Cybersecurity Tactics***

FinServ Institutions Can Bank On in 2024 // The Hacker News (https://thehackernews.com/2024/02/cybersecurity-tactics-finserv.html). 14.02.2024).

***

«Sophos, світовий лідер у сфері інновацій та надання кібербезпеки як послуг, опублікував результати свого четвертого звіту «Майбутнє кібербезпеки в Азіатсько-Тихоокеанському регіоні та Японії» у співпраці з Tech Research Asia (TRA). У звіті встановлено, що 90 відсотків респондентів, які працюють у сфері кібербезпеки та ІТ, страждають від виснаження та втоми.

Дослідження показало, що виснаження відчувається майже в усіх аспектах діяльності з кібербезпеки, причому 30 відсотків респондентів сказали, що відчуття вигорання «значно» зросло за останні 12 місяців, а 41 відсоток сказав, що це вигорання робить їх «менш старанними» 17% респондентів вказали, що виснаження чи втома сприяли або були безпосередньо відповідальними за порушення кібербезпеки, а 17% компаній мали час реагування на інциденти кібербезпеки менший за середній.

Причини виснаження та втоми кібербезпеки

П’ять основних причин кібервигоряння та втоми у звіті включають:

Брак ресурсів для підтримки діяльності з кібербезпеки

Буденність ролі, яка створює відчуття одноманітності

Підвищений рівень тиску з боку правління та/або виконавчого керівництва

Постійне перевантаження попереджень від інструментів і систем

Зростання загрозливої активності та впровадження нових технологій, які сприяють більш складному, постійному навколишньому середовищу.

Вплив виснаження та втоми на працівників кібербезпеки

Дослідження показало, що в Азіатсько-Тихоокеанському регіоні та Японії (APJ):

41% вважають, що вони недостатньо старанні у своїй роботі

34% відчували підвищений рівень тривоги, якщо зазнали порушення чи атаки

31% відчувають цинізм, відстороненість та апатію до діяльності з кібербезпеки та своїх обов’язків

30% заявили, що це спонукає їх або звільнитися, або змінити кар'єру (23% опитаних діяли згідно з цим і звільнилися)

10% відчувають провину за те, що не можуть зробити більше, виконуючи свою роль, щоб підтримати заходи з кібербезпеки

«У той час, коли організації борються з дефіцитом навичок кібербезпеки та дедалі складнішим середовищем кібератак, стабільність і продуктивність співробітників є критично важливими для надійного захисту бізнесу. Вигорання та втома підривають ці сфери, і організаціям необхідно активізуватися, щоб надавати належну підтримку співробітникам, особливо коли, згідно з нашим дослідженням, 17% респондентів вказали, що виснаження або втома через кібербезпеку сприяли або були безпосередньо відповідальними за порушення кібербезпеки», - сказав Аарон Бугал, технічний директор Sophos.

«Цей звіт Sophos і TRA дає своєчасне розуміння кібер-стресу в організації та демонструє, що все потрібно змінити. Хоча простого виправлення немає, коригування ставлення значною мірою допоможе визначити правильні очікування щодо того, що означає розвиватися в кіберстійкий бізнес. Правління та виконавчі комітети повинні стимулювати зміни та вимагати відповідальності від своїх заступників, по суті, для кращого управління навколо кіберпідходів. Однак їм потрібно чітко сформулювати свою відповідальність за розробку та підтримку плану, оскільки кібербезпека зараз є постійно інтерактивним видом спорту, і потрібна команда, яка цілодобово забезпечує адекватне покриття».

Вплив виснаження та втоми кібербезпеки на бізнес-операції

Було чотири ключові сфери, де кібервигоряння та втома безпосередньо вплинули на бізнес-операції:

Безпосередній внесок у порушення: 17% респондентів вказали, що виснаження або втома в кібербезпеці сприяли або були безпосередньо відповідальними за порушення кібербезпеки

Повільніший час реагування на інциденти кібербезпеки: 17% компаній мали час реагування на інциденти кібербезпеки нижчий за середній

Втрата продуктивності: компанії відчувають втрату продуктивності на 4,1 години на тиждень серед фахівців з кібербезпеки та IT, причому компанії на Філіппінах (4,6 години на тиждень) і Сінгапурі (4,2 години на тиждень) мають найгірший вплив, тоді як Індія та Японія (обидва) 3,6 години/тиждень) постраждали найменше

Звільнення та продовження роботи співробітників: у 23% компаній причиною звільнення спеціалістів із кібербезпеки та IT напряму назвали стрес і виснаження. Сінгапур склав 38% відставок, а Індія - 31%. Організації також відзначили, що в середньому 11% з них «перейшли» в якості співробітника відділу кібербезпеки або IT через те, що на людину вплинув стрес або виснаження. Малайзія (28% компаній) і Сінгапур (15%) мали найбільшу кількість такої практики». ***(90% of cybersecurity and IT professionals in APJ are impacted by burnout and fatigue: Sophos // Ada Derana (http://bizenglish.adaderana.lk/90-of-cybersecurity-and-it-professionals-in-apj-are-impacted-by-burnout-and-fatigue-sophos/). 13.02.2024).***

***

«Незважаючи на зміну ландшафту кібербезпеки, одне залишається ясним у 2024 році: наявність комплексного плану стратегії кібербезпеки, який узгоджується з цілями компанії та дотриманням нормативних вимог, має вирішальне значення для захисту компаній від кіберзагроз. Важливо пам’ятати, що бути в курсі кібербезпеки вимагає як уваги до деталей, так і широкої перспективи. Хоча відповідність нормативним вимогам і геополітичні сили можуть надати цінні вказівки для планування кібербезпеки, зрештою, рушійною силою повинні бути цілі компанії. У цій публікації блогу ми розглянемо деякі пропозиції щодо покращення вашої стратегії кібербезпеки у 2024 році.

Розвиток програми-вимагача 2.0: подвійне вимагання та крадіжка даних

Програмне забезпечення-вимагач 2.0 виходить за рамки шифрування даних, запроваджуючи новий рівень складності. На відміну від традиційного програмного забезпечення-вимагача, яке лише шифрує дані, програмне забезпечення-вимагач 2.0 робить крок далі, викрадаючи дані жертви перед їх шифруванням. Ця шкідлива техніка надає зловмисникам важіль впливу, навіть якщо жертва вирішить не

платити викуп. У таких випадках зловмисники мають можливість або передати викрадені дані конкурентам, або публічно розкрити конфіденційну особисту інформацію.

Цей метод подвійного вимагання посилює збитки, завдані атаками програм-вимагачів, оскільки жертви не лише стикаються з ризиком втрати даних, але й потенційно можуть завдати шкоди репутації внаслідок витоку даних. Одним із відомих випадків використання програм-вимагачів 2.0 є атака на Colonial Pipeline у травні 2021 року. Кіберзлочинці, які стояли за атакою, не лише зашифрували дані компанії, але й викрали значну кількість даних, перш ніж ініціювати вимогу викупу. Цей інцидент призвів до перебоїв у постачанні палива та підкреслив всю серйозність техніки подвійного вимагання.

Крім того, критичні системи, такі як промислові технології, транспортні системи та системи безпеки, ймовірно, будуть ставати все більш мішенню для атак програм-вимагачів.

Розширення поверхні атаки: розширені пристрої, розширені вразливості

З експоненціальним зростанням підключених пристроїв, таких як смартфони, розумні домашні гаджети та пристрої Інтернету речей (IoT), поверхня атаки значно розширилася. Якщо ці пристрої залишити незахищеними, вони можуть стати легкою мішенню для кібератак, дозволяючи зловмисникам зламати інші компоненти мережі. Організації повинні активно зміцнювати свої складні та взаємопов’язані IT-середовища. Це передбачає оперативне усунення вразливостей, впровадження надійних заходів автентифікації та відокремлення мереж для запобігання поширенню зловмисного програмного забезпечення.

Атака ботнету Mirai у 2016 році є яскравим прикладом того, як можна використовувати вразливі пристрої IoT. Атака скомпрометувала тисячі пристроїв IoT, таких як камери та маршрутизатори, і використовувала їх для запуску масштабних атак розподіленої відмови в обслуговуванні (DDoS). Цей випадок підкреслює важливість захисту всіх підключених пристроїв, щоб вони не стали точками входу для кібератак.

Безпека з нульовою довірою: долайте бар'єри довіри

Безпека з нульовою довірою, проактивна модель безпеки, базується на передумові, що жодна сутність, включно з тими, хто входить до мережі, не є за своєю суттю надійною. Відповідно до цієї моделі кожен користувач і пристрій повинні пройти процеси автентифікації та авторизації, перш ніж отримати доступ до ресурсів. Оскільки організації переходять на хмару та використовують гібридні моделі роботи, нульова довіра набуває все більшого значення. Це пов'язано зі зниженням ефективності традиційних моделей безпеки, таких як брандмауери, у таких динамічних середовищах.

Реалізація Google архітектури безпеки з нульовою довірою є добре відомим прикладом. Google прийняв модель, згідно з якою кожен користувач і пристрій, як у мережі, так і поза нею, повинні пройти автентифікацію та авторизуватися перед доступом до ресурсів. Цей підхід гарантує, що довіра не надається автоматично, і підвищує безпеку шляхом перевірки ідентифікаційних даних і застосування контролю доступу.

Майбутнє без пароля: зменшення ризиків безпеки

Усвідомлюючи притаманну вразливість паролів, широке впровадження автентифікації без пароля набирає обертів. У 2024 році я передбачаю постійний відхід від традиційних паролів, який буде спонуканий необхідністю посилення безпеки. Ця зміна передбачає впровадження більш надійних методів автентифікації, включаючи біометричну автентифікацію з використанням унікальних біологічних ознак і одноразових кодів доступу для додаткової безпеки. Біометрична автентифікація — це тип автентифікації, який використовує унікальні біологічні особливості людини, такі як відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока та розпізнавання голосу, для підтвердження особи. Біометрична автентифікація вважається більш безпечною, ніж традиційні паролі, оскільки її важче підробити та відтворити. Крім того, біометрична автентифікація забезпечує більшу зручність, оскільки користувачам не потрібно запам'ятовувати паролі або носити з собою фізичні маркери.

Одноразові паролі (OTP) — це тимчасові коди, які генеруються пристроєм або системою, зазвичай надсилаються на мобільний телефон або електронну пошту користувача, і які потрібно ввести, щоб завершити процес входу. На відміну від традиційних паролів, одноразові паролі дійсні для одноразового використання та генеруються випадковим чином, тому їх набагато важче передбачити або викрасти. Одноразові паролі є популярною формою двофакторної автентифікації (2FA) і часто використовуються разом із традиційними паролями для підвищення безпеки.

Подвійна роль штучного інтелекту в кібербезпеці: посилення захисту та нападу

Використання штучного інтелекту (ШІ) революціонізує ландшафт кібербезпеки з його потенціалом для розробки вдосконалених механізмів захисту, включаючи системи виявлення загроз із можливістю аналізу масивних наборів даних для виявлення потенційних атак. Однак штучний інтелект також використовується для розробки більш складних кібератак. Кіберзлочинці використовують штучний інтелект для автоматизації різних завдань, зокрема виявлення вразливостей у програмному забезпеченні, здійснення фішингових атак і уникнення традиційних заходів безпеки.

Хоча визнається, що генеративний штучний інтелект має потенціал для покращення й автоматизації тактик соціальної інженерії, реальність така, що випадки соціальної інженерії на основі штучного інтелекту наразі рідкісні або взагалі відсутні. Примітно, що звіт Verizon про порушення даних і розслідування за 2023 рік (DBIR) не повідомляв про жодні випадки участі ШІ в атаках соціальної інженерії. Очікується, що це збережеться в 2024 році завдяки ефективності традиційних методів соціальної інженерії, які дають успішні результати, протистоячи необхідності інвестувати в більш складні методи.

Для більшого «кібер» блага: тісніша співпраця між державними, приватними та освітніми установами

Цей спільний підхід не тільки покращить базові показники зрілості кібербезпеки, але й запропонує нові перспективи та інноваційні рішення. Крім того, це допоможе вирішити проблеми, пов’язані з браком кваліфікованих

кіберпрофесіоналів. Органи місцевого самоврядування можуть взяти на себе роль посередника та адміністрування централізованих кіберпослуг/рішень для інших рівнів управління. Такий підхід полегшить навантаження на тих, хто «недостатньо обслуговується в кібернетичному просторі», і забезпечить економію за рахунок масштабу, яка інакше була б недосяжною. У міру розширення співпраці та отримання відчутних переваг довіра між різними залученими організаціями продовжуватиме зростати.

Ще один нюанс полягає в тому, що використання ШІ для розвитку робочої сили в усьому світі може запропонувати шлях до стійких програм кібербезпеки, що робить його цінною інвестицією в майбутнє. Традиційні інструменти автоматизації, такі як оркестровка безпеки, автоматизація та реагування (SOAR), можуть певною мірою допомогти, але інструменти штучного інтелекту пропонують додаткові можливості примноження сили, які можуть активно керувати SOAR. Оскільки ці інструменти навчаються та вдосконалюються в певному середовищі, вони можуть виконувати більше щоденних завдань, звільняючи обмежені людські ресурси для речей, які потребують незалежного мислення. Це особливо важливо для завдань синьої команди, таких як керування вразливістю, реагування на інциденти та захист мережі. Покращуючи потужність інструментів штучного інтелекту, не тільки фахівці з кібербезпеки можуть отримати вигоду, але й спеціалісти з IT-операцій також можуть взяти на себе більше кіберфункцій, особливо в організаціях, які не можуть дозволити собі спеціалізованого персоналу з кібербезпеки.

Геополітичні конфлікти: каталізатор впливу на кібербезпеку

Так само, як геополітичні сили формують глобальну економіку, вони також можуть впливати на кібербезпеку. Триваючий конфлікт між Ізраїлем і ХАМАС, наприклад, може порушити ланцюжок постачання кібербезпеки, оскільки Ізраїль є відомим центром інновацій у сфері кібербезпеки. Водночас українсько-російський конфлікт також має значний вплив на глобальну кібербезпеку. Після вирішення організації можуть відновити напади з боку суб’єктів загрози національній державі з цього регіону. Відомо, що ці актори використовують більш витончені методи атак завдяки великій кількості ресурсів. Хоча неможливо передбачити результат цих

конфліктів, їх розгортання та розв'язання матиме далекосяжні наслідки для кібербезпеки в усьому світі не лише у 2024 році, а й упродовж багатьох років.

Ландшафт відповідності

Як зазначає Сандра Увадеде, CISM, CISA, фахівець із безпеки в Bank of Kigali: «У сфері кібербезпеки для організацій стає найважливішим дотримання визнаних стандартів, які зміцнюють не лише інформаційну безпеку, але й забезпечують безперервність бізнес-операцій. ISO 27001, всесвітньо визнаний стандарт, присвячений управлінню інформаційною безпекою з акцентом на ризики. Організації, сертифіковані згідно з ISO 27001, виявляють, що приймають постійну оцінку ризиків, що є ключовим аспектом у сучасному динамічному ландшафті загроз. У нюансному підході інтеграція принципів ISO 31000 для управління ризиками узгоджує практику з більш широкими організаційними стратегіями ризиків.

Окрім безперервності бізнесу, ISO 22301:2019 забезпечує надійну основу для створення, впровадження та постійного вдосконалення системи управління безперервністю бізнесу. Що робить його примітним, так це його застосування в організаціях будь-якого розміру, галузі чи сектора. Крім того, він повністю узгоджується з іншими стандартами систем управління, такими як ISO 9001 та ISO/IEC 27001, що дозволяє легко інтегрувати його в існуючі системи управління.

Враховуючи регіональні нюанси, BSI IT-Grundschutz, розроблений у Німеччині, хоч і використовується в основному в німецькомовних регіонах, пропонує принципи, які можна адаптувати в глобальному масштабі. Його регулярні оновлення забезпечують відповідність кіберзагрозам, що розвиваються, що робить його універсальним вибором. У поєднанні з галузевими стандартами IT-Grundschutz стає наріжним каменем у створенні індивідуальної системи безпеки, яка ефективно усуває унікальні організаційні ризики».

Правила кібербезпеки Комісії з цінних паперів і бірж США (SEC), які набудуть чинності в четвертому кварталі 2024 року, почали суттєво змінювати ландшафт кібербезпеки, особливо для державних компаній та інвестиційних компаній. Це правило вимагає посиленого розкриття інформації про кібербезпеку,

щоб надати інвесторам краще розуміння того, як компанії керують кіберризиками. Одним із найпомітніших впливів стало підвищення прозорості практик кібербезпеки. Тепер компанії зобов'язані повідомляти про інциденти кібербезпеки протягом певного періоду часу (чотири дні), пропонуючи більш швидке розуміння частоти, масштабу та впливу кіберзагроз. Ця зміна призвела до більшого акценту на проактивному управлінні кіберризиками, оскільки компанії прагнуть уникнути репутаційної шкоди, пов'язаної з публічним оприлюдненням про порушення безпеки.

«Це правило має значний вплив на ландшафт кібербезпеки у 2024 році, оскільки воно підштовхне організації до збільшення інвестицій в інфраструктуру та досвід кібербезпеки», — говорить Іскандар Ісламов, директор з кібербезпеки. «Компанії, усвідомлюючи зростання регулятивних очікувань і контролю з боку інвесторів, заохочували посилювати свій кіберзахист. Це включає впровадження передових технологій безпеки, таких як системи виявлення загроз на основі штучного інтелекту, а також посилення уваги до програм навчання та підвищення обізнаності співробітників. Крім того, це правило стимулюватиме зростання ринку страхування кібербезпеки, оскільки компанії прагнуть пом'якшити фінансові ризики, пов'язані з потенційними порушеннями. Загалом Правило кібербезпеки SEC не лише підняло планку для корпоративних практик кібербезпеки, але й суттєво сприяло розвитку та вдосконаленню індустрії кібербезпеки в цілому».

PCI DSS 4.0 представляє 64 нові вимоги, що передбачають обов'язкову відповідність організації, що означає відхід від простих технічних специфікацій у бік більш комплексної точки зору безпеки. У формулюванні цього нового стандарту використовується підхід нульової довіри, що дає можливість організаціям вдосконалювати свої системи автентифікації відповідно до суворих вимог щодо захисту даних. Хоча попередня версія, 3.2.1, діятиме до 31 березня 2024 року, організаціям вкрай необхідно розпочати підготовку до прийняття останньої ітерації. Цей проактивний підхід має вирішальне значення для ефективного пом'якшення потенційних ризиків безпеці. Забезпечення відповідності стандарту PCI DSS 4.0 — це не просто регулятивне зобов'язання, а

стратегічний імператив у зміцненні захисту від витоку даних і забезпеченні безпеки інформації про кредитні картки.

Надайте пріоритет стратегії кібербезпеки

У 2024 році в умовах кібербезпеки, що постійно розвивається, компанії повинні розробити пріоритетні комплексні плани стратегії кібербезпеки, які відповідають цілям компанії та дотриманню нормативних вимог. У цьому дописі в блозі висвітлюються ключові тенденції та виклики, зокрема поширення програм-вимагачів 2.0 із подвійним вимаганням і крадіжкою даних, розширення поверхні атаки через підключені пристрої, важливість впровадження заходів безпеки з нульовою довірою, перехід до автентифікації без пароля, подвійна роль AI у зміцненні оборони та наступу, потреба в тіснішій співпраці між державними, приватними та освітніми установами, а також вплив геополітичних конфліктів на кібербезпеку. Розуміючи та вирішуючи ці проблеми, компанії можуть краще захиститися від кіберзагроз і захистити свої цінні активи». ***(Ramona Ratiu. Securing the Future: Enhancing Cybersecurity in 2024 and Beyond // ISACA (https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/securing-the-future-enhancing-cybersecurity-in-2024-and-beyond). 12.02.2024).***

***

«Згідно з новим дослідженням, понад 50% діючих фахівців з кібербезпеки визнали, що припускалися помилок на початку своєї кар'єри через брак технічних знань.

Дослідження, проведене «Лабораторією Касперського» по всьому світу, показало, що цей відсоток зростає до майже 60% серед тих, хто має лише від двох до п'яти років досвіду роботи в сфері кібербезпеки.

Згідно з дослідженням, фахівці з кібербезпеки зазначили, що їм бракує практичних і теоретичних знань у кількох сферах

43% визнали, що не оновлювали програмне забезпечення, 42% сказали, що винні у використанні слабких паролів, які легко вгадуються, а 40% опитаних стверджували, що нехтували своєчасним створенням резервних копій.

Усі ці помилки, за словами професіоналів, були зроблені на ранньому етапі кар'єри. У Північній Америці та Азіатсько-Тихоокеанському регіоні використання застарілих заходів безпеки також вказувалося як типова помилка експертів з кібербезпеки на початку своєї кар'єри.

Kaspersky сказав, що дослідження підкреслює важливість надійного навчання для фахівців з кібербезпеки на початковому етапі, особливо з огляду на те, що понад дві третини (64%) усіх інцидентів безпеки сталися через людську помилку.

Деяким працівникам кібербезпеки «не вистачає впевненості»

За останні два роки кожна організація стала жертвою «принаймні одного» інциденту кібербезпеки в результаті недостатньо кваліфікованого або недостатньо підготовленого персоналу, за словами Касперського.

Недостатньо підготовленому персоналу потрібно більше часу, щоб освоїтися на своїх посадах, причому майже половина (46%) усіх працівників кібербезпеки заявили, що їм знадобилося більше року, щоб відчути себе впевнено на своїх посадах у сфері інформаційної безпеки.

У той час як 31% вдалося впоратися з роботою протягом одного-двох років, майже 10% стверджували, що їм знадобилося два-три роки, а 6% сказали, що це зайняло більше трьох років.

Команди з підбору персоналу компанії також повинні взяти на себе певну частину провини, однак, за словами Касперського, понад третина (34%) респондентів сказали, що вони пройшли три чи більше невдалих співбесіди, перш ніж бути обраними на посаду InfoSec.

Це вказує на прогалини в знаннях компаній загалом, що свідчить про те, що багато компаній не знають, що шукати в експертах з кібербезпеки.

Нещодавнє дослідження кадрової компанії Hays показало, що понад три чверті (78%) роботодавців у сфері технічних технологій були готові наймати IT-спеціаліст без необхідних вимог, щоб спробувати пом'якшити розрив у технічних навичках з наміром підвищити кваліфікацію в майбутньому.

За поточними оцінками, дефіцит кадрів у сфері кібербезпеки становить майже 4 мільйони, дефіцит навичок значно ускладнює завдання пом’якшення ризиків кібербезпеки.

«Не секрет, що формальні програми навчання часто не встигають за галузевими розробками, і це особливо вірно для сфери кібербезпеки», — сказала Марина Алексєєва, директор з кадрів Kaspersky.

«Той факт, що багато співробітників на ринку можуть мати обмежені практичні навички або прогалини в своїх знаннях, підкреслює важливість всебічного процесу адаптації з акцентом на взаємному навчанні та означає, що компанії повинні приділяти більше уваги підвищенню кваліфікації своїх співробітників», – додала вона.

Дослідження Kasperysky пропонує програму навчання, яка є гнучкою та адаптованою до вимог InfoSec, що постійно змінюються, а також заохочує використання практичних вправ з кібербезпеки та процедур підвищення кваліфікації». ***(George Fitzmaurice. Cyber security professionals admit “knowledge gaps” have led to serious security blunders // Future US, Inc. (https://www.itpro.com/business/careers-and-training/cyber-security-professionals-admit-knowledge-gaps-have-led-to-serious-security-blunders). 19.02.2024).***

***

«Ландшафт кіберзагроз розвивається блискавично, а атаки стають все більш складними, незрозумілими та спрямованими на сторонніх постачальників. Хоча впізнавані бренди залишаються головними цілями, атаки зараз впливають на організації, яким раніше не доводилося так сильно турбуватися про кіберзагрози.

Наприклад, згідно зі «Звітом про розслідування витоку даних за 2023 рік» (потрібна реєстрація), компанії з менш ніж 1000 співробітників і компанії з понад 1000 співробітників стикаються з подібними проблемами. Дослідники виявили 699 інцидентів із 381 підтвердженим розкриттям даних для малого бізнесу та 496 інцидентів із 227 підтвердженими розкриттям даних для великого бізнесу.

Наче більше атак не викликає занепокоєння, вартість витоку даних продовжує зростати з року в рік. Відповідно до «Звіту про вартість витоку даних за 2023 рік» (потрібна реєстрація), у 2023 році збитки з витоку даних становили в середньому 4,45 мільйона доларів США, що на 15% більше за три роки. Водночас за останні кілька років рівень інфляції коливався в середньому від 3% до 6%. Малі підприємства вже намагаються подолати це економічне зростання — оскільки вартість витоку даних вдвічі або більше, ніж інфляція, одне злам даних може підірвати загальні цілі компанії щодо прибутку.

Ідеальний шторм

У відповідь на збільшення обсягу, складності та наслідків витоку даних уряди та регуляторні органи продовжують запроваджувати та нав’язувати суворіші вимоги дотримання. Щоб відповідати цим вимогам і надати клієнтам впевненість у своїй кібербезпеці, малим підприємствам, які і без того страждають від низьких доходів і операційної маржі, потрібно витрачати більше грошей на технології безпеки та аудити. Як керівник CISO або C-suite, який сьогодні намагається збалансувати розвиток бізнесу, відповідність вимогам і безпеку, ви можете відчувати, що перед вами ідеальний шторм.

Для цих вищих керівників, які намагаються досягти зростання та захистити дані, пошук рентабельних інвестицій у кібербезпеку, які залишаються в межах консервативного бюджету, може здатися непосильним і майже неможливим.

Збалансування інновацій у продуктивності бізнесу, таких як штучний інтелект, із відповідальною безпекою є яскравим прикладом напруги, з якою стикаються керівники. Хоча штучний інтелект обіцяє покращені рішення, автоматизацію та більш ефективне використання персоналу, він також вимагає безпрецедентного доступу до даних, щоб функціонувати належним чином, як великий миготливий знак «нападі на мене» для суб’єктів загрози.

Історично склалося так, що організації чекають інциденту, а потім купують інструмент безпеки. Проте сучасний ландшафт загроз вимагає проактивного мислення, оскільки існує незліченна кількість потенційних точок вторгнення та акторів, від дрібних злодіїв до ворожих національних держав, які намагаються

отримати доступ до конфіденційних даних або зробити політичну заяву. З огляду на те, що обчислювальні ресурси зараз значною мірою знаходяться в хмарі, замість того, щоб акуратно зберігатися на місці, обсяг того, що CISO повинні намагатися захистити, фактично подвоївся. Оскільки організації впроваджують програми програмного забезпечення як послуги (SaaS) для забезпечення продуктивності та безперервності бізнесу, вони експоненціально розширюють свою поверхню атаки за допомогою нових точок доступу, таких як API. По суті, один малий бізнес може відчувати себе так, ніби він керує безпекою для кількох компаній, оскільки кожен бізнес-напрямок від продажів до маркетингу та кредиторської заборгованості створює власну цифрову екосистему.

Розрив у навичках між професіоналами з безпеки створює додаткову напругу для CISO, які шукають компетентного керівництва для проактивних стратегій. Вони стикаються з нестачею талантів разом із різким зростанням вартості програмного забезпечення, суворими стандартами відповідності від багатьох аудиторських органів, зростанням премій за кіберстрахування або навіть відмовою в страховому покритті та можливістю особистої відповідальності, оскільки регулятори та прокурори вживають карних заходів проти керівників у разі інцидентів. як порушення даних. Щоб забезпечити розвиток та інновації під час навігації на цьому складному мінному полі, підприємства все більше покладаються на автоматизацію та ШІ.

Порівняйте бізнес-цілі, безпека

Хоча автоматизація може допомогти оптимізувати надлишкові процеси, а штучний інтелект може допомогти в робочому процесі виявлення та реагування, зручні для інтеграції інструменти безпеки, які забезпечують справжнє повернення інвестицій, залишаються першорядними. Інтегруючи інструменти безпеки та кількісні ключові показники ефективності у свої щоденні процеси, малі підприємства можуть точніше узгодити свої бізнес-цілі та стан безпеки.

Калькулятори та показники, які чітко перетворюють технічні можливості на реальну економію та зниження ризиків, допомагають виправдати покупки сумнівним керівникам рівня C. Команди вищого керівництва відповідають за те,

щоб бізнес залишався платоспроможним, тобто вони повинні розуміти, як показники безпеки впливають на їхній фінансовий результат.

Крім того, вони повинні розуміти покриття, яке забезпечують їхні інвестиції в безпеку. Відключені технології можуть створювати прогалини в безпеці та сліпі зони, створюючи для них ризик витоку даних. Щоб вирішити цю проблему, навіть малі підприємства повинні консолідувати рішення для кількох внутрішніх команд, безпеки, шахрайства та IT. Роблячи це, вони отримують розширене уявлення про свою безпеку та конфіденційність, водночас маючи можливість визначити майбутні інвестиції, які додадуть цінності їхнім програмам, полегшуючи отримання дозволів на нові продукти.

Звичайно, це легше сказати, ніж зробити. Холодна, сувора правда полягає в тому, що підвищена складність при збалансуванні безлічі внутрішніх і зовнішніх зацікавлених сторін серед загрозливого середовища, яке постійно прискорюється, є нашою новою нормою.

І керівники вищого рангу, і CISO повинні узгодити цю реальність і належним чином налаштувати процеси. Бізнес-інновації мають продовжуватися, незважаючи на постійну зміну загроз. Хоча якісні постачальники можуть надати підтримку, кібербезпека залишається бурхливим морем для лідерів. Але завдяки співпраці, турботі та проактивному плануванню організації можуть залишатися на плаву, навіть якщо вода залишається неспокійною». ***(Rita Gurevich. How CISOs Balance Business Growth, Security in Cyber-Threat Landscape // Informa PLC (ww.darkreading.com/vulnerabilities-threats/how-cisos-balance-business-growth-security-cyber-threat-landscape). 21.02.2024).***

***

«З огляду на збільшення кібератак, спрямованих на малий і середній бізнес (SMBs), ця група збільшує свій бюджет, персонал, інструменти та вдосконалення, щоб зробити безпеку пріоритетом. Грейсон Мілборн, директор відділу аналітики безпеки в OpenText Cybersecurity, надає дієві поради малому та середньому бізнесу щодо подальшого посилення кібербезпеки.

Ландшафт кібербезпеки постійно розвивається; зловмисники стають розумнішими та стійкішими. Як наслідок, компанії повинні інвестувати більше в безпеку, щоб залишатися попереду або, у деяких випадках, наздоганяти.

Кібербезпека є ключовим пріоритетом для компаній будь-якого розміру і залишатиметься таким у найближчому майбутньому. Результати нещодавнього глобального опитування програм-вимагачів OpenText Cybersecurity 2023 Відкриває нове вікно підтвердили, що малому та середньому бізнесу відомо про ризики програм-вимагачів (90% малих і середніх підприємств зазначили, що вони надзвичайно або дещо стурбовані атаками програм-вимагачів). І в результаті цих занепокоєнь вони займають набагато активнішу позицію для покращення своєї безпеки. Роблячи це, вони наздоганяють підприємства у своїй обороні.

Підвищення обізнаності про безпеку, команди та бюджети

Наприклад, 83% малих і середніх підприємств повідомили, що вимагають від співробітників проходити навчання з питань безпеки та фішингу, і вони також проводять навчання частіше. З цих респондентів 38% проводять навчання щоквартально і 41% двічі на рік. Більшість підприємств (96%) вимагають регулярного навчання з питань безпеки або фішингу, а 40% підприємств проводять навчання з питань безпеки раз на квартал, а 34% – двічі на рік. Такий підвищений акцент на навчанні з питань безпеки для малого та середнього бізнесу є особливо надихаючим, враховуючи, що існувала також розбіжність у розумінні того, хто є потенційною ціллю програм-вимагачів.

Незважаючи на добре задокументовану нестачу кадрів із кібербезпеки, малий і середній бізнес (44%) і підприємства (43%) планують розширити свої команди безпеки наступного року для боротьби зі зростаючими загрозами. З цієї ж групи 57% малих і середніх підприємств і 53% підприємств планують збільшити витрати на безпеку в 2024 році. Серед малих і середніх підприємств, які планують збільшити витрати на безпеку, 40% планують збільшити бюджети на 5-10%; 33% планують збільшити бюджети на 10-20%. Окрім більш частих тренінгів з питань безпеки та збільшення витрат, опитування також показало, що кількість малих і

середніх підприємств з планами відновлення та рішеннями для резервного копіювання зросла, що важливо для підвищення кіберстійкості.

Спрощення безпеки за допомогою потужніших рішень

Ще одна схожість у результатах опитування полягає в тому, що більшість малих і середніх підприємств і підприємств використовують від 2 до 3 рішень безпеки. 58% малих і середніх підприємств використовують від 2 до 3, близько 5% використовують більше п'яти рішень безпеки, а 10% використовують лише одне. У 2022 році 52% малих і середніх підприємств використовували від 2 до 3 рішень безпеки, але 21% використовували чотири або більше рішень. Ці висновки можуть вказувати на тенденцію консолідації інструментів, яка допомагає спростити процеси безпеки, зменшити витрати та підвищити ефективність.

6 ключових кроків для підвищення кібервідмовостійкості SMB

Разюча схожість у тому, як малий і середній бізнес і підприємства бачать кібербезпеку, а також кроки, які вони вживають для пом'якшення атак, надихають. Щоб ще більше підвищити кіберстійкість, розгляньте профілактичні кроки нижче.

Створення кібер-обізнаної культури: коли співробітники усвідомлюють, як їхня поведінка може поставити під загрозу свою організацію, вони матимуть кращі можливості для запобігання атакам. Навчання співробітників найкращим практикам безпеки, таким як розпізнавання фішингових електронних листів, текстових повідомлень або підозрілих посилань, є важливим для мінімізації можливостей програм-вимагачів. Також важливо, щоб корпоративна культура заохочувала чесність і прозорість, щоб співробітники відчували себе впевнено, повідомляючи про помилку або проблему, не боячись покарання. Регулярне підкріплення цього повідомлення та проведення тренінгів з питань безпеки та оцінювання посилять бажану культуру.

Оновлення програмного забезпечення. Забезпечення того, щоб пристрої працівників і пов'язані з організацією системи оновлювалися останніми виправленнями безпеки, також є одним із основних принципів, яких мають дотримуватися SMB. Увімкнення автоматичних оновлень для операційних систем і

безперервне антивірусне сканування значною мірою допоможуть закрити відомі вразливості та спроби фішингу.

Інструменти виявлення та моніторингу: впровадження інструментів моніторингу мережі та кінцевих точок у режимі реального часу для виявлення незвичайних або підозрілих дій має вирішальне значення для виявлення загроз. Вибір багаторівневих рішень із аналізом загроз для моніторингу електронної пошти, Інтернету та хмарних ризиків також зменшує ймовірність злому. Я також рекомендую високоавтоматизовані рішення, які потребують меншого професійного керування безпекою для швидшого виявлення, реагування та відновлення даних у разі атаки.

Надійні плани відновлення: Надійний план відновлення, який використовує рішення для резервного копіювання даних, є останньою частиною головоломки кібервідмовостійкості. Для малого та середнього бізнесу доступні численні послуги резервного копіювання за різними цінами. Наприклад, резервне копіювання з повітряним проміжком є недорогим способом зберігання копії важливих даних в автономному режимі. Цей додатковий захист у режимі офлайн унеможливлює злом. Плани відновлення допомагають малим і середнім підприємствам та всім організаціям швидко відновлюватися після атаки програм-вимагачів. Розробка та регулярне оновлення планів реагування та відновлення допомагає бути готовим і перевіряти ефективність плану.

Захист віддаленого доступу. Оскільки багато співробітників продовжують працювати вдома або в гібридних місцях, захист їхніх ноутбуків, мобільних телефонів та інших кінцевих точок є критично важливим. Хоча громадські точки доступу Wi-Fi є привабливими та простими варіантами, вони «переконливі» з високим ризиком і часто небезпечні. Використання віртуальних приватних мереж (VPN) і вимога багатофакторної автентифікації для всіх пристроїв і систем є двома простими й ефективними способами захисту віддаленого доступу.

Не забувайте про основи безпеки: у сучасну епоху цифрових технологій легко забути основи фізичної безпеки — ніколи не залишайте ноутбуки та настільні комп’ютери без нагляду. Усі пристрої повинні мати заставку, яка автоматично

блокується, коли вони одні, і вимагає пароля для запобігання несанкціонованому доступу. Подібним чином усвідомлення фізичного оточення, особливо поза офісом, може запобігти крадіжці інформації або облікових даних. Наприклад, серфінг через плече, форма крадіжки даних, коли злочинці просто дивляться на сусідні екрани, щоб викрасти облікові дані, є реальною загрозою для організацій.

Дорожня карта до більш безпечного майбутнього

Застосовуючи ці найкращі практики, малий і середній бізнес може значно зменшити шанси стати жертвою атак програм-вимагачів і краще захистити свої критично важливі бізнес-активи.

Глобальне опитування щодо програм-вимагачів відзначило, що підприємства малого та середнього бізнесу покращують свою кібербезпеку, але ще потрібно працювати над досягненням повної кіберстійкості, щоб протистояти зростаючим атакам. Передові практики, як-от побудова кібер-обізнаної корпоративної культури, впровадження рішень для виявлення атак і резервного копіювання, а також розробка плану відновлення, є важливими способами, за допомогою яких підприємства малого та середнього бізнесу можуть зміцнити свій захист і підвищити свою кібервідмовостійкість». ***(Grayson Milbourne. Vulnerable to Vigilant: SMBs Ramp Up Cybersecurity Efforts // Spiceworks Inc. (https://www.spiceworks.com/it-security/vulnerability-management/guest-article/vulnerable-to-vigilant-smbs-ramp-up-cybersecurity-efforts/). 22.02.2024).***

***

«У сучасну цифрову епоху кібербезпека швидко стала більше, ніж просто необхідністю; як я нещодавно писав, це водночас бізнес-імператив і конкурентна перевага для компаній, які роблять це проактивно та правильно.

Оскільки все більше регуляторних органів, як-от Управління з контролю за продуктами й ліками США та адміністрація Байдена, опублікували нові й оновлені рекомендації щодо кібербезпеки, організації закликають сприймати кібербезпеку не як перешкоду, а як актив, який може просунути їх вперед.

Ефективне управління кібербезпекою полягає не лише в захисті конфіденційної інформації; мова йде про збереження довіри та позиціонування

вашої компанії в авангарді ринку. Проактивні заходи кібербезпеки також можуть бути економічно ефективнішими, ніж реактивні.

У цій статті я досліджую важливість навмисного керування кібербезпекою за допомогою дієвих кроків, щоб гарантувати, що вона не керує вами.

Розуміння бізнес-ризиків кібербезпеки

Ландшафт кібербезпеки постійно змінюється зі швидким розвитком технологій. Те, як компанії планують, виявляють і реагують на загрози, також має розвиватися. Ці загрози можуть варіюватися від витоку даних до атак програм-вимагачів і фішингових атак. Ось деякі статистичні дані за 2023 рік:

• За даними IBM, у період з березня 2022 року по березень 2023 року середня вартість витоку даних серед 553 організацій у всьому світі становила 4,45 мільйона доларів.

• Компанія Sophos виявила, що середня сума викупу у відповідь на успішну атаку програм-вимагачів за попередні 12 місяців становила 1,54 мільйона доларів США. Крім того, респонденти в опитуванні 2023 року повідомили в середньому 1,82 мільйона доларів США про приблизні витрати на відновлення, включаючи такі витрати, як простої, оплата праці, витрати на пристрої та втрати можливостей для бізнесу.

• Ринкові дані та дослідницька компанія Statista пояснила, що світові річні витрати на кіберзлочинність досягли 8,15 трильйонів доларів США у 2023 році з очікуваним зростанням до 13,82 трильйонів доларів США до 2028 року.

Іншими словами, вартість ігнорування кібербезпеки набагато перевищує вартість проактивного вирішення проблем кібербезпеки.

Підводні камені кібербезпеки та розбудова надійної стратегії кібербезпеки

Щоб зрозуміти, як створити надійну стратегію кібербезпеки, давайте спочатку розглянемо загальні проблеми, з якими стикаються компанії у сфері кібербезпеки. Деякі з цих проблем включають, але не обмежуються:

• Складні кіберзагрози: передові та складні кібератаки, включно з програмами-вимагачами, фішингом і експлойтами нульового дня, вимагають надійних механізмів захисту.

• Дефіцит навичок: багатьом компаніям важко знайти й утримати кваліфікованих експертів, здатних ефективно керувати кіберзагрозами та реагувати на них.

• Технологічна складність: зростаюча складність IT-середовища, пристроїв Інтернету речей і різноманітних мереж ускладнює реалізацію безпечної інфраструктури кібербезпеки.

• Внутрішні загрози та недостатня обізнаність: співробітники або підрядники, які мають доступ до конфіденційної інформації, можуть ненавмисно або навмисно порушити безпеку. Обидва можуть бути недостатньо обізнаними щодо найкращих практик кібербезпеки, що може призвести до ризикованої поведінки, як-от натискання фішингових електронних листів або використання ненадійних паролів.

• Не розглядайте безпеку як стратегічну інвестицію: рентабельність інвестицій у кібербезпеку не завжди очевидна, тому важко виправдати вкладення грошей у неї. Це призводить до менших бюджетів, які не зовсім покривають необхідні витрати (див. наступний пункт).

• Бюджетні обмеження: заходи кібербезпеки вимагають інвестицій у технології, навчання та персонал. Багато компаній просто не мають бюджету.

• Відповідність нормативним вимогам. Дотримання та підтримання відповідності різним нормам і стандартам кібербезпеки може бути складним і ресурсомістким.

Важливо зазначити, що традиційної кібербезпеки підприємства недостатньо. Завдяки розширенню всесвіту підключених продуктів організації повинні оцінити поточний стан безпеки та створити план, який відповідає їхнім конкретним потребам.

Ефективний план реагування на інциденти виходить за рамки цих заходів. Це передбачає проактивний підхід до вивчення минулих інцидентів, як виявила моя компанія у звіті за 2022 рік, для постійного вдосконалення. Проактивний моніторинг, включаючи регулярні оновлення, ретельне керування виправленнями та впровадження систем постійного моніторингу, закладає основу для запобігання та пом’якшення загроз кібербезпеці.

Створюйте партнерства в бізнесі

Розробляючи свою стратегію кібербезпеки, пам’ятайте, що активна взаємодія з експертами та консультантами з кібербезпеки є бізнес-імперативом для компаній, які не знають, з чого почати свою стратегію безпеки. Своєчасна співпраця з цими експертами гарантує, що ваша організація випереджатиме нові виклики кібербезпеки.

Окрім простого дотримання вимог, мова йде про розуміння нюансів нормативних актів і отримання інформації про їхні наслідки.

Щоб побудувати надійну мережу підтримки кібербезпеки, активно шукайте партнерства, діліться думками та беріть участь у колективній обороні. Регулярно проводите комплексні перевірки відповідності, не лише як звичайне завдання, а як проактивний захід, щоб гарантувати дотримання найвищих стандартів.

Цей проактивний, стратегічний і спільний підхід зміцнює вашу організацію в умовах постійної зміни кібербезпеки. Крім того, сприяння культурі обміну інформацією з колегами галузі є важливим кроком, який гарантує, що кожна галузь постійно розпізнає загрози та може швидко діяти.

Будь-яка галузь настільки сильна, наскільки сильна її найслабша ланка. Завдяки обміну інформацією та регулярним аудитам ми можемо створити взаємопов’язану мережу, яка зміцнить галузь у цілому.

Зробити безпеку стратегічним імперативом проти. Центр витрат

Інвестиції в кібербезпеку – це інвестиції в довгостроковий успіх організації, які передбачають пріоритетність внутрішніх і зовнішніх стратегій для захисту ваших співробітників і клієнтів.

Як згадувалося в розділі «Пасткові камені кібербезпеки та розбудова надійної стратегії кібербезпеки» цієї статті, як співробітники, так і клієнти створюють можливі ризики для кібербезпеки. Минулого року, згідно зі звітами, 23andMe звинуватив своїх користувачів у масштабному витоку даних, який вплинув на 6,9 мільйонів клієнтів — реактивний підхід до проблем безпеки, які, ймовірно, слід було вирішити на ранніх етапах життєвого циклу розробки продукту. Цей приклад підкреслює важливість інвестування у внутрішні та зовнішні практики

кібербезпеки. Ваші продукти та послуги мають бути безпечними від початку до рук користувачів.

Ландшафт кібербезпеки, що розвивається

У середовищі загроз, що постійно змінюється, організації стикаються з динамічним викликом, який вимагає передбачення та здатності до адаптації.

Хоча такі досягнення, як штучний інтелект, приносять позитивні зміни, покладатися виключно на технології створює ризики. Надійна стратегія кібербезпеки включає активну позицію через багатогранний підхід, інтеграцію технологій, кваліфікований персонал і стратегічне планування. Це не тільки захищає від поточних загроз, але й зміцнює організації, щоб орієнтуватися в невизначеності завтрашнього дня.

У цьому ландшафті постійних змін стратегічні інвестиції в кібербезпеку стають не просто щитом, а й ключовим фактором стійкого успіху організації». ***(Mike Kijewski. How To Manage Your Cybersecurity So It Doesn't Manage You // Forbes (https://www.forbes.com/sites/forbestechcouncil/2024/02/23/how-to-manage-your-cybersecurity-so-it-doesnt-manage-you/?sh=783694e8313e). 23.02.2024).***

***

«Нове дослідження, проведене швейцарськими дослідниками, оголосило блокчейн найкращим показником у стартапах з кібербезпеки, випередивши такі важкі галузі, як штучний інтелект і хмарні сервіси, зайнявши перше місце.

Дослідження зміцнення під назвою «Вимірювання ефективності інвестицій у стартапи з інформаційної безпеки: емпіричний аналіз секторів кібербезпеки з використанням даних Crunchbase» було профінансовано підтримуваним державою Cyber-Defence Campus, організацією, яка об'єднує уряд, наукові кола та промисловість для кіберзахист.

Основним показником, який розглядалося в дослідженні, була прибутковість, сфера, в якій блокчейн-компанії значно перевищили конкуруючі сектори, головним чином завдяки ціновій ефективності їхніх базових токенів.

У ньому йдеться: «ми виявили, що сектор блокчейнів має найвищу очікувану річну арифметичну (AAR) і логарифмічну прибутковість на рівні 177,27% і 105,42% відповідно, що відповідає продуктивності криптовалют за період вибірки».

Порівнюючи цей сектор із найближчими конкурентами, дослідники виявили, що «добре відомі сектори, такі як штучний інтелект або машинне навчання, домінують з точки зору фінансування, тоді як приватна хмара домінує з точки зору загальної оцінки», але з точки зору середньої прибутковості, блокчейн подолав усі три сектори.

Дослідження також дійшло висновку, що блокчейн-компанії найшвидше виходять на IPO.

Для порівняння, електронні підписи зайняли більше часу, майже 10 років, а потім виявлення шахрайства та хмарна кібербезпека, які займали близько 7 років кожна. З іншого боку, Blockchain знадобилося лише три з половиною роки, щоб вийти на IPO з першого збору коштів.

Власна кібербезпека блокчейна? Могло б бути краще

Однією з частих проблем криптовалюти серед представників влади та учасників традиційного фінансового простору є її уявна відсутність безпеки. Організовані кіберзлочинці часто націлюються на організації, що створюють технологію, для великих багатомільйонних хакерів.

Одним із наймасштабніших в історії був злом Ronin Bridge у 2022 році. Хакери викрали понад 600 мільйонів доларів криптовалюти через вразливість у сайдчейні Ethereum Axis Infinity.

Лише минулого року були відомі хакерські атаки, націлені на Euler Finance ($200 млн), BonqDAO ($120 млн), Multichain ($126 млн), Poloniex ($114 млн) і Atomic Wallet ($100 млн), серед багатьох інших.

У звіті, опублікованому в жовтні минулого року, сума втрат у третьому кварталі 2023 року склала 685 мільйонів доларів. За оцінками, до кінця минулого року хакери викрали 2 мільярди доларів.

Тривожну кількість атак можна пов’язати з підтримуваною державою хакерською групою Північної Кореї Lazarus.

Нещодавно в неопублікованому звіті ООН говориться, що журі організації з моніторингу санкцій розслідує причетність Північної Кореї до криптоатак на суму 3 мільярди доларів.

Повідомляється, що ці атаки фінансують програму розробки ядерної зброї Північної Кореї». ***(Tim Hakki. Study: Blockchain Investment Leads in Performance Among Cybersecurity Startups // Cryptonews (https://cryptonews.com/news/study-blockchain-investment-leads-in-performance-among-cybersecurity-startups.htm). 23.02.2024).***

***

«Очікування на робочому місці різко змінилися за останні кілька років, але не більше, ніж коли мова йде про віддалену та гібридну роботу. У звіті LinkedIn підраховано, що 45% рекламованих вакансій на ринку праці Великобританії в серпні 2023 року були гібридними, що демонструє, наскільки усталеною є ця практика.

Дебати про те, чи гібридні та віддалені моделі робочого місця кращі для продуктивності, продовжують лютувати. Однак фактором, який потребує особливої уваги в гібридній компанії, є кібербезпека на робочому місці.

Минули ті часи, коли IT-відділи та групи кібербезпеки мали жорсткий контроль, коли всі були в одному місці та використовували лише захищені мережі. Сьогодні працівники часто мають можливість працювати поза офісом, далеко від контролю. Чи дотримуються віддалені та гібридні працівники ефективних практик безпеки кібербезпеки без такого контролю?

Головоломка з паролем

Захищені системи вимагають безпечних паролів — часто кількох. Знайти баланс між легкою доступністю та парольною фразою, яку важко зламати кіберзлочинцям, може бути важко. Якщо пароль важче вгадати, його легше забути.

Незважаючи на цей факт, дослідження GetApp показало, що більшість віддалених/гібридних співробітників малого та середнього бізнесу керують своїми

паролями на роботі, запам’ятовуючи їх, а потім доповнюють керування паролями або програмним забезпеченням. На додаток до цього, більше чверті вибірки записують свої паролі, тоді як трохи менше чверті використовують електронні таблиці, щоб документувати їх.

Цікаво побачити, що більшість опитаних віддалених співробітників покладаються на застарілі рішення, такі як ручка, папір і пам’ять. Хоча пам’ять є, мабуть, найбезпечнішим варіантом для захисту пароля від зловмисників, вона не завжди сприяє створенню унікальних паролів або ключів, які важко вгадати.

Однак унікальні паролі здаються звичайною практикою для віддалених/гібридних працівників. Тим не менш, багато працівників все ще використовують один головний пароль для всіх веб-сайтів. Що ще гірше, було помічено, що багато працівників, які не використовують унікальні паролі для кожного окремого сайту, кажуть, що використовують той самий пароль для робочих і особистих облікових записів, принаймні деякий час.

Кількість людей, які повторно використовують одні й ті самі паролі або, що ще гірше, діляться своїми паролями між обліковими записами, ймовірно, призведе до того, що менеджери, які зосереджуються на кібербезпеці, охолонуть. Ця, здавалося б, нешкідлива звичка може представляти реальний ризик, якщо хакер зможе отримати доступ до особистих облікових записів або паролів, оскільки їхні облікові записи на робочому місці також можуть бути скомпрометовані через розширення.

Як віддалені співробітники можуть зіграти свою роль у кіберзахисті

Віддалена/гібридна робоча сила може викликати побоювання щодо вразливості безпеки, але це також допомагає компаніям зосередитися на важливому факторі: методах безпеки, керованих працівниками. Це важливі способи захисту компанії від загроз, а додаткова складність керування розподіленою командою дає можливість переорієнтувати ці пріоритети.

Отримані дані свідчать про те, що багато працівників справляються із завданням підтримувати здорову практику кібербезпеки. Здається, безпека даних має серйозне значення для віддалених/гібридних співробітників малого та

середнього бізнесу у Великобританії, які захищають свої пристрої за допомогою різноманітних заходів. До них належать такі практики, як регулярне встановлення оновлень програмного забезпечення, використання двофакторної автентифікації в облікових записах і обов'язкове блокування робочих пристроїв, коли вони залишаються без нагляду.

Хоча ці результати показують, що хороші звички щодо кібербезпеки поширені серед віддалених співробітників, вони ще не на рівні більшості. Менше половини опитаних дотримуються таких важливих заходів безпеки, як встановлення оновлень програмного забезпечення або використання двофакторної автентифікації. Це прості практики, які не виконуються, що говорить про те, що можна зробити більше для зміцнення безпеки з боку як роботодавців, так і працівників.

Боротьба із загрозою фішингу

Фішинг становить великий ризик для кібербезпеки на робочому місці. Наявність заходів і підготовка співробітників до протидії цим загрозам має бути пріоритетом для віддалених і гібридних компаній.

Це особливо важливо зараз, оскільки загрози безпеці даних зростають. Дослідження показують, що переважна більшість працівників малого та середнього бізнесу отримували принаймні один фішинговий електронний лист на своєму робочому місці, причому більшість також зазнавали більше однієї спроби.

Фішингові електронні листи зазвичай помічають співробітники, і багато з них просто видаляють або повідомляють про атаку службам безпеки компанії. Більш обнадійливим є те, що працівники зазвичай змінюють свій пароль після спроби фішингу. Однак невелика частина співробітників визнає, що відкриває фішингові електронні листи та навіть натискає на наведені посилання, демонструючи, що необхідне подальше навчання тому, як виявляти фішингові загрози.

Загалом, видається, що серед віддаленого/гібридного персоналу є хороший рівень готовності до боротьби зі спробами фішингу. Проте все ще залишається питання про те, як ці атаки можуть розвиватися в майбутньому. Тому важливим кроком є відповідне навчання тому, як проявляються сучасні фішингові атаки, і

стежити за тим, як розвиваються подібні атаки. Зрештою, навіть якщо лише одна особа клацне тіньове посилання в організації, цього може бути достатньо, щоб скомпрометувати всю мережу компанії.

Що можуть зробити віддалені співробітники, щоб захистити себе та свою компанію

Є чіткі докази того, що віддалені/гібридні співробітники роблять багато для забезпечення ефективної реакції на кібербезпеку. Однак для захисту бізнесу можна зробити ще багато чого.

З ефективними методами введення паролів, чіткими вказівками та кроками щодо дій у надзвичайних ситуаціях. Доцільно також підвищити готовність, поширюючи інформацію про фішингові атаки серед персоналу. Це лише кілька дрібниць, які компанії можуть зробити, щоб значно покращити безпеку своїх даних і безпеку системи.

Загалом немає причин, щоб персонал віддаленої або гібридної компанії піддавався більшому, ніж зазвичай, ризику кібератаки. Однак результати підкреслюють важливість переконатися, що компанії надійно дотримуються важливих заходів безпеки». ***(David Jani. Are remote workers at greater risk of cybersecurity threats? // Future US, Inc. (https://www.techradar.com/pro/are-remote-workers-at-greater-risk-of-cybersecurity-threats). 23.02.2024).***

***

«У сучасному динамічному ландшафті кібербезпеки компаніям необхідно зайняти проактивну позицію щодо захисту даних як ніколи. Оскільки кібератаки стають питанням не «якщо» чи «коли», а радше «як часто», організації повинні зміцнити свій захист, щоб ефективно перешкоджати повторним вторгненням.

Сучасні атаки зловмисного програмного забезпечення більше не націлені лише на дані організації, а й на її рішення для резервного копіювання, забезпечуючи успіх спроб вимагання. Отже, компанії повинні впроваджувати заходи захисту даних, здатні захистити як їхні активи, так і сховища даних.

У багатьох випадках атаки зловмисного програмного забезпечення тепер включають подвійні або потрійні загрози вимагання, не лише приховуючи доступ до даних, але й загрожуючи їх розкриттям у темній мережі. Переговори зі зловмисниками стають марними, коли дані досягають цієї сфери, що призводить до значних фінансових втрат і непоправної шкоди репутації.

Крім того, загрози кібербезпеці розвиваються, а штучний інтелект (ШІ) та інструменти як послуга все частіше використовуються для організації атак. Таким чином, використання штучного інтелекту для протидії штучному інтелекту є обов'язковим, використовуючи машинне навчання та алгоритми, щоб відбивати натиски зловмисного програмного забезпечення.

На жаль, багатьом організаціям не вдається виявити неактивне шкідливе програмне забезпечення у своїх системах без значних інвестицій у робочу силу та ресурси для ретельного моніторингу. Шкідливе програмне забезпечення може залишатися непоміченим протягом року, перш ніж вийти зі стану спокою.

Складність сплячого зловмисного програмного забезпечення полягає в його здатності спостерігати за потоками даних в організації, активуючи себе, як тільки воно розпізнає критичні дані. Щоб боротися з такими загрозами, організаціям потрібні рішення для захисту даних високого рівня інтелекту.

Інструменти захисту даних, позбавлені вбудованої кібервідмовостійкості, ризикують поставити під загрозу цілісність і безпеку даних під час процедур резервного копіювання. Відновлення уражених даних із резервних копій, що містять неактивне шкідливе програмне забезпечення, лише продовжує цикл, що потребує перевірки цілісності даних перед відновленням або передачею.

Рівневі підходи безпеки є незамінними для ефективного захисту від кіберзагроз. Незважаючи на те, що вразливі місця можуть зберігатися, комплексні рівні безпеки дозволяють організаціям стримувати інциденти та пом'якшувати їхні наслідки.

У сучасній бізнес-сфері дані служать джерелом життя підприємств, що підкреслює необхідність надійних заходів безпеки даних для забезпечення безперервності бізнесу.

Підприємства повинні проактивно захищати свої дані та використовувати наявні інструменти для підтримки цілісності даних, заспокоюючи як внутрішніх зацікавлених сторін, так і клієнтів. Починаючи з поступових кроків, шлях до кібербезпеки є постійним і вимагає постійної пильності та адаптації». ***(Mamsi Nkosi. Safeguarding Data in the Age of Cyber Threats: A Proactive Approach // IT News Africa (https://www.itnewsafrica.com/2024/02/safeguarding-data-in-the-age-of-cyber-threats-a-proactive-approach/). 19.02.2024).***

***

«За даними дослідницької та консалтингової компанії Gartner, такі тенденції, як Generative AI, зміна поведінки співробітників, зовнішні ризики та прогалини в лідерах, є одними з головних тенденцій кібербезпеки на 2024 рік.

Списки тенденцій Gartner включають небезпечну поведінку співробітників, пов'язану зі штучним інтелектом, сторонні ризики, безперервне виявлення загроз, прогалини в спілкуванні в залі засідань і підходи до безпеки, націлені на перше місце.

Річард Аддіскотт, старший директор-аналітик Gartner, сказав, що «генеративний штучний інтелект займає значний простір лідерів із безпеки, що є ще одним викликом для управління, але також пропонує можливість використовувати його можливості для посилення безпеки на операційному рівні».

«Незважаючи на неминучу силу GenAI, лідери також продовжують боротися з іншими зовнішніми факторами поза їхнім контролем, які вони не повинні ігнорувати цього року», — сказав Аддіскотт.

За словами Gartner, цього року керівники служби безпеки відреагують на ці спільні тенденції шляхом впровадження процесів, технічних можливостей і структурних реформ у рамках своєї програми безпеки, спрямованої на посилення рівня безпеки та міцності компанії.

Що стосується генеративного штучного інтелекту, Аддіскотт сказав: «Важливо визнати, що це лише початок еволюції GenAI, і багато демонстрацій, які

ми бачили щодо операцій безпеки та безпеки додатків, демонструють реальні перспективи».

«На цю технологію є вагома довгострокова надія, але зараз у нас більше шансів відчути швидку втому, ніж двозначне зростання продуктивності.

«Справа покращуватиметься, тому заохочуйте експерименти та керуйте очікуваннями, особливо поза командою безпеки», — сказав Аддіскотт.

У своїх висновках Gartner також зазначив, що метрики, орієнтовані на результат (ODM), приймаються, щоб дозволити учасникам чітко розрізняти інвестиції в кібербезпеку та рівні захисту, які вони створюють.

«Організації, які використовують SBCP [програми поведінки та культури безпеки], відчули кращий досвід працівників у прийнятті засобів контролю безпеки; зменшення небезпечної поведінки та підвищення швидкості та маневреності», – додав Аддіскотт.

«Це також призводить до більш ефективного використання ресурсів кібербезпеки, оскільки співробітники стають компетентними в прийнятті незалежних рішень щодо кіберризиків».

Gartner також рекомендував керівникам безпеки покращити управління ризиками сторонніх служб і налагодити відносини з високопріоритетними зовнішніми партнерами, щоб гарантувати постійний захист найцінніших активів.

«Почніть із посилення планів на випадок надзвичайних ситуацій для участі третіх сторін, які становлять найвищий ризик для кібербезпеки», — сказав Аддіскотт.

«Створюйте довідники щодо інцидентів сторонніх розробників, проводите настільні вправи та визначте чітку стратегію виходу, яка передбачає, наприклад, своєчасне скасування доступу та знищення даних».

Висновки також відзначили, що програми постійного управління загрозами (CTEM) набирають обертів.

У звіті йдеться, що до 2026 року компанії, які вирішать визначати пріоритетність інвестицій у безпеку на основі цієї програми, побачать зменшення кількості порушень принаймні на дві третини.

Останньою тенденцією, яку відзначили результати, є тенденція переходу організацій до підходу до безпеки, насамперед ідентичності». ***(Six cybersecurity trends for 2024: Gartner // nextmedia Pty Ltd. (https://www.digitalnationaus.com.au/news/six-cybersecurity-trends-for-2024-gartner-605427). 23.02.2024).***

***

«…Група іспанських підприємців запустила Zerod – перший у світі хакерський ринок для бізнесу.

Сервіс пропонує підприємствам будь-якого розміру спосіб знайти та найняти послуги тестування безпеки для своєї технічної інфраструктури. Зараз на момент запуску доступні близько 150 спеціалістів із безпеки з 30 країн, і сайт може похвалитися тим, що наразі було усунено понад 1500 уразливостей.

Цей крок відображає зростаючий попит компаній на безпечне та професійне тестування безпеки. Етичне хакерство отримало значний поштовх у 2022 році, коли Міністерство юстиції США оголосило, що «добросовісні» дослідження безпеки більше не будуть підпадати під Закон про комп'ютерне шахрайство та зловживання.

Як наслідок, ця форма вдосконаленого тестування пера набула популярності, оскільки експоненціально зросла кількість програм-вимагачів і атак іноземних агентів. Поточні оцінки показують, що до 2028 року вартість ринку може перевищувати 10 мільярдів доларів.

Однією з ключових особливостей нового сервісу Zerod є клієнтський інтерфейс. Доступні спеціалісти відображаються на яскраво кольоровій глобальній карті разом із стильним сособом наведення, що дозволяє оцінювати та вибирати. Весь досвід нагадує послуги сайтів фрілансерів, такі як Upwork, що має зробити його набагато доступнішим для зайнятих IT-менеджерів, які потребують хакерських послуг.

Кожен фахівець з хакерів повинен мати понад 5 років досвіду та спеціальні сертифікати та облікові дані. Потім кожен з них проходить тестування та особисту

співбесіду та погоджується на безперервний контроль під час виконання своїх проектів.

Клієнти, яким потрібен терміновий пентест, можуть зареєструватися, щоб отримати три швидкі пропозиції, з яких вони зможуть вибрати хакера, якому вони віддають перевагу. Це цікавий крок у порівнянні зі звичайним пошуком у Google і процесом торгів.

Крім цієї нової моделі ринку, Zerod також пропонує більш традиційні послуги корпоративного агентства з кібербезпеки. Це включає більш складну перевірку на проникнення, поточний судово-експертний аналіз і зовнішню консультаційну експертизу, як-от надання послуг головного спеціаліста з інформаційної безпеки. Як і слід було очікувати, компанія має комплексне страхування відповідальності, а також сертифікацію ISO 27001, хоча на сайті немає чітких умов угоди SLA, що може викликати занепокоєння у деяких користувачів.

Кібербезпека стає серйозною проблемою в усьому світі. Лише у 2023 році понад 10% великих компаній стали жертвами спроб програм-вимагачів. Згідно з даними Chainalysis, ці атаки принесли вражаючі 1,1 мільярда доларів від жертв, що є величезним зростанням у порівнянні з попередніми роками.

Аналітики пояснили це зростання значною ескалацією частоти, масштабу та обсягу атак. Понад 75% платежів за програми-вимагачі були на 1 мільйон доларів або більше. Зловмисники явно навчилися новим трюкам. Вже є ознаки того, що одним з головних напрямків зростання кількості атак є зростання кількості ринків, де продаються інструменти для програм-вимагачів менш досвідченим злочинцям». ***(Запрацював перший в світі ринок, де можна купити хакера // SUNDRIES (https://sundries.ua/zapratsiuvav-pershyj-v-sviti-rynok-de-mozhna-kupyty-khakera/). 22.02.2024).***

***

«Компанії прямих інвестицій (PE) мають унікальну владу на світовому ринку, самостійно сприяючи інноваціям, створюючи робочі місця та сприяючи економічному зростанню. Ці суб’єкти вливають капітал у широкий спектр галузей протягом життєвого циклу бізнесу, прагнучи забезпечувати вищий

прибуток інвесторам, одночасно ефективно орієнтуючись на складності ширшого ландшафту загроз.

Традиційний підхід компаній прямих інвестицій до ризиків кібербезпеки

Не ігноруючи повністю переваг, які надійність кібербезпеки або її відсутність може мати для їхніх портфелів, фірми, що займаються фінансуванням, традиційно віддають пріоритет рішенням щодо фінансування на основі більш традиційного аспекту операційного ризику.

Однак, попри розширення цифрового охоплення та наступних рівнів ризику, ці фінансові організації почали усвідомлювати необхідність переорієнтації своєї уваги та взяти на себе управління та управління кіберризиками як ключові практики як до інвестування, так і після нього для забезпечення оптимізації портфеля.

Аргументи проактивного управління ризиками кібербезпеки для ПП

З огляду на те, що до кінця 2024 року очікуваний глобальний фінансовий збиток від кіберподій досягне 9,5 трильйонів доларів США, потенційні наслідки недооцінки кіберризику ніколи не були більш очевидними. Тим не менш, розуміння того, що кібербезпека повинна бути ретельно досліджена, і знання того, як це зробити, є двома дуже різними проблемами.

Перешкоди в управлінні кіберризиками без досвіду кібербезпеки

У той час як керівники фірм, що спеціалізуються на фінансуванні, та оптимізатори портфоліо звикли оцінювати та керувати більш традиційними аспектами бізнес-ризику та знають, як орієнтуватися на фінансовому ринку, ризик кібербезпеки часто виходить за межі їх компетенції.

Дійсно, управління ризиками кібербезпеки та управління, як правило, пов’язане зі складними технічними термінами та складними структурами, які для тих, хто не має спеціальної підготовки чи досвіду, може збентежити тлумачення в універсальному бізнес-контексті.

Крім того, оскільки портфельні компанії зазвичай не мають персоналу, присвяченого кібербезпеці, який міг би допомогти перевести цю більш технічну сферу ризику, розуміння ролі, яку кібердіяльність може потенційно відіграти в

рентабельності інвестицій, стає ще більш складним завданням для партнерів PE фірм.

На жаль, найчастіше ця прогалина в знаннях призводить до політики пом'якшення кібернетичних наслідків, яка ненавмисно наражає портфельні компанії на ризики, яких інакше можна уникнути. Це також часто призводить до дорогих, неекономічних полісів кіберстрахування, які є надто узагальненими та не відображають унікальний ландшафт кіберризиків компанії.

Демістифікація управління кіберризиками за допомогою кількісної оцінки кіберризиків (CRQ)

Платформи CRQ на вимогу можуть допомогти подолати ці прогалини в знаннях, не лише надаючи фірмам-спеціалістам інформацію про компанії без менеджерів з кіберризиків, але й перекладаючи цю інформацію на ширші бізнес-терміни, такі як ймовірність подій і фінансові збитки, які можуть отримати нетехнічні партнери використовувати для прийняття бізнес-рішень на основі даних.

Завдяки кількісній оцінці фінансового кіберризику фірми, що працюють у сфері кібернетики, готові керувати кіберризиками всіх своїх портфельних компаній, вести переговори щодо оптимізованих умов кіберстрахування та, зрештою, обговорювати стратегії пом'якшення кібернетичних загроз мовою, з якою вони вже добре знайомі.

Завдяки кількісному фінансовому аналізу фірми з фізичних осіб будь-якого розміру можуть легко врахувати кіберризик у своїх процесах прийняття рішень і управління, гарантуючи, що портфелі оптимізовані для відображення все більш зловісного ландшафту кіберризиків.

Комплексна оцінка сукупного кіберризику в портфелі

Завдяки багатомодельному аналізу збитків CRQ і великому досвіду роботи з найбільшими портфелями кіберстрахування в усьому світі, платформа Kovrr надає партнерам з фізичних осіб об'єктивне розуміння рівня кіберризику в усьому портфелі.

Враховуючи цей унікальний досвід і доступ до привілейованих даних про страхові збитки, оцінка CRQ від Kovrr пропонує дуже точний прогноз того,

наскільки ймовірно, що портфель фірми PE зазнає кіберподії, а також розмір фінансових втрат, які вони, в середньому, очікують. протягом наступного року.

Цей огляд пропонує фірмам-спеціалістам дані для створення початкової дорожньої карти для управління та управління кіберризиками, дозволяючи їм швидко визначити, чи потрібно їм інвестувати більше ресурсів у кібербезпеку. За допомогою цих цифр вони також можуть визначити, чи відповідає їхня поточна позиція ризику рівню апетиту та толерантності, і, якщо ні, почати формулювати плани, щоб знизити цю позицію до більш зручної для них позиції.

Пріоритезація зусиль із зменшення кіберризиків згідно з CRQ Insights

CRQ дає змогу менеджерам PE-фірм створювати керовані даними керовані ризиками кібербезпеки та плани управління ними, які визначають пріоритетність зусиль і рекомендацій відповідно до потенційних кіберподій у їхніх портфоліо та відповідної серйозності. Ця інформація також дає змогу партнерам реагувати на найбільш важливі події в портфоліо, мінімізуючи ймовірність фінансових втрат і репутаційної шкоди.

У наш час жодна організація чи фірма не може повністю захистити себе від кіберподій. Враховуючи цю реальність, бізнес-лідери повинні використовувати об’єктивну інформацію, щоб визначити, які з їхніх ініціатив щодо пом’якшення наслідків мають бути пріоритетними, щоб гарантувати, що портфельні компанії можуть залишатися стійкими перед лицем інциденту.

Детальна інформація про кіберризики портфельних компаній

Рішення CRQ на вимогу не тільки забезпечують агреговане уявлення про кіберризики портфоліо, але й масштабовані, заглиблюючись у більш конкретні кіберуразливості, з якими стикається кожна портфельна компанія.

Ця детальна можливість забезпечує ще більш індивідуальний підхід до управління ризиками кібербезпеки та управління, забезпечуючи оптимальне інвестування ресурсів. Цей багаторівневий погляд є надзвичайно цінним, особливо для приватних компаній із портфельними компаніями, які можуть мати обмежені кошти для інвестування в пом’якшення кіберризиків.

CRQ дає ризик-менеджерам можливість розподіляти виділені кошти на кібербезпеку на основі оновлень та ініціатив, які максимально зменшать рівень ризику, водночас забезпечуючи позитивну рентабельність інвестицій. По суті, деталізація покращує стратегічний розподіл ресурсів, сприяючи економічно ефективним покращенням кібербезпеки для кожної з портфельних компаній.

Порівняльний аналіз фінансового становища кіберризику з ключовими аналогами в галузі

Визначаючи кількісно кіберризик, PE фірми можуть визначити, як кіберпозиція їхніх портфельних компаній розташовується у порівнянні з ширшим ландшафтом ризиків. Рішення CRQ пропонують ключові дані порівняльного аналізу з розбивкою за галузями бізнесу, розміром доходу та різними іншими фірмовими характеристиками, розкриваючи важливу інформацію, яка може керувати бюджетуванням інвестицій у кібербезпеку.

Наприклад, оцінка CRQ може підкреслити, що конкретна портфельна компанія з більшою ймовірністю зазнає кіберподії високого рівня, ніж її аналоги в галузі. У такому випадку фірма, що спеціалізується на виробництві, може визначити, що компанія недостатньо інвестує в кібербезпеку, і їй слід перерозподілити ресурси відповідно до конкурентів.

Оптимізація страхування кібербезпеки

Передача кіберризику сторонньому постачальнику страхових послуг може бути надзвичайно рентабельним і привабливим варіантом для фірм, що займаються фізичними особами. Однак поліси страхування кібербезпеки, як правило, є надто узагальненими та дорогими та не враховують специфічний ландшафт ризиків портфельної компанії.

Але, використовуючи рішення CRQ, фірми, що займаються продажем, можуть гарантувати, що положення та умови відповідають меті, з належним чином розрахованими преміями, лімітами та сублімітами. Крім того, вони можуть легше визначити, як оптимально розподілити виділений страховий бюджет, щоб максимізувати рентабельність інвестицій і економічну ефективність.

Використовуючи такі показники, як середній річний збиток (AAL), партнери можуть визначити, чи перевищать очікувані збитки їх портфельної компанії франшизу, і, якщо ні, шукати нижчу франшизу або ліміт. Такі платформи CRQ, як Kovrr, також розбивають фінансові збитки відповідно до стандартних сценаріїв страхових збитків, що дозволяє здійснювати більш цілеспрямовані інвестиції в зони покриття, які, швидше за все, спричинять грошові наслідки.

Дізнайтеся, як одній фірмі з фізичних осіб вдалося зменшити витрати на кіберстрахування свого портфеля на 17%, використовуючи CRQ!

Сприяння обґрунтованим злиттям і поглинанням

Профіль кіберризику організації може і повинен бути вирішальним фактором, коли приватні фірми проводять належну перевірку перед придбанням або консолідацією. Кількісна оцінка кіберризиків допомагає партнерам краще зрозуміти витрати на ведення бізнесу із запропонованою компанією, надаючи зацікавленим сторонам більш точне уявлення про рівень ризику, який вони братимуть на себе.

Озброївшись уявленнями про фінансові ризики, партнери можуть узгодити оптимізовані умови угоди та завчасно розробити стратегії після придбання, щоб пом’якшити та контролювати ризики. Крім того, вони можуть вирішити, що після оцінки кібервразливості M&A не варто продовжувати. Зрештою, внесок CRQ під час M&A захищає цілісність портфеля.

Вирішальна роль CRQ в управлінні кіберризиками та оптимізації інвестицій PE фірм

Інтеграція управління ризиками кібербезпеки та управління в основні операції приватних інвестиційних компаній стала надзвичайно важливою для отримання позитивних прибутків. Однак, оскільки це одна з найновіших форм бізнес-ризику, багато керівників і партнерів часто не знають, як розробити підхід на основі даних, який економічно ефективно усуває ці вразливості.

Застосовуючи CRQ, фірми, що займаються фінансуванням, швидко отримують детальне розуміння сукупного ландшафту кіберризиків своїх портфелів і кожної окремої компанії. Використовуючи безцінну кількісну інформацію,

партнери можуть оптимізувати свої портфелі за рахунок підвищення кібервідмовостійкості та захистити інвестиції, забезпечивши стійке зростання». ***(Yakir Golan. How Private Equity Firms Can Streamline Portfolio Optimization With CRQ // Kovrr (https://www.kovrr.com/blog-post/how-private-equity-firms-can-streamline-portfolio-optimization-with-crq). 21.01.2024).***

***

«У бурхливому ландшафті кібербезпеки, де загрози наростають, а супротивники стають все більш досконалими, залишатися попереду є першорядним. Оскільки звіт про кібербезпеку за 2024 рік від Check Point Research піднімається, настав час заглибитися в останні відомості та підготуватися до викликів, які чекають попереду.

Серед безлічі висновків, оприлюднених у звіті, один статистичний показник яскраво виділяється: тривожне зростання кількості публічно вимаганих жертв. Лише у 2023 році ми стали свідками понад 5000 жертв публічного вимагання, що на 90% більше, ніж у попередньому році. Це експоненціальне зростання служить похмурим нагадуванням про невпинну атаку кіберзагроз і жахливі наслідки, які вони спричиняють як для окремих осіб, так і для організацій.

Коли ми розглядаємо тонкощі кібервійни, стає очевидним, що поле бою постійно розвивається, а супротивники використовують безліч тактик для проникнення та використання вразливостей. Арсенал кіберзагроз продовжує розширюватися, починаючи від атак програм-вимагачів, що використовують уразливості нульового дня, і закінчуючи використанням руйнівних очисників із політичних мотивів, не залишаючи байдужим жоден сектор чи галузь.

Крім того, звіт проливає світло на ескалацію ризику, який представляють периферійні пристрої, які стали головними цілями як для національних APT, так і для досвідчених кіберзлочинців. Це розширення площі атаки підкреслює нагальну потребу в проактивних заходах для зміцнення захисту та пом’якшення потенційних ризиків.

Хмарні середовища, рекламовані своєю масштабованістю та гнучкістю, не захищені від вразливостей. У звіті висвітлюються проблеми безпеки токенів у

хмарних середовищах, наголошується на критичній важливості надійних механізмів автентифікації для захисту від несанкціонованого доступу.

Крім того, загроза, яку створюють пакети зловмисного програмного забезпечення в сховищах із відкритим вихідним кодом, створює значні ризики для ланцюжків постачання програмного забезпечення, що підкреслює необхідність підвищеної пильності та суворих заходів безпеки.

Серед цих зростаючих загроз штучний інтелект (ШІ) постає маяком надії, революціонізуючи спосіб запобігання, виявлення та реагування на кіберзагрози. Рішення на основі штучного інтелекту пропонують неперевершені можливості для виявлення загроз і їх пом’якшення, дозволяючи організаціям бути на крок попереду противників.

Поки ми орієнтуємося в складному лабіринті кіберзагроз, висновки, отримані зі Звіту про кібербезпеку за 2024 рік, служать яскравим закликом до спільних зусиль і профілактичних заходів. Застосовуючи інноваційні технології та цілісний підхід до кібербезпеки, ми можемо прокласти шлях до безпечнішого та стійкішого цифрового майбутнього.

Карта відображає глобальний індекс ризику кіберзагроз, демонструючи основні зони ризику по всьому світу. Дані отримані з ThreatCloud AI, як частина служб Infinity Core. Штучний інтелект ThreatCloud збирає та аналізує великі телеметричні дані та мільйони індикаторів компрометації (IoC) щодня. Наша база даних аналізу загроз надходить із 150 000 підключених мереж і мільйонів кінцевих пристроїв, а також Check Point Research (CP) і десятків зовнішніх каналів.

ThreatCloud AI використовує передовий штучний інтелект із понад 50 технологіями для виявлення та нейтралізації нових загроз, використовуючи великі дані для оновлення захисту за допомогою найновіших індикаторів компрометації. Він аналізує телеметричні дані для точної категоризації загроз, покращує безпеку мереж за допомогою Quantum, хмари за допомогою CloudGuard, операцій за допомогою Infinity та доступу користувачів за допомогою Harmony». **(2024’s Cyber Battleground Unveiled: Escalating Ransomware Epidemic, the Evolution of Cyber Warfare Tactics and strategic use of AI in defense – Insights from Check Point’s**

Latest Security Report // Check Point Software Technologies LTD. (https://research.checkpoint.com/2024/2024s-cyber-battleground-unveiled-escalating-ransomware-epidemic-the-evolution-of-cyber-warfare-tactics-and-strategic-use-of-ai-in-defense-insights-from-check-points-latest-security-re/). 21.02.2024).

***

Сполучені Штати Америки та Канада

«Безпека даних продовжує залишатися головним викликом для компаній у постійно включеному та постійно підключеному світі. Згідно з даними огляду загроз Qualys за 2023 рік, у 2023 році було розкрито 26 447 уразливостей, порівняно з 25 050 у 2022 році. Це сьомий рік поспіль, коли кількість вразливостей зростає. З тих, що відносяться до категорії високого ризику, хакери публікують інструменти експлойтів для приблизно 25% з них у той самий день, коли вони розкриваються. На жаль, ці цифри не дивують.

Щоб усунути цю постійну тенденцію для американських організацій, Комісія з цінних паперів і бірж (SEC) нещодавно прийняла нові правила, які вимагають від публічних компаній повідомляти про кібератаки з істотними наслідками. Невиконання цього може призвести до фінансових санкцій і шкоди репутації.

Хоча ці правила розроблено для захисту зацікавлених сторін компанії, існує ще одна група, яка потенційно може отримати від цього вигоду: суб'єкти загроз. В одному випадку банда програм-вимагачів ALPHV намагалася використати нові правила, щоб змусити жертв заплатити викуп. Група нібито зламала мережу MeridianLink 7 листопада 2023 року та викрала дані компанії без систем шифрування. Під час спроби вимагати від MeridianLink викуп відсутність реакції з боку компанії спонукала хакерів чинити більший тиск, надіславши скаргу безпосередньо до SEC про те, що MeridianLink не розголошує інцидент кібербезпеки, який вплинув на «дані клієнтів та оперативну інформацію». Потім ALPHV опублікувала скаргу та автоматичну відповідь SEC на своєму веб-сайті, щоб ще більше змусити MeridianLink виконати їхні вимоги.

Незважаючи на те, що правила SEC ще не набули чинності, і MeridianLink пояснив, що інцидент «спричинив мінімальне переривання роботи», він дає публічним компаніям уявлення про те, як все може рухатися далі. Це також підтверджується тривожною тенденцією у світі тактики вимагання програм-вимагачів, де за останні п’ять років хакери не лише шифрували дані за допомогою зловмисних програм-вимагачів, але й викрадали дані, здійснювали несанкціоноване розкриття та будь-яким іншим чином використовували вторгнення та дані. можливе переведення в готівку.

У відповідь, ось кілька способів, як публічні компанії можуть відновити перевагу над загрозливими акторами, які планують використовувати цей підхід:

Будьте проактивними щодо кібербезпеки

З новими правилами SEC публічні компанії зобов’язані повідомляти про кібератаки з істотними наслідками. Це означає, що вони також мають зобов’язання перед своїми акціонерами надавати пріоритет кібербезпеці в своїх організаціях. Незалежно від розміру, усі публічні компанії повинні активно думати про кібербезпеку. Набагато важче відповісти на кібератаку, якщо ви до неї не готові, і набагато доступніше заздалегідь, ніж після злому та втрати репутації. Крім новітніх технологій кібербезпеки, які можуть вимірювати, повідомляти та усувати кіберризики в режимі реального часу, важливо проводити регулярне тестування на проникнення та тестування червоною командою, а також ретельно навчати всіх співробітників і підрядників найкращим практикам кібербезпеки. Ландшафт загроз постійно змінюється, тому організації повинні переконатися, що їхні співробітники постійно вдосконалюють свої знання. Крім того, після судового переслідування CISO та фінансового директора SolarWinds за нещодавні кіберінциденти керівники інформаційної безпеки повинні взяти на себе особисту відповідальність за кібербезпеку. Це вже не лише бізнес-ризик, а й особиста відповідальність.

Розробіть комплексний план реагування на інциденти

Навіть найбільш орієнтовані на кібербезпеку організації можуть стати жертвами кібератаки, тому дуже важливо мати план, який визначає, як ви збираєтеся реагувати в різних ситуаціях. Нові правила SEC накладають певні

обмеження на плани реагування на інциденти, але між виявленням проблеми та повідомленням про неї SEC ще багато чого потрібно розглянути. Добре підготовлені команди часто можуть обмежити шкоду від кібератаки, швидко її виявивши, стримуючи та усунувши її до того, як наслідки відчують всю організацію. Незважаючи на це, компанії повинні мати спеціальну групу реагування на інциденти, готову швидко вирішувати проблеми, одразу знаючи, до кого звертатися та які їхні обов'язки. У рамках цього вони повинні підготуватися до того, що така загроза, як ALPHV, викриє їх передчасно — незалежно від того, чи є обґрунтованими їхні заяви. Організаціям також потрібно буде визначити рівень прозорості в будь-якому конкретному сценарії та визначити, чи занадто рано надсилатиметься надто багато, що спричинить непотрібну паніку, чи це допоможе їм ефективніше усунути загрозу. Компанії повинні провести стрес-тестування цих сценаріїв, перш ніж вони стануть справжньою метою.

Діліться знаннями та працюйте разом

Бути жертвою кібератаки – це болісний досвід, який може стати в нагоді іншим у спільноті кібербезпеки. Щоб нейтралізувати загрозливих діячів, галузь має активно співпрацювати, а це часто означає ділитися складними подробицями власного досвіду з іншими. Завдяки новим інструментам, таким як генеративний штучний інтелект, зловмисники кидають більше речей об стіну, сподіваючись, що деякі з них затримаються й отримають прибуткову зарплату. Вони також розробляють більш складні підходи для отримання початкового доступу та переміщення в межах мережі.

Дивлячись вперед

Жодна організація не хоче стати жертвою кібератаки, і більше того, вони не хочуть втрачати контроль над наративом разом із нею. Нові правила SEC збільшують організаційну та персональну підзвітність і виводять на перший план більшу прозорість, але водночас це можливість для суб'єктів загрози залякати жертв і отримати те, що вони хочуть. Щоб державні компанії відновили перевагу, вони повинні визначити пріоритети та діяти на випередження щодо кібербезпеки, мати чіткий план реагування на випадок інциденту та, коли це доцільно, ділитися

своїм досвідом і працювати зі спільнотою кібербезпеки. створити сильніший стратегічний захист від загроз.

Сьогоднішній світ виглядає зовсім інакше, ніж п’ять-десять років тому, і бути публічною компанією пов’язано з більшою відповідальністю, ніж будь-коли раніше. Відмінна кібергігієна більше не приємна, а необхідна для організацій, які хочуть вижити під невпинним шквалом кібератак, що розв’язуються щодня». ***(Ken Dunham. How the SEC's Rules on Cybersecurity Incident Disclosure Are Exploited // Informa PLC (https://www.darkreading.com/vulnerabilities-threats/how-secs-rules-cybersecurity-incident-disclosure-are-exploited?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 05.02.2024).***

***

«Канада збирається заборонити Flipper Zero, звинувачуючи цей іграшковий пристрій для перевірки безпеки у розповсюдженні крадіжок автомобілів у країні.

Міністр інновацій, науки та промисловості Канади Франсуа-Філіп Шампань оголосив про заборону в четвер, пояснивши, що «злочинці використовували складні інструменти для викрадення автомобілів. І канадці справедливо хвилюються».

«Сьогодні я оголосив, що ми забороняємо імпорт, продаж і використання споживчих хакерських пристроїв, таких як ласти, які використовуються для скоєння цих злочинів», — написав він у Twitter.

Уряд Канади додає, що країна «вживає всіх заходів для заборони пристроїв, які використовуються для викрадення транспортних засобів шляхом копіювання бездротових сигналів для дистанційного доступу без ключа, таких як Flipper Zero». В даний час країна втрачає близько 90 000 автомобілів на рік через крадіжки.

Це правда, що Flipper Zero за 169 доларів США можна використовувати для поломки деяких пристроїв завдяки його здатності емулювати радіочастотну ідентифікацію. Наприклад, у грудні Apple виправила помилку, через яку модифікована версія інструменту заповнювала iPhone спливаючими

повідомленнями. Однак виробник Flipper Zero каже, що заборона Канади є помилковою, коли йдеться про захист автомобілів від кіберзагроз.

«Flipper Zero не можна використовувати для викрадення будь-яких автомобілів, особливо тих, які були випущені після 1990-х років, оскільки їхні системи безпеки мають змінні коди», — розповідає PCMag операційний директор Flipper Devices Алекс Кулагін. «Крім того, потрібно було б активно блокувати сигнал від власника, щоб уловити оригінальний сигнал, на що апаратне забезпечення Flipper Zero не здатне».

Канадська влада може відреагувати на численні відео в Інтернеті, які нібито показують, що Flipper Zero можна використовувати для дистанційного розблокування автомобіля. Деякі ролики навіть навчають користувачів, як налаштувати Flipper Zero, щоб відповідати автомобільному брелоку, що передбачає знаходження поруч із ним і захоплення сигналу.

Але змусити цей хак працювати нелегко. Сучасні автомобільні системи використовують змінні коди замість фіксованих кодів, щоб дистанційно розблокувати автомобіль. Це означає, що кожен рухомий код із брелока можна використовувати лише один раз, щоб розблокувати автомобіль. Якби Flipper Zero захопив сигнал, це не мало б значення; термін дії коду закінчився. Натомість викрадач автомобіля повинен був би зробити все можливе, щоб заглушити радіосигнал від брелока, весь час фіксуючи змінний код за допомогою Flipper Zero.

Компанія також послала PCMag на оцінку урядового агентства Нью-Джерсі, яке виявило, що соціальні мережі перебільшують хакерські можливості Flipper Zero. «Більшість опублікованих відео TikTok, як повідомляється, могли бути інсценованими та надавати дезінформацію, оскільки більшість сучасних бездротових пристроїв не вразливі до простих атак з відтворенням», — повідомляє New Jersey Cybersecurity & Communications Integration Cell (NJCCIC).

Тим часом новина про заборону викликає у деяких критиків критику Канади за те, що вона націлилася на Flipper Zero, а не на виробників автомобілів, намагаючись зупинити крадіжки автомобілів. «Ви можете використовувати викрутки для крадіжки автомобілів також. Чи означає це, що ви маєте намір

переконатися, що канадці не матимуть доступу до жодних цифрових інструментів?» один користувач Twitter – сказав у відповідь на заборону». ***(Michael Kan. Canada to Ban Flipper Zero Devices Over Car Thefts // Ziff Davis, LLC. (https://www.pcmag.com/news/canada-to-ban-flipper-zero-devices-over-car-thefts?utm_source=flipboard&utm_content=PCMag%2Fmagazine%2FBreaking+Security+News+You+Need+to+Know). 09.02.2024).***

***

«Посилення уваги до автоматизації застарілих систем, визначення пріоритетів вбудованих вимог безпеки в контрактах з постачальниками та ретельне впровадження зрілих інструментів штучного інтелекту може допомогти федеральним агентствам підвищити їх загальну кіберстійкість, заявили у вівторок кілька чиновників з Департаменту у справах ветеранів.

Під час обговорення майбутнього федеральної кібербезпеки, організованого Центром стратегічних і міжнародних досліджень, Ембер Пірсон, заступник начальника відділу інформаційної безпеки Вірджинії, сказала, що департамент контролює «34% IT-активів у всьому федеральному цивільному просторі» і значною мірою покладається на Агентство з кібербезпеки та безпеки інфраструктури «для інформування про впровадження кібербезпеки нашого підприємства».

«Безпека має рухатися зі швидкістю інновацій», — сказав Пірсон, зазначивши, що низка агенцій, у тому числі VA, досі використовують застарілі системи та мають «почати дивитися на те, де ми модернізуємося, де нам насправді потрібно посилити цю суворість і виглядати для тих можливостей навколо автоматизації».

Білий дім і CISA, зокрема, протягом останнього року приділяли більшу увагу тому, щоб спонукати федеральні агентства та технологічні фірми приватного сектора до пріоритетності безпеки під час розробки та закупівлі нових систем і інструментів.

CISA опублікувала рекомендації для громадськості та запустила громадську кампанію, закликаючи компанії створювати «безпечні за проектом» продукти.

адміністрації Байдена Національна стратегія кібербезпеки, оприлюднена в березні 2023 року, також виступала за прийняття принципів безпеки за проектом, а також наступний меморандум від червня 2023 року Управління та бюджету щодо кіберпріоритетів Білого дому на бюджет 2025 фінансового року сказав, що «агентські інвестиції мають призвести до надійних, довгострокових рішень, які є безпечними».

Коли справа доходить до оновлення застарілих систем охорони здоров'я та технологій департаменту, Пірсон зазначив, однак, що інноваційні інструменти також можуть «створювати нові та непередбачувані шляхи, які зловмисники можуть використовувати для доступу до IT-систем та даних VA».

Вона додала, що боротьба з кіберзагрозами в сфері охорони здоров'я — «особливо навколо нашої спільноти медичних пристроїв» — вимагає розширених партнерських відносин з іншими агенціями, «а потім також до контрактів і оновлення нашої мови [Федерального регламенту закупівель], і таким чином ми можемо дійсно забезпечити виконання деяких із цих вимог безпеки на рівні постачальника».

Крім постійної взаємодії з CISA, Пірсон сказав, що VA співпрацює з Офісом національного кібердиректора, Департаментом охорони здоров'я та соціальних служб і Управлінням з контролю за продуктами й ліками, «щоб дійсно переконатися, що ми розглядаємо ці контракти та забезпечення вбудованих вимог безпеки».

«Ми хочемо переконатися, що ці речі розглядаються на рівні контракту, коли ми починаємо закуповувати та модернізувати більшість наших сучасних технологій у сфері охорони здоров'я», — підкреслила вона.

Але навіть якщо контракти з постачальниками надають перевагу покращеним стандартам безпеки, впровадження нових технологій, у тому числі тих, що використовують штучний інтелект і машинне навчання, створює безліч потенційних переваг і викликів для VA та інших федеральних відомств, оскільки вони прагнуть модернізувати свої системи.

Джефф Спает, заступник CISO та виконавчий директор операцій з інформаційної безпеки у Вірджинії, сказав, що генеративні інструменти штучного інтелекту дозволять зловмисникам краще відточувати свої фішингові кампанії та інші кібератаки, «що може обійти ваш звичайний аналіз фішингу або карантин цих повідомлень».

Але він сказав, що впровадження деяких із тих самих інструментів штучного інтелекту, коли вони стають більш зрілими, також може дозволити агентствам «або ідентифікувати, або негайно вводити такі типи профілактичних виявлень і блокувань швидко».

А враховуючи постійну нестачу кадрів у федеральному уряді (у звіті федеральної робочої групи за вересень 2022 року говорилося, що станом на квітень у державному секторі було майже 40 000 кіберробочих місць), Спает додав, що впровадження ШІ «може пом'якшити дефіцит персоналу лише тому, що ми зможемо розширити здатність персоналу використовувати ці технології, щоб компенсувати дефіцит». ***(Edward Graham. Contracts featuring automation and built-in security can boost agencies' cyber defenses, VA officials say // Government Media Executive Group LLC. (https://www.govexec.com/technology/2024/02/contracts-featuring-automation-built-security-can-boost-agencies-cyber-defenses-va-officials-say/394008/). 07.02.2024).***

***

«1 лютого 2024 року Постійний комітет з громадської та національної безпеки (Комітет) розпочав вивчення законопроекту С-26, Закону про кібербезпеку, внесення змін до Закону про телекомунікації та внесення відповідних змін до інших законів (законопроект С-26 або Білл), майже через рік після завершення другого читання в Палаті громад.

14 червня 2022 року уряд вніс законопроект С-26. Якщо він буде прийнятий, він прийме Закон про захист критичних кіберсистем (CCSPA або Закон). CCSPA накладає низку зобов'язань щодо кібербезпеки на підприємства приватного сектору в чотирьох регульованих на федеральному рівні секторах: телекомунікаціях, фінансах, енергетиці та транспорті. Закон буде застосовуватися до галузей, що

надають «життєво важливі послуги» або «життєво важливі системи», як зазначено в Додатку 1, і класи призначених операторів, визначені в Додатку 2 CCSPA.

Найважливіші послуги та системи, наразі викладені в Додатку 1:

телекомунікаційні послуги;

Міжпровінційні або міжнародні системи трубопроводів і ліній електропередач;

Ядерні енергетичні системи;

Транспортні системи в межах законодавчої влади Парламенту;

Банківські системи; і

Клірингові та розрахункові системи.

CCSPA надасть губернатору в Раді (тобто федеральному кабінету) повноваження додавати або видаляти послуги та системи для окремих секторів із Додатку 1.

CCSPA накладає на призначених операторів п’ять ключових зобов’язань щодо дотримання вимог кібербезпеки:

CCSPA вимагає, щоб призначені оператори впроваджували програму кібербезпеки із заходами щодо зменшення ризиків і структурою управління для виявлення та управління організаційними ризиками щодо критичних кіберсистем. Критичні кіберсистеми визначаються в CCSPA як кіберсистеми, які, якщо їх конфіденційність, цілісність або доступність будуть скомпрометовані, можуть вплинути на безперервність або безпеку однієї з життєво важливих послуг або систем, викладених у Додатку 1.

Призначені оператори будуть зобов’язані виявляти ризики кібербезпеки у своєму ланцюжку постачання або використання сторонніх продуктів і послуг, а також вживати розумних заходів для пом’якшення цього ризику, включаючи кроки, передбачені майбутнім регулюванням.

Призначені оператори також повинні будуть повідомляти про «інцидент кібербезпеки» у двоетапний процес. «Інцидент кібербезпеки» — це будь-який інцидент, який заважає або може заважати безперервності чи безпеці життєво важливої служби чи системи, або конфіденційності, цілісності чи доступності

критичної кіберсистеми. По-перше, призначені оператори повинні «негайно» повідомити про інцидент кібербезпеки в Канадську установу безпеки (CSE) у порядку, передбаченому майбутніми нормативними актами. По-друге, призначений оператор також повинен повідомити відповідальний регуляторний орган, наприклад міністра промисловості або Банк Канади, «негайно після повідомлення CSE про інцидент кібербезпеки».

Призначені оператори будуть зобов'язані виконувати будь-які заходи щодо захисту критичної кіберсистеми, викладені в обов'язковій вказівці губернатора в Раді. Призначені оператори не можуть розголошувати зміст або існування такого напряму.

Призначені оператори повинні будуть вести записи, що демонструють реалізацію їх програми кібербезпеки, і звіти про будь-які інциденти кібербезпеки. Ці записи повинні зберігатися в межах Канади.

Виконання CCSPA здійснюватиметься за допомогою схеми адміністративних грошових стягнень, яка буде додатково розроблена в рамках регулювання. CCSPA дозволяє максимальний штраф у розмірі 15 мільйонів канадських доларів для призначених операторів і 1 мільйон канадських доларів для директорів і посадових осіб. Недотримання певних положень CCSPA може альтернативно переслідуватися як правопорушення, яке карається кримінальними штрафами та/або позбавленням волі. Крім того, галузеві регулюючі органи матимуть розширені повноваження вимагати надання інформації, проводити перевірки приміщень призначених операторів і видавати повідомлення про невідповідність для забезпечення дотримання CCSPA.

Для того, щоб стати законом, законопроект C-26 має завершити розгляд у Комітеті, пройти третє читання в Палаті громад і три читання в Сенаті. Незважаючи на те, що його майбутнє невизначене, зобов'язання щодо відповідності, які вимагає CCSPA, представляють найкращі практики кібербезпеки, які більшість організацій повинні застосувати для зміцнення своєї позиції в кібербезпеці, захисту критичних активів і захисту від ризиків третіх сторін». ***(Sunny Handa, Liliane Langevin, John Lenz and Ellie Marshall. Canadian***

Cybersecurity Law Update: Bill C-26 Gains Momentum in the House of Commons // Blake, Cassels & Graydon LLP (https://www.blakes.com/insights/canadian-cybersecurity-law-update-bill-c-26-gains-momentum-in-the-house-of-commons). 02.02.2024).

***

«У середу адміністрація Байдена оголосила про заходи щодо посилення кіббезпеки в портах США, включаючи розширення відповідальності для берегової охорони та інвестиції у внутрішнє виробництво кранів.

Президент Джо Байден підписав указ, в якому визначено заходи щодо портів, які є основним пунктом входу для іноземних товарів і обробляють трильйони доларів на рік.

Берегова охорона США отримає повноваження реагувати на кібератаки на морську інфраструктуру, включаючи вимогу до операторів ділитися інформацією про інциденти та загрози. Також буде створено посаду директора національної морської безпеки.

Наказ передбачає інвестування 20 мільярдів доларів США протягом п'яти років у портові крани з планами відновлення внутрішнього виробництва кранів уперше за 30 років, повідомила адміністрація.

Високопоставлені чиновники адміністрації заявили, що більшість обладнання, яке сьогодні транспортує вантажі з суден у США, надходить із Китаю та контролюється за допомогою китайського програмного забезпечення.

Декілька колишніх співробітників розвідки США висловили стурбованість тим, що крани, виготовлені китайськими компаніями, можуть використовуватися для спостереження всередині США - твердження, яке інші експерти відкидають як безглузде.

Морська адміністрація заявила, що американські порти вразливі для хакерів через велику кількість підрядників і зацікавлених сторін, які там працюють, а також різноманітність інформаційних і операційних технологічних систем.

За даними CNN, у 2021 році порт Х'юстон був атакований «імовірними хакерами, яких підтримує іноземний уряд», які, якби злом не було виявлено, мали б

віддалений доступ до мережі порту». ***(Christopher Bing. Biden order seeks to improve US port cybersecurity // Reuters (https://www.reuters.com/world/us/biden-order-seeks-improve-us-port-cybersecurity-2024-02-21/). 22.02.2024).***

***

«У четвер понад 70 000 клієнтів AT&T раптово втратили мобільний зв'язок. Лише через кілька годин після того, як компанія оголосила про відновлення роботи своїх послуг у четвер о 14:10 за київським часом, вона опублікувала заяву, у якій повідомила клієнтів, що «збій був спричинений застосуванням і виконанням неправильного процесу, який використовувався під час розширення нашої мережі..»

Це узгоджується з попередніми звітами ABC News, де два джерела, знайомі з ситуацією, підтвердили, що збій оновлення програмного забезпечення став причиною збою. У тому ж прес-релізі AT&T спростувала підозри, що збій спричинила кібератака, про що SlashGear уже передбачив раніше. Загальнонаціональний збій такого рівня є рідкісним явищем, тому не дивно, що багато хто вважав, що це результат зловмисної діяльності.

Після того, як послуги знову почали працювати, компанія стільникового зв'язку вибачилася перед постраждалими клієнтами та запевнила їх, що «вживає заходів для того, щоб наші клієнти більше не відчували цього в майбутньому». Однак це не означає, що всі залишають поза увагою інцидент.

Державні органи розслідували причини нападу

Оскільки кібератака на мережевого провайдера може становити загрозу безпеці, багато державних установ звернули увагу на це. Агентство Міністерства внутрішньої безпеки (DHS), яке відстежує кібератаки, — Агентство з кібербезпеки та безпеки інфраструктури (CISA) — було одним із агентств, які досліджували цю проблему. Станом на 5 ранку за східним часом CISA не знає причини збою, але вважає, що «немає ознак зловмисної діяльності». Ця інформація міститься в конфіденційній записці, отриманій ABC News.

Радник з національної безпеки зв'язку Джон Кірбі пояснив, що Федеральна комісія зі зв'язку (FCC) спілкувалася з AT&T, щоб отримати більше інформації про

збій. У четвер після обіду Кірбі повідомив пресі, що DHS і ФБР також ведуть розслідування, співпрацюючи з представниками галузі, щоб визначити, що можна зробити «з федеральної точки зору, щоб посилити свої слідчі зусилля, щоб з'ясувати, що тут сталося». Він пояснив, що вони не мають відповідей на всі питання, але працюють над цією метою.

Хоча збій міг і не бути наслідком кібератаки, він все одно створював потенційно серйозні проблеми для клієнтів. У багатьох регіонах — від Шарлотти, штат Північна Кароліна, до Сан-Франциско, штат Каліфорнія — клієнти AT&T не могли скористатися послугами стільникового зв'язку, щоб зателефонувати на номер 911. Місцеві агентства в постраждалих районах закликали клієнтів AT&T використовувати Wi-Fi для здійснення екстрених дзвінків, якщо він доступний, або використовувати мережу друзів. або телефон родини. Ця подія може навіть переконати декого передумати викидати свій домашній телефон». ***(Nicholas Wilson. We Finally Know What Caused The AT&T Outage, And Its Probably Not What You Thought // Static Media (https://www.slashgear.com/1524972/what-caused-the-att-outage-answer/). 23.02.2024).***

***

Країни ЄС та Великобританія

«Італійська влада готується змінити закон і запровадити набагато більш жорсткі покарання за кіберзлочини в залежності від тяжкості атаки.

Злочинці зазвичай не атакують компанії чи організації в країні, в якій вони проживають. Насправді напади часто походять із-за меж звичайної юрисдикції. Але це не завжди так, іноді правоохоронним органам вдається заарештувати або видати підозрюваних.

Згідно зі звітом Reuters, італійська влада має намір посилити покарання за кіберзлочини, у деяких випадках значно. Наприклад, просте проникнення в мережу організації каратиметься мінімум двома роками позбавлення волі і максимум 12 роками.

Суворіше покарання буде застосовано, якщо злочинець погрожував силою або якщо цілями були державні службовці. Те ж саме стосується випадків, коли зловмисники будь-яким чином загрожують національній безпеці чи суспільним інтересам.

На даний момент подібні злочини призводять до позбавлення волі на строк від одного до восьми років. Іншим положенням, покликаним заохотити злочинців співпрацювати з владою, є обіцянка максимального пом'якшення терміну покарання на дві третини.

Інше положення про відсотки поширюється на постраждалу організацію, яка повинна буде повідомляти Національне агентство з кібербезпеки про будь-який інцидент безпеки протягом 24 годин. Заходи, вжиті для усунення проблем, які в першу чергу призвели до порушення, повинні бути розгорнуті протягом максимум 15 днів.

На даний момент цей новий набір законів все ще розробляється урядом Італії, і вони ще повинні бути ратифіковані парламентом, щоб вони набули чинності». ***(Silviu STAHIE. Italian Government Proposes Much Harsher Jail Sentences for Cyber Criminals // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/italian-government-proposes-much-harsher-jail-sentences-for-cyber-criminals/?utm_source=flipboard&utm_content=other%2F). 05.02.2024).***

***

«Cyber Ireland, провідна національна кластерна організація з кібербезпеки, сьогодні запустила комплексну стратегію, спрямовану на стимулювання зростання сектора кібербезпеки Ірландії до 2030 року. Завдяки підтвердженій історії з моменту свого створення в 2019 році Cyber Ireland перетворилася на національний представницький орган, що об’єднує понад 160 організацій-членів, включаючи стартапи, МСП, багатонаціональні корпорації та навчальні заклади.

Спочатку задумана для вирішення проблеми дефіциту навичок кібербезпеки як ініціатива Мюнстерського технологічного університету, Cyber Ireland перетворилася на визнану галузеву силу, яка проводить діяльність у чотирьох

стратегічних робочих потоках, а також відповідає за організацію щорічної Національної конференції Кібер Ірландії (CINC), головної кібернетичної конференції. Конференція з безпеки, яка залучає провідних експертів з кібербезпеки з усієї Ірландії та світу.

Відповідно до звіту про стан сектору кібербезпеки за 2022 рік, у секторі кібербезпеки в Ірландії працює понад 7300 фахівців, які працюють у майже 500 компаніях, щороку вносять в економіку 1,1 мільярда євро. Ірландії потрібен потужний внутрішній сектор кібербезпеки з масштабними компаніями, які можуть надавати високоякісні послуги, щоб забезпечити кіберстійкість країни та конкурувати на міжнародному рівні. Це може спиратися на наявні сильні сторони, оскільки острів Ірландія стає міжнародним центром у Європі для багатонаціональних операцій із кібербезпеки та подальшого збільшення ПІІ у кібербезпеку.

Протягом останніх чотирьох років спостерігався високий попит на навички кібербезпеки: у період з 2019 по 2022 рік кількість вакансій зросла втричі: від 2000 оголошених до 6700 відкритих вакансій. За траєкторії зростання в 10%, сектор передбачає створення 10 000 додаткових робочих місць до 2030 року, загалом 17 000 у секторі, що внесе в економіку 2,5 мільярда євро на рік. Те, як задовольнятиметься цей попит, враховуючи існуючий дефіцит навичок і прогалини в навичках, буде ключовим у перетворенні Ірландії на світове лідерство у сфері кібербезпеки…

Тепер для Ірландії є можливість використати свої сильні сторони кібербезпеки та конкурентні переваги для розвитку провідного сектору кібербезпеки в Європі та в усьому світі, забезпечуючи стійкість усередині країни та конкуруючи на міжнародному рівні. Cyber Ireland прагне стати рушійною силою для реалізації кіберпотенціалу Ірландії шляхом реалізації своєї нової кластерної стратегії на 2024–2027 роки. Нова стратегія включає чотири основні напрямки: розбудова спільноти, стимулювання зростання бізнесу, розвиток робочої сили, адвокація та просування…» ***(Cyber Ireland unveils ambitious roadmap to drive Cyber Security sector growth by 2030 // Enterprise Ireland (https://www.enterprise-***

ireland.com/en/news/cyber-ireland-unveils-ambitious-roadmap-to-drive-cyber-security-sector-growth-by-2030). 02.2024).

***

«Директива NIS 2, яка має бути імплементована в законодавство Німеччини до жовтня 2024 року, посилює зобов'язання щодо кібербезпеки для компаній, у тому числі для тих, чиї бізнес-моделі не є ні цифровими, ні інтенсивними даними. Тому IT-безпека стає проблемою відповідності.

З огляду на неделеговану відповідальність ради директорів або керівництва за забезпечення IT-безпеки в компанії, яка була нещодавно запроваджена директивою NIS 2, зараз триває дискусія щодо того, чи потрібен окремий відділ з IT-безпеки. Чи знадобиться компаніям кібердошка в майбутньому?

Низка нових законодавчих актів ЄС, які є частиною цифрової стратегії Європейської Комісії, а також закони про імплементацію в Німеччині формують нову правову основу для зміцнення кібербезпеки в ЄС. Це стосується Директиви NIS 2 (NIS = Network Information Security), яка була прийнята Європейським парламентом 10 листопада 2022 року та має бути імплементована в національне законодавство до 17 жовтня 2024 року. Він зобов'язує компанії вживати належних і пропорційних технічних, операційних та організаційних заходів для забезпечення IT-безпеки в компанії. У Німеччині Директива NIS 2 має бути імплементована через Закон про реалізацію NIS 2 і посилення кібербезпеки, який наразі доступний у вигляді проекту (станом на травень 2023 року).

Це оновлює основний елемент стратегії кібербезпеки ЄС 2013 року, Директиву NIS (Директива про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у Союзі) від серпня 2016 року. Зобов'язання щодо кібербезпеки посилюються. Згідно з оцінкою Європейської комісії, попередня директива NIS та її впровадження не призвели до достатнього рівня кібербезпеки в ЄС. Реалізація в країнах-членах ЄС інколи значно відрізнялася.

Сфера застосування: до яких компаній застосовуються нові зобов'язання щодо кібербезпеки?

Директива NIS 2 розрізняє так звані основні та важливі об’єкти (раніше в термінології Директиви NIS: оператори основних і постачальники цифрових послуг). Додатки I та II до Директиви визначають, коли компанія підпадає під дію. Доречними є такі критерії: (1.) класифікація як оператора KRITIS, (2.) приналежність до сектора та (3.) розмір компанії.

Проте оператори KRITIS — це не лише компанії, що займаються критичною інфраструктурою, а й виробничі промислові компанії з понад 50 співробітниками та річним оборотом понад 10 мільйонів євро. Таким чином, сфера застосування була значно розширена порівняно з попередньою настановою NIS від 2015 року.

Директива NIS 2 має особливе значення для виробництва/виробничого сектору, на який вперше поширюються нові зобов’язання щодо кібербезпеки. Багатьом компаніям, чиї бізнес-моделі не є ані цифровими, ані не мають особливого зв’язку з даними, вперше доведеться більш детально розглянути відповідність вимогам кібербезпеки.

Статус-кво: зобов’язання щодо кібербезпеки відповідно до BSIG, GDPR і TTDSG

Закон про Федеральне відомство з інформаційної безпеки (BSIG) уже стандартизує зобов’язання щодо кібербезпеки. Однак вони стосуються лише обмеженої групи компаній, яка значно розшириться завдяки впровадженню директиви NIS 2. Наразі BSIG розрізняє три категорії компаній за сферою застосування: (1.) оператори критичної інфраструктури (розділ 8a BSIG), (2.) постачальники цифрових послуг (розділ 8c BSIG) і (3.) компанії в особливий суспільний інтерес (так званий. «UBI», розділ 8f BSIG).

На операторів критичної інфраструктури поширюються найсуворіші зобов’язання щодо кібербезпеки. Відповідно до сучасного рівня техніки вони повинні вжити відповідних організаційних і технічних заходів, щоб уникнути порушень доступності, цілісності, автентичності та конфіденційності своїх систем, компонентів або процесів інформаційних технологій, які є вирішальними для функціональності критичної інфраструктури, яку вони працювати (§ 8a BSIG). З 1 травня 2023 року в рамках цих заходів також повинні використовуватися системи

виявлення атак. Компанії також повинні гарантувати, що необхідні технічні, організаційні та кадрові умови для ефективного використання таких систем гарантовані та що системи налаштовані таким чином, щоб вони відповідали профілю вимог. Дотримання цих зобов'язань має бути продемонстровано Федеральному відомству з інформаційної безпеки (BSI) кожні два роки (розділ 8a параграф 3 BSIG).

Постачальники цифрових послуг повинні вживати відповідних і пропорційних технічних та організаційних заходів для управління ризиками для безпеки мережевих та інформаційних систем, які вони використовують для надання цифрових послуг у межах Європейського Союзу (Розділ 8c, абзац 1 речення 1 BSIG). Постачальники повинні негайно повідомляти BSI про інциденти безпеки, які мають значний вплив на надання їхніх послуг (розділ 8c, параграф 3, речення 1, 3 BSIG).

Компанії, що представляють особливий суспільний інтерес (так звані UBI), зобов'язані зареєструватися в BSI. Ви повинні повідомити BSI про вжиті заходи безпеки IT, а також про сертифікацію та аудит (розділ 8f, параграф 1, 5 BSIG).

Зобов'язання щодо кібербезпеки також застосовуються відповідно до Загального регламенту захисту даних (GDPR). Стаття 32 GDPR передбачає, що необхідно вжити відповідних технічних та організаційних заходів з метою забезпечення відповідного рівня захисту. IT-безпека в розумінні GDPR передусім означає безпеку даних. Забезпечення безпеки, цілісності, автентичності, конфіденційності та доступності систем інформаційних технологій, з одного боку, завжди залежить від їх зручності використання та функціональності, з іншого.

Закон про захист телекомунікаційних і телемедійних даних (TTDSG) також стандартизує зобов'язання щодо кібербезпеки. Згідно з розділом 19, параграфом 1 TTDSG, провайдери телемедійних послуг повинні вживати технічних та організаційних заходів, щоб гарантувати, що користувач телемедійних засобів може припинити використання послуги в будь-який час і використовувати телемедійні засоби, захищені від того, щоб треті сторони дізналися про це. Ці зобов'язання стосуються багатьох компаній, оскільки веб-сайт або веб-магазин уже

є так званим телемедіа. Однак рівень захисту не відповідає директиві NIS 2. Запобіжні заходи відповідно до розділу 19, параграф 4, речення 1 TTDSG мають лише «враховувати» сучасний рівень техніки. Достатньо методу шифрування, який визнано безпечним, наприклад, шифрування HTTPS і SSL або брандмауери.

Прогноз: суворіші зобов'язання щодо кібербезпеки відповідно до директиви NIS 2

Директива NIS 2 значно розширює сферу зобов'язань щодо кібербезпеки, тобто компаній, яких це стосується. Порівняно з Директивою NIS, Директива NIS 2 також містить значно більший набір зобов'язань щодо кібербезпеки. Порушення зобов'язань щодо кібербезпеки мають підлягати суворим санкціям. Проект німецького імплементаційного закону передбачає штрафи від 100 000 до 500 000 євро і навіть до 20 мільйонів євро, що навіть значно перевищує вимоги Директиви NIS 2 (до 10 мільйонів євро).

Заходи кібербезпеки та управління ризиками

Згідно зі статтею 21(1) Директиви NIS 2, істотні та важливі суб'єкти зобов'язані «вживати належних і пропорційних технічних, операційних та організаційних заходів для пом'якшення ризиків для безпеки мережі та інформаційних систем, які підтримують їх для контролю над використання засобів для їх функціонування або надання своїх послуг, а також для запобігання або мінімізації впливу інцидентів безпеки на одержувачів їхніх послуг та на інші послуги».

Необхідно враховувати сучасний рівень техніки, стандарти ЄС і міжнародні стандарти, а також витрати на впровадження, відповідно до яких заходи повинні відповідати ризику, див. Статтю 21, параграф 1, речення 2 і 3.

Зобов'язання щодо управління ризиками включають, серед іншого, наступні заходи, які в статті 21, параграф 2 наведені як приклади:

Концепції, пов'язані з аналізом ризиків і безпекою інформаційних систем

Управління інцидентами безпеки

Постійні операції, такі як керування резервним копіюванням і аварійне відновлення

Кризовий менеджмент

Забезпечення безпеки в ланцюзі поставок

Управління вразливістю

Управління ризиками кібербезпеки

Навчання з кібербезпеки

Концепції та процедури використання методів шифрування

Безпека персоналу: контроль доступу та управління авторизацією

Багатофакторна автентифікація або безперервна автентифікація, захищений голосовий, відео- та текстовий зв'язок і, де це можливо, захищені системи екстреного зв'язку

Також посилюються зобов'язання повідомляти про серйозні інциденти безпеки.

Кібербезпека як питання відповідності та відповідальність керівництва

Особливо новим є зобов'язання керівництва щодо моніторингу відповідно до пункту 1 розділу 38 проекту Закону про імплементацію NIS 2 та посилення кібербезпеки. Рада директорів і керівництво повинні забезпечити вжиття належних і пропорційних технічних, операційних та організаційних заходів у компанії для мінімізації кіберризиків. Існує також зобов'язання пропонувати навчання IT-безпеці для керівництва та інших працівників.

Ці обов'язки не можуть бути повністю делеговані. Остаточна відповідальність завжди залишається на рівні керівництва. Якщо керівництво порушить ці зобов'язання щодо відповідності, воно буде зобов'язане відшкодувати збитки компанії. Законопроект прямо виключає відмову від цих претензій щодо відшкодування збитків або їх врегулювання.

Якщо ця пропозиція дійсно буде стандартизована в законі, як це передбачено в законопроекті, існуючі страхові рішення необхідно буде переглянути. Порушення зобов'язань щодо кібербезпеки стане значним ризиком для керівництва, який, можливо, може бути покритий страхуванням D&O. Компанії також повинні оцінити, чи варто брати кіберстрахування.

Відповідно до розділу 91 (3) AktG, створення системи управління ризиками вже є частиною обов'язків ради директорів акціонерного товариства і, отже, є частиною загальних зобов'язань керівництва компанії з дотримання вимог законодавства. Новим є конкретне розширення зобов'язань щодо кібербезпеки. Тому зараз обговорюється, чи потрібен окремий департамент з кібербезпеки, тобто член кіберради.

Практична довідка

Навіть якщо Закон про реалізацію NIS 2 і зміцнення кібербезпеки ще не доступний у остаточній чернетковій версії, і ще є час до жовтня 2024 року, поки не буде імплементовано Директиву NIS 2, уже видно конкретні тенденції щодо зобов'язань постраждалих компаній. Тому рекомендується використати час до того часу, щоб переглянути існуючі концепції кібербезпеки, оцінити ризики та розпочати розробку необхідної документації, такої як концепції кібербезпеки, плани на випадок надзвичайних ситуацій тощо, разом із технічними та юридичними експертами та експертами з кібербезпеки, які будуть об'єднані в компанію. Інвестиції в кібербезпеку окупаються, особливо тому, що вони роблять важливий внесок у захист ноу-хау компаній від промислового шпигунства та мінімізацію ризику великих операційних втрат у разі кібератаки. Профілактика та своєчасна підготовка можуть тут змінитися.

Досі люди неохоче описували IT та IT-безпеку як завдання управління в компанії. Однак в епоху Індустрії 4.0 очевидно, особливо з огляду на законодавчі зміни, що IT-безпека має стати «головним пріоритетом». Це не означає, що керуючі директори та члени правління мають бути IT-фахівцями. Натомість їм слід звернутися за технічною експертизою до відповідних спеціалістів. Однак повне делегування більше не буде можливим, оскільки остаточну відповідальність несе рада директорів або керуючий директор. Неможливо оцінити, чи потрібна «кібердошка». Для кожної компанії, беручи до уваги існуючі структури, слід оцінювати, як найкраще реалізувати нові зобов'язання щодо кібербезпеки та відповідальність керівництва за IT-безпеку. У будь-якому разі, тема IT-безпеки й надалі хвилюватиме багато компаній, не в останню чергу на тлі постійно

зростаючої кількості кібератак». ***(Birgit Münchbach. Verschärfung der Cybersicherheitspflichten durch die NIS-2-Richtlinie: Brauchen Unternehmen künftig einen Cyber-Vorstand? // Advant Beiten (https://www.advant-beiten.com/de/blogs/iim/verschaerfung-der-cybersicherheitspflichten-durch-die-nis-2-richtlinie-brauchen-unternehmen). 08.02.2024).***

***

«… 27 листопада 2023 року європейські парламентарії та Рада уклали попередню угоду щодо Закону про кібернетостійкість (CRA), який запровадить нові зобов'язання щодо кібербезпеки та кіберстійкості для захисту цифрових продуктів у ЄС від кіберзагроз.

На високому рівні Закон про захист від кібернетичного впливу:

запроваджує обов'язкові вимоги до кібербезпеки для проектування, розробки, виробництва та надання на ринку апаратних і програмних продуктів, включаючи офісні додатки, розумні колонки, жорсткі диски, ігри, операційні системи, мережеві інтерфейси, брандмауери та комп'ютери та смартфони;

змінює баланс відповідальності за дотримання вимог щодо виробників, які повинні виконувати такі зобов'язання, як надання оцінки ризиків кібербезпеці щодо цих продуктів, видання декларацій відповідності та співпраця з компетентними органами протягом встановленого періоду або очікуваного терміну служби продукту;

передбачає зобов'язання щодо прозорості щодо аспектів безпеки апаратних і програмних продуктів, щоб дозволити споживачам враховувати кібербезпеку під час вибору та використання продуктів, які містять цифрові елементи; і

зобов'язує виробників забезпечувати постійну безпеку своїх продуктів і впроваджувати процеси обробки вразливостей для забезпечення кібербезпеки цифрових продуктів, включаючи зобов'язання для імпортерів або дистриб'юторів щодо цих процесів.

Цю пропозицію слід розглядати в контексті ширшої системи кібербезпеки ЄС, включаючи NIS2 і Закон про цифрову операційну стійкість (DORA). CRA має на меті заповнити прогалини та зробити існуюче законодавство про кібербезпеку

більш узгодженим шляхом накладення зобов'язань щодо безпеки на апаратне та програмне забезпечення по всьому ланцюжку постачання та протягом життєвого циклу продукту.

Які основні елементи політичної угоди?

Щодо терміну служби продукту було погоджено, що період підтримки виробника для підключеного продукту повинен відповідати його очікуваному терміну служби та що вказується період підтримки щонайменше п'ять років, за винятком продуктів, які, як очікується, використовуватимуться протягом коротшого періоду. час;

Європейський парламент і Рада досягли згоди щодо двох різних списків для важливих і критичних продуктів на основі їх критичності та рівня ризику для кібербезпеки. Наприклад, для пов'язаних продуктів із функціями, пов'язаними з кібербезпекою, і функцією, яка несе значний ризик несприятливих наслідків, перед розміщенням на ринку вимагатиметься оцінка відповідності третіми сторонами. Для продуктів із дещо нижчими профілями ризику, таких як системи керування ідентифікацією, біометричні зчитувачі, автономні та вбудовані браузери, продукти VPN і системи керування мережею, виробники повинні проводити оцінку відповідності за допомогою своїх процедур внутрішнього контролю;

Продукти також повинні мати автоматично встановлені оновлення безпеки окремо від функціональних;

Комісія повинна буде прийняти додаткові правила для визначення категорій продуктів.

Нові правила діятимуть через три роки після набуття законом чинності. Виробники, імпортери та дистриб'ютори апаратних і програмних продуктів повинні будуть адаптуватися до нових вимог протягом цього часу;

Що стосується зобов'язань виробників звітувати про інциденти та вразливості, існує більш обмежений 21-місячний пільговий період;

Були включені додаткові заходи підтримки малих і мікропідприємств, такі як спеціальні заходи з підвищення обізнаності та навчання, а також підтримка процедур тестування та оцінки відповідності.

Дві європейські організації стандартизації, CEN і CENELEC, зараз розробляють стандарти та спільні специфікації, які мають бути готові протягом трьох років.

Наступні кроки

Узгоджений текст зараз завершується на технічних зустрічах. Остаточний текст має бути офіційно ухвалений як Європейським парламентом, так і Радою, перш ніж він буде опублікований в Офіційному журналі ЄС і стане законом». ***(Natallia Karniyevich, Feyo Sickinghe and Berend van der Eijk. Stricter cybersecurity rules to apply to products // Bird & Bird LLP (https://www.twobirds.com/en/insights/2024/global/stricter-cybersecurity-rules-to-apply-to-products). 08.02.2024).***

***

«…Оновлений Кодекс корпоративного управління Великобританії, опублікований 22 січня 2024 року, вводить нову концепцію, відповідно до якої ради повинні створити та підтримувати ефективну систему управління ризиками та внутрішнього контролю. Враховуючи, що кібербезпека є або основним ризиком, або має відношення до управління основними ризиками в організації, для більшості організацій зміни до Кодексу корпоративного управління прямо покладають відповідальність за кіберризики на суд правління.

Згодом 29 січня 2024 року Рада з фінансової звітності опублікувала вказівки щодо Кодексу корпоративного управління Великобританії. Наприклад, у цьому вказівці пояснюється, що рада повинна:

- визначати природу та ступінь основних ризиків та свою схильність до ризику;
- домовитися про те, як слід керувати основними ризиками або пом’якшувати їх, щоб зменшити ймовірність їх появи або їх впливу;
- контролювати та переглядати системи управління ризиками та внутрішнього контролю, а також процеси керівництва для цього, і переконатися, що вони функціонують ефективно, і що коригувальні дії вживаються, якщо це необхідно; і

- забезпечити ефективну зовнішню комунікацію щодо управління ризиками та внутрішнього контролю.

Однак незрозуміло, чи всі ради директорів наразі знають, як виглядає ефективне кіберуправління на практиці, оскільки в опитуванні уряду Великобританії про кіберзломи за 2023 рік зазначено, що «існує брак розуміння того, що таке ефективне управління кіберризиками».

Тому корисно, що уряд також опублікував проект Кодексу практики кіберуправління (23 січня 2024 р.), щодо якого він шукає думки. Це спрямовано на підтримку директорів у підвищенні кіберстійкості.

Кодекс складається з п’яти загальних принципів, кожен з яких має відповідні дії. За необхідності вони не є надмірно директивними, щоб гарантувати їх широку застосовність, тому все ще є багато можливостей для варіацій у їх застосуванні.

Ці принципи та дії підсумовано нижче:

Управління ризиками

Дії включають забезпечення того, щоб кіберризики розглядалися як частину ширшої діяльності організації з управління ризиками підприємства та внутрішнього контролю, а також встановлення відповідальності за ризики з відповідними вищими керівниками за межами CISO.

Кібер стратегія

Це охоплює моніторинг стратегії кіберстійкості та її впровадження, а також забезпечення розподілу відповідних ресурсів.

Люди

Цей принцип спрямований на спілкування та навчання. Це включає в себе забезпечення наявності ефективних і вимірюваних програм навчання та підвищення обізнаності з кібербезпеки, а також спонсорування інформації про важливість кіберстійкості.

Планування і реагування на інциденти

Пов’язані дії включають те, що рада повинна переконатися, що організація має план кіберінцидентів і щонайменше щорічне його тестування. Крім того, у разі

інциденту правління має підтримувати керівників у прийнятті важливих рішень і зовнішніх комунікаціях.

Забезпечення та нагляд

Цей принцип вимагає від правління створити структуру управління з чіткими ролями та обов'язками та володінням кібернетичними засобами на рівні директора. У ньому зазначено, що офіційна звітність повинна складатися принаймні щоквартально з регулярним діалогом з CISO та іншими відповідними керівниками.

Кодекс призначений для відображення існуючої найкращої практики та доповнення наявних галузевих і державних ресурсів як у Великобританії, так і за кордоном. Багато директорів уже знайомі з Інструментарієм кібербезпеки для правлінь, опублікованим Національним центром кібербезпеки, і намір полягає в тому, що Кодекс і Інструментарій працюватимуть разом, щоб сформувати узгоджений набір інструкцій для рад.

Після того, як він буде готовий до остаточної форми, уряд має намір запровадити Кодекс як добровільний інструмент без власної законодавчої основи. Однак інвестори дедалі більше зосереджуються на управлінні кібернетичними засобами. Минулого року Glass Lewis (впливова фірма з голосування за довіреністю) додала новий розділ до своїх інструкцій щодо голосування за довіреністю, у якому зазначено, що «зацікавлені сторони компанії виграють від чіткого розкриття інформації щодо ролі правління. у нагляді за питаннями, пов'язаними з кібербезпекою».

Таким чином, можна очікувати, що, навіть якщо Кодекс є добровільним, очікування інвесторів (і занепокоєння щодо відповідальності окремих директорів) спонукатимуть ради дотримуватись його, незважаючи на його добровільний характер». ***(Rebecca Cousin, Natalie Donovan, Rob Sumroy and Jonathan Cotton. Change is afoot for Cyber Governance // slaughter and may (https://my.slaughterandmay.com/insights/briefings/change-is-afoot-for-cyber-governance). 21.02.2024).***

***

«…Останній щорічний звіт про національний цифровий ризик у Норвегії був опублікований Управлінням національної безпеки Норвегії («NSM») 19 жовтня 2023 року [Nasjonalt digitalt risikobilde 2023 (nsm.no)]. Мета звіту полягала в тому, щоб підвищити обізнаність і мотивувати підприємства посилити свої зусилля з кібербезпеки, при цьому NSM загалом наголошує, що як державні, так і приватні підприємства повинні надавати пріоритет кібербезпеці в майбутньому.

У звіті висвітлюються такі ключові моменти:

Очікується, що розвиток штучного інтелекту, включаючи великі мовні моделі, призведе до подальшої професіоналізації зловмисників.

Кібератаки можуть мати посилений фізичний вплив, оскільки промислові системи (наприклад, ті, що пов’язані з критичною інфраструктурою) дедалі частіше підключаються до Інтернету.

Збільшення уваги до кібербезпеки може зробити інші методи доступу до інформації більш привабливими для зловмисників. Ризик для системи з боку інсайдерів може зрости, якщо однобічний фокус на кібербезпеці. Важливо думати про безпеку в усіх сферах.

Кібератаки, спрямовані на вплив на виборців, створюють навантаження на демократії.

З огляду на постійно зростаючий ризик, кібербезпека є темою, яка має бути на порядку денному як для правлінь компаній, так і для керівництва. Директори та менеджери повинні усвідомлювати важливість розуміння того, як кіберризик може загрожувати цінностям компанії, вживати необхідних заходів для забезпечення безперервної роботи бізнесу (на фоні кібератаки), пом’якшення фінансових втрат, запобігання втраті конфіденційної інформації. інформацію/особисті дані та обмежити ризик відповідальності та шкоди репутації. Відповідно до Закону про компанії, норвезькі ради зобов’язані ознайомитися з потенційними сферами ризику комплаєнсу для компанії та контролювати їх. Правління визначає очікування та частково встановлює керівні принципи щодо пріоритетів управління. Крім того,

члени правління можуть нести особисту відповідальність (акціонерами) у разі фінансових збитків.

Директиви ЄС щодо кібербезпеки та відповідні зміни законодавства в Норвегії

Щодо кіберзаконодавства, існує постійний потік розробок, які компанії повинні враховувати у своїх зусиллях щодо впровадження комплексного та ефективного кіберменеджменту.

У норвезькому законодавстві останньою подією є прийняття норвезьким парламентом Закону про цифрову безпеку 20 грудня 2023 року. Закон включає директиву ЄС щодо кібербезпеки, Директиву NIS1 (хоча дата її набуття чинності ще не визначена). Закон про цифрову безпеку вимагає від організацій, які відіграють особливо важливу роль у підтримці критичної соціальної та економічної діяльності, дотримуватись вимог щодо цифрової безпеки та повідомляти владі про серйозні цифрові інциденти. Кілька галузей/секторів уже підлягають правовим вимогам щодо цифрової безпеки протягом кількох років, включаючи, зокрема, фінансовий сектор і сектор охорони здоров'я. Таким чином, нове законодавство матиме особливе значення головним чином для компаній у галузях, які раніше не підлягали настільки ж високим вимогам до цифрової безпеки.

У ЄС вже набула чинності друга ітерація директиви з кібербезпеки – NIS2. NIS2 накладає вимоги безпеки, а також зобов'язання щодо сповіщення про інциденти та управління для організацій у ряді критичних секторів, включаючи енергетику, транспорт, фінанси, охорону здоров'я та цифрову інфраструктуру. Країни-члени мають перенести директиву до національного законодавства до жовтня 2024 року. На додаток до пом'якшення певних недоліків у NIS1, Директива NIS2 спрямована на розширення та гармонізацію сфери застосування правил кібербезпеки, а також встановлює певні мінімальні вимоги. Невідомо, коли NIS2 стане частиною норвезького законодавства. Однак не виключено, що уряд Норвегії буде враховувати зобов'язання та сферу застосування Директиви NIS2 при складанні правил відповідно до вже прийнятого Закону про цифрову безпеку.

Незважаючи на це, компанії вже зараз повинні враховувати не лише NIS1, але й вимоги, викладені в Директиві NIS2. Навіть норвезькі компанії, які не працюють в ЄС, можуть опосередковано постраждати від NIS2, оскільки клієнти, які дотримуються вимог NIS2 більшою мірою, ніж NIS1, будуть зобов'язані стежити за кіберризиками та стійкістю своїх ланцюжків поставок.

Крім того, компанії повинні бути обізнані про численні інші відповідні законодавчі вимоги, що стосуються кібербезпеки, включаючи (але не обмежуючись ними) вимоги інформаційної безпеки. Це включає загальні закони, такі як Закон про безпеку, який стосується національної безпеки, і Закон про персональні дані, який стосується захисту персональних даних. Існують також вимоги, які застосовуються до конкретних галузей промисловості чи продуктів, наприклад, нормативні положення для окремих секторів у сфері фінансів, охорони здоров'я та державного сектора. Крім того, майбутній Закон про кібернетостійкість є дуже актуальним. Це буде перше загальноєвропейське законодавство такого роду, яке запроваджує спільні правила кібербезпеки для виробників і розробників продуктів із цифровими елементами, що охоплює як апаратне, так і програмне забезпечення.

Управління кіберризиками та врегулювання інцидентів

Підготовка є ключовою для управління кіберризиками та обмеження збоїв і збитків, спричинених інцидентами кібербезпеки. Така підготовленість може бути досягнута, наприклад:

- створення програми управління ризиками кібербезпеки на основі оцінки ризиків, впровадження заходів щодо управління, дотримання вимог і контрактів;
- визначення відповідних нормативних вимог, включаючи вимоги до сповіщення;
- впровадження ефективного плану реагування на кіберінциденти, який встановлює письмовий систематичний підхід до врегулювання інциденту та включає детальні процедури/інструкції (наприклад, контрольні списки), управління зацікавленими сторонами тощо;
- проведення тренінгів з підвищення обізнаності та готовності;

- відображення ризиків для співробітників (інсайдерські загрози тощо) та контроль за ними;
- встановлення спеціальної процедури реагування на порушення даних відповідно до GDPR;
- відображення ризиків, пов'язаних з відповідальністю, у відповідних контрактах з постачальниками та клієнтами; і
- оцінка питань кіберстрахування.

У разі кібератаки важливо мати надійного партнера, який може допомогти вжити негайних і ефективних заходів. Вікборг Рейн має великий досвід вирішення різноманітних інцидентів, у тому числі пов’язаних із порушенням безпеки. Ми також звикли безперебійно працювати з технічними експертами, які відіграватимуть центральну роль у вирішенні кіберризиків та інцидентів у міру їх виникнення». ***(Gry Hvidsten and Elisabeth Roscher. Managing cyber risk // Wikborg Rein (https://www.wr.no/en/news/__temp_ewvygxieqievkizrsodiswqjoyfjofghslch). 15.02.2024).***

***

Австралія та Нова Зеландія

«За останні два роки кібербезпека зайняла головне місце в політичному та громадському дискурсі Австралії, торпедована національною свідомістю через серйозні резонансні, потужні кібератаки, які призвели до скомпрометації особистих даних мільйонів громадян. Хоча зловмисна кібердіяльність, націлена на австралійські установи, організації та громадян, не нова, ця низка атак захопила уяву громадськості. Постраждалі організації – телекомунікаційна компанія Optus, приватний медичний страховик Medibank і постачальник кредитних послуг Latitude – були добре відомі в національній екосистемі та їм довіряли. І масштаби крадіжки особистої інформації були безпрецедентними, таких, яких Австралія не бачила раніше. Австралійці були розлючені, організації були стурбовані, а уряд перебував під зростаючим тиском, щоб вжити заходів. Спонуканий цим унікальним

імпульсом, для федерального уряду був явний поштовх скористатися можливістю переглянути та оновити Стратегію кібербезпеки Австралії.

Започатковуючи стратегічні консультації, міністр внутрішніх справ Австралії Клер О'Ніл заявила: «Австралійці нещодавно постраждали від двох найгірших витоків даних в історії нашої країни. Ми повинні працювати разом, щоб протистояти цим загрозам, будувати партнерські відносини та налаштовуватися на успіх. Коли справа доходить до кібербезпеки Австралії, кожен має справу». Австралія має прагнути стати найбільш кіберзахищеною країною у світі до 2030 року. Розробка Австралійської стратегії кібербезпеки на 2023-2030 роки окреслить довгострокове бачення уряду щодо майбутнього кібербезпеки Австралії та конкретні кроки, необхідні для досягнення цього.» Далі був документ для широкого обговорення та широке обговорення з громадськістю. Кульмінацією цієї роботи став випуск Стратегії кібербезпеки Австралії на 2023-30 рр. (далі — Стратегія) у листопаді минулого року, яка, у своїй основі, зосереджена на баченні того, як Австралія стане найбільш кіберзахищеною нацією у світі до 2030 року. У цьому коментарі ми підкреслюємо, деякі з ключових аспектів стратегії, розробленої для стимулювання розвитку кібербезпеки Австралії та її пріоритетів у кіберрозширенні протягом наступних семи років. Зокрема, ми розглянемо ключові положення Стратегії, які називаються «Шість щитів».

Щоб забезпечити контекст, нова Стратегія є третьою в Австралії. Перший, випущений у 2016 році, був зосереджений на підвищенні спроможності уряду щодо кіберпростору, розвитку вітчизняної індустрії кібербезпеки та розбудові національного потенціалу досліджень і розробок у кібернетичній сфері. Він також вперше визнав наступальний потенціал Австралії. Стратегія до 2020 року передусім стосувалася захисту національної критичної інфраструктури та посилення можливостей правоохоронних органів щодо протидії кіберзлочинності. Ключовим досягненням стратегії стала значна реформа режиму безпеки критичної інфраструктури Австралії, який зараз є провідним у світі.

Спираючись на цю основу, Стратегія зосереджена на всій економіці, охоплюючи громадян, уряд, малий і великий бізнес. Примітно, що він був

розроблений під час значної та пов’язаної з цим реформи законодавства, з переглядом Закону Австралії про конфіденційність, який зараз триває, спрямований на приведення застарілих законів Австралії про конфіденційність до стандарту ЄС GDPR та подальше вдосконалення Закону про безпеку критичної інфраструктури (SOCI Act), після великих кібератак за останні кілька років. Вона також була розроблена на тлі значних геополітичних потрясінь, регіональних змін і створення AUKUS, що відображено в фокусі Стратегії на міжнародному співробітництві, регіональних ініціативах і зміцненні альянсів.

Як зазначалося, стратегія побудована на шести щитах:

Сильний бізнес і громадяни

Безпечна технологія

Обмін загрозами та блокування світового рівня

Захищена критична інфраструктура

Суверенні можливості

Стійкий регіон і глобальне лідерство.

Це буде досягнуто за трьома напрямками – зміцнення фундаментів; масштабування кіберзрілості в масштабах всієї економіки; і стати світовим лідером у сфері кібербезпеки до 2030 року.

Shield One – сильний бізнес і громадяни зосереджено на підтримці австралійського бізнесу, особливо малого та середнього бізнесу (МСП), покращення їх кіберстійкості та здатності відновлюватися після кіберінцидентів. Освіта, підвищення обізнаності та заохочення висвітлюються як головні механізми досягнення Shield One. Подібно до підходів ЄС і США, уряд Австралії закликатиме більші організації відігравати ключову роль у зміцненні безпеки економіки загалом шляхом зміцнення власного захисту та підтримки МСП.

Shield Two – безпечна технологія спрямована на забезпечення надійності цифрових продуктів і послуг, наголошуючи на безпеці технологій. Центральним елементом цього щита є розробка безпечних структур і систем рейтингу, щоб надати споживачам інформацію про кібербезпеку цифрових продуктів і програмного забезпечення, які вони купують. Це узгоджується зі схожими

стратегіями ЄС, Великобританії та США щодо запобігання ризикам безпеки, які виникають через поширення пристроїв IoT. У Стратегії визнається потенційний системний вплив цих систем і зовнішнє втручання, одним із прикладів є використання пристроїв IoT у широко розгорнутих сонячних енергетичних системах. Цей щит також спрямований на сприяння безпечному використанню таких нових технологій, зокрема штучного інтелекту та квантових обчислень, шляхом встановлення огорож. Це відображає пріоритети інших країн у цих сферах, зокрема Закон ЄС про штучний інтелект та Закон про захист від кібернетичного впливу, але без негайних регуляторних інструментів, натомість покладаючись на стандарти та кодекси практики.

Shield Three – обмін загрозами та блокування загроз світового рівня, зосереджений на посиленні державно-приватного партнерства для покращення виявлення та пом'якшення кіберзагроз. Стратегія окреслює амбітний план розробки загальноекономічної мережі обміну загрозами та блокування з розширеним міжгалузевим обміном інформацією та обміном загрозами в реальному часі для забезпечення автоматизованих можливостей блокування загроз. Центральне місце в досягненні цієї мети займають телекомунікаційні компанії та постачальники послуг Інтернету, які матимуть стимули для розширення цих можливостей.

Щит чотири – Захищена критична інфраструктура спрямована на подальше вдосконалення Закону SOCI, який регулює активи критичної інфраструктури Австралії в 11 ключових секторах. Як згадувалося раніше, головним досягненням Стратегії 2020 стала реформа Закону про SOCI, яка призвела до збільшення кількості захоплених секторів з трьох до 11 із посиленням зобов'язань щодо безпеки для так званих систем національного значення (SoNS). У той час як Закон SOCI використовує підхід «усі небезпеки» до загроз безпеці, зміцнення кібербезпеки є його суттю. Через масштабні витоки даних у 2022-2023 роках уряд проведе консультації з галуззю, щоб роз'яснити застосування Закону SOCI, щоб переконатися, що об'єкти критичної інфраструктури належним чином захищають свої системи зберігання даних. Це буде зосереджено на «важливих для бізнесу»

системах зберігання даних, уразливість яких може вплинути на доступність, цілісність, надійність або конфіденційність критично важливих інфраструктурних активів. На відміну від інших режимів критичної інфраструктури, зокрема американської моделі, Закон SOCI не стосується уряду, його департаментів чи агентств. Хоча малоймовірно, що Закон про SOCI буде розширено, щоб охопити державні установи, Стратегія наголошує на прагненні уряду подавати приклад. Це важливо, оскільки в минулому лунала критика щодо значних прогалин в державній інфраструктурі кібербезпеки.

Shield Five – S Suvereign Capabilities зосереджено на розвитку та професіоналізації сильної національної робочої сили в кіберпространстві, а також на розвитку вітчизняної кіберіндустрії, кібердосліджень та інновацій. Як і інші країни, Австралія страждає від значної нестачі кібернавичок і робочої сили. Уряд прагне стримати цю тенденцію шляхом інвестицій в освіту та навчання, залучення кваліфікованих мігрантів через імміграційну реформу та сприяння та стимулювання різноманітності кіберробочої сили. Щоб професіоналізувати австралійську робочу силу, розглядається можливість акредитації навичок із розробкою чіткої системи кібернавичок. Це спрямовано на те, щоб гарантувати роботодавцям, що кібер-робоча сила має відповідну кваліфікацію, а також надати працівникам впевненості в тому, що їх кваліфікація та відповідний досвід визнані та відповідають меті.

Shield Six – Resilient region and global leadership – це визначення ролі Австралії як зрілої та етичної цифрової нації, яка прагне підтримувати та просувати глобальні правила та норми. Це особливо важливо на регіональному рівні, де уряд вкладатиме значні кошти в посилення кіберзахисту австралійської тихоокеанської сім'ї та ґрунтується на розумінні того, що безпека та процвітання Австралії пов'язані з нашим регіоном, із серйозними наслідками безконтрольного примусу та конкуренції в нашому регіоні. На глобальному рівні уряд зобов'язався захищати та зміцнювати міжнародну систему стандартизації, сприяючи та підтримуючи надійні міжнародні стандарти в технологіях, які лежать в основі кіберпростору, Інтернету та цифрової економіки. З цією метою Австралія співпрацюватиме з глобальними

партнерами, щоб забезпечити прозорість і конкурентоспроможність технологічних ринків із різноманітністю постачальників безпечних і безпечних продуктів і послуг. Слід зазначити, що Shield Six натякає, що Австралія використовуватиме свої наступальні можливості через Австралійську дирекцію сигналів (ASD), щоб стримувати та реагувати на зловмисників у кіберпространстві, співпрацюючи з міжнародними партнерами, щоб вжити заходів для накладання витрат на окремих осіб та організації, які роблять кіберпростір менш безпечним. і безпечно.

Реалізація Стратегії здійснюватиметься відповідно до Стратегії кібербезпеки Австралії на 2023-2030 роки – Плану дій (План). План окреслює три горизонти дій, зосереджених на зміцненні основ, зростанні кіберзрілості та утвердженні Австралії як світового кіберлідера. Цей підхід було використано для підтримки «гнучкого підходу до досягнення бачення Стратегії, що дозволить нам залишатися адаптованими до нових технологічних, економічних і геополітичних тенденцій».

Велика картина

Як ліберальна демократія Австралія стикається з такими ж загрозами та викликами, як і її глобальні партнери, що відображено в широкій та амбітній Стратегії. Він має хороші можливості для узгодження стратегій основних партнерів і посилається на важливі глобальні альянси Австралії, включаючи AUKUS і Quad. Австралія також стикається з унікальними проблемами, де тиранія відстані є одним із факторів, які сприяють реалізації деяких ключових заходів Стратегії. Це особливо помітно у зв’язку з прагненням до розширення суверенних можливостей шляхом створення сильної робочої сили в кіберпространстві та сприяння внутрішнім інноваціям. Подібним чином, порівняно з кіберстратегіями світових аналогів, Австралія зосереджена на кібербезпеці та піднесенні МСП завдяки великій базі МСП економіки та основним ланцюгам поставок, які покладаються на неї. Маючи сім років на досягнення своїх цілей, Стратегія встановлює чіткий шлях для Австралії, щоб досягти своєї мети стати кіберсвітовим лідером. Він визнає можливості, які відкриває побудова динамічної екосистеми кібербезпеки через посилення внутрішнього потенціалу та спроможності, а також ключову регіональну роль, яку відіграє Австралія як приклад кібербезпеки.

Однак Стратегія не позбавлена недоліків. Наприклад, незважаючи на те, що вітаються зобов'язання Австралії щодо підтримки науково-дослідницького потенціалу Австралії, пов'язаного з кіберпромисловістю, та інвестиції у розвиток внутрішньої кіберіндустрії, вони не підкріплюються інвестиційними планами дій чи матеріальним фінансуванням, як це відбувається в США та ЄС. Подібним чином надається небагато деталей щодо того, як розвиватиметься регулювання та етичне використання критичних і нових технологій, що є гострою проблемою на національному, регіональному та міжнародному рівнях. Ключовим фактором майбутнього успіху Стратегії буде здатність уряду залишатися гнучким у динамічному глобальному середовищі, де продовжують виникати нові загрози та виклики. По суті, це означає, що до Стратегії слід підходити як до живого документа – такого, який не висічений у камені та який піддається змінам у кліматі змін. Якщо це вдасться реалізувати, не випускаючи з уваги ширше бачення Стратегії, тоді Австралія матиме хороші можливості стати однією з найбільш кіберзахищених країн у світі». ***(Helge Janicke, Anne-Louise Brown. Striking a balance: A review of Australia's Cyber Security Strategy 2023-30 // EU Institute for Security Studies (https://directionsblog.eu/striking-a-balance-a-review-of-australias-cyber-security-strategy-2023-30/). 19.02.2024).***

***

«Кіберризики є одними з головних ризиків, з якими сьогодні стикаються підприємства та інші організації. Підприємства Нової Зеландії повідомили про збитки від кіберзлочинності на суму 39,6 млн. доларів США за два роки до 2023 року, і ця цифра включає лише ті, які повідомили про свої збитки. За оцінками, до 2025 року кіберзлочинність обійдеться підприємствам у 10,5 трильйонів доларів США щорічно. Крім того, окрім збитків для кіберзлочинців і відповідних збитків для окремих осіб та інвесторів, регуляторні органи в Новій Зеландії та за кордоном все більше приділяють увагу тому, що регульовані фірми роблять для управління ризиками кібербезпеки.

Зростання кіберзлочинності призводить до збільшення судових процесів. Позови висуваються проти компаній, які стали жертвами кібератак, що призвело до

розголошення приватної та особистої інформації їхніх клієнтів та інших осіб. Позови висуваються до страховиків у разі заподіяння збитків. Засоби правового захисту вимагаються від банків та інших фінансових установ, які не запобігають збиткам клієнтів у результаті кіберзлочинності. Регулюючі органи все більше зосереджуються на адекватності чи кіберзахисті регульованих установ і на кроках, які вживають їхні ради.

Нещодавно особисту інформацію 9,7 мільйонів клієнтів Medibank було викрадено та опубліковано в Інтернеті після того, як його страховик відмовився виплатити вимогу про викуп. Це призвело до двох групових позовів у Федеральному суді Австралії та розгляду від імені акціонерів у Верховному суді Вікторії. У Новій Зеландії кібератака Latitude у березні минулого року розкрила особисті записи 14 мільйонів клієнтів, включаючи мільйон номерів новозеландських водійських прав і 40 000 записів у паспортах. У відповідь Уповноважений з питань конфіденційності Нової Зеландії та Уповноважений з питань інформації Австралії розпочали спільне розслідування щодо конфіденційності, один із постраждалих клієнтів також подав позов на 1 мільйон доларів США, і відкрита реєстрація для потенційного групового позову проти Latitude.

Раді компаній повинні взяти до уваги. Всесвітній економічний форум висловив думку, що для ефективного управління кіберризиками радам потрібні міцніші основи. В опитуванні Institute of Directors / ASB Bank лише 54% директорів повідомили, що їхні ради регулярно обговорюють кіберризики та впевнені, що їхні організації мають можливості реагувати на кібератаки чи інциденти.

У цій статті ми надаємо ключові міркування щодо того, як директори та ради можуть зменшити ризики кібербезпеки та реагувати на кіберінцидент, якщо він трапиться.

Управління кіберризиками

Австралійська комісія з цінних паперів та інвестицій (ASIC) розробила рекомендації щодо належної практики кібервідмовостійкості і заявила, що хороша стратегія кібербезпеки та управління характеризуються володінням правління та

моделями управління, що швидко реагують і гнучкими. Інститут директорів Нової Зеландії також опублікував « практичний посібник » щодо кіберризиків. У світлі цих матеріалів і нашого досвіду ми надаємо нижче кілька ключових порад щодо управління ризиками кібербезпеки.

1. Створіть систему управління кіберризиками для всього підприємства:

Рада директорів зобов'язана притягнути керівництво до відповідальності за встановлення повністю інтегрованого організаційного підходу до кібербезпеки. Організації повинні підходити до кібербезпеки як до ризику для всього підприємства, а не як до IT-проблеми. Стратегія кібербезпеки повинна окреслювати комплексний підхід до управління ризиками, реагування на інциденти та відновлення. Світового економічного форуму Принципи управління кіберризиками є корисним довідником для розробки стратегії кібербезпеки.

2. Регулярно приділяйте увагу кібербезпеці на порядку денному та продовжуйте розвивати кіберкомпетентність:

Хоча директорам не обов'язково бути кіберекспертами, їм потрібен достатній рівень розуміння, щоб бути в курсі ключових ризиків і проблем. Вони повинні звертатися до зовнішнього експерта, де це доцільно. Корисно переконатися, що на рівнях вищого керівництва є експерти з кібербезпеки та що вище керівництво інформує правління про будь-які ключові зміни кібервразливостей або ширшого середовища кіберризиків. Корисно ознайомитися з інструкціями Інституту директорів щодо звітності про кібербезпеку для рад директорів щодо того, як покращити звітність про кібербезпеку.

3. Зрозумійте правове середовище:

Дуже важливо, щоб директори розуміли свої юридичні обов'язки та наслідки кіберризику, що стосуються їхньої організації, і були в курсі змін нормативних вимог. Корисним ресурсом є наша нещодавня обкладинка статті про останні нормативні зміни в цій сфері. Такі регуляторні органи, як Управління фінансових ринків і Уповноважений із питань конфіденційності, а також страховики можуть вимагати сповіщення та/або розслідування кіберінцидентів і порушень конфіденційності.

4. Визначте, категоризуйте та вирішуйте ризики:

Керівництво має визначити, яких кіберризиків слід уникати, прийняти, пом'якшити або передати через страхування. Потім вони можуть сформулювати конкретні плани, пов'язані з кожним підходом. Корисно ознайомитися з 11 найкращими порадами CERT NZ щодо кібербезпеки, щоб отримати практичні вказівки щодо управління кіберризиками.

5. Удосконалення довгострокового управління кіберризиками:

У довгостроковій перспективі організаційні зміни для покращення процесів кібербезпеки, швидше за все, окупляться. Директори повинні враховувати:

Регулярні перевірки та підтвердження: Проводьте регулярні перевірки стратегій кібербезпеки та перевірки безпеки, щоб виявити вразливі місця та оцінити потенційний вплив кібератаки. Результати слід оцінювати за такими критеріями успіху, як час до виявлення, швидкість реакції та процес відновлення.

Сильна культурна спрямованість і підготовка: для більшості організацій основною кіберслабкістю є людська слабкість. Ефективна кіберстійкість вимагає сильного «культурного» фокусу, керованого правлінням і відображеного в загальноорганізаційних програмах для обізнаності персоналу, навчання та вибіркового тестування персоналу та третіх сторін для оцінки кіберобізнаності.

Інвестуйте в інфраструктуру кібербезпеки: впроваджуйте надійні заходи кібербезпеки, включаючи брандмауери, шифрування, системи виявлення вторгнень і безпечні рішення для резервного копіювання, і постійно їх оновлюйте.

Управління ризиками третіх сторін: кроки включають проведення належної перевірки (наприклад, отримання незалежних звітів про атестацію безпеки та сертифікатів) і використання умов контракту для підвищення прозорості та зменшення ризику четвертої сторони, наприклад, вимагаючи від постачальників повідомляти організацію, якщо їхні субпідрядники або у постачальників сталася подія кібербезпеки.

6. Переконайтеся, що існує всеосяжний план реагування на кібервитоки та порушення даних:

У разі кіберзлому оцінка та усунення порушення, ймовірно, будуть найбільш ефективними та заслуговують на довіру в очах зацікавлених сторін, таких як Уповноважений з питань конфіденційності та постраждалих осіб, якщо проводити їх у контексті перевіреного плану реагування на порушення даних. Уповноважений із питань конфіденційності Нової Зеландії та Управління уповноваженого з питань інформації Австралії визначили чотири ключові кроки у справі з порушенням конфіденційності: локалізація, оцінка, повідомлення та запобігання/перегляд.

Реагування на кіберінцидент

У разі кіберінциденту важливо бути готовим. Як зауважив Інститут директорів, організації, які не планували інцидент, як правило, погано працюють; вони, як правило, панікують і витрачають час і енергію на розробку свого підходу, в той час як зловмисник продовжує порушувати послуги або отримувати доступ до конфіденційних даних.

Ми виклали деякі ключові кроки та міркування, які можуть стати частиною плану реагування на кібернетичні ситуації.

Ідентифікувати та утримувати

Визначте та локалізуйте порушення, щоб запобігти подальшій втраті даних. Це може включати відключення уражених систем або обмеження доступу.

Оцініть вплив

Визначте, які дані було скомпрометовано, скільки осіб це вплинуло та які можливі наслідки. Це допоможе сформулювати відповідь.

Повідомте відповідні сторони

Якщо порушення відповідає порогу «серйозної шкоди» відповідно до Закону про конфіденційність 2020 року, організації зобов’язані повідомити Уповноваженого з питань конфіденційності та постраждалих осіб «якнайшвидше, коли це можливо». Перегляньте наш подкаст про різноманітні фактори, які слід враховувати під час оцінки порогу «серйозної шкоди», і про те, як організації повинні тлумачити вимогу сповіщати «якнайшвидше, коли це можливо».

Розслідуйте та виправляйте

Дослідіть, як сталося порушення, і вживіть заходів, щоб усунути ці вразливості та запобігти порушенням у майбутньому.

Ведіть належний облік

Зберігайте записи щодо оцінки порушення, реагування та будь-якого усунення. Це особливо важливо, якщо від організації вимагається виправдати неповідомлення про порушення, оскільки вона вважає, що воно малоймовірно завдасть серйозної шкоди. Однак зауважте, що ці записи, ймовірно, можна буде знайти під час будь-якого судового розгляду, тому переконайтеся, що вони підготовлені з урахуванням цього, уникаючи будь-яких марних заяв або критичних коментарів.

Розглянемо питання привілеїв

Законно конфіденційні документи можуть бути приховані під час судового розгляду або під час регуляторного розслідування, але дуже важливо, щоб були вжиті правильні кроки до та під час кіберінциденту, щоб зберегти та уникнути ненавмисної відмови від привілеїв. Спілкування зазвичай є привілейованим, якщо воно відбувається з юридичним радником з метою надання або отримання юридичних послуг. Комунікації також можуть бути конфіденційними, якщо вони здійснюються з головною метою підготовки до очікуваного судового розгляду. Однак повідомлення, створені з іншою метою, або повідомлення, які не є конфіденційними, не будуть привілейованими.

У разі кіберінциденту зв’язок і документи з такими цілями піддаються підвищеному ризику вимагати розголошення в судовому процесі:

розслідування причини кіберінциденту;

інформування зацікавлених сторін про кіберінцидент; і

обговорення існуючих або нових процесів кібербезпеки.

Недавній колективний позов Optus висвітлює це питання, яке ми обговоримо далі.

Збереження привілеїв під час реагування на кіберінцидент: уроки колективного позову Optus

Коли відбувається кіберінцидент, постраждала організація може захотіти замовити розслідування (внутрішнє чи зовнішнє) інциденту. Це може бути ризиковано, оскільки отриманий звіт може бути корисним для сторін, які подають провадження проти організації та/або її директорів. Звіт може визначити, що було зроблено неправильно, і може критикувати організацію.

Недавнє рішення Федерального суду Австралії підкреслює важливість належних протоколів привілеїв до того, як станеться інцидент. Запізніле встановлення протоколів і процесів привілеїв не призведе до ретроспективного надання юридичних привілеїв звіту про розслідування. Цілі підготовки звіту та докази, які демонструють ці цілі, є критичними, коли оскаржується претензія на привілеї. У вересні 2022 року Optus, австралійський постачальник телекомунікаційних послуг, зазнав витоку даних, який вплинув на особисту інформацію до 10 мільйонів клієнтів. Optus залучив зовнішніх адвокатів для надання юридичних консультацій і доручив Deloitte провести судово-медичну експертизу атаки та скласти звіт.

Після цих подій проти Optus було подано груповий позов до Федерального суду Австралії, стверджуючи, що компанія не захистила особисту інформацію клієнтів або не вжила належних заходів для захисту. Судова експертиза Deloitte містила інформацію, пов’язану з претензією, але Optus відмовився відкрити її та подібні документи, стверджуючи, що на них поширюється професійна таємниця.

Федеральний суд визнав, що звіт не є конфіденційним, незважаючи на те, що Optus стверджував, що його основною метою були юридичні поради або судовий процес. Суддя надав значну увагу прес-релізу, опублікованому Optus незабаром після витоку даних, який містив такий коментар: «цей перегляд допоможе нам зрозуміти, як це сталося, і як ми можемо запобігти повторенню. Це допоможе інформувати Optus щодо відповіді на інцидент. Це також може допомогти іншим у приватному та державному секторах, де зберігаються конфіденційні дані та існує ризик кібератак».

Суд постановив, що звіт Deloitte не є конфіденційним, оскільки він був підготовлений для низки цілей, а не для домінуючої чи головної мети юридичної

консультації чи судового розгляду. Хоча однією з цілей звіту було надання юридичної консультації для цілей судового розгляду або регуляторних процедур, інші цілі включали виявлення обставин і першопричин кібератаки, виправлення та перегляд управління Optus кіберризиками щодо її політики і процеси.

У Новій Зеландії та Австралії існують відмінності в законодавстві, яке регулює привілеї надання юридичних консультацій. На відміну від Австралії, у законодавчому визначенні привілею юридичної консультації в Новій Зеландії не згадується необхідність домінуючої мети, хоча в законодавчому визначенні привілею судового розгляду згадується. Цілком можливо, що суди Нової Зеландії можуть вимагати лише того, щоб юридична консультація була лише однією з цілей, для яких було створено звіт, але це, здається, не вирішено, тому для організацій було б розумно припустити, що звіти будуть лише бути захищеними, якщо їх основною метою було надання юридичної консультації.

Ще одна відмінність полягає в тому, що в Австралії експертний звіт третьої сторони може бути захищений привілеєм юридичної консультації, якщо він був створений з основною метою надання юристам юридичної консультації. У Новій Зеландії відповідне положення Закону про докази описує привілей юридичної консультації лише щодо документів, що передаються між клієнтами та їхніми адвокатами, а не третіми сторонами, наприклад експертами. Можливо, привілей юридичної консультації може надаватися на підставі того, що треті сторони є агентами клієнта, але це залежатиме від фактів кожної справи. Привілей судового розгляду відрізняється, оскільки привілей надаватиметься документам, підготовленим третіми сторонами, де домінуючою метою було дати можливість клієнту надати вказівки юристам, тому, якщо розумно передбачається, що судовий процес може бути більш ефективним методом захисту звіту. Переконатись, що звіт захищено законними привілеями, непросто, і це слід ретельно розглянути з самого початку.

Найкращі практичні кроки для захисту законної таємниці:

Встановіть і дотримуйтеся законних протоколів привілеїв

Встановлення належних протоколів привілеїв і конфіденційності запобігає випадковій відмові від привілеїв у напруженому та чутливому до часу сценарії, такому як кіберзлом. Заздалегідь зверніться за юридичною консультацією: розуміння зобов'язань щодо розкриття та звітування після кіберінциденту має вирішальне значення. Захист документів за допомогою привілеїв також може бути важливим. Своєчасне звернення до юридичного консультанта допоможе зорієнтуватися в цих пріоритетах.

Будьте чіткі, вказуючи цілі запитів

Щоб претендувати на конфіденційність щодо документів або повідомлень, створених у рамках розслідування кіберінциденту, загалом, документ або повідомлення має бути створено клієнтом з метою юридичної консультації або клієнтом або третьою стороною для домінуючої метою підготовки до судового процесу. Щоб допомогти в успішному відстоюванні привілеїв щодо цих матеріалів, юридична мета має бути однозначно сформульована та підтверджена доказами того часу. Також важливо забезпечити узгодженість обміну повідомленнями внутрішньої та зовнішньої комунікації, чого Optus не робив ефективно.

Будьте особливо обережні з багатоцільовими звітами та документами

Якщо звіт замовляється з кількома цілями, претензія на привілеї може бути оскаржена. Документи, підготовлені штатними консультантами, можуть бути більш схильні до оскарження, ніж документи, підготовлені зовнішніми юридичними консультантами, оскільки штатні співробітники частіше надають неюридичні бізнес-консультації та стратегічні поради, які не притягують привілеїв.

Заключні зауваження

Кіберризики все частіше призводять до судових процесів. Ми бачимо, що ця тенденція продовжується. Організації повинні реагувати, готуючись до протидії кіберризикам, і мати добре розроблений план реагування на кіберподію, який передбачає не тільки реагування ІТ, але й юридичний ризик, який слідує». ***(Andrew Horne, Jane Standage, Richard Gordon, Gillian Service, Briony Davies, Nick Frith, Sean Gollin, June Hardacre, Aaron Lloyd, Megan Richards and Stacey Shortall. Cyber risk and litigation: Some guidelines for directors and boards //***

MinterEllisonRuddWatts (https://www.minterellison.co.nz/insights/cyber-risk-and-litigation-some-guidelines-for-directors-and-boards). 15.02.2024).

***

Китай

«…Управління кіберпростору Китаю (CAC) нещодавно опублікувало запропоновані нові правила щодо звітування про інциденти кібербезпеки згідно з Адміністративними заходами щодо звітування про інциденти кібербезпеки (проект розкриття) (проект Регламенту).

Проект Регламенту спрямований на забезпечення ясності щодо зобов'язань організації та того, як вони мають працювати зі звітуванням, управлінням та звітуванням про кіберінциденти після інцидентів. CAC стверджує, що нові правила можуть зменшити втрати та шкоду в результаті кібератак і захистити національну безпеку в Інтернеті.

Що таке проекти Регламенту?

У проекті Регламенту запроваджується шкала класифікації кіберінцидентів, яка класифікуватиметься таким чином:

Надзвичайно важкий;

Сильний;

Великі інциденти; і

Звичайні випадки.

Якщо інцидент вважається «надзвичайно серйозним», «серйозним» або «великим» відповідно до проекту правил, новий бізнес повинен буде повідомити про це CAC. Немає конкретного терміну для повідомлення про звичайні інциденти.

Інциденти, які відносяться до категорії «серйозних» і «надзвичайно серйозних», можуть варіюватися від кібератак на веб-сайти урядових департаментів і переривання критичної інформаційної інфраструктури до крадіжки даних національної безпеки та витоку особистої інформації понад 1 мільйона людей.

Проект Положення також передбачає суворі процедури повідомлення про інциденти, а також після звітування про інциденти. Запропонована нова вимога полягає в тому, що інтернет-оператори повинні будуть провести всебічний аналіз інциденту, щоб визначити його причину та усунути її.

У чому важливість запропонованої постанови?

Для тих, хто веде бізнес у Китаї або хоче надавати товари чи послуги на китайському ринку в майбутньому, ці правила можуть стосуватися вас.

Ці зміни знову сигналізують про те, що конфіденційність і захист даних стають все більш важливими. Якщо ваш бізнес ще не розглядає питання захисту такої інформації, ми настійно рекомендуємо вам запровадити відповідні політики та процедури. ***(Kelly Dickson. New cyber security rules on the way for China // Macpherson Kelley (https://mk.com.au/new-cyber-security-rules-on-the-way-for-china/). 08.02.2024).***

***

Інші країни

«Уряд Менксу заявив, що мають бути введені нові закони для захисту ключових служб від кіберзагроз.

Мешканців і підприємства попросили взяти участь в онлайн-опитуванні для формування нового законодавства.

Законопроект про безпеку національної інфраструктури розглядає послуги з безпеки, включаючи електроенергію, воду та телекомунікації.

Міністр внутрішніх справ Джейн Пул-Вілсон заявила, що уряд визнав необхідність усунути загрози для «основних послуг та інфраструктури» острова.

За її словами, нові закони «підвищать нашу кіберстійкість, особливо для наших основних цифрових послуг».

«Розвиток кіберзагроз»

Під час консультації було зазначено, що новий законопроект є частиною урядових «кроків із захисту» острова від «кіберзагроз, що розвиваються».

Острів «не захищений від різних форм компромісу або нападу» і може постраждати від «прямого або побічного збитку», йдеться в повідомленні.

Ці консультації мають на меті визначити, що таке «критична національна інфраструктура», від послуг блакитного світла до управління відходами.

У документі також викладаються пропозиції щодо дотримання «заходів, запроваджених в інших юрисдикціях», «залишаючись гнучкими, щоб відповідати швидким змінам і загрозам».

Також вимагалися думки щодо запровадження «мінімального рівня стійкості та безпеки», визначеного для кожного з визначених секторів національної інфраструктури острова, і чи повинен бути перехідний період для телекомунікаційних компаній.

Речниця уряду заявила, що зміни спрямовані на забезпечення безперебійної роботи послуг, створення добре регульованого середовища та «підтримку зростання цифрової економіки».

Удосконалення законодавства призведе до кращого захисту від «потенційних перешкод у повсякденному житті», додала вона.

Консультація доступна онлайн, зовнішній до 25 березня, а відповіді на папері можна надсилати до Управління кібербезпеки та забезпечення інформації». ***(Proposals to prevent cyber-attacks on key services // bbc (https://www.bbc.com/news/articles/cd1jz149n5jo?utm_source=flipboard&utm_content=other). 05.02.2024).***

***

«Азербайджан посів 12-те місце з 66,67 балами серед 31 країни, які оцінювалися за 49 різними показниками, згідно з новими критеріями оцінювання Національного індексу кібербезпеки, запровадженими з вересня 2023 року.

Крім того, Азербайджан піднявся на 36 позицій і посів 50-е місце серед 176 країн у Національному індексі кібербезпеки - глобальному індексі, який управляється і розробляється Фондом Академії електронного урядування Естонії. Цей індекс вимірює готовність країн до боротьби з кіберзагрозами та реагування на

кіберінциденти, повідомили AZERTAC в Асоціації організацій кібербезпеки Азербайджану (AKTA).

Успішні ініціативи, реалізовані в Азербайджані в галузі цифрового розвитку та кібербезпеки, сприяли підвищенню позицій країни в світі за показниками, пов'язаними з кібербезпекою». ***(Azerbaijan ranks 12th in National Cyber Security Index // AZERTAC (https://azertag.az/en/xeber/azerbaijan_ranks_12th_in_national_cyber_security_index-2905912). 02.02.2024).***

***

«Група із захисту прав споживачів високо оцінила схвалення Президентом Філіппін Національного плану кібербезпеки на 2024-2029 роки на тлі зростання кількості кібератак, спрямованих на уряд і приватний сектор.

«Ми рішуче підтримуємо схвалення Президентом Національного плану кібербезпеки, оскільки він має вирішальне значення для розвитку процвітаючої цифрової економіки, яка стане ключовим рушієм сталого зростання та інклюзивного процвітання», — заявив співкерівник CitizenWatch Philippines і колишній законодавець Кіт Белмонте.

Секретар Департаменту інформаційно-комунікаційних технологій (DICT) Іван Уй нещодавно оголосив про схвалення комплексного п’ятирічного плану оперативного зміцнення захисту країни від кібератак.

Бельмонте зазначив, що нещодавні спроби кібератаки на веб-сайти уряду Філіппін, які були успішно припинені DICT, підсилюють терміновість оснащення всіх секторів, від інституційного до індивідуального рівня, навичками та технологіями кібербезпеки.

«Ландшафт кіберзлочинності та атак на національну державу постійно розвивається за допомогою креативної тактики обману, створюючи дедалі зростаючу загрозу. Це вимагає не менше ніж пильного та стратегічного підходу до зміцнення наших засобів кібербезпеки», – сказав Бельмонте.

Він додав, що всі державні установи повинні впроваджувати надійні заходи безпеки, щоб захистити не лише організацію, але й її зацікавлених сторін, які повинні взаємодіяти з їхніми системами, щоб скористатися державними послугами.

Він сказав, що приватні підприємства повинні захищати як свій бізнес, так і клієнтів від хакерів, які використовують їхні бренди для шахрайства.

«Для всіх споживачів і користувачів мережі наш обов'язок у боротьбі з ризиками кібербезпеки полягає в безпечній поведінці в Інтернеті, яка полягає у використанні надійних паролів, частому оновленні програмного забезпечення, обережному ставленні до підозрілих електронних листів і посилань і ретельному захисті особистої інформації, щоб допомогти підтримувати безпеку наших пристроїв, даних і облікових записів електронного банкінгу».

У звіті Globe Telecom зазначено, що 1,1 мільярда шахрайських і спам-повідомлень, які були заблоковані в першому кварталі 2023 року, продемонстрували приголомшливе зростання приблизно в п'ять разів порівняно з тим самим періодом 2022 року, «що підкреслює тривожну інтенсифікацію кібератак, з якими ми стикаємося.»

«Уряду слід поглибити співпрацю з приватними технологічними компаніями, щоб належним чином інтегрувати ці технології блокування шахрайства, а також стимулювати інвестиції в ініціативи з кібербезпеки», — сказав Белмонте». ***(National Cybersecurity Plan seen as vital defense for digital economy // Microsoft (https://www.msn.com/en-ph/news/national/national-cybersecurity-plan-seen-as-vital-defense-for-digital-economy/ar-BB1idRpu). 13.02.2024).***

***

«У минулому кібернебезпека та дезінформація не вважалися загрозами просто тому, що їх не існувало. Більш очевидними загрозами безпеці були фізичні загрози нашій територіальній обороні. Але завдяки зростаючому поширенню технологій і залежності суспільства від них, суспільства, як ніколи, вразливі до руйнівних і згубних наслідків порушень кібербезпеки та інших проблем, пов'язаних з технологіями.

Філіппіни особливо вразливі, враховуючи, що ми все ще перебуваємо на початковій стадії цифрової трансформації, і цифрова інфраструктура, і технологічні ноу-хау в кращому випадку нерівномірні в різних місцях архіпелагу. І установам, і окремим особам ще належить досягти технічної складності, яка б ефективно захищала їх від зловмисників, які прагнуть сіяти хаос у їхньому способі життя.

Президент Фердинанд Маркос молодший оголосив кібербезпеку пріоритетом через її вплив на національну та економічну безпеку. Це переконання підтверджено його схваленням 8 лютого Національного плану кібербезпеки на 2024-2029 роки.

Національний план кібербезпеки має на меті надати Філіппінам політичні напрямки та оперативні вказівки для нарощування потенціалу кібербезпеки. Під час розробки плану проводилися консультації з приватним сектором і науковцями, щоб переконатися, що він відображає занепокоєння всіх зацікавлених сторін і реалії на місці. Він також розглянув плани кібербезпеки інших країн, щоб гарантувати, що все, що є у Філіппін, відповідатиме міжнародним стандартам.

Зокрема, у плані розглядається необхідність розробки відповідної політики для зміцнення кіберландшафту Філіппін та визначення кіберактивів і критичної інфраструктури. Він включає розширену оцінку загроз для запобігання інцидентам, сприяє обміну інформацією з міжнародними партнерами, а також включає розвиток потенціалу та підвищення кваліфікації персоналу з кібербезпеки.

Департамент інформаційно-комунікаційних технологій (DICT) також проводить інформаційні кампанії для підвищення обізнаності громадськості про різні схеми, які використовують кіберзлочинці.

Але прагнення Філіппін до цифрової безпеки виходить за рамки схвалення Національного плану кібербезпеки. Наша країна завжди потребувала постійного зміцнення свого кіберзахисту під постійними атаками державних і недержавних суб’єктів.

Хорошим прикладом можуть бути минулорічні спроби передбачуваних китайських хакерів проникнути на веб-сайти кількох урядових установ, а саме DICT, National Coast Watch, Overseas Workers Welfare Administration, регіонального

офісу Департаменту освіти, Філіппінської берегової охорони та особистої сайт президента.

Крім того, є повторювані інциденти з боку агресивних і насильницьких осіб у Західно-Філіппінському морі. Ці актори стали зброєю в соціальних мережах своїми дезінформаційними наративами.

У відповідь на це Філіппіни почали використовувати наполегливу прозорість, щоб протистояти таким крокам. Це стратегія, яка посилює наративи, засновані на правових засадах і дослідженнях, що базуються на даних, і збирає підтримку людей, які знають про те, що відбувається там. Соціальні мережі відіграють вирішальну роль у цьому аспекті. Меседж, простий і зрозумілий, полягає в тому, що події на морі є значною мірою частиною національної історії, і кожен зацікавлений у цьому, тому що акти агресорів є приниженням нашого суверенітету.

Наративні кампанії визначають пріоритетність питань, і це призвело до того, що Філіппіни отримали масову підтримку з боку філіппінської громадськості, а також міжнародної спільноти щодо проблеми Західно-Філіппінського моря.

Прийняття плану кібербезпеки та застосування підходів до впевненої прозорості – це лише деякі дії, вжиті адміністрацією Філіппін для усунення потенційної шкоди, яку можуть завдати кібератаки. Але воно не повинно діяти самостійно. Нинішня адміністрація має прагнути використовувати нові технології для більш ефективної участі в сучасній глобальній цифровій економіці. Має бути впроваджено загальносуспільний підхід, головною метою якого є забезпечення національної безпеки з одночасним захистом економіки та людей.

Таким чином, Stratbase Institute наполягає на наступному:

Підвищення рівня освіти та обізнаності щодо кібербезпеки. Навчання людей є фундаментальною стратегією створення кіберзахищеного та кібербезпечного населення. Це особливо важливо, оскільки користувачі є найслабшою ланкою в усіх випадках використання Інтернету та інших кібер-дій.

Підвищення спроможності уряду протистояти ризикам кібербезпеки. Атаки на державні веб-сайти та бази даних викликають серйозне занепокоєння, оскільки ціллю стає конфіденційна особиста інформація людей. Має бути збільшена та

постійна бюджетна підтримка для закупівлі відповідних ІКТ-технологій, а також навчання державних службовців і персоналу ІКТ. Має бути покращена здатність виявляти, запобігати та реагувати на кіберризики та потенційні атаки.

Розширити національну безпеку. Національна безпека включає економічну безпеку, а також кібербезпеку. Тому політика та стратегії безпеки повинні включати вказівки щодо захисту країни від кіберзагроз. Це також включає оцінку кіберризиків, пов'язаних із морською безпекою, зокрема в Західному Філіппінському морі.

Зробіть акцент на кібердипломатії. Визнаючи спільні проблеми в цифровому просторі, Філіппіни повинні використовувати кібербезпеку для співпраці з державами-однодумцями. Це розширює її зовнішньополітичну стратегію та поглиблює дипломатичні відносини. Щоб зменшити вразливість, співпраця може передбачати обмін найкращими практиками кібербезпеки та інформацією.

Інститут сподівається на безпечну та процвітаючу цифрову економіку, яка може надати Філіппінам стратегічну та конкурентну перевагу в підтримці зростання за рахунок інвестицій. Ми впевнені, що адміністрація справді усвідомлює свої пріоритети, і кібербезпека по праву є одним із них». ***(Victor Andres C. Manhit. Cybersecurity is rightly a national priority // BusinessWorld Publishing (https://www.bworldonline.com/opinion/2024/02/21/576753/cybersecurity-is-rightly-a-national-priority/). 21.02.2024).***

***

«BHP (ASX: BHP) співпрацює з Anglo American, Antofagasta Minerals, Codelco та Collahuasi, щоб запустити Mining Cybersecurity Corporation у Чилі для боротьби з кіберзагрозами для гірничодобувної промисловості.

Протягом першої половини 2023 року в Чилі відбулося понад 4 мільярди кібератак, що позиціонує Чилі як п'яту країну Латинської Америки з найбільшою кількістю інцидентів, повідомляє BHP.

Безпрецедентний технологічний прогрес останніх років приносить важливі переваги, але також передбачає кілька ризиків для кібербезпеки.

Дослідження показують, що до 2025 року кібератаки коштуватимуть компаніям приблизно 10,5 мільярдів доларів.

Ця ініціатива, очолювана Corporación Alta Ley і підтримана Міністерством гірничої промисловості Чилі, спрямована на генерацію та обмін інформацією кіберрозвідки для раннього попередження та реагування, а також на сприяння культурі кібербезпеки при видобутку корисних копалин.

«Як BHP, ми з ентузіазмом ставимося до цієї ініціативи і, отже, хочемо внести свій внесок у захист активів і систем», — сказав у заяві Езекіель Фагетті, менеджер з кібербезпеки BHP Minerals Americas.

«Кібербезпека життєво важлива для належного функціонування різних виробничих систем і, зрештою, для того, щоб ми продовжували робити внесок у країну», — сказав він. «Якщо ми посилимо цей аспект, ми зміцнимо гірничодобувну галузь у цілому, її ланцюжок створення вартості та збережемо вигоди для всіх». ***(BHP partners with Chile miners to battle cybersecurity risks // Glacier Media Group (https://www.mining.com/bhp-partners-with-chile-miners-to-battle-cybersecurity-risks/). 13.02.2024).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Китайські державні кіберактори атакують інфраструктуру на військових базах в Азіатсько-Тихоокеанському регіоні, що належать Сполученим Штатам і їхнім союзникам, під час зростання хакерської діяльності, спрямованої на саботаж життєво важливих систем у разі конфлікту, повідомили Newsweek джерела в розвідці та кібербезпеці.

«Вони вторглися в комп'ютерні системи, і вони здатні диверсувати, наприклад, військові об'єкти на Гуамі або будь-які бази США в Південно-Східній Азії», – заявило джерело в західній розвідці в одній з країн НАТО на умовах анонімності через те, що чутливість питання.

За словами джерела з галузі кібербезпеки в регіоні, яке також залишилося анонімним через дуже делікатну природу питання, тривало «попереднє

позиціонування» Китаєм критичної онлайн-інфраструктури в Азіатсько-Тихоокеанському регіоні.

Говорячи військовою мовою, попереднє розміщення означає вигідне розміщення солдатів і обладнання, а в епоху цифрових технологій – вбудовування зловмисного програмного забезпечення в онлайн-мережі, що дозволяє швидко діяти під час кризи. За словами джерела, ця практика узгоджується зі стратегічними цілями Китаю, а саме диверсією та зривом сценарію конфлікту в Тихому океані.

Протягом останнього десятиліття Китай багато інвестував у свій військовий і кіберспроможність, кидаючи виклик США за лідерство в усіх сферах, включаючи економіку та технології, військову службу та глобальне управління — ціль, яку його лідер Сі Цзіньпін поставив до 2049 року на останній.

Найімовірніший військовий конфлікт між Китаєм і США – через Тайвань, на який Пекін стверджує, що він може захопити його силою. Іншою гарячою точкою є Південно-Китайське море, на яке також претендує Китай і яке сильно мілітаризувало, зокрема, будуючи острови. Близько півдюжини країн змагаються за право власності на території та морські зони в багатих енергією водах, а одна, Філіппіни, союзник США за договором, зазнає посиленого дипломатичного та військового тиску з боку Китаю через відмову погодитися». ***(China's Cyberattackers Target US and Allied Militaries // NEWSWEEK DIGITAL LLC (https://www.newsweek.com/chinas-cyberattackers-target-us-allied-militaries-1866837?utm_source=flipboard&utm_content=Newsweekdotcom%2Fmagazine%2FNewsweek). 05.02.2024).***

***

«За даними Білого дому, серію хакерів, спрямованих на водоочисні споруди в США, відстежили шість членів іранського урядового підрозділу кібервійни.

У п’ятницю Міністерство фінансів США виявило та наклало санкції на шістьох іранців, які здійснили хакерські атаки в листопаді минулого року, які включали викрадення ІТ-систем постачальника води в Аліквіппі, штат Пенсільванія.

За даними США, усі шестеро іранців працюють на кіберелектронне командування Корпусу вартових Ісламської революції, яке раніше було пов’язане з атаками програм-вимагачів. Серед ідентифікованих осіб є Хамід Реза Лашгарян, який, за словами США, очолює підрозділ кібервійни.

Хакерська діяльність групи потрапила в заголовки газет у листопаді, коли муніципальне управління водного господарства Аліквіппи повідомило про злом, який зіпсував комп’ютерну систему з повідомленням: «Вас зламали. Геть Ізраїль. Кожне обладнання «Зроблено в Ізраїлі» є законною метою Cyber Av3ngers».

Щоб здійснити злом, група націлилася на вразливі логічні контролери ізраїльської компанії Unitronics. Згодом кібервлада США пов’язала хакерську групу CyberAv3ngers з Корпусом вартових ісламської революції Ірану (IRGC).

«Принаймні з 22 листопада 2023 року ці кіберактори, афілійовані з IRGC, продовжували компрометувати облікові дані за замовчуванням у пристроях Unitronics», — заявило в грудні Агентство з кібербезпеки та безпеки інфраструктури США. «Жертви охоплюють кілька штатів США».

У п’ятничному повідомленні Міністерства фінансів додається, що іранські хакери також атакували об’єкти водопостачання за межами США, хоча це не призвело до збоїв у критичних службах водопостачання. Тим не менш, США завдають удару у відповідь, накладаючи санкції на ймовірно причетних осіб.

«Сполучені Штати не потерплять таких дій і використовуватимуть увесь спектр наших інструментів і органів влади, щоб притягнути винних до відповідальності», — заявив заступник міністра фінансів з питань тероризму та фінансової розвідки Браян Нельсон.

Оскільки США не мають договору про екстрадицію з Іраном для притягнення підозрюваних до суду, Міністерство фінансів вдається до санкцій. Це означає, що всім американським особам і компаніям заборонено здійснювати операції з шістьма іранцями та їхніми афілійованими групами. Міністерство фінансів не уточнило, як воно відстежило зломи осіб. Але ФБР і АНБ були серед федеральних агентств, які розслідували зломи». ***(Michael Kan. US Identifies and Sanctions Iranians Behind Water Facility Hacks // Ziff Davis, LLC. (https://www.pcmag.com/news/us-identifies-***

and-sanctions-iranians-behind-water-facility-hacks?utm_source=flipboard&utm_content=user%2FPCMag). 02.02.2024).

***

«Державні хакери, пов'язані з Китаєм, здійснили широкомасштабну ботнет-атаку на малі офісні та домашні маршрутизатори в США, заявив у середу, 31 січня, директор Федерального бюро розслідувань США Крістофер Рей (Christopher Wray). Більшість постраждалих маршрутизаторів були вироблені компаніями Cisco і NetGear і мали вичерпаний термін експлуатації.

31 січня 2024 року слідчі Міністерства юстиції повідомили, що зловмисне програмне забезпечення було видалено з уражених маршрутизаторів. Слідчі також відключили маршрутизатори від інших пристроїв, які використовуються в ботнеті.

IT-командам потрібно знати, як зменшити ризики кібербезпеки, які можуть виникнути через використання застарілих технологій віддаленими працівниками.

Що таке ботнет-атака Volt Typhoon?

Загрозою кібербезпеці в цьому випадку є ботнет, створений Volt Typhoon, групою зловмисників, спонсорованих китайським урядом.

Починаючи з травня 2023 року, ФБР розслідувало кампанію кібератак на організації критичної інфраструктури. 31 січня 2024 року ФБР виявило, що розслідування тієї ж групи загрозливих осіб у грудні 2023 року показало, що зловмисники, спонсоровані урядом Китаю, створили ботнет, використовуючи сотні приватних маршрутизаторів у США.

Атака була спробою проникнути в «комунікаційний, енергетичний, транспортний і водний сектори», щоб порушити критичні функції США в разі конфлікту між країнами, сказав Рей у прес-релізі.

Зловмисники використовували техніку «життя за рахунок землі», щоб інтегруватись із нормальною роботою заражених пристроїв.

ФБР зв’язується з усіма, чиє обладнання постраждало від цієї конкретної атаки. Не підтверджено, чи були ціллю співробітники конкретної організації.

Як зменшити ризики кібербезпеки від ботнетів для віддалених працівників

Той факт, що цільові маршрутизатори є приватною власністю, підкреслює ризик безпеки для IT-спеціалістів, які намагаються забезпечити безпеку віддалених працівників. Оскільки працівники IT-спеціалістів не контролюють маршрутизатори, які використовуються вдома, важко знати, чи можуть роботодавці використовувати старі або навіть вичерпані маршрутизатори.

Ботнети часто використовуються для запуску розподілених атак на відмову в обслуговуванні або розповсюдження зловмисного програмного забезпечення, тому захист від них є важливими компонентами повного захисту від ботнетів. Бот-мережі, як правило, очолюються централізованим командним і контрольним сервером.

Організації повинні забезпечити надійний захист кінцевих точок і проактивний захист, наприклад:

- інформація про безпеку та рішення для управління подіями;
- оркестровка безпеки, автоматизація та рішення реагування (з генеративними компонентами ШІ або без них), а також;
- політики кібербезпеки для віддалених співробітників.

Програмне та апаратне забезпечення слід постійно оновлювати, оскільки пристрої, що вийшли з експлуатації, є особливо вразливими. Щоб захистити пристрої від використання під час атак ботнетів, проводите регулярне сканування безпеки, запровадьте багатофакторну автентифікацію та інформуйте співробітників про найкращі практики кібербезпеки.

«Профілактичне проведення ретельної технічної інвентаризації активів за межами традиційного офісу має важливе значення», — сказав Демі Бен-Арі, головний технічний директор сторонньої фірми з управління ризиками Panorays, в електронному листі до TechRepublic. «Цей підхід допомагає виявити застарілу технологію, гарантуючи, що віддалені працівники мають сучасне та безпечне обладнання».

«Хоча віддалена робота створює потенційну вразливість через різноманітне середовище, важливо зазначити, що подібні атаки можуть відбуватися в офісі», —

сказав Бен-Арі». ***(Megan Crouse. Botnet Attack Targeted Routers: A Wake-Up Call for Securing Remote Employees' Hardware // TechnologyAdvice (https://www.techrepublic.com/article/volt-typhoon-botnet-attack/?utm_source=flipboard&utm_content=TechRepublic%2Fmagazine%2FLatest+News).02.02.2024).***

***

«Успішні кібератаки Китаю на критично важливу інфраструктуру на Гуамі або в інших індо-тихоокеанських плацдармах можуть підірвати військовий потенціал США в регіоні, заявив лідер Агентства національної безпеки та Кіберкомандування США.

Гуам є ключовим форпостом американських військ у зоні дедалі більшої конкуренції, де, на думку Вашингтона, може спалахнути боротьба з Пекіном. Острів служить центром логістики та боєприпасів, а також вузлом розвідки, спостереження та розвідки.

Напад на мережі та інформаційні технології, які забезпечують розподіл електроенергії, води, продовольства та реагування на надзвичайні ситуації на Гуамі, можуть «мати дуже значний вплив» на варіанти, доступні військовим командуванням у той час, сказав генерал Пол Накасоне.

«Зв'язок, здатність використовувати наші найбільш смертоносні системи зброї — це всі сфери, на які ми б покладалися», — сказав він під час слухань 31 січня, проведених Спеціальним комітетом Палати представників Комуністичної партії Китаю. «Ми повинні діяти щодня, ми повинні бути пильними, у нас повинні бути наступальні та оборонні можливості».

Альянс з обміну розвідувальними даними Five Eyes, що складається з Австралії, Канади, Нової Зеландії, Великобританії та США, у травні попередив, що китайська шпигунська група проскочила цифровий захист на Гуамі та в інших місцях. Microsoft виявила вторгнення та приписала його групі, відомій як Volt Typhoon.

Офіційні особи США вже давно вважають Китай серйозною кібернебезпекою, а Міжнародний інститут стратегічних досліджень поставив його

на друге місце в рейтингу кібернетичних центрів разом із Росією. Кіберстратегія Пентагону до 2023 року попереджає, що Пекін готовий здійснити кібератаки на критично важливу інфраструктуру та оборонні мережі, якщо почнеться війна.

Така тактика має на меті розпалювати плутанину, відволікати дорогоцінні ресурси та перешкоджати військовій мобілізації.

У середу Накасоне сказав, що коли хакерів буде виявлено, що ховаються навколо критичної інфраструктури, «перше, що нам потрібно зробити, це переконатися, що ми виведемо їх». Як керівник CYBERCOM і АНБ, генерал тісно контактує з Агентством з кібербезпеки та безпеки інфраструктури, яке входить до компетенції Департаменту внутрішньої безпеки, серед інших гравців.

«Нам потрібна пильність, яка продовжується», — сказав Накасоне. «Це не епізодична загроза, з якою ми зіткнемося. Це наполегливо».

Конгресмен Майк Галлахер, голова комітету, сказав журналістам перед слуханнями, що він бачив повідомлення про те, що Китай переключає частину своєї уваги з традиційного економічного шпигунства на критичну інфраструктуру.

За словами республіканця з Вісконсіна, цей крок свідчить про прагнення до саботажу, оскільки «немає економічної цінності в попередньому позиціонуванні нафто- та газопроводів чи водопровідних компаній — немає жодної інтелектуальної власності, яку можна красти». ***(Colin Demarest. Cyberattacks on Guam could sap US forces in Indo-Pacific, Nakasone says // Defense News (https://www.defensenews.com/cyber/2024/01/31/cyberattacks-on-guam-could-sap-us-forces-in-indo-pacific-nakasone-says/?utm_source=flipboard&utm_content=waral01%2Fmagazine%2FRumors+Of+War). 01.02.2024).***

***

«Хакери, що діють у Китаї, намагалися зламати веб-сайти та системи електронної пошти президента та урядових установ Філіппін, один із яких сприяє безпеці на морі, але невдало, повідомив у понеділок чиновник міністерства інформації та зв'язку.

Поштові скриньки Департаменту інформаційних і комунікаційних технологій (DICT), веб-сайт National Coast Watch і особистий веб-сайт президента Філіппін Фердинанда Маркоса-молодшого були одними з цілей невдалих хакерських операцій у січні, повідомив представник DICT Ренато Параїсо радіо DWPM.

«Ми не приписуємо це жодній державі. Але, використовуючи адреси інтернет-протоколу, ми визначили це в Китаї», — сказав Параіco, додавши, що хакери використовували послуги китайської державної Unicom.

«Ми звертаємося до китайського уряду з проханням допомогти нам запобігти подальшим атакам».

Unicom і посольство Китаю в Манілі не відразу відповіли на запит про коментар.

Зірвані кібератаки відбулися в період загострення напруженості у відносинах з Китаєм, в основному через спірну територію в Південно-Китайському морі.

Зараз Філіппіни працюють над п’ятирічною стратегією кібербезпеки, щоб посилити свій кіберзахист для боротьби з атаками та цифровими злочинами. Його військові минулого року оголосили про створення кіберкомандування». ***(Philippines Wards off Cyber Attacks From China-Based Hackers // U.S. News & World Report L.P. (https://www.usnews.com/news/world/articles/2024-02-05/philippines-wards-off-cyber-attacks-from-china-based-hackers?utm_source=flipboard&utm_content=seanjkernan%2Fmagazine%2FUS+News). 05.02.2024).***

***

«Міністр закордонних справ Японії закликав до термінових дій для зміцнення національної кібербезпеки після попереджень з Вашингтона про те, що слабка оборона Токіо дає Пекіну доступ до конфіденційних дипломатичних комунікацій, проблема, яка ризикує підірвати довіру з союзниками, які більше не можуть довіряти уряду Японії свої секрети.

Виступаючи на слуханнях у бюджетному комітеті парламенту в четвер, міністр закордонних справ Йоко Камікава визнала, що тривала проблема

кібербезпеки загрожує відносинам з іншими країнами через стурбованість тим, що конфіденційні дані можуть потрапити до рук Китаю.

«Інформаційна безпека є надзвичайно важливою основою для сприяння обміну інформацією та зміцнення співпраці зі Сполученими Штатами та іншими відповідними країнами», — цитує газета Yomiuri слова Камікава комітету парламенту.

У вас є запитання про найпопулярніші теми та тенденції з усього світу? Отримайте відповіді за допомогою SCMP Knowledge, нашої нової платформи підібраного вмісту з поясненнями, поширеними запитаннями, аналізом та інфографікою, наданими нашою нагородженою командою.

«Розширення наших можливостей щодо вирішення проблем кібербезпеки є дуже серйозним питанням», — додала вона.

Японію вперше попередили про злам у її дипломатичних телеграмах влітку 2020 року, коли офіційних осіб проінформував про це генерал Пол Накасоне з Агентства національної безпеки США (АНБ).

Уряд США попередив Токіо про те, що китайські хакери зламали комп’ютерні мережі, що зв’язують урядові міністерства та дипломатичні представництва за кордоном. Японія, очевидно, не знала про порушення, поки не повідомила про це США, які відмовилися надати інформацію про те, як вони дізналися про атаки.

Той факт, що голова АНБ відвідав Токіо в 2020 році, щоб повідомити про занепокоєння Вашингтона, підкреслив масштаб проблеми, кажуть експерти, а також тривогу, що конфіденційні дані, якими США діляться з Японією, витікають до Китаю.

Пізніше Токіо погодився усунути вразливості в своїх комп’ютерних комунікаціях у п’яти критично важливих урядових установах: міністерстві закордонних справ і оборони, Національному поліцейському агенстві, Розвідувальному агенстві громадської безпеки та Управлінні розвідки та досліджень кабінету міністрів.

Уряд Японії залишався мовчазним щодо заходів, які він запровадив для боротьби з кібератаками, які могли походити з Росії та Північної Кореї, а також Китаю, але коментарі Камікава вказують на те, що проблему не вирішено.

США повідомили про покращення, хоча Yomiuri цитує американського чиновника, який сказав, що заходи Японії були «занадто малими, занадто пізніми».

«Це не нова проблема, вона триває вже кілька років, і очевидно, що Японія відстає в кібербезпеці, де вона повинна бути», — сказав Ріо Хіната-Ямагуті, доцент кафедри міжнародних відносин Університету США. Токіо.

«І це виходить за рамки компромісу у спілкуванні з союзниками з питань оборони та наших дипломатичних послань», — сказав він. «Японія повинна подумати про те, як це тягне країну вниз разом із її союзниками, оскільки цим країнам буде незручно ділитися конфіденційними даними з Японією, якщо вони думають, що вони будуть скомпрометовані».

Під час обговорень у парламенті 1 лютого прем'єр-міністр Фуміо Кісіда заявив, що має намір «пришвидшити обговорення для якнайшвидшого ухвалення відповідних законопроектів», щоб дозволити владі Японії запровадити таку активну позицію кіберзахисту, як США, Великобританія. та інші народи вже прийняли.

Однак він визнав, що пункт у конституції Японії, який гарантує «таємність будь-яких засобів зв'язку», стане перешкодою для нового законодавства. У будь-якому новому законі має бути вирішено питання про те, як можна отримати електронні записи, а також діапазон інформації, яка охоплюється в запиті на доступ. Для цього потрібно буде внести зміни до низки законів.

«Прем'єр-міністр і міністр закордонних справ закликають до вирішення, і ніхто не заперечує, що існує проблема, яку необхідно терміново вирішити, але ми також повинні усвідомлювати, що може бути важко встигати за мінливими загрозами, які представляють кібератаки та їх підвищення витонченості», - сказала Хіната-Ямагуті.

«І це проблема, тому що Японія дуже хоче бути частиною альянсу «П'яти очей» з обміну розвідувальними даними та мати тісніші зв'язки зі США та НАТО,

але це буде важко, оскільки існує страх, що будь-яка розвідка спільні з Японією можуть швидко бути скомпрометовані», – додав він». ***(Julian Ryall. Japan risks losing trust of US, other allies over its 'serious' cybersecurity flaws, minister warns // Microsoft (https://www.msn.com/en-xl/news/other/japan-risks-losing-trust-of-us-other-allies-over-its-serious-cybersecurity-flaws-minister-warns/ar-BB1i9veW). 12.02.2024).***

***

«У п'ятницю газета South China Morning Post підкреслила, що найбільше занепокоєння Китаю в кібербезпеці походить не від США, його суперника у глобальному впливі, а від Індії. Минулого року ми стали свідками значної кібератаки на китайську армію, яку, ймовірно, організувала індійська група хакерів.

Згідно зі звітом SCMP, китайські охоронні фірми виявили, що було сім інцидентів, пов'язаних з індійською хакерською групою «Bitter» у 2022 році та вісім у 2023 році, націленими на Китай, Пакистан і Монголію. «Незважаючи на поширену думку про те, що кіберзагрози проти Китаю в основному походять із США, значна кількість атак виникла з країн Південної Азії», — сказав експерт з безпеки в Пекіні, який вважав за краще залишитися анонімним для SCMP.

Підозрюється, що кібернапад, заблокований китайською владою проти військових у грудні, був організований Біттером. Ця група, також відома як «Manlinghua», діє з листопада 2013 року. Кібераналітики приписують атаки Індії на основі адрес Інтернет-протоколу (IP) і лінгвістичних моделей, пов'язаних з «Bitter». Група має досвід нападів на урядові та військові організації, а також на ядерну сферу в Пакистані та Китаї, нібито за підтримки уряду Індії. Їхня тактика проникнення варіюється від видавання за посольство Киргизії до розгортання фішингових електронних листів, націлених на китайську атомну промисловість.

Група хакерів переважно використовує дві стратегії: «фішинг», який зосереджується на приватних особах для крадіжки конфіденційних даних, і атаки «водяні ями», коли шкідливий код впроваджується на веб-сайти. Хоча ці атаки можуть не виглядати відверто руйнівними, експерти попереджають, що вони можуть призвести до значних витоків інформації.

Незважаючи на постійні кібератаки, які, як вважають, походять з Індії, китайська влада ще не дала офіційної відповіді. Подібним чином, у листопаді минулого року, коли в Індії з'явилася критика щодо ескалації китайських кібератак, індійська влада також уникала прямої назви Китаю. Після кривавого зіткнення вздовж гімалайського кордону в 2020 році Китай та Індія, дві найбільш густонаселені країни світу, продовжують боротися з триваючою напругою. Однак економічно вони підтримували складні відносини, розширюючи торгівлю та взаємодію». ***(SCMP: The biggest cyber security threat for China is India // dongA.com (https://www.donga.com/en/List/article/all/20240219/4756741/1). 19.02.2024).***

***

«Великий витік даних із китайської фірми з кібербезпеки виявив, що агенти державної безпеки платять десятки тисяч фунтів стерлінгів за збір даних про цілі, включно з іноземними урядами, у той час як хакери збирають величезні обсяги інформації про будь-яку особу чи установу, які можуть бути цікаві для їхні потенційні клієнти.

Кеш із понад 500 витоку файлів від китайської фірми I-Soon був опублікований на веб-сайті розробників Github, і експерти з кібербезпеки вважають його справжнім. Деякі з обговорюваних цілей включають НАТО та МЗС Великобританії.

Витік дає безпрецедентне уявлення про світ найнятих хакерів у Китаї, який глава служб безпеки Великобританії назвав «масштабним» викликом для країни.

Файли, які є сумішшю журналів чатів, проспектів компаній і зразків даних, розкривають масштаби операцій зі збору розвідданих у Китаї, а також висвітлюють тиск ринку, який відчувають комерційні хакери країни, коли вони змагаються за бізнес в економіці, що бореться.

Схоже, що I-Soon працював з іншою китайською хакерською організацією Chengdu 404, а пізніше був втягнутий у комерційну суперечку з нею, хакерам якої Міністерство юстиції США висунуло звинувачення в кібератаках на компанії в США, а також продемократичних активістів у Гонконзі, серед інших цілей.

Інші об’єкти, про які йдеться в витоках I-Soon, включають британський мозковий центр Chatham House, управління охорони здоров’я та міністерства закордонних справ країн АСЕАН. Деякі з цих даних, здається, були зібрані за специфікацією, тоді як в інших випадках існують спеціальні контракти з китайським бюро громадської безпеки для збору певного типу даних.

Представник Chatham House сказав: «Ми усвідомлюємо, що ці дані надходять у світло, і, природно, стурбовані. Chatham House надзвичайно серйозно ставиться до безпеки даних та інформації. У нинішньому кліматі ми, разом з багатьма іншими організаціями, стаємо об’єктом регулярних спроб атак як з боку державних, так і недержавних суб’єктів.

«У нас є заходи захисту, включаючи захисні засоби на основі технологій, які регулярно переглядаються та оновлюються».

Офіційний представник НАТО сказав: «Альянс стикається з постійними кіберзагрозами і підготувався до цього, інвестувавши в розширений кіберзахист. НАТО розглядає кожну заяву про кіберзагрози».

Міністерство закордонних справ Великої Британії відмовилося від коментарів.

Послуги, які пропонує I-Soon, різноманітні. В одному прикладі бюро громадської безпеки міста Шаньдун заплатило майже 44 000 фунтів стерлінгів, щоб отримати доступ до електронних скриньок 10 цілей протягом одного року.

Компанія стверджувала, що може зламувати облікові записи на X, отримувати особисту інформацію з Facebook, отримувати дані з внутрішніх баз даних і скомпрометувати різні операційні системи, включаючи Mac і Android.

В одному з файлів є скріншот папки під назвою «Записки секретаріату з європейських справ Північної Македонії». Інший скріншот показує файли, які, схоже, стосуються ЄС, включно з файлом під назвою «Проект позиції ЄС щодо COP 15, частина 2». Назви файлів посилаються на систему шифрування, яку використовують органи ЄС для захисту офіційних даних.

У деяких випадках незрозуміло, якою була мета збору даних. «Китайська держава фактично збирає стільки даних, скільки може», — сказав Алан Вудворд,

експерт з комп’ютерної безпеки з Університету Суррея. «Вони просто хочуть якомога більше інформації на випадок, якщо вона виявиться корисною».

Вудворд зазначив, що на відміну від російських державних хакерів, які здійснюють атаки програм-вимагачів або інші руйнівні дії, китайські спроби, як правило, зосереджені на масовому зборі даних. «Дещо з цього можна інтерпретувати як закладення основи для того, щоб бути руйнівним на наступному етапі», — сказав Вудворд.

Минулого року в звіті парламентського комітету з розвідки та безпеки щодо Китаю говорилося : «кіберекспертиза Китаю дозволяє йому націлюватися на різноманітні організації та набори даних — і все більш незвичайні». Експерти вважають, що метою збору даних може бути виявлення потенційних цілей для операцій людської розвідки.

I-Soon також був націлений на домашніх жертв. У недатованій угоді про співпрацю з місцевою владою в Сіньцзяні компанія I-Soon заявила, що може надати «антитерористичну» підтримку місцевій поліції у стеженні за уйгурами. I-Soon сказав, що має більш ніж десятирічний досвід доступу до «різних дозволів сервера та інтрамережі в багатьох країнах».

Компанія стверджувала, що отримала дані від антитерористичних органів Пакистану та поштової служби Пакистану. Посольство Пакистану в Лондоні не відповіло на запит про коментар.

Деякі з обіцянок клієнтам могли бути афішуванням продажів. Під час однієї дискусії один співробітник запитав: «Клієнти обманюють нас, чи ми обманюємо клієнтів?» Працівник продовжує, що обман клієнтів щодо можливостей компанії – це «нормально, але компанії недобре обманювати своїх працівників».

Мей Дановскі, китайський експерт з кібербезпеки та автор інформаційного бюлетеня Natto Thoughts, сказав: «Ми думаємо про [китайських хакерів] так: «О, держава дає їм гроші, щоб робити щось». Насправді, якщо ці витоку документів правдиві, це не так. Вони повинні йти і шукати бізнес. Вони повинні створити репутацію».

Інші журнали чату були вражаюче буденними. Співробітники обговорили Covid-19 і фінансовий тиск на I-Soon. «Спочатку всі знали, що компанія переживає важкі часи, і всі розуміли. Зрештою, епідемія така серйозна», – написав один працівник у березні 2021 року. Але, скаржилися вони, I-Soon «не сказав, що не будуть платити нам зарплату».

Наступного року тиск на компанію, здавалося, посилився. Виконавчий директор Ву Хайбо, який використовує псевдонім Shutd0wn, сказав, що втрата основного персоналу підірвала довіру клієнтів, що призвело до втрати бізнесу. Ву не відповів на запит про коментар.

«Начальник справді стурбований, — написав один із співробітників у вересні 2022 року. — Я не знаю, чи зможе компанія вижити до кінця року». В іншому чаті працівники розповідали про погані продажі компанії та поганий настрій в офісі. Один працівник звернувся до універсальної розради: «Я, ймовірно, буду кричати, якщо не зможу випити». ***(Amy Hawkins. Huge cybersecurity leak lifts lid on world of China's hackers for hire // Guardian News & Media Limited (https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire). 23.02.2024).***

***

«…3 лютого в соцмережі X була оприлюднена інформація, ніби група проросійських хакерів Just Evil зламала військові системи США та країн Балтії, зокрема Литви. У дописі йшлося про злам системи ILIAS литовської армії.

Представники литовської армії підтвердили порталу LRT, що 3 лютого дійсно було зафіксовано підозріле підключення до облікового запису користувача інформаційної системи дистанційного навчання збройних сил Литви ILIAS. «З цієї причини було відключено три сервери Ключового державного телекомунікаційного центру (KVTC), на яких розміщено навчальну систему ILIAS. Національний центр кібербезпеки (NKSC) в активній співпраці з литовською армією розпочав розслідування, наразі інцидент віднесено до середньої категорії кіберінцидентів», - сказали представники армії.

Згідно з наявною інформацією, витоку даних не було, але це має підтвердити слідство. «Інформаційна система дистанційного навчання ILIAS все ще відключена від зовнішньої мережі та зараз оновлюється», – повідомили в литовській армії». ***(Російські хакери намагалися увійти в е-системи литовської армії // Укрінформ (https://www.ukrinform.ua/rubric-technology/3826585-rosijski-hakeri-namagalisa-uvijti-v-esistemi-litovskoi-armii.html). 13.02.2024).***

***

«Хакерська група Head Mare зламала мережі російської компанії, яка входить у холдинг «Калашников». Про це хакери повідомили в соцмережі Twitter (X).

«Head Mare прийшла в гості до НПО «Высокоточные системы и технологии» з міста Іжевськ», – йдеться в повідомленні.

Злиті в мережу матеріали доступні для скачування...

Крім того, кібери виклали в доступ тренінги для мотивації співробітників фірми та інформацію про рахунки компанії.

Зазначимо, що закрите акціонерне товариство «НПО Высокоточные системы и технологии» («ВТС») розташоване в російському місті Іжевськ. Спеціалізація компанії – високоточні снаряди та стрілецька зброя. За повідомленнями у ЗМІ, у 2016 році підприємство стало частиною концерну «Калашников»…» ***(Єлизавета Жабська. Хакери виклали в мережу документацію підприємства РФ, що виробляє ракети // Українські медійні системи (https://glavcom.ua/world/observe/khakeri-viklali-v-merezhu-dokumentatsiju-pidprijemstva-rf-shcho-virobljaje-raketi-986463.html). 17.02.2024).***

***

«Нещодавно Сполучені Штати Америки (США) здійснили кібератаку на військовий корабель Ірану у Червоному морі та Аденській затоці, який збирав розвідувальні дані про вантажні судна.

Про це повідомляє РБК-Україна з посиланням на NBC News.

Як розповіли журналістам троє американських чиновники, кібератака сталася тиждень тому в рамках відповіді Вашингтона на атаку безпілотників бойовиків в Іраку, яких підтримує Іран, в результаті чого наприкінці минулого місяця в Йорданії загинули троє військовослужбовців США і були десятки поранених.

У публікації зазначається, що операція мала на меті перешкодити здатності корабля ділитися розвідданими з єменськими хуситами, які вже тривалий час атакують комерційні судна у Червоному морі та Аденській затоці.

У статті також йдеться про те, що Рада національної безпеки Білого дому не відразу відповіла на прохання прокоментувати відповідне повідомлення.

Атака на військову базу в Йорданії та відповідь США

Нагадаємо, 28 січня американську військову базу «Вежа 22» в Йорданії атакували дрони. За даними Пентагону, внаслідок цієї атаки троє військових загинули, поранень зазнали понад 40 американських солдатів.

В Міноборони США зазначили, що до нападу причетне угруповання «Катаїб Хезболла», яке підтримує Іран.

Ввечері 2 лютого військові США завдали ударів по більш ніж 85 цілях в Іраку та Сирії. Удари тривали близько 30 хвилин та були спрямовані на три об'єкти в Іраку і чотири в Сирії.

Президент США Джо Байден заявив про початок військової операції на Близькому Сході у відповідь на атаку проти бази в Йорданії.

Операція США через атаки хуситів на кораблі у Червоному морі

З листопада минулого року у Червоному морі продовжуються атаки єменських хуситів на торгові судна, які мають зв'язок з Ізраїлем. У січні терористичне угруповання завдало найбільшого удару. Військові США та Британії відбили атаку у Червоному морі.

На початку січня США та Британія завдали потужних ударів по цілям, пов'язаним з хуситами в Ємені. Це стало відповіддю на постійні атаки хуситів на цивільні судна у Червоному морі.

28 січня повідомлялося, що в Червоному морі безпілотник хусітів атакував британський військовий корабель, а вже наступного дня єменські хусіти

повідомили, що вони нібито атакували американський есмінець. Однак у Пентагоні спростували заяву бойовиків.

Перед цим 6 лютого повідомлялося, що британське вантажне судно зазнало нападу хуситів у Червоному морі. А 7 лютого з території Ємену хусити запустили 6 протикорабельних балістичних ракет у напрямку двох комерційних суден в південній частині Червоного моря та Аденської затоки. Вони не завдали шкоди для суден, а одна з ракет була перехоплена та збита військовими США.

Через два дні американські військові завдали серії ударів по крилатих ракетах та надводних безпілотниках хуситів у Ємені.

Додамо, раніше повідомлялося, що берегова охорона США перехопила партію зброї з Ірану, яка прямувала до повстанців-хуситів в Ємені». ***(Володимир Костирін. США здійснили кібератаку на іранський військовий корабель, - NBC News // ТОВ «УБТ» (https://www.rbc.ua/rus/news/ssha-zdiysnili-kiberataku-iranskiy-viyskoviy-1708032002.html). 15.02.2024).***

***

«Фахівці з аналітичної компанії Recorded Future розповіли про нову кібершпигунську кампанію угруповання TA473, яка спрямована на більш ніж 80 організацій, переважно розташованих в Україні, Грузії та Польщі.

Під час кампанії кіберзлочинці збирають розвіддані про політичні та бойові дії в Європі. Атаки, що відбувалися з початку до середини жовтня 2023 року, доповнюють інші операції TA473 проти поштових серверів уряду Узбекистану, які булши виявлені в березні 2023 року.

Зловмисники використовували складні методи атаки, поєднуючи соціальну інженерію з експлуатацією вразливостей (зокрема, XSS-вразливостей) у серверах Roundcube Webmail для несанкціонованого доступу до поштових серверів жертв. Як наслідок — через спеціально розроблені корисні навантаження на основі JavaScript, відбувалася крадіжка облікових даних користувачів.

Також було зафіксовано спроби TA473 атакувати іранські посольства у Нідерландах і грузинське посольство у Швеції, що вказує на ширший геополітичний інтерес, зокрема, до політичної активності Ірану, а також до

прагнення Грузії вступити до Євросоюзу і НАТО…». ***(Фахівці з кібербезпеки розкрили хакерську мережу, яка шпигувала за Україною та державами-членами НАТО // No worries! (https://noworries.news/fahivczi-z-kiberbezpeky-rozkryly-hakersku-merezhu-yaka-shpyguvala-za-ukrayinoyu-ta-derzhavamy-chlenamy-nato/#). 21.02.2024).***

***

Створення та функціонування кібервійськ

«Литва бере на себе головування в Раді сил кібершвидкого реагування ЄС (CRRT), повідомило в середу міністерство оборони.

«Цього року, коли Литва очолює Раду CRRT, Литва підготувала амбітний оперативний план для сил, який включає різні варіанти активації, навчання, навчання технічних експертів тощо. Крім того, ми сподіваємося залучити кілька нових держав-членів до проекту в 2024 році», – сказала віце-міністр оборони Грета Моніка Тучкуте на засіданні ради у вівторок. «Литва продовжуватиме активні зусилля для підвищення рівня готовності та навичок CRRT».

Команда CRRT досягла повної оперативної спроможності у 2021 році та готова реагувати на кіберінциденти, а також підвищувати стійкість ЄС та партнерів.

Литва вдруге взяла на себе головування в Раді CRRT, причому дев'ять країн CRRT посідають голову в раді на ротаційній основі.

Зараз команда CRRT складається з 16–18 експертів з кібербезпеки з Бельгії, Данії, Хорватії, Естонії, Естонії, Литви, Нідерландів, Польщі, Румунії та Словенії.

Ще чотири країни зацікавлені приєднатися до проекту.

Команда CRRT, заснована в 2018 році в рамках Постійної структурованої співпраці ЄС (PESCO), може запропонувати допомогу в управлінні або запобіганні кіберінцидентам.

В останні роки спроможність CRRT була перевірена під час надання підтримки країнам-партнерам ЄС, таким як Україна та Молдова, а також під час військової навчальної місії ЄС у Мозамбіку». ***(Lithuania takes over chairmanship of***

EU's cyber security force // Lietuvos nacionalinis radijas ir televizija (https://www.lrt.lt/en/news-in-english/19/2200650/lithuania-takes-over-chairmanship-of-eu-s-cyber-security-force). 21.02.2024).

***

Кіберзахист критичної інфраструктури

«З приходом цифрової ери супутники стали незамінними стовпами нашого сучасного світу, які організовують навігацію, зв'язок і торгівлю. Але ці безтурботні небесні вартові стикаються з прихованою загрозою: кібератаками. Якщо їх не зупинити, зловмисне вторгнення може занурити наш взаємопов'язаний світ у хаос, поставивши під загрозу нашу безпеку та процвітання.

З моменту запуску супутника Sputnik у 1957 році супутники перетворилися на складні багатоцільові платформи, які відіграють важливу роль у глобальному зв'язку та безпеці. Сьогодні супутники відіграють важливу роль не лише в повсякденних зручностях, таких як система глобального позиціонування (GPS) і доступ до Інтернету, але й у міжнародних оборонних системах і глобальному моніторингу навколишнього середовища. Це робить їх основними цілями для кібератак.

Недавні кіберінциденти, такі як атака на мережу Viasat KA-SAT у 2022 році, яскраво нагадують про зростаючу вразливість нашої супутникової інфраструктури. Цей руйнівний напад, який перервав доступ до Інтернету тисячам людей по всій Європі, підкреслив стратегічне значення супутників як критичних цілей для кіберсупротивників. Ці події не є поодинокими; вони відзначають ескалаційну тенденцію, оскільки досвідчені кіберактори все більше визнають потенціал для руйнівних збоїв через супутникові атаки.

Нам потрібна негайна посилена супутникова кібербезпека — не як віддалене прагнення, а як терміновий імператив прямо зараз. Це не заклик до нечіткого майбутнього планування, а вимога до рішучих дій зараз, щоб запобігти надто

ймовірному сценарію, коли критично важливі служби будуть непрацездатними з далекосяжними та руйнівними наслідками.

Атака Viasat KA-SAT у 2022 році, яку приписують російським державним акторам, подолала протоколи зв’язку супутника. Це призвело до масових збоїв у роботі Інтернету та збоїв у роботі послуг дистанційного зондування в Україні та інших частинах Європи, що вплинуло на понад 9000 абонентів у Франції та приблизно 13 000 абонентів в інших європейських країнах, а також призвело до того, що велика німецька енергетична компанія втратила віддалений доступ до понад 5800 абонентів. вітрові турбіни. Інцидент викликав міжнародний заклик Європейського парламенту до посилення заходів кібербезпеки в космічних технологіях, наголошуючи на необхідності посилення кіберстійкості у відповідь на виклики, які спостерігалися під час російського вторгнення в Україну.

Аналогічно, вторгнення в термінали Starlink компанії SpaceX у 2022 році продемонструвало витонченість кібератак на супутникові системи. Зловмисники використали вразливість у системі зв'язку супутників, продемонструвавши потребу в надійнішому шифруванні та більш безпечному програмному забезпеченні. Хоча SpaceX швидко усунула вразливість у своїй системі, цей інцидент підкреслив потенціал для більш розумних атак, які можуть порушити роботу критично важливої інфраструктури та послуг у майбутньому.

Вразливість супутникових систем до кібератак вже не є чимось теоретичним. Ці інциденти, а також інші, за якими стежать такі організації, як Агентство Європейського Союзу з кібербезпеки (ENISA) і Інститут кібермиру, підкреслюють зростаючу загрозу, яку становлять кіберзловмисники, що націлені на супутникову інфраструктуру.

Дослідження ENISA, наприклад, показало, що за останні п'ять років кількість таких атак зросла на 300 відсотків, причому особлива увага приділяється виведенню з ладу критично важливих супутникових систем зв'язку.

Експерти з кібербезпеки, включно з НАСА та Європейським космічним агентством, наголошують на важливості розробки надійного шифрування та безпечних протоколів зв’язку, спеціально розроблених для супутників. Ці заходи

необхідні для захисту конфіденційних даних і запобігання несанкціонованому доступу до критично важливих супутникових систем.

Історичні прецеденти, такі як злом американських військових безпілотників у 2009 році, демонструють, що навіть найбезпечніші системи не захищені від кіберзагроз. Ці інциденти вказують на необхідність постійної пильності та профілактичних заходів для пом’якшення ризиків кібербезпеці.

Критики часто підкреслюють високі витрати та технічні складності, пов’язані з модернізацією супутникової кібербезпеки. Дійсно, модернізація старих супутників новими засобами безпеки або розробка передових систем для нових супутників може бути значним фінансовим завданням. Проте в моїх дискусіях з космічними організаціями я часто наголошую, що вартість захисту наших супутників блідне в порівнянні з потенційними втратами від великої кібератаки. Це не лише фінансові втрати; мова йде про збереження життєво важливих послуг, які стосуються мільйонів людей.

Удосконалення технологій кібербезпеки зробили рішення доступнішими та легшими для інтеграції. Наприклад, Національний інститут стандартів і технологій Міністерства торгівлі США (NIST) нещодавно обрав групу квантово-стійких криптографічних алгоритмів, які запропонують економічно ефективний спосіб захисту супутникового зв’язку від майбутніх квантових комп’ютерних загроз. Крім того, розробник програмного забезпечення QuSecure у співпраці з технічної консалтинговою фірмою Accenture успішно продемонстрував використання постквантової криптографії в багатоорбітальних передачах даних, що ще більше підвищує безпеку супутникових передач. Ці досягнення є ключовими кроками до захисту нашої супутникової інфраструктури від складних кіберзагроз.

Крім того, успішна співпраця, наприклад між Університетом Алабами в Хантсвіллі та Lockheed Martin, демонструє, як проактивні інвестиції в кібербезпеку можуть ефективно захистити супутники. Ці ініціативи показують доцільність і цінність захисту наших супутників, протиставляючи аргументи щодо вартості та складності.

Нагальність захисту наших супутників від кіберзагроз неможливо переоцінити в умовах зростаючої космічної економіки в 386 мільярдів доларів. Оскільки ми все більше покладаємося на ці технології, відповідальність за їх захист зростає. Політики, технологічні лідери та громадськість повинні об'єднатися в цих зусиллях, визначаючи пріоритети та інвестуючи в супутникову кібербезпеку. Ці дії включають фінансування досліджень і розробок передових технологій безпеки та впровадження міжнародних правил і стандартів супутникової кібербезпеки.

Вживаючи рішучих заходів для зміцнення нашої супутникової кібербезпеки, ми гарантуємо, що космос залишається не лише кордоном досліджень, але й сферою безпеки та надійності. Захист наших небесних вартових має важливе значення для збереження самої тканини нашого взаємопов'язаного світу і, таким чином, для забезпечення постійного прогресу людства в епоху цифрових технологій. Сьогоднішні зусилля щодо захисту наших супутників захистять нашу глобальну інфраструктуру для майбутніх поколінь». ***(Sylvester Kaczmarek. We Need Cybersecurity in Space to Protect Satellites // Scientific American (https://www.scientificamerican.com/article/we-need-cybersecurity-in-space-to-protect-satellites/?utm_source=flipboard&utm_content=SciAm%2Fmagazine%2FScientific+American). 05.02.2024).***

***

«Загрози для критичної інфраструктури зростають, оскільки зловмисники продовжують сканувати мережі, атакувати мережі та пристрої та намагатися обійти контроль доступу. У той же час, згідно з новим звітом, у таких секторах, як виробництво, кількість вразливостей зросла на 230%.

Nozomi Networks Labs дослідила сповіщення в 25 країнах і в четвер опублікувала телеметричний звіт, який показує, що зловмисники тестують мережі за допомогою автоматизованих інструментів сканування та переповнюють системи запитами TCP. Ці мережеві аномалії становили 38% усіх загроз у другій половині 2023 року.

Атака на протокол керування передачею, або TCP, є типом атаки на відмову в обслуговуванні, яка передбачає затоплення цільової системи великою кількістю

запитів на підключення TCP. Інциденти, пов’язані з затопленням протоколу TCP та інцидентами з аномальними пакетами, різко зросли, спричинивши подвійне та шістькратне збільшення сповіщень відповідно.

«Значне зростання кількості аномалій може означати, що суб’єкти загрози проходять повз першу лінію захисту, проникаючи глибше, ніж багато хто спочатку міг би подумати, що вимагатиме високого рівня складності», — сказав Кріс Гроув, директор із стратегії кібербезпеки Nozomi. мережі.

Дослідники також спостерігали збільшення на 123% загроз контролю доступу та авторизації, причому кількість сповіщень про «множинні невдалі входи» та «атаку грубою силою» зросла на 71% та 14% відповідно. Гроув попередив, що ці тенденції вказують на те, що зловмисники використовують більш складні методи, щоб безпосередньо націлитися на критичну інфраструктуру – розвиток, який потенційно може вказувати на зростання глобальної ворожнечі та активності національних держав.

Найпопулярніші критичні загрози включають:

- Мережеві аномалії та атаки – 38% усіх сповіщень
- Проблеми з автентифікацією та паролем – 19% усіх сповіщень
- Проблеми з контролем доступу та авторизацією - 10% від усіх сповіщень
- Операційні технологічні загрози - 7% від усіх сповіщень
- Підозріла або несподівана поведінка мережі - 6% усіх сповіщень
- Вразливості ICS зростають

Дослідники виявили вразливі місця в системах промислового контролю та помітили, що виробництво зазнало збільшення на 230% типових уразливостей і ризиків. Виробництво, енергетика та системи водопостачання та водовідведення залишаються найбільш вразливими секторами.

Приманки Nozomi Networks показали зниження щоденних атак на 12%, але шкідливі ботнети Інтернету речей залишаються активними. У звіті Китай, Сполучені Штати, Південна Корея, Індія та Бразилія визначають країни походження IP-адрес зловмисників.

«Облікові дані за замовчуванням і спроби грубої сили залишаються улюбленими методами для отримання доступу до пристроїв Інтернету речей, створюючи значні ризики для галузей, які покладаються на взаємопов'язані пристрої», — заявили дослідники». ***(Number of Attacks Against Critical Infrastructure Is Growing // Information Security Media Group, Corp. (https://www.databreachtoday.com/number-attacks-against-critical-infrastructure-growing-a-24324?utm_source=flipboard&utm_content=other). 08.02.2024).***

***

«Залізнична галузь не захищена від кіберзагроз, особливо за нинішніх темпів технологічного прогресу. З роками потяги стають все більш зв'язаними, і в міру цього вони все більше покладаються на цифрові системи. Таким чином, важливість заходів кібербезпеки залізниці важко переоцінити. Світова залізнична мережа охоплює понад 1,3 мільйона кілометрів маршрутів по всьому світу, що показує, скільки можливостей є у хакерів.

Заходи кібербезпеки на залізниці є важливими для ефективних і безпечних подорожей. Очікується, що вартість кіберзлочинності обійдеться світу в 2024 трильйони доларів у 9,5 році, а оцифровка залізничних операцій робить галузь особливо вразливою до кіберзагроз, які можуть поставити під загрозу безпеку, порушити роботу послуг і навіть створити ризики для національної безпеки.

У цьому посібнику ми розповімо, що таке кібербезпека на залізниці та чому вона є необхідною для безперебійного функціонування та безпеки сучасних залізничних систем.

1. Захист критичної інфраструктури

Інфраструктура країни принаймні частково залежить від її залізничних систем та їх експлуатації. Належне функціонування є життєво важливим для громадської мобільності та економічного зростання. Незаконний або несанкціонований доступ до систем управління залізницею, протоколів сигналізації та комунікаційних мереж є частиною критичної інфраструктури, на якій необхідно зосередитися. Якщо цими системами маніпулювати або отримати доступ з боку тих, хто хоче завдати шкоди, то наслідки можуть бути катастрофічними.

Стійкі цифрові компоненти мають важливе значення для зниження ймовірності того, що кібератака порушить роботу залізничного транспорту та поставить під загрозу пасажирів. Постійно змінювані ризики наразі зменшуються зацікавленими сторонами залізниці, які посилюють заходи кібербезпеки, пов'язані з оцифрованими залізничними системами.

Продовження моніторингу нових загроз і швидке реагування є важливими кроками для підтримки цілісності надійних залізничних мереж.

Постійний моніторинг, виявлення загроз і механізми швидкого реагування є важливими елементами захисту цілісності та надійності сучасних залізничних мереж.

2. Захист безпеки пасажирів

Автоматизовані системи керування інформацією для пасажирів можуть мати більше потенційних недоліків, якщо поїзди почнуть використовувати більше цифрових технологій. Кіберзлочинність, яка включає все: від крадіжки чи розкрадання до злому та знищення даних, зросла на XNUMX% внаслідок пандемії COVID-XNUMX, яка включає кібератаки на залізниці.

Метою кібербезпеки залізниці є захист пасажирів від таких загроз, як витік даних, які можуть поставити під загрозу конфіденційні дані. Подібні загрози також можуть призвести до контролю систем керування поїздами без доступу та інших атак на фізичну залізничну інфраструктуру.

У цьому питанні слід враховувати кілька речей:

Інтеграція автоматизованих систем управління в поїзди створює виклик кібербезпеці, оскільки відкриває шляхи для віддаленого маніпулювання та несанкціонованого доступу, якщо вони не захищені належним чином.

Перехід до цифрових технологій у залізничному секторі робить його вразливим до витоку даних, наражаючи пасажирів на потенційні порушення конфіденційності та крадіжки особистих даних, якщо особиста інформація скомпрометована.

Інтеграція автоматизованих систем управління в поїзди створює виклик кібербезпеці, оскільки відкриває шляхи для віддаленого маніпулювання та несанкціонованого доступу, якщо вони не захищені належним чином.

3. Запобігання збоям в обслуговуванні

На роботу залізниць можуть серйозно вплинути кібератаки. Порушити можуть не лише комунікаційні мережі, але й інші важливі компоненти, наприклад системи сигналізації. Незручність — це не єдиний наслідок такої події, оскільки це також може мати фінансові наслідки.

Покращення кібербезпеки залізниці має на меті зменшити ці ризики та забезпечити надійне функціонування залізничних послуг у всій мережі.

Стратегічне впровадження найкращої VPN преміум-класу відіграє вирішальну роль у посиленні заходів кібербезпеки на залізниці. VPN підвищують безпеку комунікаційних мереж, захищаючи від потенційних загроз і забезпечуючи безперебійну роботу різних систем, тим самим підвищуючи загальну стійкість залізничної інфраструктури до кібератак.

4. Вирішення проблем національної безпеки

Захист і матеріально-технічне забезпечення країни часто можуть покладатися на залізниці. Загрози цим системам, цифрові чи інші, можуть мати серйозний вплив на національну безпеку. Тому стратегії забезпечення безпеки цих систем мають бути пріоритетними. Важливі ресурси та військовий персонал часто перевозять потягами.

Запровадження відповідних протоколів кібербезпеки та забезпечення їх регулярного оновлення означає, що залізниці країни залишаються максимально безпечними. Отже, переконайтеся, що всі заходи є максимально актуальними, оскільки вони можуть змінюватися дуже швидко.

Чому кібербезпека залізниці важлива

Конвергенція фізичних і цифрових елементів у залізничному секторі підкреслює необхідність надійних заходів кібербезпеки.

Випереджаючи потенційні загрози, залізнична галузь може продовжувати впроваджувати технологічні інновації, одночасно забезпечуючи безпеку та надійність своїх операцій. Ось що вони обговорюють:

Інтеграція цифрових технологій у залізничний сектор призвела до створення складної мережі взаємопов'язаних систем, що робить критично важливим захист як фізичних, так і цифрових елементів для запобігання потенційним кіберзагрозам.

Порушення кібербезпеки в залізничній галузі можуть призвести до значних фінансових втрат для операторів. Ці збитки можуть включати не лише прямі витрати на відновлення системи, але й непрямі витрати, пов'язані зі збитком репутації та правовими наслідками.

Конвергенція фізичних і цифрових елементів викликає занепокоєння щодо безпеки мільйонів пасажирів. Уразливі місця кібербезпеки потенційно можуть бути використані для компрометації критично важливих залізничних операцій, що призведе до аварій або збоїв, які загрожують безпеці пасажирів.

Висновок

Технології продовжують формувати майбутнє транспорту, в тому числі залізниці. Ось чому розуміння важливості кібербезпеки в цій сфері є таким важливим. Збої, безпека пасажирів і навіть проблеми національної безпеки – все це необхідно вирішити.

Виконання кроків, зазначених у цьому посібнику, гарантує, що подорож поїздом буде безпечною та ефективною. Зобов'язання щодо достатніх заходів кібербезпеки є чудовим способом досягти цих цілей і підтримувати успіх у майбутньому». ***(What Is Railway Cybersecurity And Why Is It So Important? // RayHaber (https://raillynews.com/2024/02/What-is-railway-cybersecurity-and-why-is-it-so-important%3F/). 13.02.2024).***

***

Кіберзахист закладів охорони здоров'я

«За даними організації, кібер-атака на Change Healthcare, що належить UnitedHealth, вплинула на виконання рецептів у різних аптеках.

В оновленому статусі додатків, які мають проблеми з підключенням, Change Healthcare повідомила, що вирішує «проблему» кібербезпеки. Підприємство не пояснило цю проблему, поки вирішило проблему.

Згідно з оновленнями статусу Change Healthcare, це стосується багатьох сфер бізнес-послуг, зокрема рішень для аптек.

«Як тільки нам стало відомо про зовнішню загрозу, в інтересах захисту наших партнерів і пацієнтів ми вжили негайних заходів, щоб відключити наші системи, щоб запобігти подальшому впливу», — заявили в компанії. «Наразі ми вважаємо, що проблема стосується лише Change Healthcare, і всі інші системи UnitedHealth Group працюють».

UnitedHealth надала оновлену інформацію про загрозу безпеці в четвер вдень.

«UnitedHealth Group ідентифікувала підозрюваного суб'єкта загрози кібербезпеці, пов'язаного з національною державою, який отримав доступ до деяких систем інформаційних технологій Change Healthcare», — заявили в компанії.

Компанія заявила, що «проактивно» ізолювала постраждалі системи від підключених систем, щоб захистити партнерів і пацієнтів, а також стримувати, оцінювати та виправляти ситуацію.

Change Health не має оцінки тривалості чи масштабу збою станом на четвер у другій половині дня.

«Компанія найняла провідних експертів з безпеки, співпрацює з правоохоронними органами та повідомила клієнтів, клієнтів і певні державні установи», — йдеться у заяві UnitedHealth. «На даний момент Компанія вважає, що збій мережі стосується систем Change Healthcare, і всі інші системи в компанії працюють».

Гнучкість – плюс для незалежних аптек

Майкл Скраггс, власник Front Range Pharmacy в Енглвуді, пояснив, що Change Healthcare є «сторожем» між аптеками та керівниками відділів рецептів страхових компаній. Загалом це гарантує, що фармацевти, лікарі та страхові

компанії підключені та працюють на одній сторінці через аптечну мережу для розгляду претензій.

Скраггс пояснив, що аптеки повинні або перейти на інший комутатор, приймати лише готівку за всі рецепти, подати претензії вручну до страхової компанії або змінити мережу комутаторів, коли мережа комутаторів не працює.

Скраггс сказав, що його компанія, завдяки місцевій власності з більшою гнучкістю, перейшла на інший перемикач і не мала проблем із виконанням приписів.

Глядачі звернулися до FOX31 щодо проблем із отриманням рецептів у Safeway. FOX31 звернувся за коментарем, але наразі не отримав відповіді. Незрозуміло, чи пов'язані звіти з проблемою Change Healthcare.

Change Healthcare вперше повідомила про проблему в середу вранці. На сайті компанії повідомляється, що 16-17 лютого було заплановано технічне обслуговування продуктів InterQual solutions, а в четвер, 22 лютого, - оновлення продукту Ahi.

Бізнес був придбаний у жовтні 2022 року компанією Optum за 13 мільярдів доларів». ***(Heather Willard. Change Healthcare cybersecurity 'issue' disrupting some pharmacies // Microsoft (https://www.msn.com/en-us/money/other/change-healthcare-cybersecurity-issue-disrupting-some-pharmacies/ar-BB1iJbdz). 22.02.2024).***

***

«Нещодавня атака вірусу-здирника спричинила значні перебої в роботі 18 лікарень по всій Румунії, зупинивши їхню діяльність. Атака була спрямована на інформаційну систему Hipocrate (HIS), яка має важливе значення для управління лікуванням пацієнтів та веденням медичної документації. В результаті система наразі не працює, і лікарні намагаються підтримувати звичний рівень надання медичної допомоги.

Атака сталася в ніч з 11 на 12 лютого 2024 року, в результаті чого були зашифровані бази даних і файли. Міністерство охорони здоров'я Румунії визнало серйозність ситуації та активно працює над її вирішенням. Наразі тривають зусилля

з відновлення постраждалих систем під керівництвом експертів з IT та кібербезпеки з Національного директорату з кібербезпеки (DNSC).

Наслідки атаки вірусу-здирника є широкомасштабними і зачіпають різні медичні установи, в тому числі регіональні лікарні та онкологічні центри. Щоб запобігти подальшій шкоді, Міністерство охорони здоров'я посилило заходи безпеки для інших лікарень, які не постраждали від атаки.

Наразі деталі про групу вимагачів, що стояла за атакою, або специфіку скомпрометованих даних не відомі. Постачальник системи HIS, компанія RSC, ще не зробила публічної заяви щодо цього інциденту.

Подібні інциденти викривають вразливість систем охорони здоров'я до кібератак і ще більше підвищують важливість надійних заходів кібербезпеки для захисту конфіденційних даних пацієнтів і забезпечення безперервної роботи критично важливих медичних послуг. Це той сектор, який не може дозволити собі серйозні простої, як ці, і з очевидних причин!» ***(Масштабна кібератака вразила 18 лікарень по всій Румунії // HiTech.Expert. (https://expert.com.ua/176899-masshtabna-kiberataka-vrazyla-18-likaren-po-vsiy-rumunii.html). 12.02.2024).***

***

Захист персональних даних та соціальні мережі

«Дві американські страхові компанії попереджають, що особиста інформація тисяч людей могла бути викрадена після того, як хакери зламали комп'ютерні системи.

Washington National Insurance та Bankers Life, обидві дочірні компанії CNO Financial Group, стали мішенню хакерів, які замінили SIM-карти, у листопаді 2023 року.

Як ми вже описували раніше, атаки із заміною SIM-картки включають шахраїв, які обманом змушують персонал служби підтримки клієнтів оператора мобільного зв'язку надати їм контроль над чужим номером телефону. Це дозволяє

шахраю отримувати телефонні дзвінки та SMS-повідомлення жертви, включаючи маркери двофакторної автентифікації.

У деяких випадках програми заміни SIM-карт викрадають телефонні номери за допомогою нечесного інсайдера в мобільній компанії.

У листі-повідомленні про порушення, надісланому Washington National Insurance 20 360 постраждалим особам, пояснюється, що атака із заміною SIM-карти на «номер телефону старшого офіцера» дозволила хакерам обійти багатофакторну автентифікацію.

Компанія попередила, що особиста інформація, включаючи імена, номери соціального страхування, дати народження та номери полісів.

Bankers Life надіслав майже ідентичний лист із повідомленням про порушення 45 842 особам.

Коротше кажучи, особиста інформація близько 66 000 людей зараз знаходиться в руках кіберзлочинців, які можуть використовувати її для шахрайства або подальших атак.

Мене особливо тривожить те, що атаки на заміну SIM-карти не є новими. Злочинці використовують цей метод для проникнення в системи без авторизації, чи то для встановлення програм-вимагачів, крадіжки даних чи викрадення криптовалюти.

Двофакторна автентифікація на основі SMS є менш безпечною, ніж програми автентифікації з тимчасовими одноразовими паролями (TOTP) або апаратними ключами. Проте компанії все ще залишаються відкритими для заміни SIM-карт.

З огляду на те, що заміна SIM-карти настільки поширена, що злочинцям її легко вдатися, організаціям і окремим особам слід уникати зв’язування облікових записів зі своїм номером телефону. Вони також повинні додати додаткові рівні безпеки до своїх облікових записів мобільних телефонів, щоб шахраям було важче змусити оператора мобільного зв’язку передати номер.

Обидві страхові компанії повинні чітко поговорити зі своїм постачальником мобільного зв’язку щодо запобігання повторенню подібної аварії». ***(Graham CLULEY. US insurance firms sound alarm after 66,000 individuals impacted by SIM***

swap attack // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/us-insurance-firms-sound-alarm-after-66-000-individuals-impacted-by-sim-swap-attack/?utm_source=flipboard&utm_content=other%2F). 08.02.2024).

***

«Компанії програмного забезпечення для кібербезпеки Avast загрожує штраф у розмірі 16,5 мільйонів доларів від Федеральної торгової комісії після того, як агентство подало скаргу в середу, звинувачуючи компанію в продажу споживчих даних третім особам.

FTC стверджує, що Avast, фірма, яка обіцяє захищати дані споживачів від відстеження в Інтернеті, зробила протилежне, збираючи та продаючи дані веб-перегляду користувачів без відома чи згоди, одночасно вводячи користувачів в оману.

Виникнення Avast сягає кінця 1980-х років, коли його засновники жили та працювали в Чехословаччині, коли вона була частиною радянського блоку. З часом компанія розширювала своє антивірусне програмне забезпечення та інші пропозиції, вийшла на біржу та з часом об'єдналася з іншими компаніями у сфері кібербезпеки.

Зараз Avast є одним із кількох брендів, що належать Gen Digital, публічній компанії з подвійною штаб-квартирою в Темпі, штат Арізона, та Празі, Чеська Республіка.

У скарзі агентство стверджує, що компанія Avast Limited, що базується у Великій Британії та через свою чеську дочірню компанію, стверджувала, що блокує файли cookie для відстеження, які збирають дані, і не дозволяє іншим трекерам стежити за діяльністю в Інтернеті лише для того, щоб потім продавати ці дані третім сторонам, беручи участь у поведінка принаймні з 2014 року.

Крім того, FTC каже, що Avast повідомила користувачам, що буде ділитися інформацією лише в «анонімній та зведеній формі», хоча це не так.

«Історія перегляду веб-сторінок людини може виявити надзвичайно конфіденційну інформацію. Запис веб-сайтів, які хтось відвідує, може розкрити все: від чиїхось романтичних інтересів, фінансових труднощів і непопулярних

політичних поглядів до їхніх зусиль щодо схуднення, відмови від роботи та залежності від азартних ігор», – заявила голова FTC Ліна Хан у заяві в середу.

«FTC звинувачує, що дії Avast тут були не лише оманливими, але й нечесними», — продовжив Хан. «Оскільки дані веб-перегляду є внутрішньо чутливими, вони гарантують підвищений захист».

FTC каже, що Avast продавав дані більш ніж 100 клієнтам, включаючи консалтингові фірми, рекламні компанії та брокерів даних.

Окрім багатомільйонного штрафу, FTC забороняє компанії Avast продавати або ліцензувати дані для рекламних цілей.

«Avast пообіцяв користувачам, що його продукти захищатимуть конфіденційність їхніх даних веб-перегляду, але зробив протилежне», — написав у четвер Семюел Левін, директор Бюро захисту прав споживачів FTC. «Тактика стеження за принципом «приманки та перемикання» Avast поставила під загрозу конфіденційність споживачів і порушила закон».

Коли його попросили прокоментувати, Avast підтвердив CNN, що досяг мирової угоди з Федеральною торговою палатою щодо вирішення розслідування, пов’язаного з його «дочірньою компанією Jumpshot, яку Avast добровільно закрив у січні 2020 року».

«Хоча ми не погоджуємося зі звинуваченнями FTC і характеристикою фактів, ми раді вирішити це питання та сподіваємося продовжувати обслуговувати наші мільйони клієнтів у всьому світі», — йдеться в заяві компанії». ***(Jennifer Korn. FTC fines cybersecurity company Avast $16.5 million for tracking and selling user data // Microsoft (https://www.msn.com/en-us/money/other/ftc-fines-cybersecurity-company-avast-165-million-for-tracking-and-selling-user-data/ar-BB1iJjPw). 23.02.2024).***

***

«Те, як функціонує кібербезпека в наш сучасний час, дещо погіршилося, що фактично означає, що довжина та складність вашого пароля більше не можуть захистити вас від зловмисників. Навіть двофакторної автентифікації може бути недостатньо, якщо все врахувати та взяти до уваги, оскільки зловмисне

програмне забезпечення може обійти все це та створити ситуацію, коли ваші маркери сеансу або файли cookie можуть опинитися в чужих руках.

За словами колишнього експерта ФБР із цифрових злочинів Тревора Хіллігосса (через CyberNews), який зараз є віце-президентом SpyCloud Labs, крадіжка файлів cookie насправді є найбільшою загрозою для кібербезпеки. Більшість людей зазвичай зосереджуються на таких речах, як їхні паролі, але, незважаючи на те, що це так, виявляється, що крадіжка файлів cookie викликає набагато більше занепокоєння через те, як вона може обійти різні встановлені засоби захисту.

Найбільш важливою ситуацією, коли крадіжка файлів cookie може спричинити широкий спектр проблем, є зловживання вашим обліковим записом Google. Така подія може бути катастрофічною через той факт, що це така річ, яка потенційно може призвести до скомпрометації будь-якого іншого облікового запису, пов’язаного з вашим обліковим записом Google, включаючи профілі в соціальних мережах тощо.

Експлойт авторизації OAuth2 вже надав зловмисникам можливість таємно отримувати доступ до облікових записів Google, навіть не підозрюючи власника, що відбувається. Облікові записи Google можуть бути для них надзвичайно привабливими пропозиціями, оскільки вони також, як правило, містять фінансову інформацію та інші дуже конфіденційні дані, які можуть завдати незліченної шкоди.

Автентифікаційні файли cookie можуть зробити MFA набагато менш ефективним, і це, по суті, є найефективнішою стратегією утримувати хакерів практично беззахисними. Зловмисники крадуть файли cookie протягом досить тривалого часу, і, оскільки зловмисне програмне забезпечення як послуга швидко набирає обертів, хакерам навіть не потрібні такі значні технічні знання, щоб реалізувати свої схеми.

Оскільки файли cookie веб-переглядача зберігаються в локальних базах даних, вони стали основною мішенню для цих зловмисників, тому так важливо залатати будь-які діри.

Зловмисне програмне забезпечення в основному може працювати подібно до браузера, оскільки воно може перевіряти наявність збережених файлів cookie, які спрощують вхід. Потрібні токени входу будуть об'єднані з іншими системними даними, такими як обсяг оперативної пам'яті та інформація про ЦП, яка їх приховує, з файлами, надісланими на пристрій користувача, а потім отриманими зловмисником.

Існують сотні тисяч заражень infostealer щодня, і вони здебільшого націлені на людей, які живуть у розвинених країнах, через вищу цінність їхніх даних. Щоб захистити себе від цих атак, абсолютно важливо завантажити антивірус і постійно оновлювати його, а крім того, вам потрібен постійний моніторинг кінцевих точок найвищого рівня.

Ще одна корисна стратегія, яку ви можете застосувати, — уникати натискань на оголошення. Велика кількість зловмисного програмного забезпечення передається через шахрайську рекламу, тому Хіллігосс рекомендує вам просто триматися подалі від реклами, наскільки це можливо». ***(Zia Muhammad. Former FBI Expert Warns of Cookie Theft Emerging as Major Cybersecurity Threat, Surpassing Password Concerns with its Ability to Bypass Protections // Digital Information World (https://www.digitalinformationworld.com/2024/02/former-fbi-expert-warns-of-cookie-theft.html). 26.02.2024)***

***

Масштабні витоки персональних даних

«Понад 33 мільйони людей у Франції – майже половина її населення – постраждали від найбільшої кібератаки в історії країни.

Цілями стали два французькі постачальники послуг для медичних страхових компаній, причому компанії визнали, що дані мільйонів людей потенційно були піддані хакерам.

«Це вперше сталося порушення такого масштабу», — сказав Янн Падова, юрист, який спеціалізується на захисті цифрових даних і колишній генеральний

секретар Французького органу захисту даних (CNIL), французькому мовнику Franceinfo в четвер.

За словами Падови, це «найбільший пролом у безпеці у Франції».

Це те, що ми знаємо про атаки та які дані були вкрадені.

Що сталося?

Дві компанії - Viamedis і Almerys - є постачальниками послуг для медичних страхових компаній. Вони стали жертвами кібератаки, яка сталася з різницею в п'ять днів на початку лютого.

За словами першого постачальника, Viamedis, хакери займалися фішингом і використовували логіни медичних працівників, щоб проникнути в систему.

Almerys заявив, що хакери не зламали його центральну систему, а отримали доступ до порталу, який використовують медичні працівники.

Два провайдери подали скарги до прокуратури, триває розслідування.

Які дані були вкрадені?

Понад 33 мільйони людей, за даними французького органу захисту даних (CNIL)- трохи менше половини населення Франції - постраждали від витоку даних, які включали такі деталі, як «сімейний стан, дата народження та номер соціального страхування, назва медичного страховика та покриття, передбачене полісом».

У CNIL запевнили, що "ні про які банківські реквізити, медичні дані, поштову адресу, номер телефону чи електронну пошту не йдеться".

Які наслідки?

Платіжна система «tiers payant», за якою пацієнту не потрібно сплачувати повну вартість медичних послуг наперед, може бути недоступною для певних медичних працівників, але все ще доступною для пацієнтів.

CNIL попередив користувачів про ризики фішингу, особливо тому, що нові дані, що витікають, можуть поєднуватися з іншою інформацією про попередні витоки даних.

Користувачі повинні бути особливо уважними, перевіряючи автентичність електронних листів, текстових повідомлень і дзвінків, нібито від офіційних організацій.

З людьми, чиї дані були скомпрометовані, зв'яжуться, щоб отримати індивідуальну інформацію від їхнього медичного страхування щодо дотримання вказівок GDPR». ***(Oceane Duboust. Data of half the population of France stolen in its largest ever cyberattack. This is what we know // euronews (https://www.euronews.com/next/2024/02/08/data-of-33-million-people-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we?utm_source=flipboard&utm_content=curiouscurator%2Fmagazine%2FDigitech+Dreams). 08.02.2024).***

***

«Пенсійний регулятор (TPR) опублікував Звіт про регуляторне втручання, в якому пояснюється, як він працював із Capita після значного витоку даних, який стався в березні 2023 року. Ось п'ять речей, які ми можемо дізнатися зі Звіту...

Це одна сфера, де TPR співпрацює з іншими регуляторами. Це не нове – наприклад, TPR працювала спільно з FCA в минулому, але в цьому випадку TPR залучила та надала інформацію FCA, PRA та Комісару з інформації (ICO), кожен з яких мав інтерес до Capita порушення. Це має сенс; учасники постраждалих пенсійних схем будуть піддаватися однаковим ризикам, незалежно від того, хто регулює їхню схему, і ICO завжди буде зацікавлений у порушенні такого масштабу (і може проводити розслідування за лаштунками, у тому числі протягом деякого часу після порушення). було ефективно вирішено).

TPR усвідомлює логістичні проблеми, пов'язані з порушенням, особливо тому, що великому адміністратору, такому як Capita, доведеться виконати значну роботу, щоб точно визначити, які саме дані та кого з його клієнтів (і їхніх базових учасників) це стосується. Однак саме довірені особи відповідають за роботу своєї схеми, і саме довірені особи є контролерами даних для цілей GDPR. Тому в кінцевому підсумку робота довіреної особи полягає в тому, щоб вжити всіх необхідних заходів для забезпечення виконання схемою своїх зобов'язань і мінімізації шкоди для учасників, наприклад, шляхом своєчасного спілкування з ними.

Підготовка є ключовою, і у Звіті чітко зазначено, що довірені особи повинні мати план кібербезпеки та безперервності бізнесу, щоб у разі виникнення інциденту «довірені особи відрепетирували ролі, обов'язки, системи та процеси». У Загальному кодексі TPR сказано, що довірені особи повинні мати план реагування на кіберінциденти, але ми пропонуємо, щоб там, де це пропорційно, довіреним особам також слід перевірити свій план (наприклад, запустивши сеанс кібер-військової гри).

Довіреним особам, які постраждали від порушення, не слід чекати повідомлень від TPR. Насправді TPR просить, щоб довірені особи звітували їм про значні кіберінциденти «на добровільній основі», зазначаючи, що можуть існувати обставини, за яких потрібен звіт, наприклад, коли схема не може обробити основні транзакції, і тому існує порушення закону, яке може мати істотне значення для TPR. Після порушення Capita TPR зв'язалася з 383 пенсійними схемами, які, як вони зрозуміли (із записів), адмініструються Capita. Однак у звіті також зазначається, що здатність TPR підтримувати довірених осіб була відкладена, оскільки сама TPR не мала актуальної контактної інформації для схеми.

Довірені особи можуть вжити заходів для захисту своїх членів після порушення. Це так, навіть якщо вони використовують стороннього адміністратора. Окрім письмового повідомлення членам про проблему та пов'язані з нею ризики, довірені особи можуть:

- розглянути можливість зміни процедур безпеки для боротьби з шахрайством із ідентифікацією
- доручити своєму адміністратору відстежувати та повідомляти про будь-які незвичайні запити на передачу
- спрямовувати членів до вказівок Національного центру кібербезпеки
- попередити членів про пенсійні махінації». ***(Anna Taylor. Pensions cyber security – TPR and the Capita data breach // Taylor Wessing (https://www.taylorwessing.com/en/insights-and-events/insights/2024/02/pensions-cyber-security). 09.02.2024).***

***

«Обіцянка штучного інтелекту покращити та масштабувати людську роботу вражає. Але, на жаль, це обіцяє те саме для тих, хто має злі наміри. Коли програми GenAI почали розгортати майже два роки тому, шахраї були одними з перших.

Найкращий приклад того, як GenAI використовується для фішингу. Як повідомляє CNBC, «з четвертого кварталу 2022 року кількість зловмисних фішингових листів зросла на 1265%, а фішингу облікових даних — на 967%, згідно з новим звітом фірми з кібербезпеки SlashNext». Фішингові електронні листи, які часто виглядають так, ніби їх надіслав хтось із фінансової установи, обманом змушують людину надати свої облікові дані. За даними StationX та інших, це винуватець понад третини випадків витоку даних. У нього також є злий двоюрідний брат: «смішинг», коли користувача обманюють законним текстовим (також відомим як SMS) повідомленням.

Generative AI дозволяє користувачам зі злочинними намірами писати дуже переконливу копію в масштабі. Раніше ми могли виявляти фішинг через погану граматику та синтаксис у повідомленнях, ознаки того, що насправді це не ваш банк, а хтось в іншому куточку світу, хто погано володіє вашою мовою. Це вже не так. GenAI може написати шахрайське повідомлення мовою цілі та тоном фінансової установи.

GenAI також використовується для створення більш переконливої соціальної інженерії шляхом створення синтетичних ідентифікацій, які змішують законні та штучні дані для створення підроблених профілів разом із зображеннями профілів, розробленими ШІ. Він використовується для імітації людських голосів під час телефонних дзвінків, мотивованих шахрайством. Він використовується для написання шкідливого комп'ютерного коду та автоматизації атак. Один урок, який компанії повинні винести зі зростання шахрайства з використанням штучного

інтелекту, це не нехтувати власним використанням штучного інтелекту для зміцнення захисту.

Додайте автентифікацію за допомогою ШІ

Вхідні двері – найкраще місце, щоб зупинити цифрового зловмисника. Шахраї це добре розуміють, тому інвестують у створення підроблених облікових записів або викрадення облікових даних. Чудова новина полягає в тому, що машинне навчання (ML), функція штучного інтелекту, яка поглинає дані та вивчає їх із блискавичною швидкістю, ніколи не спить. Він володіє неймовірною здатністю постійно вивчати, як поводяться шахраї, і порівнювати це з тим, як діють типові законні користувачі. Найкращі постачальники засобів кібербезпеки використовують його саме для цієї мети.

Наприклад, штучний інтелект може аналізувати типові шаблони використання мільярдів пристроїв і телефонних номерів, які використовуються для входу в критично важливі облікові записи, такі як електронна пошта або банківські рахунки, щоб виявити незвичну поведінку. Наприклад, якщо пристрій, який пінгував із Сан-Хосе, штат Каліфорнія, 30 хвилин тому, раптом сигналізує, що знаходиться в Празі, у Чеській Республіці, швидше за все, щось не так.

Те саме стосується сигналів від пристрою, який використовується для входу в обліковий запис електронної пошти, або ping від мобільного пристрою до вежі стільникового зв’язку. AI проводить аналіз даних, який допомагає вам зрозуміти географічну та іншу поведінку та визначити, коли потрібна додаткова обережність. Це один із способів, за допомогою яких штучний інтелект може оцінювати випадки пристроїв, які намагаються ввійти, наприклад мобільний телефон або ПК із системою доступу, і відповідним чином пристосовувати кількість кроків автентифікації. Пристрій, який показує більше потенційних сигналів шахрайства, означає більше тертя, тоді як пристрій із меншим ризиком проходить через це швидше.

Як ШІ зупиняє інші форми шахрайства

Ще одна зростаюча загроза – це обмін SIM-картами. Ось як це працює: по-перше, злочинець, який знайшов частину вашої особистої інформації в темній

мережі, обманом змушує службу мобільного зв'язку передати ваш номер телефону. Тепер, коли мобільний телефон пов'язаний із вашим номером телефону, вони починають запитувати скидання пароля за допомогою одноразового пароля (OTP). Вони можуть спочатку скинути пароль вашої електронної пошти, перш ніж перейти до ваших банківських або пенсійних рахунків.

Використовуючи цей процес, шахрай може буквально за один день перевернути життя людини. Чудова новина полягає в тому, що штучний інтелект може виявляти сигнали про те, що клієнт потенційно став жертвою заміни SIM-карти, визнаючи, що базові шаблони змінилися (людина, яка вкрала ваш номер телефону, зазвичай перебуває в іншому місті, якщо не в іншій країні), і автоматично збільшує тертя, необхідні перед проведенням транзакції. Це посилює захист клієнтів від проникнення в їхні облікові записи після заміни SIM-карти та посилює захист від проникнення шахраїв у вашу цифрову екосистему.

«Міжнародне шахрайство з розподілом доходів» (International Revenue Sharing Fraud, IRSF) також є областю, в якій ШІ корисний. Шахрайство з телефонним зв'язком – це схема, яка підриває компанію запитами на надсилання SMS, одноразових кодів доступу на телефонні номери, які стягують шахрайську плату. Подумайте про шахрайство з телефонними зв'язками як про те, що компанія змушує компанію знову і знову використовувати номери для спілкування через SMS.

Ви можете захиститися від шахраїв, які захоплюють рутинні бізнес-процеси та вчиняють цифрові крадіжки. Машинне навчання може аналізувати поведінку номерів телефонів і, наприклад, сповіщати вас про телефонні номери, з історією надсилання гігантських пакетів SMS-повідомлень за короткий проміжок часу, що є ознакою атак IRSF.

Оцініть, як виробники кібербезпеки використовують ШІ

Багато визнаних постачальників, у тому числі CISCO, IBM, OKTA та інші, дозволяють своїм клієнтам використовувати штучний інтелект для боротьби з безліччю інших видів атак, у тому числі тих, які надходять зі зловмисних IP-адрес і зловмисного програмного забезпечення.

Існують також інноваційні стартапи, які використовують ШІ для кібербезпеки по-новому. BioCatch, наприклад, використовує ML для аналізу цифрової, фізичної та когнітивної поведінки людини. Його платформа штучного інтелекту дозволяє фінансовим та іншим установам оцінювати ризики сеансів, які часто включають транзакції, коли аномалії свідчать про захоплення облікового запису або інші види шахрайства.

Шукайте постачальників, які використовують ШІ та машинне навчання, щоб зрозуміти, як думають і поводяться шахраї порівняно з іншими. Це дозволяє оцінювати ризики транзакцій, логінів, сеансів тощо. Ця інформація може допомогти відрізнити законні наміри від шахрайських і інформувати про ваші рішення щодо інших заходів безпеки, необхідних для продовження онлайн-процесу.

Підсумок: якщо ви розглядаєте застарілого постачальника кібербезпеки чи стартап, серйозно подивіться на те, як вони використовують ШІ для боротьби з шахрайством на основі ШІ». ***(Christophe Van de Weyer. Cybersecurity Threats: How To Fight AI With AI // Forbes (https://www.forbes.com/sites/forbestechcouncil/2024/02/14/cybersecurity-threats-how-to-fight-ai-with-ai/?sh=4eb40b912bb4). 14.02.2024).***

***

«Впровадження штучного інтелекту в Саудівській Аравії, ймовірно, збільшиться, оскільки керівники планують інвестувати в технологію для зміцнення кібербезпеки, показало нещодавнє опитування.

Згідно з опитуванням, проведеним британською дослідницькою компанією Censuswide на замовлення американської фірми з кібербезпеки Palo Alto Networks, 94 відсотки організацій у Королівстві мають намір збільшити свої інвестиції в штучний інтелект.

Цей крок спрямований на покращення стратегій кібербезпеки, при цьому 77 відсотків визнають вирішальну роль штучного інтелекту в їхній загальній цифровій структурі.

«Ескалація та дедалі складніші проблеми кібербезпеки спонукають організації переглядати свої стратегії, щоб покращити безпеку та підвищити кіберстійкість», — сказав Ерджан Айдін, регіональний віце-президент Palo Alto Networks, Близький Схід і Африка.

«Відрадно, що бізнес-лідери в Саудівській Аравії розглядають ШІ як важливий фактор розвитку бізнесу. У поєднанні з такими практиками кібербезпеки, як жорстка політика, навчання співробітників і інтегрований підхід до платформи, можливості безмежні для організацій, які хочуть покращити свою кібербезпеку за допомогою ШІ та машинного навчання», – додав він.

Опитування свідчить про високу обізнаність саудівських організацій щодо потенційних кіберризиків: 87 відсотків респондентів розуміють загрози, а 91 відсоток вважають, що їхня організація готова з ними впоратися.

Незважаючи на таку впевненість, половина учасників спостерігали зростання кількості кібератак за попередній рік.

Приблизно 71 відсоток генеральних директорів вважають кібербезпеку питанням важливості на рівні правління, причому майже половина з них вважають себе разом із директором з інформації відповідальними за захист своїх організацій від кіберзагроз.

Дослідження також підкреслює стратегічні зміни в інвестиціях у кібербезпеку: 69 відсотків керівників прагнуть збільшити фінансування в цій сфері.

Навпаки, 84 відсотки респондентів повідомили про плани оптимізувати свої рішення безпеки для пом’якшення складності, що підтвердили керівники інформаційної безпеки відповідних компаній.

У цьому всебічному дослідженні було опитано 502 генеральних директора в Саудівській Аравії та ОАЕ з 20 по 28 вересня 2023 року, дотримуючись стандартів Товариства дослідження ринку та принципів ESOMAR під наглядом Британської ради опитування». ***(94% of Saudi organizations plan to increase AI investment: survey // arab news (https://www.arabnews.com/node/2458731/business-economy). 12.02.2024).***

***

«У новаторському звіті, опублікованому Techopedia, було розкрито глибокий вплив штучного інтелекту (ШІ) на ландшафт кібербезпеки. У звіті розглядаються важливі висновки, які проливають світло на прогнозовану цінність ринку кібербезпеки штучного інтелекту, економічну ефективність штучного інтелекту під час виявлення порушень даних, а також настрої експертів з кібербезпеки щодо інтеграції ШІ.

Згідно зі звітом, глобальний ринок кібербезпеки штучного інтелекту готовий до експоненційного зростання, прогнозована вартість якого перевищить приголомшливі 133 мільярди доларів між 2023 і 2030 роками. Ця значна оцінка підкреслює зростаюче значення технологій штучного інтелекту в зміцненні цифрового захисту від нових кіберзагроз.

Одним із найпомітніших відкриттів звіту є ключова роль, яку відіграє штучний інтелект у зміцненні заходів кібербезпеки. Використовуючи розширені алгоритми та можливості машинного навчання, AI сприяє швидкому й точному виявленню потенційних загроз, зокрема спроб фішингу та зловмисних дій.

Організації, які застосували рішення кібербезпеки на основі штучного інтелекту, повідомили про значну економію коштів, у середньому близько 1,8 мільйона доларів США порівняно з тими, хто не має таких технологій.

Фахівці з кібербезпеки використовують ШІ, незважаючи на труднощі

Незважаючи на незаперечні переваги ШІ в кібербезпеці, звіт також проливає світло на деякі виклики та побоювання в галузі. Хоча 69% компаній вважають штучний інтелект незамінним компонентом свого арсеналу кібербезпеки, 85% фахівців із кібербезпеки визнають, що широке впровадження штучного інтелекту призвело до сплеску кіберзлочинності.

У світлі ескалації кіберзагроз, яким сприяє ШІ, користувачів закликають залишатися пильними та вживати профілактичних заходів для захисту своїх цифрових активів. Бути в курсі останніх розробок у сфері кібербезпеки та підтримувати сучасні системи захисту є обов’язковими для пом’якшення ризиків, спричинених складними атаками, керованими ШІ.

Бути попереду: важливість профілактичних заходів

В епоху, коли домінує швидкий технологічний прогрес, профілактичні заходи мають першочергове значення, щоб випередити кіберсупротивників. Застосування надійних протоколів кібербезпеки, інвестиції в захисні механізми, керовані штучним інтелектом, і виховання культури обізнаності про кібербезпеку є необхідними кроками для зміцнення цифрової стійкості проти нових загроз». ***(James Kinoti. AI Revolutionizing Cybersecurity: Report Reveals Key Insights // Microsoft (https://www.msn.com/en-us/money/other/ai-revolutionizing-cybersecurity-report-reveals-key-insights/ar-BB1ia96S). 12.02.2024).***

***

«Як повідомляється, північнокорейські хакери використовують ChatGPT, щоб обманом змусити користувачів LinkedIn та інших платформ соціальних мереж надати конфіденційну інформацію та дані.

Материнська компанія ChatGPT OpenAI та інвестор Microsoft оголосили минулого тижня, що вони «перешкоджали п’яти пов’язаним з державою суб’єктам, які намагалися використовувати служби ШІ для підтримки зловмисної кібер-діяльності».

Використовуючи Microsoft Threat Intelligence, облікові записи, пов’язані з двома пов’язаними з Китаєм загрозливими суб’єктами, відомими як Charcoal Typhoon і Salmon Typhoon, афілійованим з Іраном загрозливим актором під назвою Crimson Sandstorm, пов’язаним з Північною Кореєю актором під назвою Emerald Sleet і пов’язаним з Росією актором відомі як Forest Blizzard, були ідентифіковані та припинені.

Microsoft, яка володіє LinkedIn, зазначила, що Емералд Сліт, також відомий як Кімсукі, видавав себе за «авторитетні академічні установи та неурядові організації, щоб спонукати жертв до відповіді експертами та коментарями щодо зовнішньої політики, пов’язаної з Північною Кореєю».

У своїй публікації в блозі вона заявила, що не знайшла доказів того, що ці суб’єкти здійснили будь-які значні кібератаки, але більшість її висновків є

«репрезентативними для супротивника, який вивчає варіанти використання нової технології».

OpenAI повідомила, що обліковий запис Північної Кореї Emerald Sleet використовував його послуги «для виявлення експертів і організацій, які зосереджені на питаннях оборони в Азіатсько-Тихоокеанському регіоні, розуміння загальнодоступних вразливостей, допомоги в базових завданнях сценаріїв і чернетки вмісту, який можна використовувати у фішингових кампаніях. »

Як північнокорейські хакери атакують LinkedIn

За даними Yonhap, державне розвідувальне агентство Південної Кореї виявило ознаки того, що Північна Корея намагалася включити генеративний штучний інтелект у свої хакерські атаки та іншу незаконну кібер-діяльність.

«Нещодавно було підтверджено, що північнокорейські хакери використовують генеративний штучний інтелект для пошуку хакерських цілей і технологій, необхідних для злому», — сказав журналістам старший чиновник Національної розвідувальної служби (NIS). NIS повідомила, що минулого року в середньому щодня фіксувалося 1,62 мільйона спроб злому в державному секторі Південної Кореї, що на 36% більше, ніж рік тому.

NIS додала, що її також підозрюють у використанні своїх закордонних IT-працівників для пошуку роботи в IT-компаніях для встановлення шкідливих кодів у програмне забезпечення, яке вони розробили в компаніях, для крадіжки криптовалют.

Ерін Плант, віце-президент із розслідувань у крипто-орієнтованій компанії з кібербезпеки Chainalysis, розповіла Financial Times, що «північнокорейські хакерські групи були помічені у створенні надійних профілів рекрутерів на професійних мережевих сайтах, таких як LinkedIn».

«Генеративний штучний інтелект допомагає спілкуватися в чаті, надсилати повідомлення, створювати зображення та нові ідентичності — усе те, що вам потрібно для побудови тісних стосунків із вашою метою», — додала вона.

OpenAI заявив, що його висновки узгоджуються із зовнішніми оцінками, вказуючи на те, що можливості GPT-4 у допомозі «зловмисним завданням

кібербезпеки» обмежені тим, що вже можна виконати за допомогою загальнодоступних інструментів, які не використовують ШІ.

Минулого року повідомлялося, що підтримувані Північною Кореєю хакери атакували клієнтів криптовалюти, проникаючи в системи американської компанії JumpCloud з корпоративного програмного забезпечення». ***(Suswati Basu. North Korean hackers use ChatGPT to scam Linkedin users // ReadWrite, INC (https://readwrite.com/north-korean-hackers-use-chatgpt-to-scam-linkedin-users/?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 19.02.2024).***

***

«Компанія Google, що належить Alphabet Inc., оголосила про ініціативу щодо надання інструментів штучного інтелекту та інвестицій для посилення онлайн-безпеки, оскільки нова технологія все частіше використовується як для захисту від кіберзлочинців, так і для їх вчинення.

Google представить новий ресурс з відкритим вихідним кодом на основі штучного інтелекту, який використовує ідентифікацію типу файлу для виявлення зловмисного програмного забезпечення, йдеться в заяві компанії в п’ятницю. Інструмент, який уже використовується для захисту продуктів, включаючи Gmail і Google Drive, буде доступний безкоштовно.

У п’ятницю на Мюнхенській конференції з безпеки в Німеччині компанія також оприлюднить білий документ, у якому детально описано, як вона використовує штучний інтелект для кіберзахисту, і в якому пропонується політичний порядок денний, який вимагає передових досліджень штучного інтелекту та огорожі для автономного кіберзахисту.

«Наша Ініціатива кіберзахисту штучного інтелекту змінює «дилему захисника», коли захисники мають бути праві весь час, а зловмисники мають бути праві лише один раз», — сказав у заяві Кент Вокер, президент Alphabet з глобальних питань. «Щоб зберегти імпульс, нам потрібна політика, яка одночасно зменшує ризики та використовує можливості ШІ».

Google також оголосила про додаткові інвестиції в дослідницькі гранти та партнерства для просування дослідницьких ініціатив у сфері кібербезпеки з використанням штучного інтелекту та розширення семінарів з кібербезпеки, включаючи модулі, орієнтовані на штучний інтелект.

Хакери також інтегрують штучний інтелект у свої кібероперації. Відповідно до звіту Microsoft Corp. цього тижня, фінансовані державою кримінальні групи використовують великі мовні моделі, такі як ChatGPT OpenAI, щоб покращити свої стратегії та вирішити технічні проблеми». ***(Agatha Cantrill. Google to provide AI cyber tools, investments to bolster online security // Business Standard Private Ltd. (https://www.business-standard.com/technology/tech-news/google-to-provide-ai-cyber-tools-investments-to-bolster-online-security-124021600077_1.html). 16.02.2024).***

***

«Еойн Хінчі, генеральний директор Tines, розвіює побоювання щодо кібератак на основі штучного інтелекту, наголошуючи на більших перевагах для команд безпеки. Дізнайтеся, як використовувати ШІ як примножувач сили для захисту організації.

У сфері кібербезпеки розвиток штучного інтелекту викликав побоювання щодо «гонки озброєнь зі штучним інтелектом», коли хакери використовують технології та інструменти на основі штучного інтелекту для здійснення більш складних і успішних атак.

Це може створити гарні заголовки — не кажучи вже про дуже ефективну маркетингову стратегію для постачальників програмного забезпечення для безпеки — але розповідь не зовсім відповідає дійсності. Штучний інтелект справді може надати хакерам нові інструменти для гри, але правда полягає в тому, що ШІ приносить набагато більше користі захисникам безпеки, ніж зловмисникам.

Чому AI пропонує обмежені переваги для зловмисників

Це правда, що штучний інтелект може допомогти хакерам розробити трохи краще шкідливе програмне забезпечення або методи соціальної інженерії. Однак також варто пам’ятати, що зловмисники успішно отримували доступ до систем задовго до появи штучного інтелекту і що традиційні вектори атак, як-от фішинг,

залишаються дуже ефективними. Люди все ще натискають фішингові листи. Той факт, що погані актори створюють трохи кращі електронні листи за допомогою ШІ, не змінить баланс сил різко.

Головні проблеми хакерів – це не проблеми, які ШІ може легко вирішити. Націлювання на потрібних жертв і збереження доступу до системи потребують обману та скритності, що алгоритмам важко знайти. Штучний інтелект може запропонувати зловмисникам деякі нові трюки, але це радикально не змінить їхню гру, роблячи її в кращому випадку поступовою перевагою.

Вирішуємо завдання «Голка в стозі сіна».

Як зазначено у звіті Voice of the SOC за 2023 рік, групи безпеки стикаються з величезним тиском, оскільки ландшафт загроз зростає, а бюджети та ресурси скорочуються. З петабайтами інформації, що надходять щодня, вручну переглядати журнали та сповіщення та виявляти аномалії, що ховаються в них, надзвичайно складно та займає багато часу.

ШІ має унікальні можливості, щоб допомогти в цьому. Завдяки машинному навчанню системи штучного інтелекту можна навчити швидко й масштабно очищати дані безпеки, виявляти закономірності та аномалії за частку часу, який знадобиться людині-аналітику. Це не тільки допомагає організаціям швидше виявляти та зменшувати ризики, але й звільняє фахівців із безпеки, щоб зосередитися на найбільш актуальних загрозах, полегшуючи ефективний розподіл ресурсів.

Економія часу була очевидною для Сніжинки. У міру того, як хмара даних зростала, виявлення, аналіз і усунення загроз ставали неймовірно громіздкими, оскільки кількість сповіщень зростала разом із кількістю співробітників і систем, які їм потрібно було захистити. Внутрішнє озеро даних безпеки Snowflake містило всю необхідну інформацію для дослідження сповіщень безпеки, але підключення відповідних даних здійснювалося вручну.

Команда реагування на інциденти Snowflake звернулася до автоматизації, щоб керувати зростаючою кількістю сповіщень у своєму середовищі. Створивши

внутрішній робочий процес керування справами, Snowflake зменшив кореляцію сповіщень вручну на 91,4% і заощадив близько десяти робочих годин на день.

Повернення часу завдяки автоматизації

Багато функцій SOC, які страждають від повторюваних завдань, є основними кандидатами на автоматизацію. Штучний інтелект легко впорається з такими кроками, як оновлення квитків, відповіді на типові запити та впровадження оновлень, а автоматизація цих процесів дозволяє аналітикам безпеки перенаправляти свою енергію на більш стратегічну, цінну роботу.

У звіті Voice of the SOC за 2023 рік фахівці з безпеки назвали те, що їх найбільше розчарувало, витрачаючи час на ручну роботу. Якби вони могли автоматизувати частину цієї роботи, групи безпеки приділяли б більше часу дослідженню та оцінюванню нових інструментів, розробці вдосконалених правил виявлення та інтеграції більшої кількості систем і журналів. Вражаючі 93% респондентів погодилися, що автоматизація на робочому місці покращить баланс між роботою та особистим життям.

Візьміть цей приклад. До недавнього часу команда InfoSec у програмній компанії майже не проводила автоматизацію, а будь-яка автоматизація, яку вони впроваджували, робилася вручну за допомогою Python. Потім вони створили один автоматизований робочий процес для розгортання оновлень багатофакторної автентифікації (MFA), а інший – для виявлення активності з некерованих IP-адрес.

Їх автоматизований процес розслідування попереджень і сортування обробив той самий обсяг роботи, який зайняв би 93 дні раніше. Автоматизація дозволяє команді проводити дослідження, які були б неможливі без технології. За оцінками компанії, автоматизація зараз виконує роботу щонайменше трьох штатних працівників.

AI також може допомогти зробити інструменти кібербезпеки більш зручними для користувачів. Такі досягнення, як великі мовні моделі (LLM), змінюють те, як системи безпеки розуміють і обробляють пов’язану з безпекою інформацію, усуваючи потребу в тому, щоб спеціалісти з безпеки були експертами з кодування або володіли унікальними мовами запитів окремих інструментів безпеки.

У міру розвитку LLM вони зможуть інтерпретувати проблеми безпеки, описані природною мовою, що дозволить фахівцям-практикам автоматизувати роботу за допомогою чогось такого простого, як інтерфейс чату. Завдяки стандартизації та спрощенню цих процесів ШІ робить інструменти безпеки більш доступними для ширшого кола співробітників у компанії, дозволяючи людям з різним рівнем технічного досвіду брати участь і робити свій внесок у заходи безпеки організації.

Бачити крізь FUD

Існують законні побоювання щодо штучного інтелекту та того, як зловмисники можуть його використовувати. Отже, важливо не захоплюватися страхом, невпевненістю та сумнівами (FUD) щодо того, наскільки це підвищує ставку. Якщо відбувається «гонка озброєнь штучного інтелекту», команди безпеки виграють її.

Зазвичай хакери шукають шлях найменшого опору, який передбачає використання людської поведінки та психології — те, на що сучасний ШІ не дуже добре оснащений. Варто також зазначити, що більшість порушень безпеки продовжують успішно справлятися без штучного інтелекту і що проблеми, з якими стикаються хакери, залишаючись непоміченими, не можуть бути вирішені лише штучним інтелектом.

На протилежній стороні таблиці ШІ представляє реальний множник сили. Усуваючи обмеження, які колись обмежували потенціал захисників, штучний інтелект значно покращує аналітичні та оперативні можливості центрів безпеки та дає змогу командам безпеки зосередитися на найважливіших частинах своєї роботи. У цьому відношенні штучний інтелект справді кардинально змінює правила кібербезпеки, але для захисників, а не для зловмисників». ***(Eoin Hinchy. How AI Empowers Cybersecurity Defenders From Hackers // Spiceworks Inc. (https://www.spiceworks.com/tech/artificial-intelligence/guest-article/how-ai-empowers-cybersecurity-defenders-from-hackers/). 21.02.2024).***

***

«Згідно з новим опитуванням Міжнародного консорціуму сертифікації безпеки інформаційних систем більшість фахівців з кібербезпеки (88%) вважають, що ШІ суттєво вплине на їх роботу; і лише 35% респондентів вже бачили вплив штучного інтелекту на їхні робочі місця. Вплив не обов'язково є позитивним чи негативним, а скоріше показником того, що спеціалісти з кібербезпеки очікують зміни своєї роботи. Крім того, виникло занепокоєння щодо дипфейків, дезінформації та атак соціальної інженерії. Опитування також охоплювало політику, доступ і регулювання.

Як штучний інтелект може вплинути на завдання спеціалістів із кібербезпеки

Респонденти опитування загалом вважають, що ШІ зробить роботу в сфері кібербезпеки більш ефективною (82%) і звільнить час для більш цінних завдань, подбавши про інші завдання (56%). Зокрема, штучний інтелект і машинне навчання можуть взяти на себе ці аспекти роботи в сфері кібербезпеки:

Аналіз моделей поведінки користувачів (81%).

Автоматизація повторюваних завдань (75%).

Моніторинг мережевого трафіку та виявлення шкідливих програм (71%).

Передбачити, де можуть статися порушення (62%).

Виявлення та блокування загроз (62%).

Опитування не обов'язково оцінює відповідь «ШІ зробить деякі частини моєї роботи застарілими» як негативну; натомість це розглядається як підвищення ефективності.

Основні проблеми кібербезпеки ШІ та можливі наслідки

З точки зору атак на кібербезпеку, опитаних професіоналів найбільше хвилювали:

Діпфейки (76%).

Дезінформаційні кампанії (70%).

Соціальна інженерія (64%).

Поточна відсутність регулювання (59%).

Етичні проблеми (57%).

Порушення конфіденційності (55%).

Ризик отруєння даних, навмисного чи випадкового (52%).

Опитана спільнота суперечила щодо того, що штучний інтелект буде кращим для кібер-зловмисників чи захисників. На запитання про твердження «ШІ та ML приносять більше користі фахівцям з кібербезпеки, ніж злочинцям», 28% погодилися, 37% не погодилися, а 32% не впевнені.

З опитаних професіоналів 13% сказали, що вони впевнені, що можуть остаточно пов’язати зростання кіберзагроз за останні шість місяців з ШІ; 41% сказали, що вони не можуть встановити остаточний зв’язок між ШІ та зростанням загроз. (Обидві ці статистичні дані є підмножинами групи з 54%, які сказали, що спостерігали значне зростання кіберзагроз за останні шість місяців.)

Зловмисники можуть скористатися перевагами генеративного штучного інтелекту, щоб розпочати атаки зі швидкістю та обсягом, які неможливо досягти навіть великій команді людей. Однак досі незрозуміло, як генеративний ШІ вплинув на ландшафт загроз.

Постійно: впровадження політик ШІ та доступ до інструментів ШІ в бізнесі

Лише 27% респондентів опитування ISC2 сказали, що їхні організації мають офіційну політику щодо безпечного та етичного використання ШІ; ще 15% сказали, що їхні організації мають офіційну політику щодо захисту та розгортання технології штучного інтелекту. Більшість організацій все ще працюють над розробкою політики використання ШІ того чи іншого типу:

39% компаній респондентів працюють над політикою етики ШІ.

38% компаній респондентів працюють над політикою безпечного та надійного розгортання ШІ.

Опитування виявило дуже широкий спектр підходів до надання співробітникам доступу до інструментів ШІ, зокрема:

Моя організація заблокувала доступ до всіх генеративних інструментів ШІ (12%).

Моя організація заблокувала доступ до деяких генеративних інструментів ШІ (32%).

Моя організація надає доступ до всіх генеративних інструментів ШІ (29%).

У моїй організації не було внутрішніх дискусій щодо дозволу чи заборони генеративних інструментів ШІ (17%).

Я не знаю підходу моєї організації до генеративних інструментів ШІ (10%).

Запровадження штучного інтелекту все ще триває і, безсумнівно, зміниться значно більше, оскільки ринок росте, падає або стабілізується, а фахівці з кібербезпеки можуть бути в авангарді обізнаності щодо генеративних проблем штучного інтелекту на робочому місці, оскільки він впливає як на загрози, на які вони реагують та інструменти, які вони використовують для роботи. Незначна більшість опитаних фахівців з кібербезпеки (60%) заявили, що вони впевнені, що зможуть очолити розгортання ШІ у своїй організації…

Як слід регулювати генеративний ШІ

Способи регулювання генеративного штучного інтелекту значною мірою залежатимуть від взаємодії між державним регулюванням і основними технологічними організаціями. Чотири з п’яти респондентів опитування сказали, що вони «бачать явну потребу в комплексних і конкретних правилах» щодо генеративного ШІ. Яким чином це регулювання може бути здійснено, є складним питанням: 72% респондентів погодилися з твердженням, що різні типи ШІ потребуватимуть різних правил.

63% сказали, що регулювання штучного інтелекту має відбуватися завдяки спільним зусиллям уряду (забезпечення стандартизації через кордони).

54% сказали, що регулювання штучного інтелекту має здійснюватися національними урядами.

61% (опитаних в окремому питанні) хотіли б, щоб експерти зі штучного інтелекту об’єдналися, щоб підтримати зусилля з регулювання.

28% підтримують саморегулювання приватного сектора.

3% хочуть зберегти нинішнє нерегульоване середовище.

Методологія ISC2

Опитування було розповсюджено серед міжнародної групи з 1123 фахівців з кібербезпеки, які є членами ISC2, у період з листопада по грудень 2023 року.

Сьогодні визначення «ШІ» іноді може бути невизначеним. Хоча у звіті використовуються загальні терміни «штучний інтелект» і машинне навчання, предмет описується як «широкодоступні мовні моделі», такі як ChatGPT, Google Gemini або Meta's Llama, зазвичай відомі як генеративний штучний інтелект». ***(Megan Crouse. ISC2 Research: Most Cybersecurity Professionals Expect AI to Impact Their Jobs // TechnologyAdvice (https://www.techrepublic.com/article/isc2-cybersecurity-ai-survey/). 22.02.2024).***

***

«Федеральна комісія зі зв'язку (FCC) планує 14 березня створити добровільну програму маркування кібербезпеки для бездротових споживчих продуктів IoT.

Згідно з програмою, кваліфіковані споживчі інтелектуальні продукти, що відповідають стандартам кібербезпеки, матимуть маркування, включно з новим «Знак кібердовіри США», що допоможе споживачам приймати обґрунтовані рішення про покупку, відрізняти надійні продукти на ринку та створюватиме стимули для виробників відповідати вищим вимогам. стандарти кібербезпеки.

Відповідні продукти можуть включати домашні камери безпеки, пристрої для покупок із голосовою активацією, підключені до Інтернету пристрої, фітнес-трекери, пристрої для відкривання дверей гаража та радіоняні.

Вирішення проблем безпеки

Програма з'являється, оскільки ринок споживчих продуктів IoT, які спілкуються через бездротові мережі, продовжує зростати. Ці продукти складаються з різних пристроїв і базуються на багатьох технологіях, кожна з яких представляє власний набір проблем безпеки.

«Розумні продукти можуть зробити наше життя набагато зручнішим, але вони можуть… становити загрозу безпеці та конфіденційності», — сказала голова правління Джессіка Розенворсел у заяві для преси 21 лютого.

«Ця програма полегшить споживачам вибір безпечніших інтелектуальних продуктів для своїх домівок, заохотить компанії відповідати вищим стандартам кібербезпеки та зміцнить екосистему для підключених продуктів».

Деталі програми

Правила програми, за які має проголосувати повний склад комісії, включають:

Логотип US Cyber Trust Mark, який з'являтиметься на бездротових споживчих продуктах IoT, які відповідають базовим стандартам кібербезпеки;

Логотип супроводжуватиметься QR-кодом, який споживачі зможуть сканувати, щоб отримати докладну інформацію про безпеку продукту, включаючи гарантований мінімальний період підтримки для продукту та автоматичні виправлення програмного забезпечення та оновлення безпеки;

Добровільна програма спиратиметься на державно-приватну співпрацю, при цьому FCC забезпечуватиме нагляд, а затверджені сторонні адміністратори етикеток керуватимуть такими діями, як оцінка заявок на продукт, дозвіл на використання етикетки та навчання споживачів; і

Тестування на відповідність проводиться акредитованими лабораторіями.

Цей крок з боку Федеральної комісії з зв'язку (FCC) стався тому, що лише за перші шість місяців 2021 року було зафіксовано понад 1,5 мільярда атак на пристрої IoT, згідно з оцінкою третьої сторони. Інші оцінюють, що до 2030 року буде працювати понад 25 мільярдів підключених пристроїв IoT.

Державне, приватне партнерство

Програма маркування кібербезпеки базується на роботі державного та приватного секторів, яка вже триває з кібербезпеки та маркування IoT, підкреслюючи важливість постійного партнерства, щоб споживачі могли насолоджуватися перевагами цієї технології з більшою впевненістю та довірою, за словами представників FCC.

У серпні минулого року комісія запропонувала та запитала коментарі щодо розробки добровільної програми маркування кібербезпеки для IoT. На основі цього запису була розроблена програма, за яку голосуватимуть наступного місяця.

«Подібно до того, як програма ENERGY STAR навчала громадськість і створювала стимули для виробників пропонувати більш енергоефективні прилади, наша програма маркування кібербезпеки проклала б шлях зробити те саме з

розумними продуктами», — сказав Розенворсель». ***(James Hickey. U.S. Cyber Trust Mark Program would help consumers make informed purchasing decisions and encourage manufacturers to meet higher cybersecurity standardsc // Emerald X, LLC. (https://www.rfidjournal.com/u-s-government-advances-plan-for-cybersecurity-labeling-program-for-smart-products). 23.02.2024).***

***

«Дослідники з Іллінойського університету в Урбані-Шампейні виявили, що нову версію чат-бота GPT-4 від OpenAI можна використати для злому ШІ. Це може будь-яку людину перетворити на хакера, передає New Scientist.

Модель штучного інтелекту (ШІ) GPT-4 здатна зламувати вебсайти й красти інформацію з онлайн-баз даних без допомоги людини. Учені кажуть, що будь-який користувач, який не має досвіду кібератак, може використовувати ШІ для злому.

«Вам не потрібно нічого розуміти — ви можете просто попросити чат-бот зламати сайт», — прокоментував один із авторів дослідження Деніел Канг.

Канг і його колеги хотіли подивитися, наскільки добре GPT-4 й інші великі мовні моделі, які зазвичай використовуються в службах чат-ботів, можуть працювати як «автономні хакери». Вони вирішили протестувати 10 різних моделей ШІ, зокрема GPT-4 та GPT-3.5 від OpenAI, а також моделі з відкритим вихідним кодом, як-от LLaMA від Meta. Дослідники використовували легкодоступні модифіковані версії, призначені для розробників застосунків на базі ШІ, які можуть взаємодіяти з веббраузерами, читати документи про загальні принципи вебхакінгу та планувати злом.

Навчені AI-боти зробили 15 спроб злому сайтів — від простих до складних. Водночас вони не володіли жодною інформацією про конкретні вразливості. Завдання перед ними стояло таке: отримання несанкціонованого доступу до онлайн-бази даних із використанням шкідливого коду SQL (SQL — мова програмування для зберігання й обробки інформації в певних базах даних, — ред.). За умовами завдання чат-боти могли маніпулювати вихідним кодом JavaScript для крадіжки інформації в користувачів веб-сторінок.

Більшість моделей повністю провалилися, але GPT-4 впорався з 11 з 15 завдань (73% успіху) та навіть виявив реальну вразливість на сайті, хоча таке завдання йому й зовсім не ставили.

За словами Канга, одна спроба злому обійдеться користувачеві в 10 доларів, тоді як залучення експерта з кібербезпеки обійдеться у 80 доларів за одну спробу.

Канг і його колеги поділилися своїми висновками з компанією-розробником OpenAI.

«Результати незалежного дослідження просто разючі, особливо на тлі нещодавньої заяви OpenAI та Microsoft про те, що їхні ШІ-моделі «мають у своєму розпорядженні лише обмежені можливості», стверджуючи, що боти не становлять жодної небезпеки, — каже Джессіка Ньюман із Каліфорнійського університету в Берклі. — Розбіжність між цими висновками наголошує на необхідності незалежного оцінювання реальної шкоди, на яку здатен ШІ»…» ***(Ірина Рефагі. Chat GPT-4 може будь-яку людину перетворити на хакера: ось як це відбувається // Фокус (https://focus.ua/uk/digital/628942-chat-gpt-4-mozhe-bud-yaku-lyudinu-peretvoriti-na-hakera-os-yak-ce-vidbuvayetsya). 23.02.2024).***

***

Кіберзлочинність та кібертероризм

«Веб-сайт агентства судів штату Пенсільванія зазнав кібератаки, яка, здається, не скомпрометувала жодних даних, але призвела до вимкнення деяких онлайн-систем, повідомили чиновники в неділю ввечері.

Провідне агентство з кібербезпеки федерального уряду, Міністерство внутрішньої безпеки США та ФБР розслідували напад, заявила голова Верховного суду Дебра Тодд у заяві.

Вона назвала це кібератакою «відмова в обслуговуванні», використовуючи опис федерального уряду, коли зловмисники «заповнюють цільовий хост або мережу трафіком, доки ціль не зможе відповісти або просто вийде з ладу, перешкоджаючи доступу для законних користувачів».

Судове агентство, Адміністративний офіс судів Пенсільванії, не відразу ідентифікувало нападників або мотив. Агентство також не повідомило, чи спрацювали його заходи з кібербезпеки, чи вимагали зловмисники гроші чи викуп.

Серед вимкнених онлайн-систем було використання онлайн-документів та електронного порталу подання документів у справі.

Суди штату залишалися відкритими, сказала Тодд». ***(Pennsylvania Statewide Court Agency's Website Hit by Disabling Cyberattack, Officials Say // U.S. News & World Report L.P. (https://www.usnews.com/news/best-states/pennsylvania/articles/2024-02-05/pennsylvania-statewide-court-agencys-website-hit-by-disabling-cyberattack-officials-say?utm_source=flipboard&utm_content=seanjkernan%2Fmagazine%2FUS+News). 05.02.2024).***

***

«Витончені шахрайства заполонили повсякденне життя. За даними Федеральної торгової комісії, шахрайство в соціальних мережах із січня 2021 року по червень 2023 року коштувало споживачам 2,7 мільярда доларів США, тоді як шахрайство на веб-сайтах і в додатках призвело до збитків у 2 мільярди доларів.

Мандрівники мають багато недоліків: фальшиві готелі/житло, маркетинг «безкоштовної відпустки», скасовані рейси та бронювання, а також путівки на відпустку від нелегальних компаній. Виявляти шахрайство стає все важче, і стало відомо, що один із найбільших у світі сайтів бронювання готелів може не застрахований від шахраїв.

Протягом останнього року Booking.com викликає критику споживачів через відсутність заходів безпеки для захисту користувачів від шахрайства. Користувачі TikTok стверджують, що хитромудрі електронні листи та повідомлення з офіційного порталу виманюють у людей сотні доларів, і стати їх жертвами стає все частіше.

Що відбувається?

Booking.com наполягає, що його не зламали, але хакери націлені на окремі готелі, які використовують портал. Booking.com попереджає своїх готельних партнерів, що зловмисники використовують фішингові методи, щоб отримати доступ до даних гостей. Фішинг — це кібератака, за допомогою якої хакери видають себе за когось іншого, щоб викрасти дані.

«Шахраї можуть спробувати імітувати наші електронні листи, щоб підманити ваше ім'я користувача та пароль з метою заволодіння вашим обліковим записом. Ці фішингові електронні листи можуть привести до веб-сторінки, яка виглядає дуже схожою на сторінку входу в екстранет Booking.com, але якщо ви подивіться на адресний рядок URL-адреси, ви помітите відмінності», — пояснює Booking.com у своєму попередженні». ***(Apeksha Bhateja. Hackers Are Targeting You Via Your Hotel Bookings With a Major Scam // fodors (https://www.fodors.com/news/news/hackers-are-targeting-booking-com-with-a-sophisticated-scam-heres-what-you-need-to-know?utm_source=flipboard&utm_content=mhartley2012%2Fmagazine%2FCYBER%3A+Privacy%2C+Crime%2C+%26+Security). 01.02.2024).***

***

«Кенійські фірми та приватні особи стикалися зі все більш ворожим онлайн-середовищем, оскільки напади з боку кіберзлочинців зросли до високого рівня за три місяці до грудня минулого року.

У новому звіті Управління зв'язку Кенії (CA) показано, що кіберзагрози, виявлені Координаційним центром реагування на комп'ютерні інциденти Кенії (Ke-CIRT/CC), зросли на 943 відсотки.

За словами CA, це сталося завдяки збільшенню можливостей локального моніторингу та відсічі загроз, а також через обмежені інвестиції в кібербезпеку та застарілі системи безпеки.

Незважаючи на різке зростання кількості загроз, фірми, здається, не надто обережно повідомляють про атаки, оскільки, за даними CA, кількість запитів на розслідування впала на 10 відсотків.

«Протягом тримісячного періоду з жовтня по грудень 2023 року Національний KE-CIRT/CC виявив понад 1,29 мільярда подій кіберзагрози, що становить 943,01 відсотка збільшення порівняно з 123 мільйонами подій загрози, виявлених у попередній період (з липня по вересень). 2023).

«Це експоненціальне зростання пов’язано з розширенням наших можливостей моніторингу кіберзагроз і існуванням уразливих систем через неправильну конфігурацію системи», — йдеться в звіті CA про кібербезпеку за квартал до грудня.

«Крім того, збільшення використання «вразливостей системи» також узгоджується з глобальними тенденціями та пов’язане з глобальним сплеском розгортання та використання пристроїв Інтернету речей (IoT), які за своєю суттю є небезпечними».

Найбільш поширеними були атаки з неправильною конфігурацією системи, за допомогою яких хакери намагалися отримати доступ – іноді успішно – до систем організацій, у тому числі державних установ, кількість яких становила 1,27 мільярда.

«Більшість атак були спрямовані на організації в секторі ІКТ. Зловмисники націлилися на сервери баз даних, операційні системи та інфраструктуру, що належать різним постачальникам послуг Інтернету (ISP) і хмарні служби», — заявили в CA.

«Більшість зловмисників використовували вразливості в застарілих операційних системах і витік облікових даних користувача.

«Експоненціальне зростання використання вразливостей системи, що є вектором, який протягом тривалого часу використовувався акторами кіберзагроз, можна пояснити поширенням пристроїв IoT, які за своєю суттю є небезпечними».

Також на 89,6 відсотка зросла кількість атак грубої сили, які в основному були націлені на сектор ІКТ та державні системи.

За даними CA, зловмисники націлилися на облікові дані користувача та сервери баз даних, що належать державним організаціям і хмарним службам.

Більшість зловмисників використовували вразливості в протоколі віддаленого робочого столу та облікових даних користувача.

Протягом кварталу на 94 відсотки зросла кількість атак, спрямованих на мобільні додатки, націлені на мобільні пристрої, такі як телефони та смарт-телевізори (Android).

«Винуватці цих атак в основному прагнули викрасти конфіденційні дані користувача, такі як ідентифікаційна інформація, облікові дані для входу та фінансові дані, для зловмисних цілей», — заявили в CA щодо атак, спрямованих на мобільні пристрої, додавши, що для мінімізації атак користувачі повинні вимкнути Android Debug Bridge (ADB). на своїх пристроях, завантажувати програми з надійних джерел, перевіряти дозволи програм і підтримувати програмне забезпечення в актуальному стані.

Запити на цифрові розслідування, отримані Ke-CIRT, зменшилися на 10 відсотків». ***(Macharia Kamau. Cyber attacks increase tenfold on outdated security systems // The Standard Group PLC. (https://www.standardmedia.co.ke/business/business/article/2001489817/cyber-attacks-increase-tenfold-on-outdated-security-systems). 09.02.2024).***

***

«Поки публічна бібліотека Торонто поступово працює над відновленням повноцінного обслуговування після жахливої жовтневої кібератаки, експерти попереджають, що громадські організації повинні знайти способи зміцнити свій захист від програм-вимагачів, незважаючи на обмежені ресурси.

Через кілька місяців після атаки на бібліотеку ще одна міська установа зазнала цифрового зламу: минулого місяця зоопарк Торонто оголосив, що особисту інформацію його нинішніх, колишніх і пенсіонерів співробітників було викрадено.

У зоопарку заявили, що зловмисники отримали доступ до інформації про минулі доходи, номера соціального страхування, дати народження, номери телефонів і адреси співробітників ще з 1989 року.

Мережа місцевих бібліотек і міський зоопарк можуть не відразу здатися головними цілями для глобальної індустрії програм-вимагачів, але один експерт сказав, що вони можуть багато чого запропонувати потенційним зловмисникам.

Чарльз Фінлей, виконавчий директор Rogers Cybersecure Catalyst з Університету Торонто Метрополітен, сказав, що громадські організації є хорошими цілями, оскільки вони зберігають значні обсяги особистих даних співробітників і тому, що платники податків очікують від них відкритості та функціонування.

Громадські організації «не зможуть залишатися без роботи дуже довго, і це дає можливість зловмисникам-вимагачам вимагати (платежі)», — сказав він. «Зловмисники вважають, що ці організації мають ресурси для сплати значних викупів».

Немає жодних ознак того, що бібліотека заплатила викуп, але відновлення послуг було кропітким процесом.

У заяві, опублікованій у понеділок, більш ніж через три місяці після нападу, Публічна бібліотека Торонто заявила, що починає повертати книги на полиці, але її каталог і особисті облікові записи, ймовірно, залишаться в автономному режимі до кінця цього місяця.

Здається, що напад на зоопарк завдав значно меншої шкоди з точки зору операцій, але зоопарк запропонував усім потенційно постраждалим нинішнім і колишнім співробітникам безкоштовну дворічну послугу кредитного моніторингу як «проактивний крок».

Фінлей сказав, що для захисту від майбутньої шкоди державним організаціям необхідно застосовувати найкращі методи кібербезпеки, включаючи двофакторну автентифікацію, регулярні оновлення програмного забезпечення та паролів і не натискати посилання в електронних листах від ненадійних відправників.

Зловмисники швидко пристосовуються, і державні органи повинні розвиватися в міру зміни загроз, додав він.

«Програми-вимагачі — це багатомільярдна глобальна індустрія», — сказав він. «Це надзвичайно прибуткова галузь. Це дуже складна галузь із власними

ланцюгами поставок. Це галузь, яка впроваджує інновації дуже швидкими темпами.

«Якщо ви можете зробити це трішки дорожчим, трішки складнішим для банди програм-вимагачів успішно атакувати вашу організацію, вони підуть і шукатимуть щось інше», — сказав він.

Експерт з кібербезпеки Девід Шиплі з Beauceron Security у Фредеріктоні зазначив, що зловмисники зазвичай атакують у місцях, де вони не живуть, щоб зменшити ймовірність того, що їх переслідують правоохоронні органи.

«Більшість кіберзлочинців знають, що це дійсно безглуздо зламувати в тій самій юрисдикції, де ви живете, тому що саме тоді вас найімовірніше спіймають і притягнуть до відповідальності», — сказав він.

Кім Кроулі, відомий автор кібербезпеки, зазначив, що навіть корпораціям, які отримують значні прибутки, часто не вистачає бюджету на цифрову безпеку.

«Уявіть, що ви державна служба, яка існує не для отримання прибутку, як бібліотека», — сказала вона.

«Ці організації існують не для того, щоб заробляти гроші, тому може бути ще менше стимулів витрачати гроші на кібербезпеку. І тоді ви не можете навіть просто вирішити витрачати гроші на кібербезпеку, тому що тоді, якщо це буде оскаржено в бібліотечної ради чи в мерії?»

За її словами, громадські та громадські органи повинні об’єднати ресурси для посилення колективної оборони.

Міська влада Торонто нещодавно заявила, що планує об’єднати свої різні ради та агентства під єдину центральну IT-систему. Міська влада заявила, що ані зоопарк, ані бібліотека не були частиною його центральних IT-систем до недавніх атак, а також не підпадали під відповідальність Офісу головного спеціаліста з інформаційної безпеки.

Кроулі зазначив, що одна з проблем полягає в тому, що деякі особи, які приймають рішення, все ще вважають витрати на кібервитрати марною тратою грошей.

«Я сподіваюся, що це тривожний дзвінок для Публічної бібліотеки Торонто та інших організацій», - сказала вона. «Якщо вони не можуть дозволити собі керувати власним центром безпеки, вони можуть поділитися ним з іншими організаціями».

Цей звіт The Canadian Press було вперше опубліковано 14 лютого 2024 року». ***(Toronto library, zoo attacks show public bodies need to boost cybersecurity: experts // Microsoft (https://www.msn.com/en-ca/news/canada/toronto-library-zoo-attacks-show-public-bodies-need-to-boost-cybersecurity-experts/ar-BB1ig34n). 14.02.2024).***

***

«Швейцарська газета Aargauer Zeitung опублікувала статтю про те, як хакери зламали 3 млн електричних зубних щіток для атаки на сайт компанії. Проте ця новина виявилася фейком. Про це повідомляє Gizmodo.

Експерти з безпеки наголошують, що цей сценарій є нереалістичним, оскільки розумні зубні щітки підключаються до Bluetooth, а не до інтернету. Таким чином, використання їх для створення ботнету є малоймовірним. Компанія Fortinet, яка вважається провідною у сфері кібербезпеки, заявила, що журналісти з Aargauer Zeitung неправильно інтерпретували слова експертів, тому поширили неправдиву історію.

Висвітлення тем кібербезпеки може бути складним завданням, оскільки дослідники та компанії, що займаються безпекою, можуть мати свої інтереси, щоб залучити більше уваги. Газета, яка опублікувала цю неправдиву історію, звинуватила Fortinet у виникненні цієї ситуації, але Fortinet заперечує ці звинувачення, стверджуючи, що вони надали газеті деталі про атаку, але не стверджували її правдивість.

Раніше, 6 лютого, відповідний звіт представила міністр оборони Нідерландів Кайса Оллонгрен. Зауважимо, що це стало першим випадком, коли Нідерланди публічно приписують Китаю кібершпигунство. Спецслужби назвали це частиною тенденції китайського політичного шпигунства проти Нідерландів та їхніх союзників…» ***(Новина про злам 3 мільйонів зубних щіток для кібератак***

виявилася фейком // UA.NEWS (https://ua.news/ua/technologies/novyna-pro-zlam-3-miljoniv-zubnyh-shhitok-dlya-kiberatak-vyyavylasya-fejkom). 12.02.2024).

***

«…Дослідження, проведене комерційною страховою компанією NFU Mutual, показало, що 23 відсотки опитаних сказали, що вони або їхній бізнес зазнали кібератаки чи кібератак у 2023 році.

Опитування також підкреслило, що сім із кожних 10 підприємців стурбовані загрозою кіберзлочинності, яка вплине на них та їхній бізнес, причому 35 відсотків із них сказали, що вони «дуже стурбовані».

Незважаючи на те, що переважна більшість торговців були стурбовані кіберзлочинністю, 14 відсотків визнали, що вони байдужі або дуже байдужі, що спонукало комерційну страхову компанію закликати всіх у галузі не сприймати загрозу легковажно.

Джеймс Тревіс, кіберспеціаліст NFU Mutual, сказав: «Кіберзлочинність, на жаль, є постійно зростаючою загрозою для наших галузей – і торговці не відрізняються, – тому ми закликаємо босів і співробітників залишатися пильними та робити все можливе, щоб не стати жертвами.

«Важливо пам’ятати, що якщо ви будь-яким чином використовуєте цифрові технології для ведення свого бізнесу, ви потенційно наражаєтеся на загрози кібербезпеці, і наслідки можуть бути дуже серйозними.

«Від фінансового шахрайства та втрати доходу до репутаційної шкоди та навіть юридичної відповідальності, торговці повинні знати про кіберризики, з якими вони стикаються.

«Комерсанти є опорою наших спільнот, тому дуже важливо, щоб вони відчували свій захист і підтримку, якщо станеться найгірше».

NFU Mutual виділила наступні цифрові технології, які будуть під загрозою для торговців:

Використання ноутбуків і комп’ютерів, планшетів або мобільних телефонів для спілкування з клієнтами, замовлення матеріалів і бронювання вакансій.

Сервери або цифрові сховища для зберігання даних клієнтів і співробітників.

Веб-сайт для просування вашого бізнесу та бронювання робіт.

Використання онлайн-банкінгу для переказу коштів, придбання витратних матеріалів і отримання платежів від клієнтів.

Пристрої, підключені до Інтернету, такі як офісні комп'ютерні мережі, відеоспостереження та освітлення.

Щоб захистити ваш торговий бізнес, NFU Mutual рекомендує наступне:

Використовуйте надійні паролі, але важливо не використовувати однакові дані для входу чи паролі для кількох облікових записів і служб, завжди розділяйте особисті та бізнес-акаунти.

Застосуйте двоетапну перевірку (багатофакторна автентифікація) – це простий метод, який вимагає двох різних методів, щоб «підтвердити» вашу особу, перш ніж ви зможете використовувати службу, як правило, пароль плюс ще один метод, наприклад текстове повідомлення або відбиток пальця.

Переконайтеся, що все програмне забезпечення оновлено та регулярно оновлюється.

Щотижня створюйте резервні копії файлів і даних і зберігайте їх на окремому безпечному пристрої.

Розкажіть співробітникам про кіберзлочинність, зокрема про те, як виявляти потенційно небезпечні або шахрайські листи.

Встановіть брандмауер і антивірусне програмне забезпечення на всі пристрої компанії та оновлюйте їх.

Переконайтеся, що заводські паролі змінено, а обладнання налаштовано з урахуванням безпеки.

У відповідних випадках використовуйте віртуальну приватну мережу (VPN), коли надаєте співробітникам віддалений доступ до систем компанії. Переконайтеся, що це теж захищено двоетапною перевіркою.

Не нехтуйте фізичною безпекою – переконатися, що всі пристрої компанії надійно зберігаються та замикаються, коли вони не використовуються, так само важливо». ***(Alan Beresford. Firms urged to step up digital security measures as cyber threats rise // Highland News and Media Ltd. (https://www.forres-***

gazette.co.uk/news/businesses-urged-to-step-up-digital-security-measures-as-cyb-342877/). 21.02.2024).

***

«Оскільки кібератаки на нерухомість стають все більш витонченими, їх вплив на такі галузі, як нерухомість, не можна недооцінювати. Титульні компанії, які відіграють ключову роль у спрощенні операцій з нерухомістю, є основними цілями для таких атак, що потенційно може спричинити значні збої.

Застереження про форс-мажор звільняють сторони від відповідальності чи зобов'язань, коли надзвичайні, неконтрольовані події заважають їм виконувати договірні обов'язки. Однак класифікація кібератак як форс-мажорних обставин підлягає юридичному тлумаченню та вимагає детального та продуманого підходу до розробки контракту, щоб утримувати транзакції на потрібному рівні.

Чи є кібератака форс-мажором?

Застереження про форс-мажор звільняють сторони від відповідальності чи зобов'язань, коли надзвичайні, неконтрольовані події заважають їм виконувати договірні обов'язки. Традиційно до форс-мажорних обставин відносяться стихійні лиха, війни тощо. Оскільки ці положення можуть мати такий значний вплив на договірні відносини між сторонами, вони суворо тлумачаться судами Техасу. Після Covid-19 положення про форс-мажор викликали гострі судові суперечки та обговорення, оскільки багато з них не були складені належним чином, щоб покрити затримки через пандемію. Сьогодні зростає кількість аргументів щодо включення до цієї категорії кібератак, які впливають як на сторони, так і на сторони контракту, враховуючи їх непередбачуваний характер і потенціал суттєвого порушення операцій.

Кібератаки титульної компанії – чи єдині вони?

В останні місяці деякі з найбільших і найвідоміших титульних компаній зазнали серйозних кібератак. Ці інциденти спричинили збої в роботі через припинення функцій депонування, а також припинили можливість переказувати кошти, видавати виписки про розрахунки чи зобов'язання про право власності та мати доступ до електронної пошти. Ці атаки завадили покупцеві та/або продавцю

виконувати більшість угод купівлі-продажу. Крім того, зобов'язання щодо прав власності були відкладені після термінів, визначених у контракті, і, що ще гірше, закриття не могло відбутися через те, що компанії, що мають право власності, не мали доступу до систем депонування та фінансування.

Однак, хоча титульна компанія може укласти угоду купівлі-продажу для підтвердження отримання, вона насправді не є стороною самого контракту. Цей факт змусив багатьох покупців і продавців поспішати перечитувати положення про форс-мажор у своїх угодах купівлі-продажу, щоб визначити, чи ці атаки якимось чином покриваються, чи сторони будуть змушені вести переговори про внесення змін до свого контракту. Таким чином, ці атаки підкреслюють критичну потребу в надійних заходах кібербезпеки та ретельному складанні договірних умов для усунення таких ризиків.

Хоча титульні компанії мають вирішальне значення для придбання та відчуження нерухомості, вони не єдині сторони, на яких покладаються покупці та продавці, щоб здійснити закриття. Наприклад, щоб належним чином фінансувати закриття, титульні компанії повинні отримати сертифіковані кошти для закриття від відповідних фінансових установ. Якщо банк закрито через кібератаку, а позикодавець або продавець не може перерахувати сертифіковані кошти до титульної компанії для закриття протягом чіткого терміну, чи охоплює це питання положення про форс-мажор у контракті?

Висновок

Щоб забезпечити повний захист і ясність для всіх сторін, залучених до операції з нерухомістю, доцільно чітко включати кібератаки в положення про форс-мажорні обставини. Зверніться до свого адвоката, щоб вирішити це для вашої компанії.

Зростаюча поширеність кіберзагроз вимагає проактивного та детального підходу до розробки контрактів, особливо в галузях, уразливих до таких ризиків, як нерухомість. Включивши чіткі положення щодо кібератак у положення про форс-мажорні обставини, титульні компанії, покупці та продавці можуть створити чітку структуру для управління такими збоями. Однак дуже важливо поєднати ці

договірні засоби захисту з надійними заходами кібербезпеки, щоб зменшити ризик атак. Консультація юридичного радника має важливе значення, щоб переконатися, що положення про форс-мажор є вичерпним, пристосованим до конкретного контексту транзакції та відповідає відповідним правовим стандартам». ***(Tiffany Melchers and Camrii H. Alexcee. The Impact of Real Estate Cyber Attacks on Transactions // BoyarMiller (https://www.boyarmiller.com/the-impact-of-real-estate-cyber-attacks-on-real-estate-transactions/). 20.02.2024).***

***

«MGM Resorts International (MGM.N) повідомила, що державні та федеральні регулятори розслідують кібератаку на її системи, яка сталася у вересні і призвела до зниження результатів компанії в третьому кварталі на 100 мільйонів доларів.

Оператор казино має намір відповісти на запити в установленому порядку, йдеться в повідомленні MGM, опублікованому в п'ятницю.

У вересні Федеральне бюро розслідувань (ФБР) заявило, що розслідує атаку на MGM, яка призвела до відключення систем компанії після того, як в готелях Лас-Вегаса утворилися черги, а ігрові автомати почали показувати повідомлення про помилки.

Хакерська група AlphV заявила про причетність до злому.

Джерела повідомили Reuters у вересні, що AlphV працював з іншою організацією під назвою Scattered Spider, щоб зламати системи MGM і викрасти дані для вимагання.

Scattered Spider також стояв за інцидентом кібербезпеки в Caesars Entertainment (CZR.O), де було скомпрометовано багато даних учасників програми лояльності, включаючи їхні водійські права та номер соціального страхування, як повідомила компанія у вересні.

Caesars також отримав запити від державних регуляторів щодо атаки, йдеться в щоквартальній нормативній документації в жовтні». ***(MGM Resorts says regulators probing September cyberattack // Reuters***

(https://www.reuters.com/technology/cybersecurity/mgm-resorts-says-state-federal-regulators-probing-september-cyberattack-2024-02-23/). 23.02.2024).

***

«Trustwave, провідний постачальник послуг з кібербезпеки та керованої безпеки, опублікував комплексне дослідження, яке розкриває унікальні загрози кібербезпеці, з якими стикаються навчальні заклади. У звіті «2024 Education Threat Landscape: Trustwave Threat Intelligence Briefing and Mitigation Strategies» досліджуються специфічні галузеві ризики та надаються лідерам кібербезпеки в освітньому секторі практичні ідеї та стратегії для зміцнення свого захисту.

Системи початкової школи обробляють конфіденційні дані про неповнолітніх, тоді як вищі навчальні заклади повинні захищати дані інтелектуальної власності, що робить їх основними мішенями для кібератак. Ці атаки не лише загрожують безпеці викладачів і адміністраторів, але вони ставлять під загрозу конфіденційність студентів, персоналу та інших пов’язаних осіб.

Останні дослідження Trustwave SpiderLabs вивчають потік атак, які використовують групи загроз, проливаючи світло на їхню тактику, методи та процедури. Сектор освіти стикається зі значними ризиками кібербезпеки, починаючи від шахрайства з пропозиціями роботи, націлених на студентів, і закінчуючи критичним впливом мережевих пристроїв через уразливості загальнодоступних програм.

Корі Деніелс, директор з питань інформації та безпеки Trustwave, сказав: «Сектор освіти стикається з неймовірним викликом у навігації різноманітною та мінливою поверхнею атак із зростаючим фінансовим тиском, залишаючи мало місця для помилок, оскільки цифрові лідери прагнуть підтримувати стійкість до загроз.

«Дані про студентів, співробітників, випускників і викладачів є різними спокусами та мотивами для зловмисників, щоб зловмисно націлитися на навчальний заклад або пов’язаних з ним осіб. Наш останній брифінг щодо загроз служить життєво важливим ресурсом для кіберзахисників, надаючи їм практичну

інформацію щодо навігації щодо останніх загроз і засобів захисту їхніх студентів, співробітників і даних».

У звіті Trustwave SpiderLabs аналізуються групи загроз та їхні методи протягом усього циклу атаки, від початкового опору до вилучення. Кілька ключових висновків зі звіту включають:

Група загроз LockBit спричинила 30 відсотків інцидентів програм-вимагачів, націлених на сектор освіти.

Apache Log4j (CVE-2021-44228) продовжує залишатися найпоширенішою спробою експлойту проти навчальних закладів, на яку припадає 74 відсотки спроб.

Відомо значне виявлення критично важливих систем і пристроїв, зокрема 1,8 млн. пристроїв, пов'язаних із освітньою галуззю…» ***(New Trustwave SpiderLabs research exposes unique cybersecurity threats facing education industry // iTWire (https://itwire.com/guest-articles/guest-research/new-trustwave-spiderlabs-research-exposes-unique-cybersecurity-threats-facing-education-industry.html). 23.02.2024).***

***

«Щодня 30 000 сайтів стають жертвами хакерів. Хоча більшість атак спрямовані на малий бізнес, ніхто не застрахований від кібератак у сучасному оцифрованому світі. Багато в чому ваші особисті дані – це скарб, який зберігається у віртуальному сховищі. І як у фільмі про пограбування, кіберзлочинці постійно планують зламати ці сховища. Ось тут і з'являється концепція симуляції взлому та атаки (BAS), яка виступає як остаточна репетиція збереження ваших цифрових скарбів.

Що таке симуляція вторгнення та атаки?

Простіше кажучи, симуляція вторгнення та атаки — це як пожежна тренування для вашої системи онлайн-безпеки. У протипожежних тренуваннях ми моделюємо пожежу, щоб перевірити план евакуації в будівлі. Подібним чином BAS передбачає імітацію кібератак для перевірки захисту організації. Це проактивний підхід до кібербезпеки, коли ви не чекаєте справжньої атаки, щоб виявити слабкі місця вашої системи. Натомість BAS допомагає визначити та усунути ці

вразливості заздалегідь, як репетиція маршруту евакуації перед справжньою пожежею.

Потреба в симуляції прориву та атаки

Чому б не дотримуватися традиційних заходів кібербезпеки та/або посилити їх? Традиційні заходи безпеки, хоч і важливі, часто відстають у сучасному середовищі швидкого розвитку загроз.

Як згадувалося раніше, BAS — це не просто ще одна лінія захисту; це проактивна стратегія залишатися на крок попереду потенційних зловмисників. Інструменти BAS імітують різні кібератаки, перевіряючи захист організації в сценаріях реального часу. Від фішингу до розширених постійних загроз, ці симуляції виявляють слабкі місця в поточних налаштуваннях безпеки.

Цей проактивний підхід має вирішальне значення, оскільки він забезпечує перевірку реальності. Він показує не лише стан кібербезпеки організації, але й намічає шляхи для вдосконалення. По суті, BAS — це як внутрішній супротивник, який працює на вас і постійно кидає виклик вашому захисту, щоб переконатися, що він якомога надійніший.

Як працює симуляція вторгнення та атаки?

Процес починається з того, що інструменти BAS вибирають цілі у вашій системі – це може бути будь-що, від серверів електронної пошти до баз даних. Потім вони імітують різноманітні кібератаки на ці цілі, імітуючи стратегії, які використовують справжні хакери. Це схоже на футбольну команду, яка грає в бійку; вони намагаються з'ясувати, де їхній захист слабкий. Потім результати моделювання аналізуються, щоб оцінити, наскільки добре система відреагувала на атаки. Нарешті, на основі цих висновків оновлюються та вдосконалюються заходи кібербезпеки. Це безперервний цикл тестування, аналізу й удосконалення, що гарантує, що захист безпеки залишається надійним.

Відчутні переваги симуляції вторгнення та атаки

Найголовнішою перевагою використання симуляції зламу та атаки (BAS) є значне підвищення стійкості кібербезпеки. Постійно досліджуючи та тестуючи захисні механізми, BAS підтримує організації не просто підготовленими, а й

гнучкими. BAS також надає безцінні відомості про дотримання галузевих стандартів і правил, гарантуючи, що заходи безпеки організації є не тільки надійними, але й юридично надійними.

Ще однією важливою перевагою є економічна ефективність BAS. Загалом, інвестиції в інструменти моделювання можуть бути набагато дешевшими, ніж потенційні втрати від успішної кібератаки. Це може заощадити мільйони на контролі збитків, судових зборах і втраті довіри клієнтів. Це стратегічна інвестиція, яка створює міцну основу, здатну протистояти сьогоднішнім і завтрашнім штормам». ***(Amir Bakian. Breach and Attack Simulation: The Cybersecurity Fire Drill // Dallas Morning News (https://www.dallasnews.com/marketplace/contributor-content/2024/02/22/breach-and-attack-simulation-the-cybersecurity-fire-drill/). 22.02.2024).***

***

«Кібератаки обходяться світовій цифровій економіці понад 10,5 трильйонами доларів на рік. Кількість, яка зростатиме разом із зростанням кіберзлочинності. Хоча це жахливо, це ускладнюється тим, що компанії стикаються з величезною нестачею кадрів у сфері кібербезпеки. Виявляється, є місця, які потрібно заповнити. Посади, які вимагають навичок кібербезпеки.

Відповідно до результатів нещодавнього Kaspersky Cybersecurity Weekend, 41 відсоток компаній у всьому світі стикаються з нестачею кваліфікованих фахівців з кібербезпеки. Ця проблема є ще більш чутливою для регіону Близького Сходу, Туреччини та Африки (МЕТА), де 43 відсотки компаній мають брак персоналу. Найбільше бракує персоналу серед аналітиків зловмисного програмного забезпечення та дослідників інформаційної безпеки.

За даними Всесвітнього економічного форуму та ISC2 – провідної світової організації-члена професіоналів з кібербезпеки – світові терміново потрібні 4 мільйони експертів з кібербезпеки.

Оскільки частота та складність атак зростає, а попит на спеціалістів InfoSec у бізнесі зростає, кількість практиків, які відповідають вимогам компанії щодо навичок та рівня досвіду, зменшується. Дослідження, проведені компаніями з

кібербезпеки та міжнародними організаціями, вже підкреслили брак професіоналів InfoSec. Дослідження, проведене (ISC)2 cybersecurity workforce study, показало, що у 2022 році брак робочої сили становив майже 4 мільйони працівників InfoSec.

Опитування вказує на те, що «дефіцит навичок, відсутність спеціалістів InfoSec і збільшення кількості кіберзагроз створюють порочне коло. Ця проблема існує вже багато років: однак багато кіберпрофесіоналів стверджують, що розрив у навичках не зменшився. Стало ще гірше».

Розглядаючи потреби в кібербезпеці в різних галузях, державний сектор повідомив про найбільший попит на фахівців з кібербезпеки та визнав, що майже половина (46 відсотків) необхідних йому ролей InfoSec залишаються незаповненими. Сектори телекомунікацій і засобів масової інформації недоукомплектовані на 39 відсотків, за ними йдуть роздрібна та оптова торгівля та охорона здоров'я, де 37 відсотків посад залишаються вакантними.

«Щоб зменшити дефіцит кваліфікованих фахівців у сфері InfoSec, компанії пропонують високі зарплати, кращі умови праці та бонусні пакети, а також інвестують у сучасне навчання з використанням найновіших знань», — зазначив Володимир Дащенко, проповідник безпеки, ICS CERT, Kaspersky. «Однак результати досліджень показують, що цих заходів не завжди достатньо. Темпи зростання внутрішнього IT-ринку в деяких регіонах, що розвиваються, змінюються настільки швидко, що ринок праці не може виховати та навчити відповідних спеціалістів із необхідними навичками та досвідом у такі стислі терміни, додав він.

Щоб мінімізувати негативні наслідки дефіциту глобального персоналу кібербезпеки, експерти рекомендують наступне:

Використовуйте керовані послуги безпеки, щоб отримати додаткові знання без додаткового найму. Це допомагає захиститися від кібератак і розслідувати інциденти, навіть якщо в компанії не вистачає працівників служби безпеки.

Інвестуйте в додаткові курси з кібербезпеки для своїх співробітників, щоб вони були в курсі останніх знань. Професіонали InfoSec можуть вдосконалити свої навички та захистити свої компанії від атак.

Використовуйте інтерактивні тренажери, щоб перевірити свій досвід і оцінити спосіб мислення в критичних ситуаціях. Гейміфікація дозволяє спостерігати за тим, як ІТ-відділ компанії розгортає, розслідує та реагує на атаку та приймає життєво важливі рішення разом із головним героєм гри.

Використовуйте централізовані та автоматизовані рішення, щоб зменшити навантаження на команду ІТ-безпеки та мінімізувати ймовірність помилок. Завдяки агрегації та кореляції даних із кількох джерел в одному місці та використовуючи технології машинного навчання ці рішення забезпечують ефективне виявлення загроз і швидке автоматизоване реагування.

Дослідження «Портрет сучасного професіонала з інформаційної безпеки» було проведено за участю 1012 професіоналів InfoSec у 29 країнах Азіатсько-Тихоокеанського регіону, Європи, регіону МЕТА, Північної та Латинської Америки. Він оцінив поточний стан ринку праці та проаналізував точні причини дефіциту навичок кібербезпеки». ***(Carol Odero. Wanted: 4 Million Cybersecurity Experts // CIO Africa (https://cioafrica.co/wanted-4-million-cybersecurity-experts/). 26.02.2024).***

***

«У 2023 році кіберзлочинці побачили більше можливостей «увійти в систему» замість того, щоб зламати корпоративні мережі через дійсні облікові записи, що робить цю тактику кращою зброєю для загрозливих акторів, згідно з Індексом розвідки загроз X-Force IBM за 2024 рік.

Атаки на критичну інфраструктуру виявляють помилки галузі

У майже 85% атак на критичні сектори компрометацію можна було пом’якшити за допомогою виправлення, MFA або принципів із найменшими привілеями – це вказує на те, що те, що індустрія безпеки історично описувала як «базову безпеку», може бути важче досягти, ніж зображують.

Атаки програм-вимагачів на підприємства минулого року впали майже на 12%, оскільки великі організації відмовляються від оплати та дешифрування на користь відновлення своєї інфраструктури. У зв’язку з тим, що ця дедалі більша відмова може вплинути на очікування зловмисників щодо доходів від здирництва

на основі шифрування, було помічено, що групи, які раніше спеціалізувалися на програмному забезпеченні-вимагачі, звернулися до інфокрадіїв.

Аналіз X-Force передбачає, що коли одна генеративна технологія штучного інтелекту наближається до 50% частки ринку або коли ринок консолідується до трьох або менше технологій, це може викликати масштабні атаки на ці платформи.

«Хоча «основи безпеки» не викликають стільки голови, як «атаки, розроблені штучним інтелектом», залишається те, що найбільша проблема безпеки підприємств зводиться до основного та відомого, а не до нового та невідомого», – сказав Чарльз Хендерсон, глобальний менеджер Партнер IBM Consulting та керівник IBM X-Force. «Ідентифікація знову і знову використовується проти підприємств, проблема, яка погіршуватиметься, оскільки супротивники інвестуватимуть кошти в ШІ для оптимізації тактики».

Глобальна криза ідентичності наближається до загострення

Експлуатація дійсних облікових записів стала шляхом найменшого опору для кіберзлочинців, оскільки сьогодні в темній мережі доступні мільярди скомпрометованих облікових даних. У 2023 році X-Force спостерігав, як зловмисники дедалі більше інвестували в операції з отримання ідентифікаційних даних користувачів – на 266% зросла кількість зловмисних програм для крадіжки інформації, призначених для викрадення особистої інформації, як-от електронні листи, облікові дані соціальних мереж і програм для обміну повідомленнями, банківські реквізити, дані крипто-гаманця та більше.

Такий «простий вхід» для зловмисників важче виявити, що викликає дорогу реакцію з боку підприємств. Згідно з даними X-Force, серйозні інциденти, спричинені зловмисниками, які використовують дійсні облікові записи, були пов’язані з майже на 200% більш складними заходами реагування з боку команд безпеки, ніж середні інциденти – захисникам потрібно було розрізняти законну та зловмисну активність користувачів у мережі.

Насправді, у звіті IBM про вартість витоку даних за 2023 рік було встановлено, що для виявлення та відновлення зломів, спричинених викраденими

або скомпрометованими обліковими даними, потрібно приблизно 11 місяців – це найдовший життєвий цикл реагування, ніж будь-який інший вектор зараження.

Таке широке охоплення онлайн-активності користувачів стало очевидним у тому, що у квітні 2023 року ФБР та європейські правоохоронні органи ліквідували глобальний форум кіберзлочинців, на якому зібрано дані для входу понад 80 мільйонів облікових записів користувачів. Загрози на основі ідентифікації, ймовірно, продовжуватимуть зростати, оскільки зловмисники будуть використовувати генеруючий ШІ для оптимізації своїх атак. Уже у 2023 році X-Force спостерігав понад 800 000 публікацій про штучний інтелект та GPT на форумах темної мережі, підтверджуючи, що ці інновації привернули увагу та інтерес кіберзлочинців.

Зловмисники «входять» у мережі критичної інфраструктури

У всьому світі майже 70% атак, на які X-Force відповіла, були спрямовані на організації критичної інфраструктури. Це тривожний висновок, який підкреслює, що кіберзлочинці роблять ставку на те, що ці високоцінні цілі потребують безперебійної роботи для досягнення своїх цілей.

Майже 85% атак, на які X-Force відповіла на цей сектор, були спричинені використанням загальнодоступних програм, фішинговими електронними листами та використанням дійсних облікових записів. Останнє створює підвищений ризик для сектора, оскільки DHS CISA стверджує, що більшість успішних атак на державні установи, організації критичної інфраструктури та державні органи державного рівня у 2022 році включали використання дійсних облікових записів. Це підкреслює необхідність для цих організацій часто проводити стрес-тестування свого середовища на предмет потенційного впливу та розробляти плани реагування на інциденти.

Щоб кіберзлочинці бачили рентабельність інвестицій у свої кампанії, цільові технології мають бути повсюдними для більшості організацій у всьому світі. Подібно до того, як минулі технологічні механізми сприяли кіберзлочинній діяльності – як це спостерігалося з програмами-вимагачами та домінуванням на ринку Windows Server, шахрайством BEC та домінуванням Microsoft 365 або

криптозломом і консолідацією ринку інфраструктури як послуги – ця модель, швидше за все, поширюватиметься на ШІ.

X-Force оцінює, що після встановлення домінування на ринку генеративного ШІ – коли одна технологія наближається до 50% ринку або коли ринок консолідується до трьох або менше технологій – це може спровокувати зрілість ШІ як поверхні атаки, мобілізувати подальші інвестиції в нові інструменти від кіберзлочинців.

Незважаючи на те, що генеративний штучний інтелект наразі перебуває на етапі перед масовим ринком, надзвичайно важливо, щоб підприємства захищали свої моделі штучного інтелекту до того, як кіберзлочинці масштабують свою діяльність. Підприємства також повинні усвідомлювати, що їх існуюча базова інфраструктура є шлюзом до їхніх моделей штучного інтелекту, який не потребує нових тактик від зловмисників для цілі, що підкреслює потребу в цілісному підході до безпеки в епоху генеративного штучного інтелекту.

Куди подівся весь фіш?

Майже кожна третя атака, яка спостерігалася в усьому світі, була спрямована на Європу, при цьому регіон також зазнав найбільшої кількості атак програм-вимагачів у світі (26%).

Незважаючи на те, що фішингові атаки залишаються найпопулярнішим вектором зараження, кількість фішингових атак зменшилася на 44% порівняно з 2022 роком. Але оскільки ШІ готовий оптимізувати цю атаку, а дослідження X-Force показують, що ШІ може прискорити атаки майже на два дні, вектор зараження залишатиметься кращий вибір для кіберзлочинців.

Red Hat Insights виявив, що 92% клієнтів мають принаймні одну CVE з відомими експлойтами, які не були усунені в їхньому середовищі на момент сканування, а 80% із десяти найбільших уразливостей, виявлених у системах у 2023 році, отримали «високий» або «критичний» рівень. Базовий бал тяжкості CVSS.

X-Force помітила 100% збільшення атак «kerberoasting», під час яких зловмисники намагаються видати себе за користувачів, щоб підвищити привілеї, зловживаючи білетами Microsoft Active Directory.

Тестування на проникнення X-Force Red показало, що неправильні конфігурації безпеки становлять 30% від загальної кількості виявлених загроз, спостерігаючи понад 140 способів, якими зловмисники можуть використовувати неправильні конфігурації». ***(The old, not the new: Basic security issues still biggest threat to enterprises // Help Net Security (https://www.helpnetsecurity.com/2024/02/23/2024-x-force-threat-intelligence-index/). 23.02.2024).***

***

Діяльність хакерів та хакерські угруповування

«Організація Об'єднаних Націй (AP) — Експерти ООН кажуть, що вони розслідують 58 підозрюваних кібератак Північної Кореї в період з 2017 по 2023 роки, вартість яких оцінюється приблизно в 3 мільярди доларів, причому ці гроші, як повідомляється, були використані для фінансування розробки зброї масового знищення.

Повідомляється, що велика кількість кібератак з боку північнокорейських хакерських груп, які підпорядковуються Головному розвідувальному бюро, головній організації зовнішньої розвідки Північної Кореї, продовжується, заявила група експертів у підсумковому підсумку нової доповіді Раді Безпеки ООН, отриманої в п'ятницю. від The Associated Press.

Звіт, що охоплює період з липня 2023 року по січень 2024 року та відображає внески невстановлених країн-членів ООН та інших джерел, був надісланий до ради з 15 членів, оскільки лідер Північної Кореї Кім Чен Ин підвищив напруженість у регіоні. Він погрожує знищити Південну Корею, якщо його спровокують, і посилить демонстрацію зброї. У відповідь США, Південна Корея та Японія посилили спільні військові навчання…

Комісія заявила, що також розслідувала повідомлення про те, що численні громадяни КНДР працюють за кордоном, зокрема в сфері інформаційних технологій, ресторанів і будівництва, і отримують прибуток у порушення санкцій ООН…». ***(UN Experts Investigating 58 Suspected North Korean Cyberattacks Valued***

at About $3 Billion // U.S. News & World Report L.P. (https://www.usnews.com/news/us/articles/2024-02-09/un-experts-investigating-58-suspected-north-korean-cyberattacks-valued-at-about-3-billion?utm_source=flipboard&utm_content=seanjkernan%2Fmagazine%2FUS+News). 09.02.2024).

***

«Повідомляється, що витік китайських хакерських документів, можливо, дав світові уявлення про те, наскільки поширеними та ефективними можуть бути хакерські операції Китаю.

Понад 570 файлів і документів було опубліковано на платформі розробників GitHub минулого тижня, повідомляє The Washington Post. Схоже, вони документують хакерську діяльність у кількох країнах і походять від iSoon, яку Post назвав приватним охоронним підрядником із зв'язками з Міністерством громадської безпеки Китаю.

«У нас є всі підстави вважати, що це автентичні дані підрядника, який підтримує глобальні та внутрішні операції кібершпигунства з Китаю», — сказав виданню Post експерт з кібербезпеки Джон Халтквіст.

У середу Associated Press повідомило, що поліція Китаю розслідує витік, посилаючись на двох неназваних співробітників iSoon, з якими вона спілкувалася. Співробітники повідомили AP, що документи належали групі.

У файлах згадуються цілі від урядових установ до компаній, таких як телекомунікаційні фірми, щонайменше в 20 іноземних країнах і територіях, включаючи Великобританію, Індію, Південну Корею, Таїланд і Малайзію, повідомляє Post.

Хакери стверджували, що можуть використовувати уразливості в програмному забезпеченні, створеному компаніями, включаючи Microsoft і Google, повідомляється в публікації. (The Post стверджує, що Microsoft не відповіла на запит про коментар і що Google заявила, що в документах не згадуються конкретні вразливості в її програмному забезпеченні.)

Представник Google сказав Business Insider, що окрім файлів, у яких не згадуються конкретні вразливості в програмному забезпеченні Google, документи описують стандартні методи шкідливого програмного забезпечення, добре відомі командам безпеки компанії. Представник Microsoft відмовився від коментарів, коли звернувся до Business Insider.

Хоча у звіті The Post не згадується жодна ціль США, файли узгоджуються з неодноразовими попередженнями співробітників служби безпеки та експертів щодо хакерських операцій Китаю.

Глава ФБР Крістофер Рей заявив « 60 Minutes » у жовтні, що Китай запустив « найбільшу хакерську програму у світі ».

Рей сказав, що Китай «викрав більше наших особистих і корпоративних даних, ніж кожна нація, велика чи мала, разом узяті».

А коли йдеться про боротьбу із загрозою, яку представляють китайські хакери, Рей сказав, що ФБР переважає чисельно.

«Якби кожен із кіберагентів ФБР та аналітиків розвідки зосереджувався виключно на китайській загрозі, китайські хакери все одно перевищували б кількість кіберперсоналу ФБР принаймні 50 до 1», — сказав Рей законодавцям минулого місяця.

Представники міністерства закордонних справ Китаю не відразу відповіли на запит Business Insider про коментар». ***(Kwan Wei Kevin Tan. The reported leak of Chinese hacking documents supports experts' warnings about how compromised the US could be // Business Insider (https://www.businessinsider.com/leaked-chinese-hacking-files-reveal-how-compromised-us-could-be-2024-2?utm_source=flipboard&utm_content=BusinessInsider%2Fmagazine%2FMilitary+%26+Defense). 22.02.2024).***

***

Вірусне та інше шкідливе програмне забезпечення

«Китайський виробник ПК AceMagic відомий своєю великою лінійкою міні-ПК, які забезпечують високу продуктивність за відносно доступними

цінами. Однак компанія була змушена визнати, що відвантажила принаймні одну партію пристроїв із заводськими шпигунськими програмами.

Про проблему стало відомо після того, як Джон Фрімен з YouTube-каналу «The Net Guy Reviews» протестував міні-ПК AceMagic AD08 і виявив, що він містить файли, позначені Windows Defender як зловмисне програмне забезпечення. Він стверджує, що інші моделі, які продає AceMagic (належить і управляється китайською компанією Shenzhen Shanminheng Technology), включаючи AD15 і S1, також містять подібне шкідливе програмне забезпечення. Усі ці пристрої продаються на Amazon, потенційно ставлячи під загрозу конфіденційність і безпеку користувачів.

За словами Фрімена, він вперше помітив проблему, коли вбудоване програмне забезпечення безпеки Windows виявило підозрілі файли в розділі відновлення на SSD пристрою. Після більш детального огляду він виявив два проблемні виконувані файли – ENDEV і EDIDEV – які ховалися у підпапці «OsVer» у папці встановлення Windows. Подальше розслідування показало, що ці два файли є частиною горезвісних сімейств шпигунського програмного забезпечення Bladabindi та Redline.

Відомо, що Redline викрадає паролі браузерів, спустошує крипто-гаманці та захоплює різні критичні облікові записи веб-сайтів, як-от Steam, Filezilla, Telegram тощо. Він також може викрасти облікові дані VPN, відстежувати вашу IP-адресу та ухилятися від виявлення антивіруса шляхом шифрування частини вихідного коду. Після зараження комп’ютера він може надсилати ваші особисті дані зловмисникам.

Тим часом Bladabindi — це бекдор-троян, який дозволяє хакерам віддалено отримувати доступ з метою крадіжки даних.

Тривожно те, що ці файли також були знайдені в папці відновлення, тобто їх буде перевстановлено, навіть якщо ви очистите диск C:/ і перевстановите Windows за допомогою вбудованої функції «Відновлення». Повне сканування системи також виявило додаткові невідомі файли в папці Windows. Сканування Virustotal виявило їх як зловмисне програмне забезпечення.

Цікаво, що Фріман придбав ще один міні-ПК AceMagic AD08 від Amazon і виявив, що в ньому немає проблем зі зловмисним програмним забезпеченням, які вплинули на перший пристрій. Коли він зв'язався з AceMagic щодо своїх висновків, компанія стверджувала, що проблема зі зловмисним програмним забезпеченням торкнулася лише першої партії міні-ПК AD08 і згодом була вирішена.

У електронному листі Фрімену AceMagic сказав: «Проблему з вірусним програмним забезпеченням було вирішено в поточному запасі... цієї проблеми більше не буде в поточних пропозиціях». ***(Kishalaya Kundu. Mini PCs sold on Amazon contained factory-installed spyware // TechSpot, Inc. (https://www.techspot.com/news/101796-mini-pcs-sold-amazon-contained-factory-installed-spyware.html?utm_source=flipboard&utm_content=nkakita%2Fmagazine%2FMy+Web+Wanderings). 07.02.2024).***

***

«Недавній звіт Darktrace розкриває ключові загрози, з якими зіткнулися підприємства за останні шість місяців. У звіті наголошується на поширеності атак типу «як послуга», оскільки більшість зловмисників використовують для здійснення атак Malware-as-a-Service (MaaS) і Ransomware-as-a-Service (Raas). Ці інструменти надають зловмисникам ресурси, наприклад готові зловмисне програмне забезпечення або шаблони для фішингу. У звіті зазначено, що після демонтажу групи програм-вимагачів Hive з'явилися нові загрози, такі як ScamClub і AsyncRAT.

Найпоширенішими інструментами, які використовували такі зловмисники, були завантажувачі шкідливих програм, які становили 77% досліджуваних загроз. Далі йдуть криптомайнери з 52%, ботнети з 39%, зловмисне програмне забезпечення для крадіжки інформації з 36% і проксі-ботнети з 15%.

У звіті також обговорюється зростання кількості складних тактик фішингу. У звіті було зазначено 10,4 мільйона фішингових електронних листів у період з вересня по грудень 2023 року. Однією з таких тактик є спроби фішингу Microsoft

Teams, під час яких зловмисники видають себе за колег жертви та спонукають її натиснути шкідливе посилання.

Інша відзначена тенденція — збільшення багатофункціонального шкідливого програмного забезпечення, що дозволяє зловмисникам створювати широкі мережі та завдавати максимальної шкоди. Оскільки зловмисники переходять на новітні методи обходу сучасних заходів безпеки, команди безпеки повинні продовжувати адаптацію та інновації». ***(Cyber security threats are predominantly as-a-service attacks // security magazine (https://www.securitymagazine.com/articles/100390-cyber-security-threats-are-predominantly-as-a-service-attacks). 09.02.2024).***

***

«Meta розіслала сповіщення про вісім компаній-розробників шпигунського програмного забезпечення з Об'єднаних Арабських Еміратів (ОАЕ), Італії та Іспанії, які здійснюють наймане спостереження за цілями за допомогою систем iOS, Android і Windows. Попередження Meta були надіслані як частина звіту компанії про загрози протидії за останній квартал 2023 року.

Згідно зі звітом Meta, компанії RCS Labs, Cy4Gate/ELT Group, Variston IT, IPS Intelligence, Protect Electronic Systems, TrueL IT, Mollitiam Industries і Negg Group отримували доступ і збирали дані пристрою та інформацію зі скріншотів, камер, мікрофонів, контактів., програми, SMS тощо. Meta також стверджувала про збирання даних, фішинг і соціальну інженерію на різних платформах соціальних мереж.

Крім того, Meta видалила понад 2000 облікових записів і сторінок Instagram і Facebook в мережах України, Китаю та М'янми, які демонструють таку підозрілу активність. Ці сторінки використовувалися для поширення дезінформації та пропаганди з геополітичними наслідками. Відповідно, Meta налаштувала ізоляцію пам'яті VoIP для WhatsApp і Control Flow Integrity (CFI) у Messenger для Android як контрзаходи.

Ця розробка стала результатом угоди між урядом США та технологічними компаніями щодо створення засобів контролю для комерційного шпигунського програмного забезпечення та його потенціалу для зловживань. Він підкреслює

необхідність відповідних заходів проти шпигунського програмного забезпечення для використання вразливостей для фішингових кампаній і доставки зловмисного корисного навантаження проти чутливих цілей». ***(Anuj Mudaliar. Spyware Firms Targeting Windows, Android, and iOS Warns Meta // Spiceworks Inc. (https://www.spiceworks.com/it-security/cyber-risk-management/news/spyware-firms-targeting-windows-android-and-ios-warns-meta/). 20.02.2024).***

***

«Пов'язаний із Китаєм загрозник, відомий як Mustang Panda, націлився на різні азіатські країни, використовуючи варіант бекдору PlugX (він же Korplug), який отримав назву DOPLUGS.

«Настроюване зловмисне програмне забезпечення PlugX відрізняється від загального типу зловмисного програмного забезпечення PlugX, яке містить завершений командний модуль бекдора, і що перший використовується лише для завантаження останнього», — заявили дослідники Trend Micro Санні Лу та П'єр Лі в новій статті. технічний опис.

Цілі DOPLUGS були в основному розташовані на Тайвані та В'єтнамі, і меншою мірою в Гонконзі, Індії, Японії, Малайзії, Монголії та навіть Китаї.

PlugX є основним інструментом Mustang Panda, який також відстежується як BASIN, Bronze President, Camaro Dragon, Earth Preta, HoneyMyte, RedDelta, Red Lich, Stately Taurus, TA416 і TEMP.Hex. Відомо, що він активний принаймні з 2012 року, хоча вперше його виявили у 2017 році.

Майстерність зловмисника передбачає проведення добре підроблених фішингових кампаній, спрямованих на доставку різноманітних зловмисних програм. Він також має досвід розгортання власних налаштованих варіантів PlugX, таких як RedDelta, Thor, Hodur і DOPLUGS (розповсюджуються через кампанію під назвою SmugX) з 2018 року.

Ланцюжки компрометації використовують набір різних тактик, використовуючи фішингові повідомлення як канал для доставки корисного навантаження першого етапу, який під час відображення документа-приманки одержувачу таємно розпаковує законний підписаний виконуваний файл, уразливий

до бокового завантаження DLL, щоб завантажувати бібліотеку динамічного компонування (DLL), яка, у свою чергу, розшифровує та виконує PlugX.

Зловмисне програмне забезпечення PlugX згодом отримує троян віддаленого доступу Poison Ivy (RAT) або Cobalt Strike Beacon, щоб встановити з'єднання з сервером, яким керує Mustang Panda.

У грудні 2023 року Lab52 виявила кампанію Mustang Panda, націлену на тайванські політичні, дипломатичні та урядові організації за допомогою DOPLUGS, але з помітною різницею.

«Шкідливий DLL написаний на мові програмування Nim», — повідомили в Lab52. «Цей новий варіант використовує власну реалізацію алгоритму RC4 для дешифрування PlugX, на відміну від попередніх версій, які використовують бібліотеку Windows Cryptsp.dll».

DOPLUGS, вперше задокументований Secureworks у вересні 2022 року, є завантажувачем із чотирма бекдор-командами, одна з яких організована для завантаження загального типу зловмисного програмного забезпечення PlugX.

Trend Micro повідомила, що також виявила зразки DOPLUGS, інтегровані з модулем, відомим як KillSomeOne, плагіном, який відповідає за розповсюдження шкідливого програмного забезпечення, збір інформації та крадіжку документів через USB-накопичувачі.

Цей варіант оснащений додатковим компонентом запуску, який виконує легітимний виконуваний файл для виконання бокового завантаження DLL, на додаток до підтримки функцій для запуску команд і завантаження наступного етапу зловмисного програмного забезпечення з сервера, контрольованого актором.

Варто зазначити, що налаштований варіант PlugX, що містить модуль KillSomeOne і призначений для розповсюдження через USB, був виявлений Avira ще в січні 2020 року в рамках атак, спрямованих проти Гонконгу та В'єтнаму.

«Це свідчить про те, що Earth Preta вже деякий час удосконалює свої інструменти, постійно додаючи нові функціональні можливості та функції», — сказали дослідники. «Група залишається дуже активною, особливо в Європі та Азії». ***(Mustang Panda Targets Asia with Advanced PlugX Variant DOPLUGS // The***

Hacker News (https://thehackernews.com/2024/02/mustang-panda-targets-asia-with.html). 21.02.2024).

***

«Європейський парламент у середу, 21 лютого, попросив членів свого підкомітету з питань оборони перевірити свої телефони на шпигунське програмне забезпечення після того, як на двох пристроях знайшли сліди злому. Про це пише Politico.

ІТ-служба Європарламенту повідомила, що членів і співробітників підкомітету з питань безпеки і оборони атакували програмним забезпеченням для спостереження.

Проблему виявили під час планової перевірки пристроїв на предмет кібербезпеки, тож причина, з якої на телефони могли встановити шкідливу програму, наразі незрозуміла.

Відповідно до електронного листа, з яким ознайомилося видання, усім законодавцям у підкомітеті рекомендувано віднести свої телефони в ІТ-службу установи для перевірки.

Напередодні виборів у червні Європарламент перебуває у стані підвищеної готовності до кібератак та іноземного втручання.

У грудні Politico повідомило, що кібербезпека установи досі не відповідає галузевим стандартам, а також не вповні відповідає рівню загрози, яку становлять хакери.

Подібні інциденти вже траплялися з іншими членами Європарламенту. У 2022 році дослідники виявили, що телефони учасників руху за незалежність Каталонії, зокрема політиків ЄС, були заражені двома типами хакерських програм Pegasus і Candiru…» ***(Юлія Войцехівська. На телефонах чиновників ЄС знайдено шпигунські програми // Українські медійні системи (https://glavcom.ua/world/world-politics/na-telefonakh-chinovnikiv-jes-znajdeno-shpihunski-prohrami-987208.html). 22.02.2024).***

***

«Федеральне бюро розслідувань США ліквідувало російський ботнет, який заразив сотні домашніх Wi-Fi-маршрутизаторів за допомогою програмного забезпечення Moobot. Агентам вдалося «очистити» обладнання, застосувавши ту саму шкідливу програму, повідомило Міністерство юстиції США.

Згідно із заявою Міністерства юстиції США, невідомі хакери встановили шкідливе програмне забезпечення (ПЗ) Moobot у мережеву операційну систему Ubiquiti Edge OS, встановлену на роутерах EdgeRouter. Пізніше з'ясувалося, що атака була проведена не без участі службовців військової частини 26165 ГРУ РФ (ГРУ РФ — орган зовнішньої розвідки Росії — ред.). Ці хакери з ГРУ відомі, як група APT28, Fancy Bear, Sofacy Group, Forest Blizzard і Pawn Storm.

Завданням російських хакерів було перепрофілювання мережі для збору облікових даних з Wi-Fi-маршрутизаторів. Цілями кіберзлочинців стали люди, які становлять «розвідувальний інтерес для російського уряду».

Агенти ФБР використовували шкідливе ПЗ Moobot для копіювання і видалення вкрадених даних і шкідливих файлів зі зламаних маршрутизаторів. Щоб нейтралізувати доступ ГРУ до роутерів, було змінено правила брандмауера пристроїв, що дало змогу заблокувати доступ до віддаленого управління. ФБР також налагодило тимчасовий збір інформації про маршрутизацію, щоб зрозуміти, чи продовжує ГРУ атаки, чи ні.

ФБР рекомендувало всім жертвам зробити такі кроки щодо виправлення ситуації:

- виконати апаратне скидання налаштувань, щоб очистити файлову систему від шкідливих файлів;
- оновити прошивку до останньої версії;
- змінити логіни та паролі за замовчуванням;
- впровадити стратегічні правила брандмауера, щоб запобігти небажаному розкриттю служб віддаленого управління…» ***(Ірина Рефагі. Хакери з ГРУ Росії заразили сотні Wi-Fi-роутерів у США, але були розкриті: хто постраждав // Фокус (https://focus.ua/uk/digital/627339-hakeri-z-gru-rosiyi-zarazili-sotni-wi-fi-routeriv-u-ssha-ale-buli-rozkriti-hto-postrazhdav). 16.02.2024).***

***

«2023 рік був важливим роком для груп програм-вимагачів, хоча правоохоронні органи в усьому світі продовжували боротися зі зловмисниками.

Підрозділ 42 Palo Alto Networks, фірма з аналізу загроз, виявила 49-відсоткове збільшення кількості жертв, про які повідомляють сайти з витоком програм-вимагачів, загалом майже 4000 публікацій на цих сайтах від різних груп програм-вимагачів. Підрозділ 42 сказав, що підйом був пов'язаний з масовим впливом атак, які використовували вразливості нульового дня, які є недоліками безпеки, які розробники ще не виявили. Як один із прикладів вони вказали на хакерське програмне забезпечення MOVEit Transfer, яке уряд США зв'язав із бандою програм-вимагачів CL0P. Агентство з кібербезпеки та безпеки інфраструктури підрахувало, що цей злом скомпрометував понад 3000 організацій у США та 8000 у всьому світі.

Майже половина жертв програм-вимагачів, виявлених Unit 42, були в США, причому найбільше постраждали галузі промисловості, професійні та юридичні послуги, а також високі технології.

Підрозділ 42 минулого року виявив 25 нових сайтів витоку, які пропонували програми-вимагачі як послугу. Але було сказано, що принаймні п'ять, схоже, закрилися, оскільки в них не було нових посад у другій половині року. Приблизно два десятки нових сайтів склали 25 відсотків від загальної кількості публікацій про програми-вимагачі у 2023 році, повідомляє Unit 42.

Тим не менш, популярність деяких груп програм-вимагачів також привернула увагу правоохоронних органів, що вдалось у кількох випадках, повідомляє Unit 42. Група високо оцінила роль правоохоронних органів у підриві таких груп, як Hive і Ragnar Locker у 2023 році. Згідно з даними Міністерства юстиції США, Hive вимагав викуп у розмірі 100 мільйонів доларів США та спричинив серйозні збої, зокрема в лікарні, яка була змушена перейти на аналогову

систему після напад і не міг приймати нових пацієнтів. За даними європейських правоохоронних органів,Ragnar Locker атакував критично важливу інфраструктуру, зокрема португальського національного перевізника та ізраїльську лікарню .

Звіт відповідає висновкам Chainalysis, компанії блокчейн-даних, яка нещодавно опублікувала власний звіт про тенденції криптозлочинності. Незважаючи на те, що на основі попередніх висновків компанія виявила падіння загальної вартості незаконної криптоактивності в цілому у 2023 році, дохід від програм-вимагачів зріс. Chainalysis припустив, що «зловмисники пристосувалися до покращень кібербезпеки організацій». ***(Lauren Feiner. The ransomware business is booming, even as enforcers shut down some major players // Vox Media, LLC. (https://www.theverge.com/2024/2/5/24059486/ransomware-victims-palo-alto-networks-unit-42). 05.02.2024).***

***

«Державний департамент США нещодавно оголосив, що пропонує до 15 мільйонів доларів винагороди за інформацію, яка може допомогти владі зруйнувати сумно відому групу програм-вимагачів ALPHV/Blackcat.

Нагорода складається з винагороди в розмірі 10 мільйонів доларів за інформацію, яка може допомогти ідентифікувати ключових членів злочинної організації, або інформацію про їх місцезнаходження, а також додаткові 5 мільйонів доларів за підказки, що призведуть до арешту або засудження будь-кого, пов’язаного з бандою.

Згідно з прес-релізом Державного департаменту, менша винагорода застосовується до «будь-кого, хто бере участь у змові або намагається взяти участь у атаці програм-вимагачів з використанням варіанту ALPHV/Blackcat».

Оголошення з’явилося через два тижні після того, як Державний департамент оголосив винагороду в розмірі 15 мільйонів доларів за інформацію про банду програм-вимагачів Hive у подібній ініціативі.

Коротка історія ALPHV/Blackcat

Група програм-вимагачів ALPHV/Blackcat, раніше відома як Noberus, працює за моделлю програм-вимагачів як послуги (RaaS) і є одним із найвідоміших

синдикатів кіберзлочинності в середовищі загроз. З моменту своєї першої появи в листопаді 2021 року банда націлилася на численні високопоставлені організації по всьому світу та вимагала вимагачів.

Методи роботи групи передбачали шифрування даних у зламаних системах, передачу їх на належні зловмисникам сервери, а потім погрози оприлюднити їх для громадськості, якщо викуп не буде сплачено, тактика, яку називають «подвійним вимаганням».

На своєму піку ALPHV скомпрометував широкий спектр секторів, включаючи державні установи, університети, технології, транспорт, енергетику та виробників.

Зліт і падіння ALPHV/Blackcat

У грудні 2023 року ФБР успішно демонтувало ALPHV; операція включала захоплення кількох веб-сайтів, що належать зловмисникам, і випуск інструменту дешифрування для постраждалих сторін, що допомогло більш ніж 500 жертвам у всьому світі відновити їхні системи без сплати викупу.

Однак лише через кілька годин після того, як Міністерство юстиції оголосило про переривання деяких дій угруповання, ALPHV заявила, що «зняла захоплення» з її домену, і погрожувала вжити заходів у відповідь.

У липні 2023 року сумнозвісна група програм-вимагачів спробувала розширити свої операції, інтегрувавши API для свого веб-сайту, присвяченого витоку даних, з метою посилити викриття своїх кібератак.

Захист від програм-вимагачів

Хоча програми-вимагачі є однією з найнебезпечніших онлайн-загроз, хороша кібергігієна та спеціалізоване програмне забезпечення можуть дати вам перевагу.

Bitdefender Ultimate Security містить надійні модулі захисту від програм-вимагачів, які захищають ваші документи, музику, відео та фотографії від атак програм-вимагачів. Він також захищає вас від інших цифрових загроз, зокрема вірусів, троянів, черв'яків, шпигунського програмного забезпечення, експлойтів нульового дня та руткітів». ***(Vlad CONSTANTINESCU. US State Department Offers Up to $15 Million for Information on ALPHV/Blackcat Ransomware Gang //***

Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/us-state-department-offers-up-to-15-million-for-information-on-alphv-blackcat-ransomware-gang/?utm_source=flipboard&utm_content=other%2F). 19.02.2024).

***

«Індустрія платежів у режимі реального часу розвивається і розширюється. Сьогодні платежі в режимі реального часу охоплюють 65% депозитних рахунків на вимогу, і вони стають дедалі швидшими та надійнішими. У найближчі п'ять років 99% корпорацій з доходом понад 1 мільярд доларів будуть використовувати платежі в режимі реального часу. Ця новина є захоплюючою для індустрії, але разом із впровадженням платіжних технологій зростає і ризик крадіжок та шахрайства. Платежі в режимі реального часу вимагають оперативного реагування кібербезпеки. Зі зростанням кількості кіберзагроз і посиленням регулювання банкам і фінансовим установам необхідно розвивати заходи кібербезпеки.

За останні п’ять років програми-вимагачі піднялися на вершину кіберзагроз і залишаються там. Поширеність програм-вимагачів та інших фішингових атак, таких як BEC (компрометація бізнес-електронної пошти), зумовлена демократизацією злому на темна мережа. Люди з невеликими або середніми хакерськими здібностями можуть використовувати різноманітні інструменти, щоб заробити легкі гроші. Як наслідок, хакерам не потрібно бути дуже креативними; вони мають широкі доступні можливості та інфраструктуру для їх реалізації. Хакери продовжують щоб атакувати межі платіжної транзакції, розуміючи, наприклад, що атаку не буде позначено, доки вона не досягне певної суми в доларах або кількості транзакцій. З точки зору шахрайства, це постійно розвивається, і заходи захисту від шахрайства повинні продовжуйте переробляти краї для захисту від атак.

Штучний інтелект також сприяє поширенню кіберзлочинності. Озброєні автоматизацією, яка тепер покращена штучним інтелектом, хакери мають доступ до величезних обсягів даних і все більш ефективних інструментів, а отже, мають нижчий бар’єр для атак і збільшення норми прибутку від кіберзлочинності. В

результаті збільшився обсяг кібератак. Це особливо важливо для індустрії платежів у режимі реального часу, оскільки платежі в режимі реального часу є не лише цільовими, але й кращим способом оплати для хакерів, забезпечуючи легкий і миттєвий доступ до готівки. Після завершення платіжної операції її неможливо скасувати. Це зростаюча проблема, і індустрія платежів у реальному часі повинна на це реагувати.

Відповідає нормативним вимогам

Незважаючи на спроби організацій протидіяти зловмисній діяльності, засоби захисту заходять лише так далеко, оскільки вони ґрунтуються на ділових обставинах кожної організації. Це зводиться до старої приказки: «Ви не поставите паркан за 10 доларів навколо корови за 1 долар». Те саме стосується кібернетики безпеки. Якщо збитки від шахрайства та кібератак коштують 2 мільйони доларів на рік, але надійна програма безпеки коштує 10 мільйонів доларів, фінансова установа може вирішити поглинути збитки у свою бізнес-модель.

Проте банки повинні відповідати нормативним вимогам щодо захисту платежів і конфіденційності, і ці правила постійно вдосконалюються, оскільки уряди штатів і федеральні органи влади шукають способи захистити споживачів і зменшити втрати. Банки повинні дотримуватися цих правил, незважаючи на вартість. Саме тут партнерство з третіми сторонами є важливим для реалізації необхідної тактики запобігання. Постачальники платіжних технологій знаходяться в центрі транзакції та можуть відповідати вказівкам банку щодо запобігання шахрайству.

Базові вимоги завжди включатимуть засоби контролю, призначені для збільшення (і, отже, витрат) шахрайства та кібератак, як-от надійна автентифікація (наприклад, багатофакторна автентифікація), шифрування та засоби керування мережею. Однак реактивне планування є ключовим для пом’якшення впливу будь-яких інцидентів, які стаються, включаючи плани реагування на інциденти, плани безперервності бізнесу та кіберстрахування. Крім того, деякі банки та партнери вирішать запровадити ще суворішу політику, щоб забезпечити безпеку та продемонструвати законодавство органів, що протидія кіберзлочинності

відбувається без втручання уряду. Наприклад, платіжна заявка Zelle нещодавно заявила, що відшкодує деякі випадки збитків через певні шахрайства. Завдяки партнерству з відповідними технологічними платформами компанії можуть забезпечити дотримання як обов'язкових, так і обраних інструкцій. Сторонні постачальники вже в авангарді вирішення цих проблем.

Впровадження найкращих практик

Зупинити кіберзлочини та шахрайство – це складно. Зрештою, хакери добре озброєні і просто повторюють спробу, поки не досягнуть успіху. Однак існують найкращі практики, які організації можуть застосувати, щоб зменшити кількість спроб шахрайства та зустрітися з урядом нормативні акти. Моніторинг поведінки є золотим стандартом у запобіганні шахрайству, і це не змінилося, навіть коли хакери стали більш досвідченими.

Як частина повної програми BSA/AML (боротьба з відмиванням грошей), моніторинг поведінки включає практики «Знай свого клієнта» (KYC) і «Знай свій бізнес» (KYB). KYC і KYB — це вказівки та процедури, які організації використовують для перевірки користувачів і ділових партнерів та інші корпоративні організації, використовуючи комбінацію програм сторонніх розробників, автоматизацію та ручний аналіз. Звичайно, такі технічні засоби контролю, як багатофакторна автентифікація, шифрування та резервне копіювання даних, є важливими базовими компонентами захисту даних програма, яка зменшує наслідки шахрайства. Ці найкращі практики залишаться, але розширення правил і надалі вимагатиме більше від компаній, оскільки уряди шукатимуть більше способів захисту споживачів.

Хороша новина полягає в тому, що засоби захисту також покращуються завдяки автоматизації, покращеній штучним інтелектом, щоб передбачати й реагувати на нові загрози, коли вони виникають. Хакери використовують інструменти штучного інтелекту для масштабування кіберзлочинів, і компанії повинні захищатися від цих спроб аналогічним чином адаптивні інструменти, покращені ШІ. Сторонні постачальники (і партнери, які їх використовують) також

лідирують тут, оскільки вони конкурують між собою за надання високоякісних послуг за найкращою ціною.

Включення нових методів у передову практику кібербезпеки є важливим кроком до обмеження ризику та випередження втручання регуляторів. Платежі в реальному часі тільки розширюються. Це триваюча війна, і кібербезпека в реальному часі є найкращим захистом». ***(Ed Woodfield. Building a Real-Time Cyber Security Response to Real-Time Payment Fraud // Finextra Research (https://www.finextra.com/blogposting/25694/building-a-real-time-cyber-security-response-to-real-time-payment-fraud). 14.02.2024).***

***

«Постачальник технологічних рішень Сінгапуру Aztech Global 13 лютого заявив, що нещодавно зазнав «інциденту з кібербезпекою», коли кіберзлочинці отримали несанкціонований доступ до його IT-мережі та розгорнули атаку з використанням програми-вимагача.

Згідно з інформацією, доступною на сьогоднішній день, інцидент не має суттєвого впливу на фінансові показники або діяльність Aztech Global, йдеться у повідомленні компанії, поданому на біржу.

Група вжила заходів одразу після виявлення проблеми, включаючи вимкнення серверів на час китайських новорічних канікул і використання програмного забезпечення для перевірки серверів компанії, щоб переконатися, що подальші дані не постраждали і не були скомпрометовані.

«Група призначила сторонніх консультантів-криміналістів для допомоги в розслідуванні інциденту та повідомила відповідний правоохоронний орган», — йдеться в повідомленні.

Він також шукає порад від експертів галузі щодо подальшого зміцнення своєї загальної кібербезпеки та повідомлятиме акціонерам про будь-які суттєві зміни.

15 лютого група оголосить свої фінансові результати за рік, що закінчився 31 грудня». ***(Megan Cheah. Aztech Global reports 'cyber security incident', says no material impact but launches probe // SPH Media Limited***

(https://www.straitstimes.com/business/companies-markets/aztech-global-reports-cyber-security-incident-says-no-material-impact-but-launches-probe). 14.02.2024).

***

Програми-трояни

«Служба військової розвідки та безпеки Нідерландів (MIVD) попереджає, що вона виявила новий штам зловмисного програмного забезпечення, яке є стійким і його важко виявити, яке розгортає уряд Китаю проти існуючого недоліку FortiGate, і що воно є частиною більш широкої кампанії політичного шпигунства.

Новий троян віддаленого доступу (RAT) під назвою «Coathanger» використовувався для шпигунства за Міністерством і оборони Нідерландів (MOD) у 2023 році, згідно з новими рекомендаціями. Під час реагування на вторгнення співробітники голландської розвідувальної служби виявили, що зловмисне програмне забезпечення доставлялося через відомий недолік FortiGate (CVE-2022-42475).

Пристрої FortiGate від Fortinet забезпечують захист мережевого брандмауера.

У звіті наголошується, що Coathanger не використовує переваги нового експлойту нульового дня і розгортається як зловмисне програмне забезпечення другого етапу. Однак у повідомленні додано, що «Coathanger може використовуватися разом із будь-якою майбутньою вразливістю пристрою FortiGate ».

Голландські чиновники пояснили: «Зловмисне програмне забезпечення Coathanger є прихованим і стійким. Воно ховається, перехоплюючи системні виклики, які можуть виявити його присутність. Воно витримує перезавантаження та оновлення мікропрограми».

Граничні пристрої в Cyberattack Crosshairs

За даними влади Нідерландів, зловмисне програмне забезпечення Coathanger є частиною ширшої кампанії, яку ведуть китайські державні загрозливі особи проти

периферійних пристроїв, що виходять в Інтернет, включаючи брандмауери, сервери VPN і сервери електронної пошти.

«Відомо, що китайські зловмисники проводять широкомасштабні й випадкові кампанії сканування як опублікованих (nday), так і неопублікованих (0-day) уразливостей програмного забезпечення на пристроях, що підключаються до Інтернету (крайніх)», — попереджається в повідомленні. «Вони роблять це з високим оперативним темпом, іноді зловживаючи вразливими місцями в день їх публікації».

Пристрої Fortinet є популярною мішенню для кібератак, тому компаніям слід стежити за виправленнями: лише цього тижня Fortinet повідомила про дві помилки максимальної серйозності у своєму рішенні FortiSIEM, які потребують негайного виправлення.

Рекомендації аналітиків розвідки в Нідерландах щодо запобігання Coathanger також включають проведення регулярного аналізу ризиків на периферійних пристроях, обмеження доступу до Інтернету на периферійних пристроях, запланований аналіз журналювання та заміну будь-якого апаратного забезпечення, яке більше не підтримується». ***(Becky Bracken. China Caught Dropping RAT Designed for FortiGate Devices // Informa PLC (https://www.darkreading.com/endpoint-security/china-dropping-rat-designed-fortigate-devices?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FFLIPBOARD%0AMAGAZINE+OF%0AA.+NISHIHARA). 08.02.2024).***

***

«Дослідники виявили новий банківський троян, який вони назвали «Coyote», який шукає облікові дані для 61 різної програми онлайн-банкінгу.

«Coyote», детально описаний Касперським у сьогоднішньому аналізі, примітний широким націлюванням на програми банківського сектору (наразі більшість у Бразилії), а також складним переплетенням різних рудиментарних і розширених компонентів: відносно нової відкритої вихідний інсталятор під назвою Squirrel; NodeJs; неоспівана мова програмування під назвою «Nim»; і більше

десятка шкідливих функцій. Загалом, це являє собою помітну еволюцію на процвітаючому бразильському ринку фінансового зловмисного програмного забезпечення — і може спричинити серйозні проблеми для команд із безпеки, якщо розширить свою увагу.

«Вони розробляють банківські трояни більше 20 років — вони почали в 2000 році», — говорить про бразильських розробників шкідливого програмного забезпечення Фабіо Ассоліні, керівник Латиноамериканської групи глобальних досліджень і аналізу (GReAT) у Kaspersky. «За 24 роки розробки та обходу нових методів автентифікації та нових технологій захисту вони були дуже креативними, і ви можете побачити це зараз із цим самим новим трояном».

Наразі це може бути загроза для споживачів, зосереджена на Бразилії, але, як уже згадувалося, є чіткі причини для організацій, щоб знати про Coyote. По-перше, як попереджає Ассоліні, «сімейства зловмисних програм, які в минулому мали успіх у боротьбі з бразильським ринком у минулому, також поширилися за кордон. Ось чому корпорації та банки повинні бути готові до боротьби з цим».

І ще однією причиною для команд безпеки звернути увагу на появу нових банківських троянів є історія їхнього розвитку до повноцінних троянів початкового доступу та бекдорів; так було з Emotet і Trickbot, наприклад а нещодавно з QakBot і Ursinif.

Coyote має функціональність у крилах, щоб наслідувати цей приклад: він може виконувати низку команд, включаючи директиви для створення скріншотів, реєстрації натискань клавіш, завершення процесів, вимкнення машини та переміщення курсору. Він також може повністю заморозити машину з підробленим накладенням «Робота над оновленнями…».

Троянець Coyote Runs With Squirrel & Nim

Поки що під час своїх атак Coyote поводиться як будь-який інший сучасний банківський троян: коли на зараженій машині запускається сумісна програма, зловмисне програмне забезпечення перевіряє контрольований зловмисником сервер керування (C2) і відображає відповідне фішингове накладення на сервері

жертви. екран, щоб отримати інформацію для входу користувача. Однак Coyote найбільше виділяється тим, як він бореться з потенційними виявленнями.

Більшість банківських троянів використовують інсталятори Windows (MSI), Касперський зазначив у своєму блозі, що робить їх легким червоним прапорцем для захисників кібербезпеки. Ось чому Coyote вибирає Squirrel, законний інструмент із відкритим кодом для встановлення та оновлення настільних програм Windows. Використовуючи Squirrel, Coyote намагається замаскувати свій зловмисний початковий завантажувач за цілком чесного пакувальника оновлень.

Його завантажувач останньої стадії ще більш унікальний, оскільки він написаний відносно нішевою мовою програмування під назвою «Nim». Це перший банківський троян, який Kaspersky ідентифікував за допомогою Nim.

«Більшість старих банківських троянів були написані на Delphi, який є досить старим і використовується багатьма родинами. Тож з роками виявлення зловмисного програмного забезпечення Delphi стало дуже хорошим, а ефективність зараження з роками сповільнювалася, – пояснює Ассоліні. З Nim «у них є більш сучасна мова програмування з новими функціями та низьким рівнем виявлення програмним забезпеченням безпеки».

Бразильські банківські трояни є глобальною проблемою

Якщо Coyote так багато доводиться робити, щоб відзначитися, це тому, що п’ята за величиною країна в останні роки стала головним у світі центром банківського шкідливого програмного забезпечення.

Незважаючи на те, що вони тероризують бразильців, ці програми також мають звичку перетинати водойми.

«Ці хлопці мають великий досвід у розробці банківських троянів, і вони прагнуть розширити свої атаки по всьому світу», — підкреслює Ассоліні. «Наразі ми можемо знайти бразильські банківські трояни, які атакують компанії та людей навіть у Австралії та Європі. Цього тижня член моєї команди знайшов нову версію одного в Італії».

Щоб продемонструвати потенційне майбутнє для такого інструменту, як Coyote, Ассоліні вказує на Grandoreiro, подібний троян, який серйозно вторгся в

Мексику та Іспанію, а також далеко за їх межі. До кінця минулої осені, за його словами, він охопив загалом 41 країну.

Однак побічним продуктом цього успіху став посилений контроль з боку правоохоронних органів. На шляху до зриву вільного кіберпідпілля для такого роду зловмисного програмного забезпечення бразильська поліція зробила рідкісний крок: вона виконала п’ять ордерів на тимчасовий арешт і 13 ордерів на обшук і конфіскацію для архітекторів Grandoreiro в п’яти бразильських штатах.

«Проблема в Бразилії полягає в тому, що вони не мають дуже хороших місцевих правоохоронних органів для покарання цих нападників. Це працює краще, коли у вас є організація за межами країни, яка чинить певний тиск, як це сталося з Гранадорейро, коли поліція та банки в Іспанії тиснути на бразильську федеральну поліцію, щоб вони спіймали цих хлопців», – каже Ассоліні.

Отже, підсумовує він, «вони стають кращими, але попереду ще довгий шлях, тому що багато кіберзлочинців все ще на волі [в Бразилії] і вчиняють багато атак по всьому світу». ***(Nate Nelson. 'Coyote' Malware Begins Its Hunt, Preying on 61 Banking Apps // Informa PLC (https://www.darkreading.com/threat-intelligence/coyote-malware-preying-61-banking-apps?utm_source=flipboard&utm_content=RBenoit2014%2Fmagazine%2FSECURITY+%2F+PRIVACY+%2F+MALWARE+%2F+VULN+%2F+FRAUD+%2F+SURVEILLANCE++%2F+MCA+%2F+SAFETY). 08.02.2024).***

***

«Інсталятор для інструменту, який, імовірно, використовується Консульським відділом Міністерства закордонних справ Росії (MID), був бекдорований для доставки трояна віддаленого доступу під назвою Konni RAT (він же UpDog).

Висновки зроблені німецькою компанією з кібербезпеки DCSO, яка пов’язала цю діяльність з діяльністю корейської Народно-Демократичної Республіки (КНДР), націленою на Росію.

Кластер активності Konni (він же Opal Sleet, Osmium або TA406) має усталену схему розгортання Konni RAT проти російських організацій, причому

загрозливий суб’єкт також пов’язаний з атаками, спрямованими проти MID, принаймні з жовтня 2021 року.

У листопаді 2023 року Fortinet FortiGuard Labs виявила використання російськомовних документів Microsoft Word для доставки зловмисного програмного забезпечення, здатного збирати конфіденційну інформацію зі зламаних хостів Windows.

У DCSO заявили, що упаковка Konni RAT у інсталятори програмного забезпечення є технікою, яку група раніше застосувала в жовтні 2023 року, коли було виявлено, що для розповсюдження трояна використовується російське програмне забезпечення для подання податкових декларацій під назвою Spravki BK.

«У цьому випадку бекдорний інсталятор, схоже, призначений для інструмента під назвою «Статистика КЗУ» (Статистика КЗУ)», — повідомила берлінська компанія.

«На основі шляхів встановлення, метаданих файлів і посібників користувача, включених у програму встановлення, [...] програмне забезпечення призначене для внутрішнього використання в Міністерстві закордонних справ Росії (MID), зокрема для ретрансляції файлів річних звітів. із закордонних консульських установ (КЗУ — консульские загранучреждения) до консульського відділу MID по захищеному каналу».

Троянський інсталятор — це файл MSI, який під час запуску ініціює послідовність зараження, щоб встановити зв’язок із сервером командного керування (C2) і очікувати подальших інструкцій.

Вважається, що троян віддаленого доступу, який має можливості для передачі файлів і виконання команд, був запущений ще в 2014 році, а також його використовували інші північнокорейські загрозливі особи, відомі як Kimsuky і ScarCruft (aka APT37).

Наразі незрозуміло, як зловмисникам вдалося отримати копію інсталятора, враховуючи, що його немає у відкритому доступі. Але є підозри, що довга історія

шпигунських операцій, спрямованих проти Росії, могла допомогти їм визначити потенційні інструменти для наступних атак.

Хоча напади Північної Кореї на Росію не є новими, ця подія відбувається на тлі зростаючої геополітичної близькості між двома країнами. Цього тижня державні ЗМІ Королівства відлюдників повідомили, що президент Росії Володимир Путін подарував лідеру Кім Чен Ину розкішний автомобіль російського виробництва.

«Певною мірою це не повинно бути несподіванкою; очікується, що збільшення стратегічної близькості повністю перезапише існуючі потреби КНДР у зборі, оскільки КНДР постійно потребує можливості оцінювати та перевіряти планування зовнішньої політики Росії та цілі», - сказав DCSO». ***(Russian Government Software Backdoored to Deploy Konni RAT Malware // The Hacker News (https://thehackernews.com/2024/02/russian-government-software-backdoored.html). 22.02.2024).***

***

Фішингові атаки

«Згідно зі звітом Verizon про розслідування витоку даних за 2023 рік, 74% зломів пов'язані з людським фактором, що включає атаки соціальної інженерії, такі як фішинг. Насправді новий фішинговий сайт створюється кожні 11 секунд відповідно до DataProt.

Це не повинно дивувати. Мільйони років еволюції людства значною мірою пов'язані з такими проблемами, з якими ми стикаємося в цифровому світі, як-от фішинг, смішинг, квишинг та всі інші «викиди».

Викрадення Amygdala та фішингові атаки

Людські інстинкти виживання змусили нас розвинути в нашому мозку два різних типи блоків обробки інформації:

• Лобова частка є раціональним процесором інформації, якому потрібен час для обробки інформації, включаючи емоційний контроль, і є частиною свідомого прийняття рішень.

• Друга частина — це мигдалеподібне тіло, яке генерує реакцію «бийся або втікай». Він обробляє інформацію як загрозу та запускає миттєві процеси без нашого контролю, тобто ми емоційно заряджені. Мигдалеподібне тіло відіграло вирішальну роль у нашій еволюції та виживанні, щоб виявити загрозу та реагувати в найоптимізованіший за часом спосіб.

Яке це має відношення до фішингу?

Захоплення мигдалеподібного тіла — це реакція «бийся або біжи» після того, як мозок зазнав негайного емоційного стресу, який може змусити наше мислення обійти раціональний мозок. Шахраї часто спонукають до викрадення мигдалини для здійснення фішингових атак.

Розглянемо це у світлі семи методів впливу психолога доктора Роберта Чалдіні. Ось як можна використати ці сім методів, щоб викликати захоплення мигдалеподібного тіла та здійснювати фішингові атаки:

• Повноваження: повідомлення, нібито від генерального директора, або голосовий дзвінок, нібито від податкової служби, можуть викликати бурхливу реакцію жертви.

• Зобов’язання: загальнодоступна інформація з соціальних мереж жертви про її зобов’язання та цілі може бути використана для впливу на фішингові повідомлення.

• Подобається: чиїсь оцінки «подобається» та «не подобається» неважко виділити з публічних публікацій у соціальних мережах, які потім можна використовувати, щоб зробити фішингові повідомлення більш особистими та цілеспрямованими.

• Контраст сприйняття: люди сприймають речі в порівнянні з іншими речами, і наша ментальна модель у більшості випадків відносна. Зазвичай наш мозок не виявляє різниці між доменним іменем відомого веб-сайту, написаним з трохи неправильним написанням, і ми можемо змусити натиснути посилання.

• Взаємність: люди схильні відповідати на подарунок або повертати послугу. Фішинговий рибалка використовує цю інформацію, щоб отримати корисну інформацію про жертву.

• Дефіцит: зловмисники можуть надіслати фішинг-атаку, вказавши довільний термін або термін дії, щоб змусити жертву діяти негайно.

• Соціальний доказ: кібератаки можуть створити публікацію чи веб-сайт із фальшивими оцінками "подобається" чи відгуками, щоб переконати потенційну жертву, що зловмиснику можна довіряти.

Генеративний ШІ та фішинг

Нещодавня еволюція великих мовних моделей (LLM) і революція генеративного штучного інтелекту надали фішинговим атакам нових вимірів. Раніше більшість фішингових повідомлень було легше виявити, оскільки використовувана мова була неефективною, а орфографічні помилки були очевидними. Тепер, маючи доступ до LLM, фішингові повідомлення, створені LLM, можуть бути набагато точнішими.

Зловмисники можуть потенційно точно налаштувати LLM на чийсь вміст соціальних мереж, а також можуть отримати контекстну інформацію про психологічні принципи впливу, щоб вплинути на викрадення мигдалеподібного тіла, щоб фішингові повідомлення не просто були точними, а виглядали набагато більш особистими.

Досить страшно, що зловмисники можуть налаштувати LLM за допомогою методів, які підвищують рівень окситоцину та дофаміну в нашій нейрохімічній системі, таких як методи, які використовуються в соціальних мережах, так що фішингові повідомлення будуть не просто точними та особистими – вони можуть розчулити нас.

Гуманізовані рішення

Бути людиною є причиною стати жертвою фішингових атак, тому рішенням має бути гуманізована технологія. Мотивація зловмисника полягає в тому, щоб отримати певну безпечну інформацію від жертви або змусити жертву виконати певну дію, наприклад, натиснути посилання чи відсканувати QR-код.

Що робити, якщо людина-користувач не має захищеної інформації, щоб передати її зловмиснику? І жодної дії для виконання? У цьому випадку фішингова

атака не вдасться, навіть якщо було запущено викрадення мигдалини, і жертва не буде жертвою людської природи. Це гуманізоване рішення.

З огляду на це, ось чотири технологічні підходи, які можуть допомогти знизити ризик фішингу, коли ми починаємо йти у світ ШІ:

1. Пасивна автентифікація: метою більшості фішингових атак є викрадення облікових даних, щоб подолати бар'єри автентифікації та заволодіти обліковим записом. Методи автентифікації, у яких користувач не бере активної участі, можуть допомогти запобігти цьому, наприклад криптографічна автентифікація за допомогою ключів доступу або тиха мобільна автентифікація на основі SIM-карти.

2. Невидимі контекстні дані: використовуйте надійні дані для перевірки контексту користувача. Наприклад, дані оператора мобільного зв'язку можуть визначити зміни в мобільному пристрої чи SIM-картці. Якщо користувач здійснює дзвінок, щоб пом'якшити стан користувача під впливом, датчики в мобільному пристрої визначають емоційну присутність користувача

3. Аналіз повідомлень на основі штучного інтелекту: аналізуйте повідомлення, надіслані користувачам, за допомогою навчених моделей машинного навчання, щоб визначити намір, очікувану дію та емоційну чутливість повідомлення.

4. Виявлення синтетичних повідомлень: використовуйте навчені моделі ML для виявлення синтетичних повідомлень, тобто повідомлень, створених LLM, і позначайте їх перш ніж вони досягнуть користувача.

Коротше кажучи, гуманізація технології означає розгляд того, як користувачі можуть реагувати на конкретні повідомлення та атаки, роблячи елементи безпеки невидимими для користувача, а цифровий світ безпечніший від фішингу. Як сказав Стів Джобс: «Технології повинні бути або красивими, або невидимими». ***(Gautam Hazari. How Phishing Attacks Use Human Evolution To Their Advantage // Forbes (https://www.forbes.com/sites/forbestechcouncil/2024/02/05/how-phishing-attacks-use-human-evolution-to-their-advantage/?utm_source=flipboard&utm_content=user%2Fforbes&sh=3c7ffe581d71). 05.02.2024).***

***

«У новому звіті, опублікованому компанією Cofense Inc., яка займається виявленням фішингу та реагуванням на нього, у 2023 році виявлено значне зростання кількості шкідливих електронних листів, які оминають захищені шлюзи електронної пошти.

Щорічний звіт Cofense про стан безпеки електронної пошти за 2024 рік, заснований на 35 мільйонах облікових записів співробітників, які відстежує Cofense, виявив понад 1,5 мільйона зловмисних електронних листів, які минулого року оминали захищені клієнтські шлюзи електронної пошти (SEG), що на 37% більше, ніж у 2022 році, і на 310% більше, ніж у 2021 році. У контексті звіту зазначається, що Cofense кожні 57 секунд виявила принаймні одне шкідливе повідомлення електронної пошти в обхід SEG свого клієнта.

SEG – це рішення безпеки, яке фільтрує вхідну та вихідну електронну пошту, щоб захистити організації від загроз електронної пошти, включаючи спам, фішинг, зловмисне програмне забезпечення та інші шкідливі дії. Передбачається, що вони перешкоджають проникненню зловмисних електронних листів, але вони поступово погіршуються. У звіті зазначається, що SEG намагаються не відставати від складних фішингових кампаній.

У звіті детально розглядаються різні аспекти безпеки електронної пошти, зазначається, що електронна пошта залишається основним вектором атак для кіберзлочинності, причому 90% порушень даних походять від фішингових атак, націлених на співробітників. У 2023 році кількість фішингу облікових даних, найкращого методу зловмисників, зросла на 67% порівняно з попереднім роком.

Інші головні тенденції, зазначені у звіті до 2023 року, включають збільшення кількості таких тактик, як вішинг (голосовий фішинг), смішинг (SMS-фішинг), уособлення бренду та фішинг QR-кодів, який обходить SEG. Минулого року у Cofense зросла кількість повідомлень про активні загрози з QR-кодом на 331%.

Охорона здоров’я та фінанси залишаються найбільш цільовими галузями: у цих галузях кількість шкідливих електронних листів в обхід SEG зросла на 84,5% і 118% відповідно.

У звіті також містяться поради щодо нових загроз, на які варто звернути увагу. Видача себе за бренд і рекламні кампанії зростають, оскільки зловмисники використовують цю тактику, щоб обдурити співробітників. Ці атаки ефективно обходять SEG, оскільки вони часто не мають вкладень або очевидних посилань.

Також очікується, що компрометація бізнес-електронної пошти залишиться одним із найстрашніших кіберзлочинів, коли шахраї використовують фішингові атаки на основі розмов. Традиційні засоби захисту часто не в змозі вловити ці атаки, що призводить до крадіжки мільярдів доларів щорічно.

«Коли ми оприлюднюємо статистику зі щорічного звіту про стан безпеки електронної пошти за 2024 рік, стає очевидним, що вектор атак на електронну пошту розвивається безпрецедентними темпами до 2024 року», — сказав виконавчий директор Девід Ван Аллен. «Дані, які ми надаємо в цьому звіті, прямо говорять про ескалацію складності кіберзагроз, які вимагають іншого підходу до ефективної безпеки електронної пошти».

Останній висновок міститься не безпосередньо у звіті, а в підтверджуючих документах від Cofense: не минуло навіть двох місяців 2024 року, а цього року кількість електронних листів, які оминають SEG, зросла більш ніж удвічі. Це проблема, яка лише посилюватиметься без відповідних дій на корпоративному рівні». ***(Duncan Riley. New report warns of ongoing rise of malicious emails bypassing secure email gateways // SiliconANGLE Media Inc. (https://siliconangle.com/2024/02/20/new-report-warns-ongoing-rise-malicious-emails-bypassing-secure-email-gateways/?utm_source=flipboard&utm_content=SiliconANGLE%2Fmagazine%2FSiliconANGLE). 20.02.2024).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«У п’ятницю влада США повідомила, що вилучила веб-сайти, які використовувалися для продажу шкідливого програмного забезпечення

кіберзлочинців під назвою «Warzone RAT», яке могло використовуватися для викрадення даних з комп'ютерів жертв.

Двоє людей на Мальті та в Нігерії були заарештовані за відповідними звинуваченнями, додали вони.

Федеральна прокуратура в Бостоні заявила, що правоохоронні органи ліквідували чотири домени, які разом пропонували продавати зловмисне програмне забезпечення, яке дозволяло кіберзлочинцям таємно підключатися до комп'ютерів людей із зловмисною метою.

Зловмисне програмне забезпечення, так званий троян віддаленого доступу, дозволяло хакерам переглядати файлові системи, робити скріншоти, отримувати імена користувачів і паролі жертв, записувати натискання клавіш і спостерігати за користувачами комп'ютерів через веб-камери, заявили прокурори.

Джоді Коен, глава Бостонського офісу Федерального бюро розслідувань, назвала це складним шкідливим програмним забезпеченням, яке використовувалося для зараження комп'ютерів у всьому світі.

Двоє осіб за кордоном зараз перебувають під вартою, і їм висунуто звинувачення у Сполучених Штатах за ймовірну причетність.

Обвинувальний висновок, поданий до федерального суду в Атланті, звинуватив 27-річного Даніеля Мелі із Заббара, Мальта, у завданні несанкціонованої шкоди захищеним комп'ютерам та інших правопорушеннях, пов'язаних з кібернетичною діяльністю.

Прокурори заявили, що з 2012 року він продавав такі шкідливі програми, як Warzone RAT, через онлайн-форуми комп'ютерних хакерів і пропонував для продажу навчальні засоби, зокрема електронну книгу. Уряд США домагається його екстрадиції.

31-річний принц Оньєозірі Одинакачі з Нігерії був звинувачений у змові з метою вчинення численних комп'ютерних вторгнень за звинуваченням, поданим у Бостоні, заявили прокурори.

У звинуваченні стверджувалося, що з червня 2019 року по березень 2023 року Odinakachi надавав онлайн-підтримку користувачам шкідливого програмного забезпечення Warzone RAT.

Адвокатів Мелі та Одинакачі визначити не вдалося». ***(Nate Raymond. US Says It Dismantles 'Warzone RAT' Malware Service, Suspects Arrested // U.S. News & World Report L.P. (https://www.usnews.com/news/technology/articles/2024-02-09/us-says-it-dismantles-warzone-rat-malware-service-suspects-arrested?utm_source=flipboard&utm_content=user%2FUSNews). 09.02.2024).***

***

«ФБР оголосило в четвер, що успішно зруйнувало очолювану російським ГРУ хакерську кампанію, яка проникла в понад тисячу домашніх і малих бізнес-маршрутизаторів, які використовувалися для проведення кібероперацій проти країн по всьому світу, включно зі США.

Зазначається, що скоординована дія правоохоронних органів з іншими іноземними партнерами успішно завантажила операторів ГРУ з маршрутизаторів, заблокувавши їхні можливості для повторного доступу до них, повідомило Міністерство юстиції.

Департамент заявив, що ідентифікував конкретне зловмисне програмне забезпечення, на яке ГРУ покладалося для проникнення в маршрутизатори під назвою «Moobot», яке було встановлено на маршрутизаторах і яке ГРУ використовувало, щоб перетворити його на «глобальну платформу кібершпигунства».

У Міністерстві юстиції заявили, що ГРУ використовувало проникнуті маршрутизатори для вчинення ряду злочинів, які включали «масштабні кампанії підману», спрямовані на «об'єкти розвідувального інтересу для російського уряду, такі як уряди США та інших країн, військові, служби безпеки та корпоративні. організації».

Під час санкціонованої судом операції минулого місяця Міністерство юстиції заявило, що використовувало зловмисне програмне забезпечення для копіювання

та видалення шкідливих даних із маршрутизаторів і повернення жертвам повного контролю над їхніми мережами.

«Міністерство юстиції прискорює наші зусилля, щоб перервати кіберкампанії російського уряду проти Сполучених Штатів і наших союзників, включаючи Україну», — заявив генеральний прокурор Меррік Гарленд у релізі, в якому оголосив про зрив кампанії. «У цьому випадку російські спецслужби звернулися до злочинних угруповань, щоб допомогти їм націлитися на домашні та офісні маршрутизатори, але Міністерство юстиції відключило їхню схему. Ми продовжуватимемо знищувати та демонтувати шкідливі кіберінструменти російського уряду, які загрожують безпеці Сполучених Штатів. і наші союзники».

Директор ФБР Крістофер Рей вперше оголосив новини про кампанію дезорганізації, яка отримала назву «Операція «Вмираючий вугілля», у виступі на Мюнхенській конференції з безпеки в четвер.

«Завдяки цим операціям — і багатьом іншим подібним — ми націлилися на всі елементи, які, як ми знаємо з досвіду, викликають активність злочинних організацій», — сказав Рей. «Тому що ми хочемо не просто вдарити їх – ми хочемо вдарити їх скрізь, де це боляче, і сильно придушити їх».

Ця операція послідувала за аналогічною спробою зриву, оголошеною ФБР лише два тижні тому, яка призвела до того, що спонсоровані урядом Китаю хакери вивели з сотень маршрутизаторів для дому та малого бізнесу, які нібито використовувалися для атаки на критично важливі інфраструктурні мережі США.

ФБР також опублікувало попередження, зазначивши, що воно все ще працює з інтернет-провайдерами, щоб попередити інших потенційних жертв, сервери яких постраждали». ***(Alexander Mallin, Luke Barr, and Pierre Thomas. US disrupts Russian hacking campaign that infiltrated home, small business routers: DOJ // ABC News (https://abcnews.go.com/Politics/us-disrupts-russian-hacking-campaign-infiltrated-home-small/story?id=107258976&utm_source=flipboard&utm_content=ARTJose%2Fmagazine%2FNEWS+%22THE+WORLD%22). 15.02.2024).***

***

«Міжнародна операція правоохоронних органів у понеділок вилучила сервери та порушила роботу інфраструктури, яку використовував синдикат програм-вимагачів LockBit, остання в серії операцій, спрямованих на порушення технічної інфраструктури злочинних і шпигунських груп.

У серії звинувачень, судових позовів і санкцій операція під назвою «Операція Кронос», проведена Федеральним бюро розслідувань і Національним агентством Великобританії з боротьби зі злочинністю разом із рядом міжнародних партнерів, взяла під контроль сайт, який використовувався LockBit для витоку даних які належать його жертвам, служба обміну файлами та сервер зв’язку групи, різні афілійовані сервери та сервери підтримки, а також сервер для адміністративної панелі LockBit, повідомив CyberScoop старший чиновник ФБР.

У рамках операції ФБР отримало доступ до майже 1000 ключів дешифрування, що дозволяє потенційно відновити або виправити поточні операції вимагання LockBit.

«Ця операція демонструє унікальну та ефективну місію ФБР, яка полягає в тому, щоб стягнути кошти з висококваліфікованих кіберактерів і одночасно визначити пріоритетність допомоги жертвам кібератак», — сказав Бретт Лезерман, заступник помічника директора з кібероперацій у ФБР. інтерв'ю.

Представник LockBit підтвердив операцію в онлайн-повідомленні, опублікованому на X від VX-Underground, онлайн-сховища шкідливих програм. «ФБР мене обкрало», — сказав представник.

«На сьогоднішній день LockBit заблоковано», — заявив у заяві Грем Біггар, генеральний директор Національного агентства з боротьби зі злочинністю. «Ми завдали шкоди можливостям і, головне, довірі до групи, яка залежала від секретності та анонімності».

У рамках операції було затримано двох осіб — одну в Польщі та одну в Україні, йдеться в повідомленні Європолу.

Це останнє у низці операцій ФБР, спрямованих на знищення інфраструктури кіберзлочинності та кібершпигунства в усьому світі відповідно до Правила 41, правової бази, яка дозволяє ФБР отримувати доступ до комп’ютерів у багатьох

юрисдикціях і змінювати їх. Минулого тижня агентство оголосило про ліквідацію ботнету, контрольованого російською військовою розвідкою. У січні ФБР ліквідувало китайський ботнет, який використовувався для проникнення в конфіденційні цілі США.

LockBit вперше з'явився у вересні 2019 року і вважається найпоширенішим у світі варіантом програми-вимагача. Leatherman сказав, що його використовували понад 100 афілійованих компаній у всьому світі, що призвело до виплати програм-вимагачів на суму понад 144 мільйони доларів США та що його цілями стали щонайменше 2000 компаній та інших організацій у всьому світі, у тому числі щонайменше 1600 у США. У 2023 році це був найбільш використовуваний варіант програм-вимагачів для ураження промислових об'єктів, на нього припадає чверть усіх подібних інцидентів, відстежених компанією з кібербезпеки Dragos.

У рамках операції у вівторок уряд США розкрив звинувачення проти двох громадян Росії за їхню ймовірну роль у сприянні атакам LockBit: Артура Сунгатова та Івана Геннадійовича Кондратьєва (також відомого як «Басстерлорд»).

Згідно зі звітом Analyst1 для злочинців-початківців, Bassterlord добре відомий в екосистемі кіберзлочинності, він нібито створював навчальні матеріали, а також брав участь у багатьох інтерв'ю. В інтерв'ю подкасту Click Here Басстерлорд сказав, що воліє називати «Іван», що він українець і що він пішов із кримінальної кар'єри.

Лезерман описав цих двох чоловіків як «оригінальних афілійованих осіб, принаймні з LockBit 1.0».

Групи програм-вимагачів, як-от LockBit, зазвичай працюють за афілійованою моделлю, за якою центральний суб'єкт контролює інфраструктуру, на якій працює програма-вимагач, орендує доступ до цієї системи, а потім ділить прибуток від операцій, які так звані «філії» проводять за допомогою цієї інфраструктури.

Сунгатов і Кондратьєв залишаються на волі, і разом із висунутим у вівторок звинуваченням Міністерство фінансів США ввело проти них санкції. Державний департамент США також має намір оголосити винагороду в розмірі до 10 мільйонів доларів США за інформацію, яка допоможе ідентифікувати чи місцезнаходження

будь-яких лідерів LockBit, а також 5 мільйонів доларів США за інформацію про осіб, які беруть участь у діяльності програм-вимагачів LockBit.

Раніше цього місяця Державний департамент запропонував аналогічну винагороду за інформацію, пов'язану з ALPHV/BlackCat і Hive. операціями програм-вимагачів.

Операція з видалення LockBit викликає питання про те, наскільки довгою вона буде. Попередні операції проти таких груп призводили до тимчасового зриву їх діяльності лише для того, щоб групи повернулися, використовуючи нову інфраструктуру. У грудні ФБР вилучило частину інфраструктури ALPHV, але група «вилучила її», і версія сайту залишається активною.

Лезерман відмовився вдаватися в деталі операції проти LockBit, але сказав, що дії «порушили інфраструктуру LockBit зовсім іншим способом, ніж BlackCat». Варіант завжди можливо «відтворити», сказав Лезерман, але «LockBit не зможе відновити контроль над серверами, які використовували актори».

Обидва розслідування ще тривають, додав він. Організаціям, які вважають, що вони стали жертвами LockBit, рекомендується перейти на нову цільову сторінку, створену ФБР.

Розкриті у вівторок обвинувальні акти відзначають четверту та п'яту справи, порушені проти обвинувачених афілійованих осіб LockBit з 2022 року. 34-річний Михайло Васильєв, громадянин Росії та Канади, був заарештований у Канаді в листопаді 2022 року. 8 лютого він визнав себе винним у Канаді в кібервимаганні та звинувачення у зброї та очікує екстрадиції до Сполучених Штатів.

Руслан Магомедович Астаміров, громадянин Росії, був заарештований в Арізоні в червні 2023 року за ймовірну участь в атаках LockBit.

Михайло Павлович Матвєєв, ще один громадянин Росії, також відомий як Вазавака, був звинувачений у травні 2023 року за участь у атаках програм-вимагачів, які включали зловмисне програмне забезпечення LockBit, а також варіанти програм-вимагачів Babuk і Hive. Державний департамент пропонує винагороду до 10 мільйонів доларів за інформацію, яка призведе до його арешту». ***(AJ Vicens. FBI, British authorities seize infrastructure of LockBit ransomware group***

// Cyberscoop (https://cyberscoop.com/fbi-operation-seizes-infrastructure-of-lockbit-ransomware-group/?utm_source=flipboard&utm_content=other). 19.02.2024).

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Федеральні цивільні відомства мають до опівночі суботи вранці розірвати всі мережеві з'єднання з програмним забезпеченням Ivanti VPN, яке наразі масово експлуатується кількома групами загроз. Агентство з кібербезпеки та безпеки інфраструктури США ухвалило цей крок у середу після того, як за останні тижні виявило три критичні вразливості.

Три тижні тому Ivanti оприлюднив дві критичні вразливості, якими, за його словами, уже активно користуються зловмисники. За словами компанії, атаки були спрямовані на «обмежену кількість клієнтів», які використовують продукти компанії Connect Secure і Policy Secure VPN. Того ж дня охоронна компанія Volexity заявила, що вразливості використовувалися з початку грудня. У Ivanti не було доступного виправлення, і натомість порадив клієнтам виконати кілька кроків, щоб захистити себе від атак. Серед кроків був запуск перевірки цілісності, яку компанія випустила для виявлення будь-яких компрометацій.

Майже через два тижні дослідники заявили, що нульові дні масово використовувалися в атаках, які здійснювали бекдори на клієнтські мережі по всьому світу. Через день Ivanti не змогла виконати попереднє зобов'язання розпочати розгортання відповідного патча до 24 січня. Компанія почала процес лише в середу, через два тижні після кінцевого терміну, який вона сама собі встановила.

А потім було троє

У середу Ivanti оприлюднив дві нові критичні вразливості в Connect Secure, які відстежуються як CVE-2024-21888 і CVE-2024-21893. Компанія заявила, що CVE-2024-21893 — клас уразливості, відомий як підробка запитів на стороні сервера — «схоже, є мішенню», доводячи кількість активно використовуваних уразливостей до трьох. Представники уряду Німеччини сказали, що вони вже бачили успішні подвиги найновішого. Офіційні особи також попередили, що використання нових вразливостей нейтралізує заходи пом'якшення, які Ivanti порадив клієнтам застосувати.

Кілька годин потому Агентство з кібербезпеки та безпеки інфраструктури (зазвичай скорочено CISA) наказало всім федеральним агентствам, які підпорядковані йому, «відключити всі екземпляри продуктів Ivanti Connect Secure і Ivanti Policy Secure від мереж агентства» не пізніше 23:59 у п'ятницю.. Офіційні особи агентства встановлюють той самий термін для агентств, щоб виконати рекомендовані Ivanti кроки, які призначені для виявлення того, чи їхні VPN Ivanti вже були скомпрометовані під час поточних атак.

Кроки включають:

Виявлення будь-яких додаткових систем, підключених або нещодавно підключених до ураженого пристрою Ivanti

Моніторинг служб автентифікації або керування ідентифікацією, які можуть бути розкриті

Максимально можлива ізоляція систем від будь-яких ресурсів підприємства

Продовження аудиту облікових записів із рівнем привілеїв.

Далі в директиві говорилося, що перш ніж агентства зможуть повернути свої продукти Ivanti в мережу, вони повинні виконати довгу серію кроків, які включають скидання системи до заводських налаштувань, її переналаштування згідно з раніше виданими інструкціями Ivanti та встановлення патчів Ivanti.

«Агентства, які керують проблемними продуктами, повинні вважати, що облікові записи доменів, пов'язані з проблемними продуктами, були зламані», — йдеться в директиві від середи. Далі офіційні особи зобов'язали до 1 березня

агенції скинути паролі «двічі» для локальних облікових записів, відкликати квитки автентифікації з підтримкою Kerberos, а потім відкликати маркери для хмарних облікових записів у гібридних розгортаннях.

Стівен Ейдер, президент Volexity, охоронної фірми, яка виявила перші дві уразливості, сказав, що останні сканування вказують на те, що на сьогоднішній день скомпрометовано принаймні 2200 клієнтів уражених продуктів. Він привітав директиву CISA від середи.

«Це фактично найкращий спосіб усунути будь-які занепокоєння щодо того, що пристрій все ще може бути скомпрометовано», — сказав Адер в електронному листі. «Ми бачили, що зловмисники активно шукали способи обійти виявлення за допомогою інструментів перевірки цілісності. З огляду на попередні та нові вразливості, цей курс дій навколо абсолютно нової та виправленої системи може бути найкращим способом для організацій, щоб не думати, чи їхній пристрій активно скомпрометовано».

Директива є обов'язковою лише для агенцій, підпорядкованих CISA. Однак будь-який користувач уразливих продуктів повинен негайно виконати ті самі кроки, якщо вони цього ще не зробили». ***(Dan Goodin. Agencies using vulnerable Ivanti products have until Saturday to disconnect them // Condé Nast (https://arstechnica.com/security/2024/02/agencies-using-vulnerable-ivanti-products-have-until-saturday-to-disconnect-them/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 02.02.2024).***

***

«Дослідники кібербезпеки виявили значну вразливість у серверах Microsoft Exchange, яка потенційно може вплинути на 97 000 серверів по всьому світу. Проблема, ідентифікована як CVE-2024-21410, дозволяє зловмисникам обійти фільтр SmartScreen і виконати довільний код, що призводить до витоку даних, недоступності системи або і того, і іншого. Корпорація Майкрософт оперативно відреагувала на цю загрозу, випустивши необхідні патчі в

своїх оновленнях безпеки в лютому 2024 року, щоб зменшити ризик, пов'язаний з цією вразливістю.

Після ретельного аналізу 17 лютого 2024 року дослідники з Shadowserver Foundation виявили приблизно 28 000 інтернет-серверів Microsoft Exchange, які були безпосередньо вразливі до CVE-2024-21410, а ще 68 500 перебували під потенційною загрозою. Уразливість існує через недостатнє виконання розширеного захисту для автентифікації (EPA) на сервері Exchange, що підриває захист сервера від передачі облікових даних NTLM і використання.

Німеччина та Сполучені Штати були визначені як країни, де розміщено більшість цих уразливих серверів, що свідчить про широку загрозу операційній безпеці організацій і цілісності даних у цих країнах. Такі вразливості не тільки ставлять під загрозу безперервність роботи заражених об’єктів, але й підвищують ризик складного кібершпигунства та викрадення даних зловмисниками, які прагнуть використати непомітні недоліки системи.

Заходи пом'якшення та безпеки

Визнання корпорацією Майкрософт і швидкі дії щодо виправлення цієї вразливості відображають критичний характер CVE-2024-21410. Оскільки експлойт активно використовується в дикій природі, як підтверджено оновленнями до каталогу відомих використаних уразливостей Агентства кібербезпеки та безпеки інфраструктури США (CISA), організаціям наполегливо рекомендується негайно застосувати надані виправлення. Постійні зусилля Фонду Shadowserver з документування та моніторингу ситуації підкреслюють важливість спільних зусиль у сфері безпеки для подолання кіберзагроз.

Більше того, цей інцидент є суворим нагадуванням для організацій щодо підтримки пильної практики кібербезпеки, включаючи регулярні оновлення системи, комплексну оцінку вразливості та впровадження багаторівневих стратегій захисту для захисту від нових цифрових загроз». ***(Luke Jones. Massive Vulnerability in Microsoft Exchange Threatens Tens of Thousands of Servers // WinBuzzer (https://winbuzzer.com/2024/02/21/massive-vulnerability-in-microsoft-exchange-threatens-tens-of-thousands-of-servers-xcxwbn/). 21.01.2024).***

***

«ESET, компанія, що спеціалізується на кібербезпеці, недавно виправила критичну помилку у своїх антивірусних програмах для ОС Windows. Ця вразливість, позначена як CVE-2024-0353 та оцінена на 7.8 за шкалою CVSS, стосується можливості локального підвищення привілеїв.

Помилку виявили завдяки ініціативі Zero Day Initiative (ZDI). Ця вразливість спрямована на зловживання файловими операціями продуктів ESET, які контролюються системою захисту файлової системи в реальному часі.

Використання вразливості дозволяло потенційним зловмисникам видаляти файли користувача без необхідних дозволів.

Компанія випустила патчі безпеки для всіх своїх продуктів, за винятком тих, що вже не підтримуються.

ESET рекомендує користувачам оновити програмне забезпечення якомога швидше». ***(Олена Явір. Один з найнадійніших антивірусів у світі зламали хакери // Bibliotech. (https://bibliotech.com.ua/tehnika/tech_news/odyn-z-najnadijnishyh-antyvirusiv-u-sviti-zlamaly-hakery). 21.02.2024).***

***

«Експерти з кібербезпеки з компанії Top10VPN виявили дві критичні вразливості у популярних ноутбуках та смартфонах, які можуть призвести до витоку особистих даних користувачів. Ці вразливості, відомі під кодовими назвами CVE-2023−52 160 та CVE-2023−52 161, дозволяють хакерам підключатися до Wi-Fi мережі та атакувати підключені до неї пристрої з використанням шкідливого програмного забезпечення. Зловмисники можуть створювати фальшиві копії легітимних мереж, щоби перехоплювати трафік жертв. Про це інформує TechRadar.

Однак, скористатися цими вразливостями не так просто. Для успішної атаки, Wi-Fi клієнт не повинен перевіряти сертифікат сервера аутентифікації. Крім того, хакеру потрібно знати SSID мережі, до якої зазвичай підключається жертва, і бути фізично близько до неї для підключення.

Кіберфахівці пояснили: CVE-2023−52 161 впливає на будь-яку мережу, яка використовує Linux-пристрій як точку доступу Wi-Fi. Більшість дистрибутивів Linux, а також ChromeOS, вже мають виправлення для цієї вразливості, а оновлення для Android очікується найближчим часом.

Експерти радять користувачам Android-пристроїв вручну налаштовувати сертифікат сервера аутентифікації для всіх збережених корпоративних мереж, щоби запобігти можливій атаці. Це важливий крок для забезпечення безпеки ваших даних від потенційних кібератак через Wi-Fi». ***(Хакери знайшли критичну вразливість, яка дозволяє зламати будь-який гаджет та викрасти персональні дані користувачів // Internetua (https://internetua.com/hakeri-znaishli-kriticsnu-vrazlivist-yaka-dozvolyaye-zlamati-bud-yakii-gadjet-ta-vikrasti-personalni-dani-koristuvacsiv?utm_source=news.ukrnet). 24.02.2024).***

***