**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

№ 7 (липень)

Київ – 2023

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №7 (липень) . – 270 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.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2023
© Національна бібліотека України імені В.І. Вернадського, 2023

ЗМІСТ

«Заступник Секретаря Ради національної безпеки і оборони України Сергій Демедюк провів 22 засідання Національного координаційного центру кібербезпеки.

Учасники засідання обговорили питання щодо розбудови кібердипломатії, стану виконання Стратегії кібербезпеки України та підвищення ефективності щорічного планування реалізації її завдань, а також про додаткові заходи кібербезпеки систем управління технологічними процесами на об'єктах критичної інфраструктури.

Про це повідомляє Рада національної безпеки і оборони України.

У заході взяли участь фахівці Апарату РНБО України, керівного складу Міністерства оборони України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства закордонних справ, Міністерства цифрової трансформації України, Національної поліції України, Національного банку України, керівного складу розвідувальних органів держави, народні депутати України.

«Міжнародна практика засвідчує, що напрямок „кібердипломатії" дедалі частіше стає окремим напрямком зовнішньополітичної діяльності провідних країн світу. В умовах збройної агресії рф проти України, яка здійснюється, зокрема, і в кіберпросторі, питання кібердипломатії набуває ще більшої актуальності для нашої держави», — зазначив Сергій Демедюк.

Учасники засідання підтримали пропозицію заступника Секретаря РНБО України щодо необхідності формування підходів до реалізації заходів у сфері кібердипломатії Міністерством закордонних справ України, а комунікації з міжнародними партнерами — за участю НКЦК та основних суб'єктів національної системи кібербезпеки для забезпечення узгодженої позиції. У цьому контексті обговорено питання щодо створення міжвідомчої робочої групи та відповідної цифрової платформи.

Крім того, учасники засідання заслухали доповідь заступника голови Держспецзв'язку щодо виконання Стратегії кібербезпеки України.

За результатами засідання ухвалено ряд рішень для вирішення зазначених завдань». ***(В умовах збройної агресії рф питання кібердипломатії набуває ще більшої актуальності — Сергій Демедюк // АрміяInform (https://armyinform.com.ua/2023/07/28/na-zasidanni-nkczk-obgovoreno-pytannya-shhodo-rozbudovy-kiberdyplomatiyi-ta-stanu-vykonannya-strategiyi-kiberbezpeky-ukrayiny/). 28.07.2023).***

***

Правове забезпечення кібербезпеки в Україні

«Це просто не налазить на голову. Держспецзв'язку (воно ж - ДССЗЗІ) хоче керувати кібербезпекою і всього держсектору, і приватного бізнесу, і українського війська, прагне давати всім цінні вказівки, дозволяти чи забороняти програми, навіть призначати своїх «офіцерів кіберзахисту» в ЗСУ. Для цього пропихується тотально-корупційний законопроект 8087, але про це пізніше.

Справа у тому, що Держспецзв'язку сама не в змозі забезпечити базову, примітивну безпеку ключових державних веб-ресурсів – тобто виконати свої прямі обов'язки.

Ось черговий приклад: світові гіганти вважають веб сайт української Державної податкової служби – незахищеним (Safari, на скріні). Chrome вважає його «ненадійним».

Нагадаю, що кібербезпека центральних органів виконавчої влади є прямою сферою відповідальності Держспецзв'язку. А там, як бачите, - кінь не валявся. Понтів – до неба, амбіцій – як в Наполеона Бонопарта, бездонні кишені вимагають бабла. А от роботу робити, якісно та відповідально – це не до них, це «не на часі».

«Дайте нам значно більше влади та повноважень» – буквально кричить законопроект 8087, який агресивно просувається через Верховну Раду псевдо-цифровим нардепом паномФ.

Попри шалений спротив громадськості, попри очевидний для всіх шкідливий характер законопроекту, попри його кричущу корупційність. Попри різко негативний висновок головного юридичного управління Верховної Ради. Навіть попри пряму шкоду інтересам українському війську. Про таку шкоду, до речі, публічно заявив заступник міністра оборони з питань цифрової трансформації В. Дейнега.

Все це свято корупційного свавілля очевидне для всіх, – окрім вигодонабувачів 8087, якими є Держспецзв'язку та його куратор, головний «цифровізатор» країни. І їм неможливо нічого довести, їм чхати на аргументи. Тому що у них дві справжні цілі: Бабло та Контроль.

Якщо Держспецзв'язку, одне з найбільш корумпованих відомств, стає монополістом з абсолютно усіх питань кібербезпеки в масштабах країни – це збільшить корупцію у цій сфері просто в десятки раз. Одночасно, рівень кіберзахищеності країни - точно не підвищиться.

А от наявність власних «комісарів» в усіх структурах влади (на додаток до вже існуючих так званих CDTO) та навіть у приватних організаціях – створює (точніше розширює) таку собі «державу в державі» імені Федорова. З відповідним прямим доступом до усієї інформації в усіх мережах, на усіх пристроях, в усіх приміщеннях. Переважно у державному секторі, але також і у ключових приватних структурах. А попереду у нас вибори… Натяк достатньо зрозумілий?

Наразі ж питання доволі просте: чи можна організації, яка не здатна виконати елементарне завдання – проконтролювати наявність https/сертифіката на головних веб сайтах ЦОВВ – доручати значно складніші та відповідальніші речі?

І ще одне питання: чи можна приймати під час війни закон, проти якого категорично проти Міністерство оборони України?

Якщо мислити категоріями здорового глузду та інтересів України – відповідь на ці питання одна. Але якщо мова йде про велике бабло та мету за будь-яку ціну утриматися при владі – відповідь буде іншою. Чию сторону обере Верховна Рада України – побачимо найближчим часом. Яким шляхом піде українська національна кібербезпека – цивілізованим чи дикунським, демократичним чи авторитарним,

корупційним чи європейським, і чи ламатимуть українське суспільство через коліно – про це дізнаємося 14 липня, коли Рада розглядатиме законопроект 8087». ***(Костянтин Корсун. Розвиток корупції у сфері кібербезпеки України // Цензор.НЕТ (https://censor.net/ru/blogs/3430501/rozvytok_koruptsiyi_u_sferi_kiberbezpeky_ukrayiny). 12.07.2023).***

***

«За результатами громадських слухань щодо законопроекту № 8087 підприємці, юристи, експерти дійшли згоди, що законопроект потребує суттєвого серйозного доопрацювання через невідповідність сучасним європейським стандартам у сфері кібербезпеки та створення загроз для бізнесу.

Відповідні звернення були відправлені на президента, голові Верховної Ради, всім головам комітетів.

Утім, у порядку денному Верховної Ради у п’ятницю, 14 липня, є голосування за цей законопроект. Тобто, голос бізнесу почутий не був.

Раніше звернення за результатами громадських слухань, організованих Українським союзом промисловців і підприємців спільно з Радою адвокатів Київської області, спрямували на адресу президента Володимира Зеленського, голови Верховної Ради України Руслана Стефанчука та у всі комітети та фракції Ради.

Громадські слухання відбулися 29 червня за участі представників Міністерства оборони України, уряду, адвокатської спільноти, представників антикорупційних органів, громадськості, ІТ-бізнесу, експертів.

Учасники погодилися, що законопроект потребує суттєвого доопрацювання і вдосконалення.

По-перше, він в багатьох моментах не відповідає, а іноді навіть суперечить положенням Директиви ЄС про мережеву та інформаційну безпеку (NIS2

Directive), яку було прийнято 14 грудня 2022 року і яка вступає в дію на території ЄС 18 жовтня 2024 року.

Наприклад NIS2 Directive не діє щодо суб'єктів, діяльність яких здійснюється у сфері національної безпеки, а також встановлює чіткий перелік критеріїв щодо компаній, щодо яких вона застосовується. Водночас законопроєкт № 8087 охоплює усі без виключення державні органи та суб'єкти господарювання, навантажуючи непомірним адміністративним та фінансовим тягарем навіть найменші з них.

Крім того, поки увесь цивілізований світ зараз рухається в бік децентралізації систем кібербезпеки і посилення їх взаємодії між собою (про що також ідеться у NIS2 Directive), в Україні можуть запровадити ще одну вертикаль, яка об'єднує всі державні інформаційні ресурси. Це робить її більш вразливою до кібератак.

По-друге, законопроект № 8087 зачіпає не тільки питання кібербезпеки загалом і кібербезпеки державного сектору зокрема. Він, як йдеться у його тексті, який дещо суперечить назві самого законопроекту, стосується також значною мірою приватного інформаційного сектору, бізнес-клімату, інвестиційної привабливості тощо.

Основним недоліком законопроєкту № 8087 на громадських слуханнях назвали значне розширення повноваження Державної служби спеціального зв’язку та захисту інформації (Держспецзв'язку) та покладає на неї безпрецедентно широкі повноваження.

Серед іншого, контролюючий орган отримає право здійснювати перевірки будь-яких підприємств, доступ до їх споруд і приміщень, будь-якої їх документації та інформації, надавати обов’язкові для виконання вимоги будь-якому суб'єкту господарювання, незалежно від того, чи буде це велика корпорація, підприємство ІТ-бізнесу, чи самозайнята особа (ФОП, адвокат тощо). До того ж Держспецзв’язку матиме право залучати до таких перевірок будь-які інші органи, зокрема СБУ та кіберполіцію.

Така ситуація безконтрольності та відсутності обмежувальних механізмів для Держспецзв’язку створює величезні корупційні ризики, створює можливості для блокування діяльності будь-якого бізнесу, тиску на нього, «рейдерства» тощо.

На громадських слуханнях помітили, що розширення вказаних повноважень державних органів може не узгоджуватись із положеннями відповідного процесуального законодавства (перш за все кримінального-процесуального), а також може зумовити безпідставне і необґрунтоване розкриття персональних даних і іншої інформації (наприклад адвокатської таємниці тощо).

Реалізація нормативних положень законопроекту № 8087 може негативно вплинути на стан захисту в Україні прав людини та не узгоджуватись із відповідною практикою Європейського суду з прав людини». ***(Депутати готуються проголосувати за законопроект про кібербезбеку, проти поточної редакції якого виступив бізнес, юристи, Міноборони та експерти // Ракурс® (https://racurs.ua/ua/n184973-vlada-proignoruvala-golos-biznesu-schodo-doopracuvannya-zakonoproektu-pro-kiberbezpeku.html). 10.07.2023).***

***

Кібервійна проти України

«Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, попередила про можливі нові атаки на державні органи.

Про це повідомляє Держспецзв'язку.

Фахівці проаналізували актуальні тактики, техніки та процедури, що використовують хакери одного з найбільш активних та небезпечних російських хакерських угруповань – UAC-0010 (Armageddon / Gamaredon). До нього належать колишні «офіцери» із СБУ в АР Крим, які у 2014 році зрадили Батьківщину і почали прислужувати ФСБ РФ.

Основним завданням угруповання є кібершпигунство щодо сил безпеки та оборони України. Також відомо щонайменше про один випадок здійснення деструктивної діяльності на об'єкті інформаційної інфраструктури.

У CERT-UA додають, що кількість одночасно інфікованих комп'ютерів, які переважно функціонують в межах інформаційно-комунікаційних систем державних органів, може сягати кількох тисяч.

Як атакують хакери?

Як вектор первинної компрометації хакери здебільшого використовують електронні листи та повідомлення в месенджерах (Telegram, WhatsApp, Signal), які розсилають через заздалегідь скомпрометовані облікові записи.

Найпоширенішим способом є надсилання жертві архіву, що містить HTM або HTA-файл, відкриття якого ініціює ланцюг інфікування.

Для розповсюдження шкідливих програм передбачена можливість ураження знімних носіїв інформації, легітимних файлів (ярликів), а також модифікації шаблонів Microsoft Office Word, що забезпечує інфікування всіх створюваних на ЕОМ документів через додавання відповідного макросу.

Після початкового ураження зловмисники можуть викрадати файли з розширеннями.doc,.docx,.xls,.xlsx,.rtf,.odt,.txt,.jpg,.jpeg,.pdf,.ps1,.rar,.zip,.7z,.mdb протягом 30-50 хвилин. Здебільшого це відбувається шляхом застосування шкідливих програм GAMMASTEEL.

Комп'ютер, що функціонує в ураженому стані близько тижня, може налічувати від 80 до 120 і більше шкідливих (інфікованих) файлів, без урахування тих файлів, що будуть створені на знімних носіях інформації, які будуть підключатися до системи протягом цього періоду». ***(Анастасія Жарикова. Держспецзв'язку попереджає про можливу хвилю кібератак держорганів // Економічна правда (https://www.epravda.com.ua/news/2023/07/14/702239/). 14.07.2023).***

***

«Фахівці Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, проаналізували актуальні тактики, техніки та процедури, що використовують хакери одного з

найбільш активних та небезпечних російських хакерських угруповань — UAC-0010 (Armageddon / Gamaredon).

Про те, що до цього хакерського угруповання належать колишні «офіцери» із СБУ в АР Крим, які у 2014 році зрадили Батьківщину і почали прислужувати фсб росії, на урядовому порталі нагадала Державна служба спеціального зв'язку та захисту інформації України.

Основним завданням угруповання є кібершпигунство щодо сил безпеки та оборони України. Також відомо щонайменше про один випадок здійснення деструктивної діяльності на об'єкті інформаційної інфраструктури.

За даними CERT-UA, кількість одночасно інфікованих комп'ютерів, які переважно функціонують в межах інформаційно-комунікаційних систем державних органів, може сягати кількох тисяч.

Як атакують

Як вектор первинної компрометації хакери здебільшого використовують електронні листи та повідомлення в месенджерах (Telegram, WhatsApp, Signal), які розсилають через заздалегідь скомпрометовані облікові записи. Найпоширеніший спосіб — надсилання жертві архіву, що містить HTM або HTA-файл, відкриття якого ініціює ланцюг інфікування.

Для розповсюдження шкідливих програм передбачена можливість ураження знімних носіїв інформації, легітимних файлів (зокрема, ярликів), а також модифікації шаблонів Microsoft Office Word, що забезпечує інфікування всіх створюваних на ЕОМ документів через додавання відповідного макросу.

Після початкового ураження зловмисники можуть викрадати файли з розширеннями.doc,.docx,.xls,.xlsx,.rtf,.odt,.txt,.jpg,.jpeg,.pdf,.ps1,.rar,.zip,.7z,.mdb протягом 30-50 хвилин — здебільшого із застосуванням шкідливих програм GAMMASTEEL.

Комп'ютер, що функціонує в ураженому стані близько тижня, може налічувати від 80 до 120 і більше шкідливих (інфікованих) файлів, без урахування тих файлів, що будуть створені на знімних носіях інформації, які будуть підключатися протягом цього періоду до ЕОМ.

Інші деталі щодо кібератак угруповання, рекомендації щодо захисту — на сайті CERT-UA за посиланням https://cert.gov.ua/article/5160737.

Також фахівці Урядової команди реагування на комп'ютерні надзвичайні події України застерігають військовослужбовців ЗСУ: якщо на комп'ютері відсутній засіб захисту класу EDR (не «антивірус») — негайно зверніться до Центру кібербезпеки ІТС (в/ч А0334; email: csoc@post.mil.gov.ua) для встановлення відповідного програмного забезпечення.

У групі підвищеного ризику — ЕОМ, розміщені за межами периметру захисту, зокрема ті, які для доступу до інтернету використовують термінали Starlink.

Відсутність згаданої технології захисту підвищує вірогідність кібератак як на окремий комп'ютер, так і на всю інформаційно-комунікаційну систему (мережу) підрозділу.

У разі виявлення факту ураження за наведеними CERT-UA індикаторами — невідкладно повідомляйте Центр кібербезпеки ІТС. (Урядова команда реагування на комп'ютерні надзвичайні події України застерігає щодо нових кібератак держорганів // АрміяInform». ***(https://armyinform.com.ua/2023/07/15/uryadova-komanda-reaguvannya-na-kompyuterni-nadzvychajni-podiyi-ukrayiny-zasterigaye-shhodo-novyh-kiberatak-derzhorganiv/). 15.07.2023).***

***

«…Російські хакери спрямували чимало зусиль на те, щоб порушити нормальну діяльність об'єктів критичної інфраструктури України, зокрема в енергетичному та фінансовому секторах, а також у сфері надання державних послуг.

За підрахунками Державної служби спеціального зв'язку та захисту інформації, які ППЛ щомісяця отримує у відповідь на запити, за перші чотири місяці повномасштабної війни окупанти майже 800 раз спробували втрутитися в українські мережі. Найбільше атакували уряд і місцеві органи влади, сектор безпеки та оборони, фінансовий сектор, комерційні організації та енергетичну

сферу. Також кіберзлочинці завдавали шкоди транспортній інфраструктурі та телекомунікаціям.

Темпи кібератак, спрямованих проти України, неухильно зростають. Їх уже фіксують мільйонами – за п’ять місяців 2023-го у Держспецзв’язку повідомили про більше ніж 85 мільйонів нападів на державний сектор і сайти суспільного користування. І якщо на початку повномасштабного вторгнення напади були спрямовані на військові цілі задля порушення українського військового зв'язку, то з часом хакери все більше почали націлюватися на портали послуг, якими користуються люди в повсякденному житті, та інформаційні ресурси.

Вже у цьому році зафіксовані атаки на Міністерство культури та інформаційної політики, Міністерство захисту довкілля та природних ресурсів, систему електронної пошти судової системи України, Міністерство юстиції. Хакери також намагалися втрутитися в мережі Інституту масової інформації та проєкту Ukraïner, який є майданчиком історій з України для всього світу. Кібератак зазнали й українські медіа – у тому числі, інформагентство «Укрінформ», миколаївські інтернет-видання «Преступности.НЕТ» і «NikLife» та Суспільне мовлення.

До речі, сайт Суспільного тимчасово вже переставав працювати 1 березня 2022 року – якраз у той день, коли окупанти обстріляли київську телевежу, – що говорить про координацію хакерських атак зі збройною агресією. Ще одним прикладом таких скоординованих нападів у Держспецзв'язку називають втручання росіян у мережі ДТЕК минулого літа.

Кібератаки РФ на критично важливу та цивільну інфраструктуру, скоєні в той же час, що і ракетні удари, офіційний Київ вважає військовими злочинами. Відповідну інформацію збирають і передають до Міжнародного кримінального суду в Гаагу.

Кремлівські хакери полюють як за державними системами України, так і за її простими громадянами. Для цього найактивніше використовують фішинг – улюблену тактику інтернет-зловмисників.

Існують різні його типи, та найпоширеніший – фішинг в електронних листах. Хакери надсилають шкідливі гіперпосилання або вкладення. Їх відкриття запускає програму, що надає доступ до даних або навіть може паралізувати цілі ІТ-системи. На перший погляд, такі посилання та вкладення виглядають як безпечні файли з резюме чи, наприклад, банківською випискою.

За допомогою фішингу російські спецслужби намагаються зібрати про українців усю можливу інформацію, в їхньому фокусі – персональні дані. За перші п’ять місяців цього року Департамент кіберполіції НПУ отримав понад 15 тисяч звернень від громадян, які постраждали від фішингових атак.

Як видно зі звіту «Війна у цифровому вимірі та права людини» за лютий 2023-го, урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, що діє при Держспецзв’язку, зафіксувала масове розповсюдження небезпечних електронних листів начебто від імені Печерського районного суду Києва. Листи містили додаток у вигляді rar-архіву, після відкриття якого на комп’ютері користувача встановлювалася програма для віддаленого контролю та викрадення даних. Також у лютому фахівці CERT-UA виявили небезпечний сайт, який імітував офіційний веб-ресурс Міністерства закордонних справ України і за допомогою якого зловмисники намагалися викрадати дані.

Інформація як зброя

Свою збройну агресію Росія супроводжує масштабною інформаційною війною проти України. Експерти ППЛ щомісяця фіксують більше 150 дезінформаційних повідомлень, які ворог розповсюджує в інтернеті, щоб формувати суспільні думки та настрої українців, вигідні Кремлю. Для досягнення своєї мети пропагандисти використовують різноманітні інформаційні ресурси та залучають до цього величезну кількість людей.

Наприклад, як показав моніторинг дотримання цифрових прав, у березні 2023 року СБУ викрила в Хмельницькій області ботоферму, через яку поширювалися фейки про війну в Україні. Понад 2 тисячі ботів «розганяли» дезінформацію про ситуацію на фронті та закликали українців ухилятися від мобілізації. Також проросійський осередок займався дискредитацією військово-політичного

керівництва та підрозділів Сил оборони нашої держави. Замовляли послуги ботоферми представники спецслужб Росії. Вони купували фальшиві акаунти та використовували їх у популярних соцмережах нібито від імені пересічних українців. А вже у травні СБУ ліквідувала мережу ботоферм з аудиторією майже в 200 тисяч користувачів, які поширювали дезінформацію для розхитування суспільно-політичної ситуації в Україні.

Якщо в перші місяці широкомасштабного вторгнення фейки, що зустрічалися в мережі, переважно виправдовували російську агресію «денацифікацією» України та «загрозою» з боку НАТО, сіяли паніку в нашому суспільстві та залякували світ вигадками про біолабораторії, які нібито діють в Україні, то під кінець 2022 року риторика Кремля почала змінюватися. Поразки на фронті примушували ворога шукати нові теми, щоб якось виправдати власні невдачі та перекласти відповідальність за скоєні злочини на ЗСУ.

У 2023-му російська пропаганда стала наполегливо поширювати в своїх повідомленнях зневіру українців у ЗСУ, перемозі та підтримці міжнародних партнерів, підривати довіру людей до центральної влади та місцевого самоврядування, створювати негативний образ України як держави, якою керує Захід. Кремль перестав «рятувати Україну від неонацистів» – у вигаданому ним інформаційному просторі РФ уже «воює з Заходом».

Постачання Україні зброї іноземними партнерами та контрнаступ ЗСУ – також актуальні зараз теми для розповсюдження фейків у проросійських медіа й анонімних телеграм-каналах. Українці такі повідомлення трактують по-своєму: мовляв, чим більше росіяни нагнітають в інформаційному просторі, тим вони слабші на фронті. Принаймні, так було в минулому році, коли ми раділи звільненню Херсона. У Кремлі тим часом готували для українців – та й для усього світу – нову інформаційну операцію, вибудовану на сценаріях підриву Каховської ГЕС.

У ніч з 5 на 6 червня дамбу таки підірвали, трагедія стала головною світовою новиною, а окупанти вдавалися до своєї звичної тактики – «це все не ми, то українці самі собі нашкодили». Більше про дезінформаційні повідомлення, які

супроводжували в мережі цю подію можна прочитати на сайті ППЛ в аналітичному звіті «Війна у цифровому вимірі та права люди» за червень.

Зараз в кіберпросторі вже проводиться нова інформаційна операція – тепер уже навколо питання «а що ж буде із ЗАЕС?». Завдання України в кібервійні – так само вчасно давати відсіч ворогу, як і на полі бою. Бути пильними в інтернет-просторі – завдання кожного й кожної з нас.

Платформа прав людини продовжує й надалі збирати, досліджувати та узагальнювати дані про події, що в умовах війни мають вплив на цифрові права громадян і громадянок. Окрім того, медіаюристи ППЛ працюють над захистом свободи слова, вираження поглядів і права доступу до публічної інформації – гарантованих законом прав і свобод, які через повномасштабне російське вторгнення та загрозу національній безпеці в Україні зазнають обмежень, і не завжди правомірних». ***(Ірина Шаталова. Кібератаки як воєнні злочини: огляд моніторингу дотримання цифрових прав українців // LB.ua (https://lb.ua/blog/koalitsiia_ua5am/565304_kiberataki_yak_voienni_zlochini_oglyad.html). 14.07.2023).***

***

«Кількість DDoS-атак у всьому світі щороку зростає. Черговий масштабний спалах кіберзагроз стався 2022 року, коли Росія розпочала проти України повномасштабну війну, частиною якої є кіберфронт. Так, російські спецслужби та пов’язані з ними групи кіберзлочинців намагаються паралізувати роботу держустанов, критичної інфраструктури, банків і бізнесу як в Україні, так і поза її межами. Як захищатися від кіберагресорів?

Урядова команда реагування на комп’ютерні надзвичайні події України (CERT-UA) звітує, що загалом протягом 2022 року кількість зареєстрованих кіберінцидентів в Україні зросла майже втричі проти 2021 року.

А впродовж березня-квітня вже 2023-го експерти фіксували зростання кількості кібератак на комерційні організації: майже вдвічі проти січня-лютого 2023 року. Наприклад, в Агентстві національної безпеки США в квітні заявляли,

що російські хакери атакують камери відеоспостереження в українських кав'ярнях, аби відстежувати рух колон із гуманітарною допомогою.

Тож загальна тенденція така: кіберзагроз, зокрема й DDoS-атак, дедалі більшає, і спрямовані вони на дедалі ширше коло цілей — як державних, так і комерційних. Саме тому організаціям слід забезпечити собі надійний кіберзахист.

DDoS-атака: що це й для чого?

Це спроба зловмисників порушити нормальний інтернет-трафік і зупинити роботу сервера, мережі або інфраструктури, перевантаживши їх потоком фейкових запитів. Якщо простіше, то це схоже на раптовий затор, який перенавантажує головну дорогу муляжами автомобілів і заважає справжньому транспорту продовжувати рух.

Чому ж потрібно турбуватися про DDoS-атаки й, найголовніше, як можна захистити свій бізнес від них? Насамперед варто зазначити, що жоден бізнес не застрахований від таких кіберзагроз. Навіть найбільші компанії змушені враховувати це. А для багатьох малих і середніх підприємств, які використовують технології VoIP, імовірність атаки ще вища. Адже системи VoIP зазвичай доступні через мережу Інтернет. А як ми розуміємо, будь-яка програма, підключена до Інтернету, ризикує бути атакованою зловмисниками. Системи VoIP зазвичай не мають такого ж рівня захисту, як більш традиційні IT-системи, що відразу враховують захист від DDoS-атак.

Мотиви DDoS-атак можуть бути різними — від ідеологічних і воєнних до виключно економічних у межах нечесної конкуренції. Розгляньмо головні.

Ідеологічні. Групи хакерів здійснюють DDoS-атаки на уряди, політиків і компанії різних країн через ідеологічні розбіжності.

Кібервоєнні. Пов'язані з ідеологічними. Групи хакерів можуть працювати на державу або в координації з нею та цілитись на критично важливу інфраструктуру ворога, зокрема й фінансові, медичні, транспортні та комунікаційні послуги. Нині Україна постійно стикається з такими нападами на кіберфронті.

Кібервандалізм. Кібервандали — це окремі особи чи групи, які здійснюють кібератаки без будь-яких очевидних раціональних мотивів із метою завдати шкоди.

Вимагання. В цьому випадку кіберзлочинці влаштовують DDoS-атаки або погрожують їх влаштувати, наприклад, аби отримати гроші.

Димова завіса. Зловмисники іноді використовують DDoS-атаки, щоб відвернути увагу співробітників служби безпеки та IT-фахівців або послабити системи безпеки. Це допомагає їм штучно створювати вразливості для масштабнішої кампанії атак, таких як проникнення в мережу, крадіжка даних і зараження шкідливим програмним забезпеченням.

Нечесна конкуренція. Мотив DDoS-атаки в цьому випадку — завдання шкоди бізнесу конкурента. Ціллю є, наприклад, порушення роботи вебсайту, що може спонукати клієнта відмовитися від його послуг, а також завдати фінансових і репутаційних збитків.

Негативні наслідки для бізнесу

Відповідальність за захист бізнесу від кібератак лежить безпосередньо на самому бізнесі. Водночас втрати в разі успішних дій зловмисників проти вашої організації можуть бути величезними. Адже DDoS-атаки фактично зупиняють роботу, доки атаку не буде виявлено й усунено. А це означає втрату продуктивності, продажів і зниження якості обслуговування клієнтів. А ще є репутаційний чинник, який може позначитися на бізнесі на місяці чи роки наперед.

Проте є конкретні кроки, до яких ваша компанія може вдатися вже зараз, аби, по-перше, запобігти атакам, а, по-друге, мінімізувати втрати, якщо ви вже постраждали.

Кібероборона

IT-команда, навчена передових методів безпеки. Ваші фахівці мають розуміти, як правильно налаштовувати кіберзахист, а також мати засоби моніторингу кіберзагроз. Це дасть змогу вчасно виявляти та реагувати на DDoS-атаки, що своєю чергою зменшить час простою й мінімізує втрати. Проводьте з командою регулярні тренінги, а також симуляції кіберзагроз, аби перевірити готовність до реальної атаки.

Якщо ви вважаєте, що вже вжили всіх заходів безпеки, тоді дієвим варіантом буде перевірка. Можете звернутися до української компанії, яка спеціалізується на

інформаційній безпеці. Вона за вашою згодою проведе комплекс тестів із проникнення в систему на всіх рівнях. Можна назвати це таким собі «білим хакінгом». Після цього у вас з'явиться додаткова інформація про стан безпеки в компанії.

План реагування на DDoS-атаки. Всі організації повинні мати план безперервної роботи бізнесу, зокрема й план реагування на DDoS-атаки. В ньому має бути задокументовано, як ви підтримуватимете бізнес-процеси в разі успіху DDoS-атаки, а також усі технічні компетенції та досвід, які будуть потрібні. Призначте відповідальних за реагування на атаку, повідомлення ключових зацікавлених сторін і забезпечення зв'язку в усій організації.

Захист власної інфраструктури. Забезпечте свою мережу, програми та інфраструктуру багаторівневими стратегіями захисту від DDoS-атак. Це можуть бути брандмауери, VPN, захист від спаму, фільтрування контенту та інші сервіси для відстеження трафіку, який може виявитися DDoS-атакою.

Налаштуйте, наприклад, Cloudflare. Він може аналізувати вхідний трафік на сайт і визначати аномальні активності, подібні до DDoS-атаки.

Деякі провайдери зв'язку для бізнесу користуються такою системою, як Arbor Sightline. У режимі реального часу вони можуть відстежувати атаку на канали клієнта, а програмне забезпечення та фізичне обладнання дають змогу "фільтрувати" трафік. Так можна прибрати до 95% спамних переходів.

Хмарні рішення, приміром, такі як UCloud, уже містять захист від мережевих атак. А також є економічно вигідними для бізнесу будь-якого масштабу. Адже в цьому випадку клієнту не доводиться купувати й інтегрувати дороге програмне забезпечення та обладнання для кіберзахисту. Натомість він лише щомісяця вносить абонентську плату за користування хмарою.

Оновлення власних систем. Адже застарілі системи часто мають найбільшу кількість лазівок, якими можуть скористатися зловмисники та хакери.

Ліцензування — один з найпростіших шляхів до безпеки. Наявність підтримки від виробника програмного забезпечення — це не лише доступ до всіх

можливостей застосунків чи програмних комплексів, а й змога отримувати свіжі оновлення безпеки.

Як уже зазначалося, хакери знаходять прогалини в застарілих системах. Наприклад, через вебверсію Outlook можна було віддалено запускати виконання шкідливого коду на вразливих серверах Microsoft Exchange. Упоравшись із такими викликами, компанія Microsoft публікує оновлення програмного забезпечення й надсилає повідомлення в застосунку або ж на пошту щодо його оновлення. Тож не варто забувати вчасно все інсталювати.

Реагування на DDoS-атаку

Після того, як ви підтвердите, що зазнали DDoS-атаки, дуже важливо вдатися до негайних дій, аби пом’якшити вплив і відновити нормальну роботу. Реагування може бути програмним, із використанням спеціального ПО, та людським, із залученням IT-фахівців.

Програми. На ринку нині є безліч цифрових продуктів, які пропонують послуги з виявлення DDoS-атак і керування реакціями на них. Також через них можна моніторити пропускну здатність мережі, що дає змогу перебудовувати мережевий трафік для ефективнішого використання.

Люди. Бізнес залучає IT-фахівців, які працюють на компанію й мають план реагування на кіберзагрози. Вони своєю чергою застосовують найпоширеніші методи усунення DDoS-атак, такі як налаштування обмеження швидкості брандмауера на боці сервера, обмеження швидкості запитів до сервера, змінюють записи DNS для домену тощо.

Водночас ці два шляхи реагування можуть бути складними в адмініструванні й утриманні, тому бізнес часто шукає партнерів, котрі знають, як підтримувати інфраструктуру кіберзахисту. Такий підхід часто є найефективнішим для швидкого запобігання DDoS-атакам і забезпечення довгострокової кібербезпеки. Надійні партнери мають бути готові допомогти зменшити час, необхідний для реагування на інцидент, звести до мінімуму його вплив і допомогти швидше відновитися.

Водночас правда полягає в тому, що жодне рішення ніколи не буде ефективним на 100%, натомість за допомогою деяких простих заходів ваші

співробітники можуть бути краще підготовленими до запобігання DDoS-атакам, а ваша IT-команда — впевненішою в своїй здатності запобігати їм». ***(Данило БЄЛОВ. DDOS-атаки на вашу інтелектуальну власність: чим загрожують і як від них захиститися // Укррудпром (https://ukrrudprom.com/digest/DDOSataki_na_vashu_ntelektualnu_vlasnst_chim_zagroguyut__yak_vd_nih_zahistitisya.html). 17.07.2023).***

***

«Суспільне», Мінрозвитку, «24 канал», українські інтернет-провайдери, Південний ГЗК і постійні «деанони» відомих медійних персон — усе це справа рук одного з найактивніших на сьогодні хакерських угруповань окупантів «Солнцепек». Видання Dev.ua провело невелике розслідування та спробувало з'ясувати в експертів, хто стоїть за цими хакерами та наскільки небезпечні їхні атаки.

Хто став жертвами «Солнцепек»

Одна з найперших помітних атак хакерів сталася на мережу Мінрозвитку, 25 квітня їм удалося пробитися через слабкозахищену пошту одного зі звільнених співробітників установи. ЗМІ привело цитату глави відомства Олександра Кубракова, проте потім виявилася фейком, запущеним РФ для дискредитації українських кіберсил.

На початку травня хакери зламали сайт «24 каналу» й опублікували на його сторінках безліч фейків і погроз на адресу Президента Володимира Зеленського. Того ж дня були атаковані українські провайдери Citylan, Gigabit-net, UOS, UA Group, FiberNet та інші.

Однією з найнебезпечніших атак можна вважати спробу злому серверів Південного гірничо-збагачувального комбінату, що, за заявою кіберзлочинців, «не дасть змоги отримати ЗСУ бронежилети, бронеавтомобілі, безпілотники, гаубиці DANA та Zuzana 2». Група «Солнцепек» заявила, нібито «знищила понад 30 серверів і викрала важливу інформацію», але в пресслужбі підприємства Фокус тоді запевнили, що атаку відбито і всі наслідки усунуто.

У середині червня був атакований сайт «Суспільного», і зараз розслідуванням цієї атаки займається Держспецзв'язку.

Крім цього, хакери з російського угруповання «Солнцепек» активно публікують у себе в Telegram-каналі «деанонімізуючу інформацію» про відомих медійних персон, наприклад, там з'являлися особисті дані активіста Сергія Стерненка й телеведучої Наталії Мосейчук. Публікують на каналі й особисту інформацію українських військових.

Хто «кришує» хакерів із «Солнцепек»

Багато хакерських угруповань із Росії діють під заступництвом спецслужб. На думку експертів, «Солнцепек» не стала винятком, і її курують співробітники Головного розвідувального управління РФ.

«Активність цих кібератак відстежується CERT-UA із ідентифікатором UAC-0165. Водночас із високим рівнем упевненості ця активність асоціюється з діяльністю угруповання Sandworm», — розповіли в Держспецзв'язку.

Фокус розповідав своїм читачам про це відоме російське хакерське угруповання, за яким стоїть ГРУ Росії. Його члени добре відомі спецслужбам України та всього світу. Припускають, що саме вони стоять за діями «Солнцепека». Хакерів угруповання навіть затримували в Нідерландах, коли вони планували зламати Організацію із заборони хімічної зброї в Гаазі (ОЗХЗ).

Найбільшої шкоди всьому світу кібертерористи із Sandworm завдали за допомогою свого вірусу NotPetya, який зашифровував усі файли на комп'ютерах своїх жертв. Основні атаки велися на банки, урядові структури та великі компанії. За підрахунками фахівців, збиток, якого завдали підконтрольні ГРУ РФ хакери із Sandworm, оцінюють у $10 млрд.

Передбачається, що члени Sandworm є штатними офіцерами розвідки та підпорядковуються ГРУ, деякі з них давно перебувають у розшуку та під санкціями. Але тепер, мабуть, «Солнцепек» став підконтрольний Sandworm як одна з «філій» для дрібнішої та не такої масштабної роботи, як у «старших колег».

«Якщо уважно подивитися на їхній канал, то абсолютно очевидно, що це чергова вивіска ГРУ РФ. Вони неуважні та припускаються помилок», — заявив журналістам експерт із кібербезпеки Андрій Баранович.

Наскільки небезпечні хакери із «Сонцепека»

Офіційний коментар, який надали журналістам у СБУ, не надто інформативний: «Кіберфахівці відомства системно та в цілодобовому режимі моніторять усе, що відбувається в мережі інтернет. Однак інформування суспільства про роботу здійснюється з урахуванням правових обмежень на розголошення інформації про контррозвідувальну та оперативно-розшукову діяльність. Про результати роботи спецслужби обов'язково буде поінформовано громадськість».

За стилем і масштабом атак можна припустити, що діяльність хакерів із «Солнцепека» обмежується хоч і частими, але нескладними кібероперaціями на слабозахищені об'єкти, а результативність досить слабка. Можливо, вони лише відвертають увагу служб кіберзахисту від масштабніших і серйозніших атак самого Sandworm.

«Їхні звичні, обкатані схеми просто перестали працювати, ось вони намагаються змінювати свою тактику і в технічному, і в медійному плані. Поки що без особливих результатів, як на мене», — прокоментував хакер Андрій Баранович». ***(Хакери із «Солнцепек» — маріонетки ГРУ РФ? Хто стоїть за групою кібертерористів // Фокус (https://focus.ua/uk/digital/576403-hakeri-iz-solncepok-marionetki-gru-rf-hto-stoyit-za-grupoyu-kiberteroristiv). 03.07.2023).***

***

«Державна команда реагування на надзвичайні ситуації у галузі комп’ютерів CERT-UA України у своїх соцмережах заявила, що комп’ютерам із доступом до інтернету через термінали Starlink можуть загрожувати кібератаки з Росії.

Представники компанії зазначають, що одна з кіберзагроз походить від колишніх офіцерів Служби безпеки України (СБУ), які у Криму з 2014 року працюють на Федеральну службу безпеки (ФСБ) РФ.

«У групі підвищеного ризику знаходяться ЕОМ, які знаходяться за межами периметра захисту, зокрема ті, які використовують термінали Starlink», – пояснили в CERT-UA.

У червні прем'єр-міністр Сполученого Королівства Ріші Сунак говорив, що Великобританія виділить Україні в найближчі два роки до £25 млн ($32 млн за поточним курсом) на зміцнення кібербезпеки.

Фінансування дозволить захистити критично важливу національну інфраструктуру та життєво важливі служби України, а також протистояти кіберзагрозам з боку Росії». ***(Стало відомо про можливу кіберзагрозу для українських комп'ютерів із терміналами Starlink // GSMinfo (https://gsminfo.com.ua/149570-stalo-vidomo-pro-mozhlyvu-kiberzagrozu-dlya-ukrayinskyh-kompyuteriv-iz-terminalamy-starlink.html). 15.07.2023).***

***

«Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA зафіксувала збільшення активності російського хакерського угрупування Armageddon.

Про це повідомляє Держспецзв'язку.

Основним завданням зловмисників є кібершпигунство щодо сил безпеки та оборони України. Також повідомляється про щонайменше одну атаку на об'єкт інформаційної інфраструктури.

За даними CERT-UA, кількість одночасно інфікованих комп'ютерів, що працюють в мережі державних органів, може сягати кількох тисяч.

Як хакери Armageddon атакують комп'ютери держорганів

Зараження починається з розсилання інфікованих файлів електронною поштою або в месенджерах. Для цього використовуються вже скомпрометовані облікові записи.

Шкідливі програми можуть інфікувати й знімні носії інформації, що сприяє їх розповсюдженню.

Після цього зловмисники можуть викрасти файли протягом 30-50 хвилин. За один тиждень уражений комп'ютер накопичує від 80 до 120 шкідливих файлів без урахування тих, що були створені на підключених носіях.

CERT-UA військовослужбовців ЗСУ перевірити наявність засобів захисту класу EDR. В разі їх відсутності треба негайно звернiться до Центру кібербезпеки ІТС для встановлення відповідного ПЗ». ***(Богдан Камінський. Російські хакери Armageddon нарощують присутність в IT-системах держорганів України // speka.media (https://speka.media/rosiiski-xakeri-armageddon-naroshhuyut-prisutnist-v-it-sistemax-derzorganiv-ukrayini-9d8dqv). 14.07.2023).***

***

«…Хакери, яких підозрюють у роботі на російську зовнішню розвідку, намагалися зламати комп'ютери десятків дипломатів у посольствах в Україні, використовуючи фейкову рекламу вживаного авто, пише Reuters з посиланням на звіт підрозділу Palo Alto Networks фірми з кібербезпеки Unit 42.

Польський дипломат, який відмовився назвати свою особу з міркувань безпеки, у середині квітня 2023 року розіслав електронною поштою рекламне оголошення про продаж вживаного седана BMW 5 серії, розташованого в Києві, колегам з різних посольств.

Хакери, відомі як APT29 (Cozy Bear), перехопили цей лист і вставили в нього шкідливе програмне забезпечення, яке надасть їм віддалений доступ до пристроїв отримувачів, замаскувавши його під альбом фотографій вживаного BMW. Видозміненого листа надіслали десяткам інших іноземних дипломатів, які працюють у Києві. Це стосувалося представників щонайменше 22 із приблизно 80 іноземних представництв, що працюють в Києві.

Для того, аби фейкове оголошення було більш привабливим, російські хакери знизили ціну на авто до 7,5 тисяч євро. Це і допомогло розкрити хакерське втручання. Польський дипломат сказав, що хтось з отримувачів листа йому

передзвонив, і назвав значно нижчу ціну під час розмови. Так стало зрозуміло, що йдеться про різні оголошення.

«Дипломатичні місії завжди будуть високоцінною мішенню для шпигунства. Шістнадцять місяців російського вторгнення в Україну, розвідувальні дані про Україну та дипломатичні зусилля союзників майже напевно є високим пріоритетом для російського уряду», – зазначає Unit 42 у звіті.

Після інциденту дипломат вирішив спробувати продати автівку на території Польщі, оскільки «після цієї ситуації не хоче більше мати проблем»...» ***(Російські хакери втрутилися в роботу посольств в Україні // Україна кримінальна (https://cripo.com.ua/news/crime/rosijski-hakery-vtrutylysya-v-robotu-posolstv-v-ukrayini/). 12.07.2023).***

***

Міжнародне співробітництво у галузі кібербезпеки

«…Національне агентство з розвитку інформаційних технологій (NITDA) та Сертифікований інститут судової експертизи та сертифікованого дослідника шахрайства Нігерії (CIFCFIN) збираються співпрацювати, щоб створити лабораторію кібербезпеки у 2024 році.

Кашіфу Інува, генеральний директор NITDA, запевнив у понеділок у заяві пані Хадізи Умар, керівника відділу корпоративних справ і зовнішніх зв'язків в Абуджі.

Пан Інува, приймаючи президента CIFCFIN доктора Іліясу Гашинбака та його команду, сказав, що співпраця необхідна для просування цифрової криміналістики, оживлення технологічної екосистеми та боротьби з кіберзлочинністю в цифровому просторі.

Генеральний директор сказав, що виконавці кіберзлочинів значні кошти вклали в дослідження, інформаційні технології, потужні інструменти для здійснення атак, а вжиття активних заходів для протидії їм не підлягає обговоренню.

«Ми інвестували в інші технології, такі як Digital Fabrication Lab (FABLAB 1.0) та інші лабораторії по всій країні, але нам ще належить створити лабораторію кібербезпеки.

«Ми вже маємо на увазі, де він буде розташований, але нам потрібно, щоб усі відповідні зацікавлені сторони були частиною цього, щоб можна було швидко відслідковувати розробку та впровадження центру.

«Інвестиції NITDA у проект будуть здійснені з наступного року, центр не називатиметься Лабораторією судової експертизи, але також включить кібербезпеку до своєї номенклатури для охоплення інших важливих сфер інтересів», — сказав він.

Пан Інува засудив небезпечний вплив кіберзлочинності на економіку країни, організації та окремих осіб, а отже, необхідність нарощування потенціалу для захисту від недобросовісних елементів.

Він також зазначив, що деякі організації не беруть до уваги необхідність забезпечення кібербезпеки під час розробки своїх цифрових сервісів, що підживлює атаки інтернет-шахраїв.

«Ми завжди повинні проектувати або оцифровувати з урахуванням безпеки, що б ми не робили, тому що це єдиний спосіб бути в безпеці.

«NITDA активно вживає важливих заходів для захисту кіберпростору шляхом підвищення обізнаності, нарощування потенціалу та інфраструктури.

«Хоча ми робимо все можливе в цьому відношенні, ми знаємо, що не можемо досягти успіху в ізоляції, це пояснює, чому ми вітаємо співпрацю, працюємо з ключовими зацікавленими сторонами та іншими суверенними державами для досягнення найкращого результату», — сказав він.

За словами Інува, у міністерствах, департаментах і агенціях (MDA) проводилися різні навчальні програми з кібербезпеки, додавши, що тисячі нігерійців наразі пройшли навчання як на платформах Cisco Academy, так і на платформах Coursera.

Він привітав групу з Актом про заснування інституту 2022 року, який було успішно підписано 23 грудня.

Гашинбак звернувся за комп'ютерною підтримкою для Нігерійського коледжу криміналістики та розслідувачів шахрайства (NCFFI), технічною допомогою для розгортання комбінованого електронного порталу та платформ електронного навчання, а також для аспірантської програми та програм стипендій.

Він сказав, що інститут буде відданий у виконанні своїх обов'язків заради успіху налагодженої співпраці.» ***(Arafat Abdulrazaq. NITDA, forensic institute to establish cybersecurity lab in 2024 // News Digest (https://newsdigest.ng/forensic-to-establish-cybersecurity-lab/). 17.07.2023).***

***

«Делегація представників Апарату Ради національної безпеки і оборони України в Брюсселі зустрілася з представниками Європейської служби зовнішньої діяльності (ЄСЗД), Генерального директорату з комунікаційних мереж, контенту і технологій (DG CONNECT) та ENISA.

Про це повідомляє пресслужба РНБО.

Українська делегація поділилася досвідом у протидії кіберагресії рф.

«Зокрема, йшлося про ефективні заходи запобігання кібератакам, побудову кібероборони та тісну співпрацю між суб'єктами кібербезпеки держави як ключовий фактор успішної боротьби з кіберзагрозами. Також обговорили питання збільшення рівня міжнародної кіберзлочинності через активне долучення зловмисних акторів з боку рф. Міжнародним партнерам було представлено ефективні заходи протидії, що вживаються Україною, зокрема поінформовано про впровадження системи фільтрації фішингових доменів Protective DNS», — йдеться у повідомленні.

Зустріч також стала платформою для обговорення організації третього раунду кібердіалогу між Україною та Європейським Союзом. Сторони обговорили успіхи України та напрями подальшої гармонізації законодавства України із законодавством ЄС у сфері кібербезпеки.

«Сьогодні Україна стоїть на передовій боротьби з агресією рф й у кіберпросторі, і ми прагнемо ділитися нашим досвідом з Європейським Союзом.

Зустріч з представниками ЄС є важливим кроком поглиблення співпраці та зміцнення обороноздатності обох сторін. Дякуємо Європейському Союзу за підтримку України у війні, яка також триває й у кіберпросторі», — зазначила керівник служби з питань інформаційної безпеки та кібербезпеки Апарату Ради національної безпеки і оборони України Наталія Ткачук.

У заході також взяли участь представники Міністерства оборони України, Національного координаційного центру кібербезпеки, Служби безпеки України, Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації, Національної поліції України та Офісу Генерального прокурора». ***(Україна та Європейський Союз зміцнюють співпрацю в боротьбі з кібератресією // АрміяInform (https://armyinform.com.ua/2023/07/14/ukrayina-ta-yevropejskyj-soyuz-zmicznyuyut-spivpraczyu-v-borotbi-z-kiberagresiyeyu/). 14.07.2023).***

***

Світові тенденції в галузі кібербезпеки

«Згідно з попередніми очікуваннями, фінансові угоди, злиття та поглинання (M&A) у секторі кібербезпеки, схоже, знизилися у другому кварталі. Однак аналітики, які спостерігають за ринком, мають більш оптимістичні оцінки щодо решти 2023 року — порівняно з трьома місяцями тому — більшість очікує помірного відновлення на обох фронтах до кінця року.

Велика частина оптимізму пов'язана з тим, що підприємства продовжують інвестувати значні кошти в кібербезпеку, незважаючи на уповільнення інших витрат. Дослідницька компанія IDC очікує, що цього року організації витратять близько 219 мільярдів доларів на продукти та послуги безпеки — або приблизно на 13% більше, ніж у 2022 році — для усунення загроз, підтримки гібридних робочих середовищ і відповідності вимогам. Сфери, які отримають найбільше витрат, це керовані послуги безпеки, безпека кінцевих точок, мережева безпека та керування ідентифікацією та доступом.

«Хоча тема консерватизму та очікування продовження зустрічного вітру залишалися протягом першої половини року, ми очікуємо, що стратегічна активність почне повільно відновлюватися у другій половині 2023 року та в 2024 році», — говорить Ерік Макалпайн, засновник і керівник партнер аналітичної компанії Momentum Cyber. За його словами, діяльність у сфері фінансування та злиття та поглинання врешті-решт пожвавиться, оскільки компанії, яким до цього часу вдавалося заробляти фінансово, почнуть відчувати потребу в свіжому капіталі для розвитку свого бізнесу.

Дані Pinpoint Search Group показують, що компанії з кібербезпеки залучили близько 1,9 мільярда доларів США в 97 раундах фінансування у другому кварталі. Це на 35% менше, ніж 2,9 мільярда доларів минулого кварталу, і приблизно на 55% менше, ніж фінансування, яке компанії з кібербезпеки залучили в кварталі минулого року.

«Оскільки відсоткові ставки охолодили мультиплікатори та вихід з ринку, венчурний капітал, орієнтований на кібербезпеку (VC), безумовно, сповільнився, особливо порівняно з 2021 і 2022 роками», — говорить Алекс Долл, партнер інвестиційної компанії з кібербезпеки Ten Eleven Ventures. «Оцінки стали жорсткішими, а вимоги інвесторів бачити чіткі ознаки попиту та тяги зросли», — каже він. За словами Долла, прийом на роботу компаніями, які підтримуються венчурним капіталом, також значно сповільнився, оскільки компанії перепрогнозували очікування та планували довший час роботи.

Декілька великих інвестицій у кіберпростор у другому кварталі

Минулого кварталу компанії венчурного капіталу та інші здійснили кілька значних інвестицій у компанії з кібербезпеки. Безперечно, найбільшою серед них були 190 мільйонів доларів США, які постачальник систем керованого виявлення та реагування (MDR) BlackPoint Cyber залучив у раунді інвестицій у зростання під керівництвом Bain Capital за участю Accel та кількох інших інвесторів. BlackPoint використає кошти для подальшого розвитку MDR компанії, керованого контролю програм, хмарного реагування, а також технологій журналювання та відповідності.

Іншою великою транзакцією стали 132 мільйони доларів США, які постачальник онлайн-перевірки ідентифікаційної інформації ID.me отримав у квітні в раунді фінансування Серії D під керівництвом Viking Global Investors за участі Morgan Stanley Counterpoint, CapitalG, FTV Capital та інших. Завдяки інвестиціям компанія з Макліна, штат Вірджинія, залучила від інвесторів 275 мільйонів доларів США з моменту запуску в 2010 році.

Дві інші транзакції фінансування досягли позначки в 100 мільйонів доларів. Однією з них були інвестиції в розмірі 100 мільйонів доларів США в Cybereason, які Softbank та інші інвестори зробили в квітні для підтримки планів розвитку компанії на ринку XDR і EDR. Наразі Cybereason залучив понад 850 мільйонів доларів від різних інвесторів, включаючи Google. Останнє грошове вливання відбулося лише через шість місяців після того, як компанія звільнила 17% своєї робочої сили в жовтні минулого року, і підкреслило незмінну довіру інвесторів до Cybereason.

Тим часом раунд фінансування серії B у розмірі 100 мільйонів доларів, який Cyera залучила в червні, підкреслив інтерес інвесторів до ринку, що розвивається, технологій « керування безпекою даних ».

«Хоча інвестиції у другому кварталі загалом скоротилися, високоефективні компанії з надійними фундаментальними показниками продовжують отримувати великі раунди фінансування, навіть у складних економічних умовах», — зазначає Макалпайн.

Стратегічні злиття та поглинання тривають

Pinpoint повідомила, що в другому кварталі нарахувала 18 транзакцій злиття та поглинання в секторі кібербезпеки — це значне падіння порівняно з 31 аналогічною транзакцією, зафіксованою в першому кварталі року.

Найбільшим із лотів — зі стратегічної точки зору — було придбання компанією F-Secure за 223 мільйони доларів бізнесу Lookout із мобільної безпеки споживачів. Макалпайн каже, що F-Secure описав цю покупку як можливість майже втричі збільшити свою присутність на ринку США та зміцнити свої позиції в сегменті постачальників послуг зв’язку.

Рік Тернер, аналітик Omdia, назвав купівлю Cisco Lightspin у березні та Armorblox у травні — обидва за нерозголошену суму — це ще два придбання, на які варто звернути увагу. Купівля Cisco компанії Lightspin забезпечує її присутність на ринку хмарної безпеки, хоча вона все ще дещо відстає від Palo Alto Networks у цій сфері, каже Тернер.

«Буде цікаво подивитися, чи поєднується ця технологія з тим, що вона отримала через два місяці, коли купила Armorblox», — зазначає Тернер.

Купівля IBM Polar, знову ж таки за нерозголошену суму, також заслуговує уваги, каже Тернер. «Ми спостерігали за DSPM, який до цього придбання був сектором, який майже повністю складався з стартапів», — зазначає він. Вихід IBM на ринок може спровокувати захоплення ринку іншими великими постачальниками, зазначає Тернер.

Нові можливості для приватних інвестиційних компаній

Тим часом, падіння оцінок продовжувало створювати нові інвестиційні можливості для компаній прямих інвестицій (PE), як це було в першому кварталі. Серед найбільш помітних трансакцій PE у 2023 році було придбання компанією Crosspoint Capital ванкуверського постачальника засобів захисту кінцевих точок Absolute Software за 657 мільйонів доларів у травні та придбання компанією Cinven постачальника програмного забезпечення для управління, ризиків і відповідності Archer за приблизно 1,3 мільярда доларів у квітні.

Ціна придбання Crosspoint становила приблизно 34% премії порівняно з ціною акцій Absolute у 8,58 доларів США 10 травня 2023 року. Після завершення придбання акціонери Absolute отримають 11,50 доларів США готівкою за звичайну акцію.

«Одна річ, яку варто спостерігати, — це те, як Crosspoint накопичує справжню стабільну кіберкомпанію», — каже Тернер. Фірма вже володіє або має частки в Forescout, ExtraHop, ReversingLabs, Digicert, RSAC, McAfee, Cyware та інших, зазначає Тернер, додаючи, що цілком можливо, що Crosspoint може зайнятися «корпоративним проектуванням» і об’єднати різні частини цих компаній

на якийсь момент. Або компанія PE могла б «просто влити трохи капіталу в усі з них, щоб повернути їх назад, коли прийде відповідний час», говорить він.

Тим часом Cinven не розкриває фінансові деталі покупки Archer у RSA Security у квітні. Однак дані, зібрані Momentum Cyber з різних галузевих джерел для звіту про фінансові результати за другий квартал, оцінюють вартість транзакції в 1,3 мільярда доларів.

Сектори, які отримали значне фінансування протягом 2023 року, включають управління ідентифікацією та доступом, управління безпекою даних (DSPM) і виявлення даних і реагування (DDR), каже Макалпайн. Він додає: «Ми також спостерігаємо підвищену увагу інвесторів до стартапів, які допомагають компаніям безпечно використовувати нові форми ШІ — великі мовні моделі та генеративний ШІ».

Забігаючи вперед, Долл з Ten Eleven Ventures каже, що хоча венчурне фінансування в цілому сповільнилося порівняно з іншими секторами, кібербезпека продовжує представляти привабливу можливість для інвесторів. «Для правильних компаній капітал безперечно доступний», — каже Долл. Кібербезпека також продовжує залишатися пріоритетом для корпоративних організацій, і є ознаки нових інвестицій у такі сфери, як штучний інтелект: «Ми вважаємо, що інвестиції в сектор знову прискоряться в наступні 12-18 місяців», – зазначає Долл. «Попереду значне зростання, оскільки атаки тривають — фактично завдяки штучному інтелекту — і нові вектори атак, такі як сам ШІ, стають більш очевидними». ***(Jai Vijayan. Analysts: Cybersecurity Funding Set for Rebound // Informa PLC (https://www.darkreading.com/operations/analysts-cybersecurity-funding-uptick-2h-2023?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 11.07.2023).***

***

«Исследование Cohesity показывает, что организации готовы платить выкуп из-за проблем с киберустойчивостью и пробелами в восстановлении данных.

Новое исследование, проведенное по заказу Cohesity, компании, занимающейся безопасностью и управлением данными, показывает, что большинство организаций в Австралии и Новой Зеландии не имеют необходимых стратегий киберустойчивости или возможностей защиты данных для борьбы с растущими сегодня киберугрозами.

Сравнивая перспективы кибербезопасности на 2023 и 2022 годы, 94% респондентов заявили, что в 2023 году они считают, что угроза атак программ-вымогателей для их отрасли возросла.

Вызывает тревогу тот факт, что более половины респондентов (56%) подтвердили, что их организация стала жертвой атаки программы-вымогателя в предыдущие шесть месяцев, в то время как почти каждый десятый (9%) не был уверен ни в том, ни в другом случае.

Респонденты также сообщили, что возможности их организаций в области киберустойчивости и безопасности данных не поспевают за ними, при этом 79% выразили обеспокоенность по поводу их стратегии киберустойчивости и того, может ли она «решить сегодняшние кибервызовы».

Непрерывность бизнеса имеет решающее значение даже при возникновении неблагоприятных киберсобытий. Однако Cohesity подчеркивает, что организации реагируют медленно, потому что не могут быстро восстанавливать данные и восстанавливать бизнес-процессы.

На вопрос, сколько времени потребуется их организации для восстановления данных и бизнес-процессов в случае кибератаки, более 99% респондентов ответили, что им потребуется более 24 часов. Более того, 80% заявили, что это займет более четырех дней, в то время как почти половина (47%) респондентов заявили, что потребуется более недели.

7 из 10 респондентов (71%) заявили, что у них нет полной уверенности в том, что их компания сможет восстановить их данные и важные бизнес-процессы в случае общесистемной кибератаки.

Более подробно анализируя ожидания в отношении киберустойчивости и восстановления данных по сравнению с реальностью, 95% респондентов заявили,

что их организации рассмотрят вопрос о выплате выкупа, если это означает возможность восстановления данных и бизнес-процессов или более быстрого восстановления.

Майкл Альп, управляющий директор Cohesity Australia & New Zealand, говорит: «Организации не могут позволить себе быть в автономном режиме и не могут поддерживать работу, особенно более одного дня».

«Однако суровая реальность такова, что многие организации уязвимы для использования киберпреступниками, потому что они не могут быстро восстановить свои данные и бизнес-процессы, когда это необходимо».

«Поэтому неудивительно, что менее 5% респондентов заявили, что их организации не рассматривают возможность выплаты выкупа для поддержания непрерывности бизнеса, и что подавляющее большинство респондентов считают, что их организации заплатят выкуп киберпреступникам», — говорит Альп.

На вопрос о наиболее серьезных препятствиях, препятствующих возобновлению работы их организации в случае кибератаки, респонденты ответили, что тремя главными проблемами для них являются отсутствие координации между ИТ и безопасностью (33%), отсутствие своевременных и подробные оповещения (32%) и отсутствие свежей, чистой, неизменной копии данных (30%).

Респонденты внесли дополнительную ясность в отношении своих проблем с безопасностью данных: менее половины заявили, что они уверены, что все их данные, хранящиеся в облаке (45%) или на периферии (38%), были безопасными и защищенными. Для сравнения, только каждый шестой респондент (17%) уверен, что данные, хранящиеся локально, безопасны и защищены.

Следовательно, 88% респондентов заявили, что для победы в войне с программами-вымогателями поставщики данных и средств кибербезопасности должны сотрудничать, чтобы предоставлять комплексные и интегрированные решения для защиты от программ-вымогателей.

91% респондентов считают, что их организация выиграет от платформы для обеспечения безопасности и управления данными, которая дает представление об их состоянии безопасности и устойчивости к киберугрозам.

Cohesity говорит, что это особенно важно, учитывая, что адекватные услуги резервного копирования и восстановления данных имеют решающее значение для получения права на страхование от киберугроз.

В то время как 3 из 4 (75%) респондентов подтвердили, что их компания имеет киберстрахование, почти половина (48%) всех респондентов заявили, что сейчас получить киберстрахование сложнее, чем в 2020 году.

Респонденты также поделились, что тремя наиболее важными технологиями или возможностями, необходимыми для обеспечения киберстрахования, являются: «надежное шифрование» (39%), многофакторная аутентификация (37%) и «возможность проверки целостности резервных копий» (34%).

Альп объясняет: «ИТ-специалисты и службы безопасности должны совместно владеть результатами киберустойчивости организаций, чтобы выявлять конфиденциальные данные и защищать, обнаруживать, реагировать и восстанавливаться после кибератак».

«Опираться на традиционные системы резервного копирования и восстановления, которым не хватает современных средств защиты данных, в сегодняшней изощренной среде киберугроз — это прямой путь к катастрофе».

«Вместо этого организациям следует искать платформы для обеспечения безопасности данных и управления ими, которые интегрируются с их существующими решениями в области кибербезопасности и обеспечивают прозрачность их состояния безопасности и повышают устойчивость к киберугрозам», — говорит Альп». ***(Kaleah Salmon. Cohesity exposes gaps in cyber resilience and security // TechDay (https://securitybrief.co.nz/story/cohesity-exposes-gaps-in-cyber-resilience-and-security). 04.07.2023).***

***

«Технологии продолжают делать замечательные достижения, которые улучшают нашу жизнь. Однако это также усложняет риски, с которыми мы сталкиваемся в нашем цифровом мире. Учитывая постоянно меняющийся ландшафт угроз, невозможно переоценить важность надежной устойчивости к кибербезопасности.

В этой статье освещаются ключевые тенденции, которые продолжат формировать рынок в 2023 году, от растущего внедрения генеративного искусственного интеллекта (GenAI) и машинного обучения (ML), укрепляющих кибербезопасность, до проблем с получением страховки и поддержанием надлежащего уровня персонала. вне.

GenAI и машинное обучение

GenAI и ML обладают беспрецедентным влиянием на кибербезопасность. Эти технологии, обладая огромным потенциалом для улучшения защитных механизмов, одновременно открывают возможности для собственного оружия.

Злоумышленники уже используют ИИ и машинное обучение для создания вредоносных программ и программ-вымогателей для организации основных кибератак — хотя на данном этапе они находятся в зачаточном состоянии, они являются тревожным предшественником будущих кибервойн. Хотя разработчики инструментов искусственного интеллекта и чат-ботов прилагают усилия для сдерживания этой новой угрозы, злоумышленники продолжают приспосабливаться и выявлять лазейки, которые можно использовать.

Заглядывая в будущее, мы ожидаем, что эволюция ИИ приведет к созданию более сложных и непредсказуемых киберугроз. Чтобы противостоять этим угрозам со скоростью машины, технологии и процессы также должны развиваться и адаптироваться. Автоматизация и использование ИИ при принятии решений позволит быстро обнаруживать аномальное поведение и автоматически реагировать на будущие угрозы.

Основное внимание будет уделяться усилению технологий против угроз, для противодействия которым они были разработаны, чтобы искусственный интеллект

служил надежной защитой в нашем арсенале, а не использовался для выявления уязвимостей.

Облачные технологии и нулевое доверие

Переход к облаку в сочетании с внедрением сред с нулевым доверием будет продолжать формировать ландшафт кибербезопасности из-за растущего риска компрометации облака и продолжающегося воздействия угроз изнутри.

В начале 2023 года мы наблюдали, как облачные экземпляры становятся прибыльными целями для злоумышленников, взламывающих облачные экземпляры для кражи данных, крипто-майнинга или для запуска дальнейших кибератак. Это подчеркивает острую необходимость внедрения комплексных мер безопасности, включая нулевое доверие, в облачных средах и локально для смягчения этих развивающихся угроз.

Модель нулевого доверия, основанная на принципе «никогда не доверяй, всегда проверяй», значительно снижает возможности хакеров перемещаться по сетям и системам. Мы по-прежнему наблюдаем, как субъекты угроз программ-вымогателей успешно перемещаются в боковом направлении после того, как они закрепились в сети. Мы предполагаем, что организации будут все чаще согласовывать свои политики безопасности с установленными структурами нулевого доверия, такими как архитектура нулевого доверия Национального института стандартов и технологий (NIST), используя их в качестве плана для защиты своих цифровых активов.

Внедрение облачных технологий и новые инструменты безопасности

По мере того, как организации переходят на облачные инфраструктуры, потребность в инвестициях в новые специализированные инструменты безопасности становится преобладающей тенденцией. Однако внедрение этих важных инструментов отстает от темпов внедрения, что создает уязвимости при переходе от локальной среды к облаку.

Успешная миграция вызывает потребность не только в сложных инструментах, но и в специальных знаниях облачных платформ, чтобы обеспечить плавный и безопасный переход и постоянную безопасность. Например, Microsoft

Azure приобрела значительную популярность, что побудило многие организации сделать выбор в пользу комплексного стека инструментов Microsoft для обеспечения безопасности.

Несмотря на эти достижения, недостатки в мониторинге безопасности, гигиене и ведении журналов в облачных развертываниях по-прежнему распространены. Чтобы устранить пробелы в безопасности, организациям необходимо защитить свои облачные инфраструктуры с помощью надежных мер безопасности и постоянного мониторинга. Это гарантирует, что они используют эффективность и масштабируемость облака без ущерба для безопасности.

Регуляторное правоприменение

Еще одной важной тенденцией, сформировавшей ландшафт кибербезопасности в 2023 году, стала ориентация регулирующих органов на правоприменение. Эта тенденция была особенно распространена в США, где в течение первых пяти месяцев года были предприняты значительные правоприменительные меры.

В то же время законы о конфиденциальности данных быстро распространяются во многих штатах, примером чего является Калифорнийский закон о защите прав потребителей (CCPA). Кроме того, законы о конфиденциальности данных в таких странах, как Китай, Индия и Саудовская Аравия, продолжают развиваться, используя принципы Общего регламента ЕС по защите данных (GDPR).

Европа ужесточает правила кибербезопасности, вводит Закон о цифровой операционной устойчивости (DORA), вносит поправки в Закон ЕС о кибербезопасности и заменяет Директиву о сетях и информационных системах (NIS) на NIS2.

Эти изменения направлены на расширение соответствующих отраслей, таких как управляемые услуги безопасности, чтобы помочь регулировать цепочку поставок, а также производителей аппаратных и программных продуктов и устройств Интернета вещей (IoT) для защиты экосистемы ЕС. DORA также вводит

новые требования к тестированию на проникновение, поставщикам кибербезопасности и отчетности об инцидентах.

Эти события подчеркивают глобальную нормативную тенденцию к большей прозрачности и подотчетности в отношении кибербезопасности в различных отраслях и цепочках поставок.

Объединение программ кибербезопасности и конфиденциальности

Интеграция программ кибербезопасности, конфиденциальности и управления данными, а также интеграция IoT, операционных технологий и ИТ остается в центре внимания. Организации все больше осознают ценность объединения этих программ под одной крышей, часто с руководителями по информационной безопасности (CISO), которые теперь берут на себя обязанности по защите данных, операционной устойчивости и управлению данными.

Однако по-прежнему существуют пробелы в передовых методах управления данными, а также в операционных технологиях (где это уместно), которые необходимо устранить, чтобы снизить воздействие программ-вымогателей. Расследования программ-вымогателей продолжают выявлять тревожные недостатки в хранении данных и разделении между ИТ и ОТ. Нередко можно найти организации с плохой сегрегацией сети, а также организации, которые не осведомлены о деятельности по краже данных или не имеют надежных политик и средств контроля хранения данных, что значительно увеличивает влияние взлома. Отсутствие комплексных оценок рисков, разделения сетей, точных реестров данных и эффективных механизмов обнаружения систем данных остается серьезной проблемой.

Эти проблемы подчеркивают важность целостного подхода, интеграции всех цифровых технологий и внедрения эффективных методов управления данными для обеспечения не только безопасности, но и подотчетности, целостности и конфиденциальности данных во всех операционных процессах для надлежащей защиты киберпространства в будущем.

От предотвращения к быстрому реагированию

Парадигма кибербезопасности претерпевает значительный сдвиг от традиционного подхода, ориентированного на предотвращение, к подходу, ориентированному на быстрое обнаружение, реагирование и общую устойчивость. Это изменение положительно подкрепляется страховыми компаниями, которые вознаграждают организации, демонстрирующие надежные механизмы обнаружения и стратегии устойчивости.

Расширенное обнаружение и реагирование выходят на передний план этой тенденции, фактически становясь новой многофакторной аутентификацией с точки зрения ее незаменимости. Его способность быстро обнаруживать киберугрозы и реагировать на них значительно поднимает планку стандартов безопасности. Кроме того, страховщики и брокеры рассматривают возможность внедрения упреждающих услуг для повышения устойчивости и общей готовности к кибератакам.

По мере продвижения вперед основное внимание будет по-прежнему уделяться расширению возможностей быстрого обнаружения и общей устойчивости не только для прямой выгоды, но и для страховых преимуществ, которые они представляют.

Получение киберстраховки

Еще одна тенденция, которая сохранится в 2023 году, — это постоянная задача для организаций обеспечить киберстрахование на соответствующем уровне покрытия, поскольку операторы ужесточают свои требования к андеррайтингу и расширяют свои исключения и ограничения покрытия.

Это результат растущей сложности и частоты кибератак, требующих более осторожного подхода к андеррайтингу. Тем не менее, эта сложная среда также привела к инновациям на страховом рынке. Новые участники изобретают новые способы оценки риска и предлагают страхование, создавая альтернативные пути к покрытию.

Эти новые подходы включают в себя предложение политик с более низкими барьерами для входа при сниженных уровнях покрытия или принятие моделей разделения рисков. Они предоставляют организациям гибкие возможности для

обеспечения необходимого покрытия, добавляя новое измерение к отношениям между кибербезопасностью и страховой отраслью.

Кадровые проблемы

В 2023 году проблема нехватки кадров в области кибербезопасности по-прежнему остается проблемой. Хотя всплеск увольнений в США привел к притоку квалифицированных кандидатов, эта тенденция не наблюдается во всем мире, что приводит к постоянной нехватке квалифицированных специалистов в области кибербезопасности в других регионах.

В ответ компании все чаще обращаются к поставщикам управляемых услуг, чтобы смягчить последствия увольнения персонала и поддерживать эффективную деятельность по обеспечению безопасности. Более того, отрасль находится на пороге революционной волны, движимой искусственным интеллектом, особенно в ключевых дисциплинах кибербезопасности.

Инструменты искусственного интеллекта могут автоматизировать и оптимизировать такие задачи, как анализ вредоносных программ, тестирование на проникновение и общие операции в рамках облачных технологий. Используя эти достижения, организации смогут уменьшить нехватку киберперсонала, особенно в центрах обеспечения безопасности и группах реагирования на инциденты.

В центре внимания злоумышленников

Наблюдаемой тенденцией в 2023 году стало возрождение злоумышленников (например, BlackCat, Black Basta и CI0p), которые более последовательно переориентировали свое внимание на европейские и американские организации. Этот сдвиг стал особенно заметен с марта 2023 года, когда атаки программ-вымогателей снова вернулись.

Злоумышленники диверсифицируют свои методы, используя новые векторы атак для получения несанкционированного доступа к компаниям помимо традиционно используемого целевого фишинга. Эти новые тактики включают «вредоносную рекламу», использование «журналов кражи» и использование брокеров доступа. Они также усиливают свои атаки с помощью тройных стратегий

вымогательства, включая прямое взаимодействие с жертвами, чтобы усилить на них давление.

Кроме того, все чаще используются уязвимости в VMWare, локальных системах Microsoft Exchange, программном обеспечении, таком как MOVEit, а также атаки «sys dev», что способствует росту нарушений безопасности — часто глобальных по своему характеру и требующих глобального реагирования.

В этой меняющейся среде угроз группы кибербезопасности должны сохранять бдительность и быстро реагировать, адаптируя свои стратегии и наборы инструментов к изменяющейся тактике и направленности этих субъектов угроз. Эта готовность необходима для защиты целостности нашего цифрового пространства.

Консолидация пространства поставщиков кибербезопасности

По мере приближения 2023 года мы стали свидетелями усиления консолидации в пространстве поставщиков средств кибербезопасности, как в области инструментов, так и услуг. Недавний спад венчурного финансирования инструментов безопасности будет способствовать дальнейшему развитию этой тенденции, что приведет к снижению стоимости многих поставщиков. Это, в сочетании с вытекающими из этого финансовыми ограничениями, сделает консолидацию не только вероятной, но и во многих случаях неизбежной.

Однако консолидация может упростить рынок кибербезопасности, уменьшить фрагментацию и потенциально привести к более надежным комплексным решениям. Мы ожидаем, что долгосрочные последствия могут привести к более сильным, более интегрированным решениям в области кибербезопасности, лучше оснащенным для защиты организаций от развивающихся угроз.

Краткое содержание

2023 год оказался еще одним интересным годом для специалистов по кибербезопасности и конфиденциальности данных. Обоюдоострый меч захватывающих усовершенствований цифровых технологий и достижений в области облачных вычислений, искусственного интеллекта и Интернета вещей

принесет новые риски и возможности для всех. Принятие киберустойчивого подхода поможет тем, кто хочет воспользоваться преимуществами, которые приносит эта эволюция, и свести к минимуму связанные с ней потенциальные риски». ***(Ryan Rubin, Ahsan Qureshi. Cyber security trends in 2023 and beyond // Financier Worldwide (https://www.financierworldwide.com/cyber-security-trends-in-2023-and-beyond). 07.2023).***

***

«Кибербезопасность имеет решающее значение в эпоху удаленной работы. Поскольку все больше людей работают из дома и имеют удаленный доступ к корпоративным системам и данным, вероятность кибератак и утечек данных значительно возросла. Удаленная работа создала новые уязвимости, которыми могут воспользоваться киберпреступники. Одна из самых больших проблем кибербезопасности при удаленной работе заключается в том, что может быть сложнее контролировать и защищать доступ к данным, системам и приложениям компании. Например, сотрудники могут получать доступ к корпоративным сетям и информации через незащищенные домашние сети или общедоступные сети Wi-Fi, что делает их уязвимыми для кибератак, таких как фишинг, вредоносные программы и программы-вымогатели. Кроме того, сотрудники могут быть более восприимчивы к фишинговым атакам или мошенничеству с использованием социальной инженерии, когда они физически не находятся в одном офисе со своими коллегами. Кроме того, удаленная работа может затруднить ИТ-отделам мониторинг и реагирование на инциденты безопасности в режиме реального времени.

Кибератака или утечка данных могут иметь серьезные последствия для компании, включая финансовые потери, ущерб репутации и юридические обязательства. Поэтому компании должны уделять первоочередное внимание мерам кибербезопасности, чтобы защитить своих сотрудников и их конфиденциальные данные.

Есть несколько ключевых методов, которые компании могут внедрить для обеспечения безопасности своих сотрудников и данных в эпоху удаленной работы. Во-первых, компании должны установить четкие политики и рекомендации для удаленной работы, включая правила использования устройств, доступа к данным и их хранения, а также каналов связи. Это помогает гарантировать, что сотрудники осознают свои обязанности и понимают, что от них ожидается. Во-вторых, компании должны обеспечить безопасный удаленный доступ к своим системам и приложениям. Это можно сделать с помощью виртуальных частных сетей (VPN), многофакторной аутентификации (MFA) и других мер безопасности, чтобы гарантировать, что только авторизованные пользователи могут получить доступ к ресурсам компании. В-третьих, компаниям следует внедрить меры безопасности конечных точек для защиты устройств, используемых для удаленной работы, например, антивирусное программное обеспечение, брандмауэры и другие инструменты безопасности. В-четвертых, компании должны обучать сотрудников передовым методам обеспечения безопасности, в том числе тому, как избежать фишинга, как создавать надежные пароли и как выявлять подозрительную активность. В-пятых, компаниям следует проводить регулярные оценки безопасности для выявления уязвимостей в своих системах и приложениях. Это может помочь обеспечить актуальность и эффективность мер безопасности. В-шестых, компании могут использовать облачные решения для обеспечения безопасности для защиты своих данных и систем. Эти решения могут обеспечить непрерывный мониторинг, обнаружение угроз и возможности быстрого реагирования. Наконец, компании должны иметь план реагирования на инциденты, включая шаги по выявлению инцидентов безопасности и реагированию на них, уведомлению соответствующих сторон и восстановлению после инцидента. В целом, компаниям рекомендуется применять ряд мер, направленных как на технические, так и на человеческие факторы, а также постоянно отслеживать и обновлять эти меры по мере необходимости.

Становится все более очевидным, что кибербезопасность имеет первостепенное значение в эпоху удаленной работы. Уделяя приоритетное

внимание кибербезопасности и применяя целостный подход к кибербезопасности, организации могут лучше защищать свои данные, поддерживать непрерывность бизнеса и обеспечивать безопасность своих сотрудников и клиентов...» ***(Coraleine J. Kitt. 7 Key Practices Companies Should Implement to Ensure Cyber Safety in the Age of Remote Work // Flaster/Greenberg (https://www.flastergreenberg.com/CybersecurityDataPrivacyLawBlog/7-key-practices-companies-should-implement-to-ensure-cyber-safety-in-the-age-of-remote-work). 12.07.2023).***

***

«По мере того как предприятия вступают в новую цифровую эру, отмеченную быстрыми инновациями и взаимосвязанностью, кибербезопасность перестает быть дополнением и превращается в критическую необходимость. Оцифровка бизнес-операций повысила эффективность и доступность, но также повысила уязвимость к широкому спектру киберугроз. По мере развития и эскалации этих угроз концепция киберустойчивости стала более актуальной, чем когда-либо.

Киберустойчивость относится к способности организации постоянно обеспечивать ожидаемые результаты перед лицом неблагоприятных киберсобытий. Речь идет не только о предотвращении кибератак, но и о том, как ваша компания реагирует и восстанавливается, когда эти инциденты неизбежно происходят. Создание киберустойчивой компании — это путь, который включает в себя тщательное выявление рисков, разработку комплексной стратегии кибербезопасности, внедрение проактивной и реактивной защиты, а также тщательное обучение вашей команды. Каждый из этих шагов заслуживает пристального внимания и рассмотрения.

Оценка риска

Каждый путь к киберустойчивости начинается с оценки рисков. Он закладывает основу для вашей стратегии, помогая вам понять свое текущее состояние, выявляя уязвимости и определяя потенциальные последствия различных

киберугроз. В двух словах, оценка рисков заключается в выявлении ваших ценных активов, которые могут стать потенциальными целями, таких как оборудование, программное обеспечение, данные, сети и персонал.

Затем вам нужно точно определить угрозы, с которыми могут столкнуться эти активы, и уязвимости, которые могут быть использованы. Затем эти риски должны быть оценены и расставлены по приоритетам в зависимости от их серьезности. Этот шаг является итеративным, и его следует часто повторять для учета новых активов, возникающих угроз и обнаруженных уязвимостей.

Разработать и поддерживать стратегию кибербезопасности

Осознав потенциальные риски, ваш следующий шаг — разработать целостную стратегию кибербезопасности, которая их снизит. Ваша стратегия должна начинаться с анализа пробелов, который сопоставляет ваши текущие меры кибербезопасности с желаемым состоянием. Здесь вы, по сути, сравниваете свои существующие методы с отраслевыми стандартами или структурами, такими как NIST или ISO 27001, чтобы выявить любые пробелы.

После анализа пробелов следует тщательный анализ рисков, при котором каждый риск, выявленный в ходе оценки риска, погружается глубже. Это позволяет лучше понять характер каждого риска и дает информацию о соответствующих ответных мерах. Кроме того, в рамках вашей стратегии вам необходимо разработать план резервного копирования и восстановления. Регулярное резервное копирование играет важную роль в восстановлении данных, потерянных или скомпрометированных во время кибер-инцидентов. В этом плане должно быть указано, какие данные подлежат резервному копированию, как часто следует выполнять резервное копирование, а также процесс восстановления данных в чрезвычайных ситуациях.

Надежная стратегия кибербезопасности также включает план реагирования на инциденты, в котором описаны действия вашей организации в случае инцидента кибербезопасности. Он должен охватывать, кто что делает, процедуры эскалации, стратегии коммуникации и шаги для анализа и извлечения уроков из инцидента. Наконец, проведение регулярных аудитов кибербезопасности необходимо для

оценки эффективности ваших мер безопасности, выявления слабых мест в вашей защите и информирования о необходимых улучшениях.

Внедряйте упреждающие меры кибербезопасности

Надежная стратегия кибербезопасности должна быть упреждающей, постоянно выявлять и устранять угрозы до того, как они материализуются. Это предполагает постоянное обновление информации о последних угрозах и тенденциях в области кибербезопасности, что позволяет вам предвидеть потенциальные риски и соответствующим образом укреплять свою защиту. Регулярные обновления и исправления ваших систем и приложений могут предотвратить использование уязвимостей безопасности.

Внедрение строгого контроля доступа также имеет решающее значение. Убедитесь, что сотрудники имеют доступ только к тем данным, которые им необходимы для выполнения своих функций, чтобы ограничить потенциальный ущерб в случае взлома учетной записи. Кроме того, использование многофакторной аутентификации (MFA) добавляет дополнительный уровень безопасности, требуя дополнительных учетных данных помимо пароля.

Внедрить реактивную техническую защиту

Несмотря на ваши самые активные меры, некоторые киберугрозы проникнут в вашу систему защиты. Средства реактивной защиты, такие как брандмауэры и антивирусное программное обеспечение, помогают свести к минимуму ущерб при возникновении таких инцидентов. Межсетевые экраны отслеживают и контролируют входящий и исходящий сетевой трафик на основе заданных правил безопасности, формируя первую линию защиты от киберугроз. Антивирусное программное обеспечение дополняет брандмауэры, обнаруживая, предотвращая и удаляя вредоносные программы.

Системы обнаружения и предотвращения вторжений (IDS/IPS) отслеживают вашу сеть на наличие подозрительных действий и потенциальных угроз, предупреждая вас о потенциальной атаке и, в некоторых случаях, предпринимая действия для смягчения угрозы. Шифрование — еще одна ценная реактивная мера, которая делает ваши конфиденциальные данные недоступными для чтения кем-

либо без соответствующего ключа дешифрования, тем самым защищая их, даже если они попадут в чужие руки. Системы управления информацией и событиями безопасности (SIEM) обеспечивают анализ в режиме реального времени и создание отчетов о предупреждениях безопасности, генерируемых приложениями и сетевым оборудованием. Они помогают обнаруживать инциденты на ранней стадии и оперативно реагировать.

Обучение персонала

Человеческий фактор часто является наиболее уязвимым звеном в системе кибербезопасности организации. Зная об этом, киберпреступники склонны атаковать сотрудников с помощью таких тактик, как фишинг. Таким образом, тщательное обучение сотрудников является жизненно важной частью построения киберустойчивой компании. Сотрудники должны быть осведомлены о своей роли в поддержании кибербезопасности посредством регулярных тренингов по повышению осведомленности, которые охватывают распространенные угрозы, безопасные онлайн-практики и важность протоколов безопасности.

В зависимости от их роли некоторым сотрудникам могут потребоваться определенные навыки кибербезопасности, такие как понимание того, как использовать инструменты безопасности, выявление и реагирование на определенные угрозы или безопасное обращение с конфиденциальными данными. Регулярное проведение смоделированных атак, таких как фишинговые тренировки, может помочь сотрудникам понять, как может выглядеть реальная атака и как они должны реагировать.

Киберугрозы постоянно развиваются, и поэтому ваше обучение должно способствовать непрерывному обучению и быть в курсе последних угроз и средств защиты. Создание киберустойчивой компании — это путешествие, а не пункт назначения. Это требует постоянных усилий, обучения и адаптации. Однако отдача огромна: это не только защищает вашу организацию от разрушительных кибератак, но также может дать конкурентное преимущество. В мире, который становится все более взаимосвязанным, клиенты, партнеры и инвесторы высоко ценят организации, которые серьезно относятся к кибербезопасности.

Таким образом, киберустойчивость — это способность поддерживать бизнес-операции, несмотря на неблагоприятные кибер-события. Он включает в себя тщательную оценку рисков, разработку комплексной стратегии кибербезопасности, реализацию как упреждающих, так и ответных мер и обучение ваших сотрудников. Стимулируя культуру кибербезопасности на всех уровнях, предприятия могут не только защитить себя от потенциальных угроз, но и установить уровень доверия со своими клиентами, будучи уверенными в том, что их конфиденциальные данные находятся в надежных руках. В мире, где утечка данных становится все более распространенным явлением, создание киберустойчивой компании — это инвестиция в долгосрочную устойчивость и успех вашей компании». ***(Jim Koohyar Biniyaz. How to Build a Cyber-Resilient Company From Day One // Entrepreneur Media, LLC (https://www.entrepreneur.com/science-technology/how-to-build-a-cyber-resilient-company/455347?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 14.07.2023).***

***

«Мир становится цифровым; практически каждый тип трансграничной деловой операции теперь имеет цифровой компонент. Использование компаниями цифровых технологий открывает им новые отношения с клиентами и деловыми партнерами и новые возможности для бизнеса.

Но, как стало ясно из недавних заголовков, сам факт подключения к внешнему миру экспоненциально увеличивает риски организаций — провал проекта, утечка данных или что-то похуже.

В эту эпоху глобальных цифровых потоков компании должны предпринять все возможные шаги для создания надежных возможностей кибербезопасности. Стратегии защиты не могут быть сосредоточены исключительно на технологическом контроле и планах восстановления.

Компании также должны использовать человеческий фактор. Они должны стремиться к созданию устойчивой к цифровым технологиям культуры, в которой

кибербезопасность является не случайной проблемой, а повседневной задачей для основных заинтересованных сторон бизнеса на всех уровнях, как внутри организации, так и за ее пределами.

Но пробелы в доверии к кибербезопасности существуют на многих уровнях корпоративной экосистемы. Вот четыре основных пробела и способы их устранения:

Разрыв в доверии 1: совет директоров и топ-менеджеры

Взаимоотношения между членами совета директоров и высшим руководством могут быть напряженными по целому ряду причин, но первой в списке является то, что кибербезопасность обычно не является главным пунктом в повестке дня многих заседаний совета директоров. Его часто представляют как часть более широкой дискуссии по вопросам ИТ, если вообще упоминают.

Многие члены советов директоров, как правило, менее осведомлены о технологиях и проблемах кибербезопасности, чем о стандартных финансовых и операционных вопросах, за исключением того, что они читают о последних нарушениях корпоративной или государственной безопасности. Они подходят к столу с вопросами о программах кибербезопасности компании.

Решение: найти общий язык

Члены высшего звена должны обеспечить большую прозрачность и наладить более тесную связь с советом директоров. Руководители высшего звена должны регулярно официально оценивать зрелость своих программ кибербезопасности и представлять свои выводы совету директоров не реже одного раза в год, но желательно даже чаще.

Это мероприятие должно включать в себя структурированное рассмотрение членами старшего руководства и другими сотрудниками ИТ и бизнес-подразделений серьезности и вероятности атак на основные корпоративные активы. Например, какие внутренние и внешние угрозы являются самыми большими и какая ценность для бизнеса поставлена на карту?

Разрыв доверия 2: бизнес-подразделения и ИТ-организация

Отношения, основанные на доверии, между отдельными лицами в бизнес-подразделениях, ИТ-организацией и службой кибербезопасности могут быть сложными для поддержания — отчасти потому, что эти группы иногда работают с противоположными целями.

Группа кибербезопасности может навязывать определенные протоколы безопасности, которые неудобны для сотрудников бизнес-подразделений или иным образом мешают их повседневной работе. Такое раздражение может перерасти с индивидуального уровня на уровень бизнес-подразделения.

Решение: наращивание усилий по обучению

Организация может предоставить всестороннее обучение кибербезопасности для сотрудников всех уровней, чтобы помочь сократить разрыв в доверии между службой ИТ и кибербезопасности и бизнесом.

Это может включать в себя специальные общие собрания, семинары и учебные модули, направленные на выявление различных типов киберугроз и определение соответствующих мер реагирования, когда сотрудники становятся свидетелями подозрительной активности. Такое обучение может помочь сотрудникам бизнес-подразделений понять смысл протоколов кибербезопасности и повысить их осведомленность.

В конце концов, кибербезопасность — это общая ответственность.

Разрыв в доверии 3: компания и ее поставщики

Отношения между компаниями и поставщиками их технологий и цепочки поставок всегда были сложными. Точно так же, как потребители полагаются на компании в плане обеспечения безопасности своих данных и использования их только разрешенными ими способами, предприятия должны доверять своим ИТ-поставщикам и поставщикам цепочки поставок в том, что касается конфиденциальности информации о конкурентах.

Автопроизводители, например, должны быть уверены, что их производители оригинального оборудования (OEM) имеют достаточный контроль кибербезопасности для защиты интеллектуальной собственности, которой они совместно пользуются. Это особенно актуально в эпоху, когда все больше и больше

компаний передают на аутсорсинг управление своей ИТ-инфраструктурой или своими операциями по кибербезопасности.

Решение: сблизить партнеров

Чтобы преодолеть этот разрыв в доверии, ИТ-руководители и бизнес-руководители компании должны запланировать регулярные беседы с поставщиками и партнерами по цепочке поставок, чтобы подтвердить уровни безопасности, необходимые для защиты общей бизнес-информации.

Такие встречи должны проводиться ежеквартально или раз в два года; при частых контактах продавцы и должностные лица компании могут вступать в настоящее деловое партнерство, а не в простые деловые отношения. Они могут обсудить и разработать четкие планы восстановления и компенсации.

Разрыв в доверии 4: компания и правительство

Неудивительно, что в последние годы местные, национальные и федеральные органы власти побуждают организации частного сектора лучше осознавать проблемы кибербезопасности и активизировать свои усилия по защите данных.

Кибератаки на крупные финансовые учреждения могут повлиять на общую стабильность рынка. Взломы энергосистем также могут представлять угрозу для всей страны, как мы узнали из недавних попыток взлома дюжины электростанций в Соединенных Штатах.

Государственным учреждениям необходимо, чтобы компании своевременно сообщали о кибератаках и других инцидентах, чтобы усилить всеобъемлющие меры по защите.

Решение: видеть общую картину

Ни одна из сторон не может позволить себе бороться с кибератаками в одиночку. Компании нуждаются в официальном одобрении и авторитете, которые государственные органы могут предоставить в качестве координаторов расследований в области кибербезопасности и обсуждения конфиденциальной информации. Правительствам нужна обратная связь и технические ресурсы, которые могут предоставить организации частного сектора.

Культура доверия необходима для повышения кибербезопасности

Сами по себе технологии не могут удержать кибер-злоумышленников в страхе. Культура доверия также важна для успеха корпоративных инициатив в области кибербезопасности. Все заинтересованные стороны в экосистеме компании — члены совета директоров, руководители ИТ, бизнесмены, поставщики и т. д. — должны прийти к взаимному пониманию рисков компании и работать вместе, чтобы выбрать наилучший подход к устранению этих рисков.

Как мы узнали, достижение и сохранение такого уровня согласия и доверия может быть затруднено, особенно из-за естественной напряженности, связанной с усилиями по защите данных: повседневная работа группы кибербезопасности имеет последствия для бизнеса и наоборот.

Но если компании осознают человеческий фактор в кибербезопасности и предпримут шаги для устранения пробелов в доверии путем обеспечения большей прозрачности, они могут увеличить шансы на успех своих программ кибербезопасности — не только в ближайшей перспективе, но и в долгосрочной перспективе, независимо от виды угроз, которые могут возникнуть». ***(Kapil Bareja. Four major cybersecurity trust gaps across organizations and how to fix them // World Economic Forum (https://www.weforum.org/agenda/2023/07/how-to-bridge-the-cybersecurity-trust-gaps-in-your-organization/). 04.07.2023).***

***

«**Эволюция сложности кибербезопасности продолжается, и теперь организациям требуются экспертные навыки и надежные решения в области кибербезопасности для эффективной защиты своих конфиденциальных данных и систем.**

К сожалению, в отчетах указывается, что 40% южноафриканских компаний изо всех сил пытаются найти и удержать таланты в области кибербезопасности, а 64% согласны с тем, что нехватка возможностей кибербезопасности увеличивает организационные киберриски.

По мере того, как количество специалистов в Южной Африке сокращается, а спрос растет, организациям необходимо будет передавать различные функции

кибербезопасности на аутсорсинг. Тем не менее, аутсорсинг приносит свои собственные проблемы, поскольку организации должны отслеживать и управлять ценностью, полученной от нескольких поставщиков услуг.

«К счастью, с такими решениями, как Pretect, — говорит Кевин Вотшела, управляющий директор Magix, признанного поставщика кибербезопасности, — лица, принимающие бизнес-решения, могут революционизировать свой подход к кибербезопасности». Magix внедрил инновации, создав платформу Pretect, которую можно адаптировать к уникальным потребностям и бюджетам любой организации.

Pretect, которому уже доверяют более 40 компаний, с его веб-приложением и командой киберэкспертов эффективно предотвращает и обнаруживает широкий спектр киберугроз, от обычных фишинговых атак до неизвестных внутренних угроз.

Специалисты по кибербезопасности Magix, разработавшие Pretect, понимают, что создание и поддержка квалифицированной внутренней команды по кибербезопасности может стать серьезным бременем для предприятий, особенно малых и средних предприятий (МСП).

«После работы с несколькими компаниями и получения информации, — говорит Вотшела, — стало ясно, что каждая компания имеет уникальные требования и набор внутренних навыков. Вы не можете просто установить один и тот же пакет, программное обеспечение или продукт во все из них».

«Благодаря интеграции наших предложений и представлению их в виде «шведского стола» за небольшую часть стоимости компании, как большие, так и малые, теперь могут выбирать услуги, наиболее соответствующие потребностям их бизнеса», — добавляет он.

Pretect, созданный для борьбы с постоянно меняющимся ландшафтом цифровых угроз, предлагает комплексное решение для кибербезопасности, которое включает в себя несколько передовых методов кибербезопасности.

Клиенты получают доступ к первоклассным продуктам и опытным лучшим в своем классе инженерам по кибербезопасности по доступной ежемесячной цене с оплатой по мере использования.

После развертывания это круглосуточное решение:

– Обеспечивает непрерывное управление уязвимостями для упреждающего выявления и устранения рисков.

– Регулярно проводит тестирование на проникновение для имитации реальных атак и обнаружения уязвимостей, которые могут быть пропущены при автоматическом сканировании.

– Включает оценку брандмауэра для обеспечения правильной настройки и оптимальной защиты от потенциальных угроз.

– Запускает симулированные фишинговые кампании для оценки восприимчивости организации к таким атакам, которые остаются распространенным направлением кибератак.

– Предлагает обучение по вопросам безопасности, чтобы информировать сотрудников о рисках, связанных с попытками фишинга, вооружая их знаниями для выявления и надлежащего реагирования на потенциальные угрозы.

– Обеспечивает комплексное сканирование веб-приложений для выявления потенциальных слабых мест в общедоступных системах.

Кроме того, пользователи платформы могут легко оценивать, отслеживать и повышать уровень безопасности, используя единый интерфейс с единой панелью управления. Они также получают выгоду от безопасного центрального хранилища всех своих отчетов о кибербезопасности.

Чтобы максимизировать ценность Pretect, компании могут участвовать в ежемесячных сеансах обратной связи с опытными специалистами по кибербезопасности. Эти сессии дают возможность обсудить результаты оценки, решить проблемы и получить экспертные рекомендации по укреплению методов обеспечения безопасности.

«Для нас было крайне важно максимизировать ценность наших затрат на кибербезопасность. По сравнению с созданием внутренней кибер-команды партнерство с Pretect как нашим комплексным кибер-решением сократило наши прогнозируемые затраты на кибербезопасность на 35%. Что еще более важно, это обеспечило нам душевное спокойствие, зная, что у нас есть постоянная видимость

нашего состояния безопасности и доступ к команде специалистов», — говорит Крейг Хиллс из WhoYou.

Этьен Шмидт, руководитель отдела информационной безопасности в Nutun, добавляет: «Консультации и идеи, предоставленные киберэкспертами Pretect, позволили нашей команде принимать обоснованные решения, постоянно улучшая состояние безопасности нашей компании».

Положительным аспектом аутсорсинга услуг в области кибербезопасности является то, что с правильным партнером в области кибербезопасности вы можете преодолеть разрыв в области нехватки навыков в области кибербезопасности, сэкономить деньги, снизить риски и повысить производительность, и при этом быть уверенным в том, что данные и системы вашей компании находятся в безопасности». ***(Mamsi Nkosi. Evolving Cybersecurity Complexities Demand Expert Skills and Robust Solutions // African Technology Advisory (Pty) Ltd. (https://www.itnewsafrica.com/2023/07/evolving-cybersecurity-complexities-demand-expert-skills-and-robust-solutions/?utm_source=flipboard&utm_content=cindi_%2Fmagazine%2FCYBERSEC+%E2%80%A2+INFOSEC+%E2%80%A2+PRIVACY). 14.07.2023).***

***

«Optiv, лидер в области консультирования и решений в области кибербезопасности, опубликовал отчет, основанный на недавнем опросе лидеров кибербезопасности, который показывает, что 73% организаций заметили снижение воздействия разрушительных киберинцидентов благодаря их партнерству с управляемыми службы безопасности (MSS) и поставщики управляемого обнаружения и реагирования (MDR). Это выгодно отличается от 14%, не заметивших никакого влияния.

В опросе дополнительно исследуются многие аспекты пользовательского опыта и предпочтений, связанных с услугами MSS и MDR. Опрос проводился с декабря 2022 г. по апрель 2023 г. в сотрудничестве с Information Security Media Group (ISMG)…

По мере увеличения дефицита специалистов в области кибербезопасности услуги MSS и MDR позволяют организациям использовать аутсорсинговые решения для повышения зрелости кибербезопасности без увеличения численности персонала. Клиенты могут воспользоваться услугами внешних экспертов для эффективного управления ресурсами безопасности, не перегружая свой ИТ-персонал.

В условиях меняющегося ландшафта угроз руководители систем безопасности все чаще обращаются к решениям MSS/MDR для быстрого решения новых проблем благодаря передовым возможностям и технологиям внешних поставщиков. Шестьдесят четыре процента респондентов охарактеризовали выполнение своих программ обеспечения безопасности (SecOps) как «сложную» или «чрезвычайно сложную».

Когда их попросили определить три основные проблемы (из списка восьми вариантов) их программы SecOps, наиболее часто ранжировались следующие:

Найм/удержание талантов в сфере безопасности (58%)

Повышение сложности субъектов угроз (57%)

Постоянно расширяющаяся поверхность атаки (57%)

Кроме того, 33% респондентов назвали «слишком много плохо интегрированных инструментов безопасности» одной из трех главных проблем, что точно отражает тенденцию, наблюдаемую Optiv на рынке.

Удовлетворенность поставщика MDR относительно высока

Удовлетворенность текущими поставщиками MSS/MDR от 1 (низкая) до 5 (высокая)

31% оценили своего поставщика услуг на 4–5 баллов.

Тринадцать процентов с рейтингом 1-2

Пятьдесят шесть процентов были удовлетворены (оценка 3)

Организации видят преимущества использования партнеров для обеспечения комплексной безопасности

На вопрос, предпочитают ли они получать консультационные услуги по безопасности у существующего поставщика MSS/MDR:

Да: 31 %, потому что действующий поставщик услуг может быть лучше знаком с окружающей средой, что может улучшить результаты при оказании услуг.

Да: 14 %, потому что это может помочь консолидировать поставщиков.

426 ответов поступили из различных секторов, включая финансовые услуги, производство и здравоохранение. Пятьдесят девять процентов респондентов находятся на уровне директоров по информационной безопасности/системе безопасности, ИТ-директоров, вице-президентов и директоров, а 48% — в организациях с более чем 5000 сотрудников». ***(Cybersecurity Leaders Report Reduction in Disruptive Cyber Incidents With MSS/MDR Solutions // Informa PLC (https://www.darkreading.com/operations/cybersecurity-leaders-report-reduction-in-disruptive-cyber-incidents-with-mss-mdr-solutions?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 13.07.2023).***

***

«Кібербезпека є серйозним викликом для організацій будь-якого типу та розміру, включаючи невеликі організації з обмеженими ресурсами для програми кібербезпеки. Канадський центр кібербезпеки (CCCS), Агентство кібербезпеки та безпеки інфраструктури США (CISA) та Австралійський центр кібербезпеки (ACSC) нещодавно випустили вказівки, щоб допомогти невеликим організаціям запровадити базові заходи кібербезпеки, щоб розпочати формування стійкості кібербезпеки.

Проблема кібербезпеки

Кібербезпека важлива для всіх канадських організацій. CCCS Національна оцінка кіберзагроз на 2023-2024 рр. попереджає, що кіберзлочинність продовжує залишатися кіберзагрозою, яка найімовірніше вплине на канадців, а програми-вимагачі є постійною загрозою для канадських організацій.

Кіберзлочинці все частіше атакують малі та середні організації, в тому числі для отримання даних про їхніх клієнтів і як засіб доступу до систем інформаційних технологій і даних їхніх ділових партнерів. У грудні 2022 року Канадська

федерація незалежного бізнесу повідомила результати опитування, згідно з якими майже половина малих підприємств (45%) зазнали випадкової кібератаки в попередньому році, а 27% зазнали цілеспрямованої атаки.

Кібератаки можуть призвести до того, що невеликі організації зазнають потенційно руйнівних фінансових втрат і зобов'язань. Однак складні програми управління кіберризиками не під силу фінансовим і людським ресурсам більшості невеликих організацій. З цих причин урядові установи та інші організації випустили інструкції з кібербезпеки, призначені для невеликих організацій. Наприклад, у 2019 році CCCS видав інструкції під назвою «Базові засоби контролю кібербезпеки для малих і середніх організацій», щоб допомогти канадським організаціям підвищити ефективність своїх інвестицій у кібербезпеку. Рекомендовані базові засоби контролю відображають думку про те, що організації можуть пом'якшити більшість кіберзагроз за допомогою обізнаності та передових практик і успішно застосувати правило 80/20 – отримати 80% вигоди від 20% зусиль – у сфері кібербезпеки…

Останні вказівки

CCCS, CISA та ACSC нещодавно випустили інструкції з кібербезпеки, розроблені для невеликих організацій.

CCCS

CCCS Основні дії щодо кібербезпеки для невеликих організацій рекомендують базові заходи безпеки (з контрольними списками та посиланнями на додаткові ресурси), які невеликі організації можуть вжити, щоб розпочати підвищення стійкості своєї кібербезпеки. Нижче подано резюме:

Облікові дані: використовуйте різні складні паролі та багатофакторну автентифікацію («MFA») для кожного пристрою та облікового запису.

Оновлення/виправлення: автоматично оновлюйте та виправляйте операційні системи та програми.

Резервне копіювання: створюйте та безпечно зберігайте резервні копії даних.

Інструменти безпеки: інсталюйте інструменти превентивної безпеки (наприклад, антивірусне програмне забезпечення та віртуальну приватну мережу) у мережах і пристроях і використовуйте захисну систему доменних імен.

Навчання: навчіть співробітників основам кібербезпеки.

Готовність до реагування на інциденти: Створіть і перевірте план реагування на інциденти.

Керівництво рекомендує малим організаціям проводити регулярну інвентаризацію своїх активів інформаційних технологій, щоб визначити та визначити пріоритети захисту цінних активів. Керівництво також рекомендує невеликим організаціям розглянути можливість передати діяльність з кібербезпеки постачальнику послуг на основі вказівок CCCS «Вибір найкращого рішення для кібербезпеки для вашої організації».

CISA

CISA Кіберпосібник для малого бізнесу надає вказівки (з посиланнями на додаткову інформацію та ресурси) для створення ефективної програми кібербезпеки, організованої за ролями та обов'язками, придатними для малого бізнесу. Керівництво містить завдання для боротьби з «найпоширенішими атаками». Нижче подано резюме:

Генеральний директор: Генеральний директор організації повинен: (1) створити культуру безпеки; (2) вибрати та підтримувати «Керівника програми безпеки» та отримувати регулярні звіти від керівника; (3) переглянути та затвердити план реагування на інциденти; (4) брати участь у регулярних навчаннях з імітації атаки (тобто настільні навчання); та (5) підтримувати IT-лідерів.

Менеджер програми безпеки: Менеджер програми безпеки організації повинен: (1) забезпечити, щоб увесь персонал пройшов офіційне навчання щодо ключових питань і завдань кібербезпеки; (2) написати та підтримувати план реагування на інциденти; (3) проводити щоквартальні настільні вправи; та (4) переконатися, що весь персонал використовує MFA для доступу до ключових систем.

IT-керівник: Керівник інформаційних технологій організації повинен: (1) переконатися, що MFA доручено використовувати технічні засоби контролю; (2) увімкнути MFA для всіх облікових записів системного адміністратора; (3) виправляти та оновлювати програмне забезпечення з пріоритетом відомих уразливостей, що використовуються; (4) виконувати та тестувати плани резервного копіювання та відновлення; (5) видалити права адміністратора з ноутбуків користувачів; і (6) увімкнути шифрування диска для ноутбуків.

У посібнику наголошується на важливості використання MFA для доступу до облікового запису. Посібник також пояснює потенційні переваги безпеки використання безпечних хмарних служб, а не локальних служб.

ACSC

Посібник ACSC з кібербезпеки для малого бізнесу містить контрольний перелік основних заходів кібербезпеки та докладний посібник, який допоможе малому бізнесу захиститися від типових загроз кібербезпеці. Нижче подано резюме:

Захистіть облікові записи: використовуйте MFA та менеджер паролів, обмежте використання спільних облікових записів і обмежте доступ на основі необхідності знати.

Захист пристроїв/інформації: автоматичне оновлення пристроїв і програмного забезпечення, регулярне резервне копіювання інформації, використання програмного забезпечення безпеки для регулярного сканування пристроїв, отримання професійних порад щодо захисту мереж, захисту веб-сайтів, відновлення заводських налаштувань пристроїв перед їх продажем/утилізацією, налаштування пристроїв на автоматичне блокування після короткий час бездіяльності, розуміти бізнес-дані та відповідальність за їх захист.

Підготуйте персонал: навчіть співробітників питанням кібербезпеки, створіть план реагування на інциденти кібербезпеки та зареєструйтеся в програмі партнерства ACSC.

Посібник також заохочує невеликі організації до впровадження першого рівня зрілості стратегій зменшення кіберризику The Essential Eight для захисту підключених до Інтернету мереж Microsoft Windows.

Основні заходи кібербезпеки, рекомендовані CCCS, CISA та ACSC, є важливими, але їх може бути недостатньо для дотримання чинних законів або галузевих вимог. Наприклад:

Особиста інформація. Організації, які обробляють особисту інформацію, повинні дотримуватися зобов'язань згідно з канадськими законами про конфіденційність/захист особистої інформації щодо захисту особистої інформації, яка знаходиться під їхнім контролем, із застосуванням заходів безпеки, які відповідають конфіденційності інформації, включно з елементами (наприклад, система управління конфіденційністю та безпекою). які виходять за рамки основних заходів кібербезпеки...

Регульовані галузі: організації в регульованих галузях (наприклад, індустрія фінансових послуг) повинні пам'ятати про нормативні вимоги та вказівки щодо кібербезпеки, видані відповідними регуляторами…

Емітенти, які звітують: організації, які випустили цінні папери для громадськості, повинні встановити процеси ідентифікації та оцінки кіберризиків, а також внутрішні процедури звітності про інциденти, необхідні для дотримання зобов'язань щодо постійного розкриття інформації згідно з канадськими законами про цінні папери...

Вирішуючи, чи запроваджувати рекомендовані базові заходи кібербезпеки та як, організації повинні враховувати наступне:

Відповідність чинному законодавству: багато заходів кібербезпеки мають юридичні наслідки, зокрема дотримання законів про конфіденційність/захист особистої інформації, праці/зайнятості та прав людини. Своєчасна юридична консультація може допомогти організації законно запровадити засоби контролю кібербезпеки.

Транзакції злиття та поглинання. Стартапи та інші малі організації, які планують продаж або інший вихід, повинні пам’ятати про зростаючу важливість конфіденційності та кіберризиків у транзакціях злиття та поглинання…

Аутсорсинг діяльності з кібербезпеки: аутсорсинг діяльності з кібербезпеки (наприклад, постачальнику керованих послуг безпеки) може становити юридичні ризики, включаючи дотримання законів загального застосування (наприклад, законів про конфіденційність/захист особистої інформації) і галузевих вимог. Відповідно, організаціям слід розглянути питання про передачу найкращих практик, рекомендованих державними установами, регуляторами, уповноваженими з питань конфіденційності та іншими авторитетними джерелами, на аутсорсинг...

Готовність до реагування на інциденти. Ефективна реакція на інциденти кібербезпеки потребує не лише плану реагування на інциденти...

Мінімізація даних: мінімізація даних є основним принципом канадських законів про захист особистої інформації та може допомогти зменшити конфіденційність і кіберризики...

Юридичні привілеї: у відповідних випадках організації повинні вживати заходів для встановлення та підтримки юридичних привілеїв щодо комунікацій і документів, що стосуються їхньої діяльності з кібербезпеки, включаючи підготовку та тестування їхніх планів реагування на інциденти та навчання їх груп реагування на інциденти…» ***(Cybersecurity guidance for small organizations // Borden Ladner Gervais LLP (https://www.blg.com/en/insights/2023/07/cybersecurity-guidance-for-small-organizations). 11.07.2023).***

***

«За даними Бюро статистики праці, у епоху цифрових технологій не дивно, що кібербезпека є однією з найшвидше зростаючих і затребуваних професій.

Незважаючи на попит, брак навичок залишається, і багато вакансій у сфері кібербезпеки все ще потрібно заповнити. Дуже багато людей можуть не звертати уваги на кібербезпеку як на кар’єру, тому що вони не бачать себе «техніком». Вони

можуть уявляти, що кібербезпека призначена лише для комп'ютерних майстрів або хакерів, які використовують код, але реальність така, що кібербезпека потребує різноманітних навичок і людей для захисту від онлайн-загроз.

Ось чотири причини розглянути кібербезпеку, якщо ви змінюєте кар'єрний шлях або тільки починаєте роботу.

Гарантія роботи та більш висока винагорода

Вакансій у сфері кібербезпеки або інформаційної безпеки (infosec) багато, і вони можуть похвалитися конкурентоспроможністю

За даними Statista, у 2023 році було понад 750 000 вакансій у сфері кібербезпеки. А Zippia повідомляє, що середня національна зарплата інженера з кібербезпеки становить 99 492 долари США.

Як професіонал з кібербезпеки, навряд чи ви коли-небудь залишитеся без роботи чи варіантів. Кібербезпека також є гнучкою, тому є можливості для позаштатної чи віддаленої роботи.

У кібербезпеці є місце для всіх

Щоб працювати в сфері кібербезпеки, не обов'язково бути хакером чи комп'ютерним спеціалістом. Вивчаючи основи, ви отримаєте користь, але кібербезпека — це широка сфера, і багато ролей потребують різноманітних навичок, окрім технічних.

До нетехнічних функцій у сфері кібербезпеки належать аналітики відповідності, аналітики ризиків безпеки, інженери з продажу безпеки, обізнаність у сфері інформаційної безпеки або аудитори безпеки. Ці ролі часто передбачають передавання навичок, які ви, можливо, вже маєте, як-от управління проектами, дослідження, обслуговування клієнтів і спілкування.

Кібербезпека має значний вплив

За кожним бізнесом чи організацією стоять реальні люди, співробітники, клієнти та громадяни, які покладаються на кібербезпеку, щоб захистити нас від дестабілізуючих порушень даних і програм-вимагачів. Іншими словами, робота фахівців з кібербезпеки, яку виконують у цифровій сфері, має реальні наслідки в нашій фізичній реальності.

Кібербезпека відповідає вимогам, якщо робота, яка позитивно впливає на суспільство, допомагає вам прокидатися вранці.

Фахівці з кібербезпеки потрібні в кожній галузі

У цифровому світі кожна галузь є індустрією технологій. Як фахівець з кібербезпеки, пул потенційних секторів, у яких ви можете працювати, практично безмежний.

Ви можете стати інженером з кібербезпеки в охороні здоров'я, виробництві, фінансах, медіа та розвагах, освіті, роздрібній торгівлі чи уряді – це лише деякі з них. З таким цінним навиком можливості для зростання та цікаві кар'єрні шляхи є динамічними та захоплюючими…» ***(4 reasons to consider a career in cybersecurity // KSL.com (https://www.ksl.com/article/50684026/4-reasons-to-consider-a-career-in-cybersecurity). 11.07.2023).***

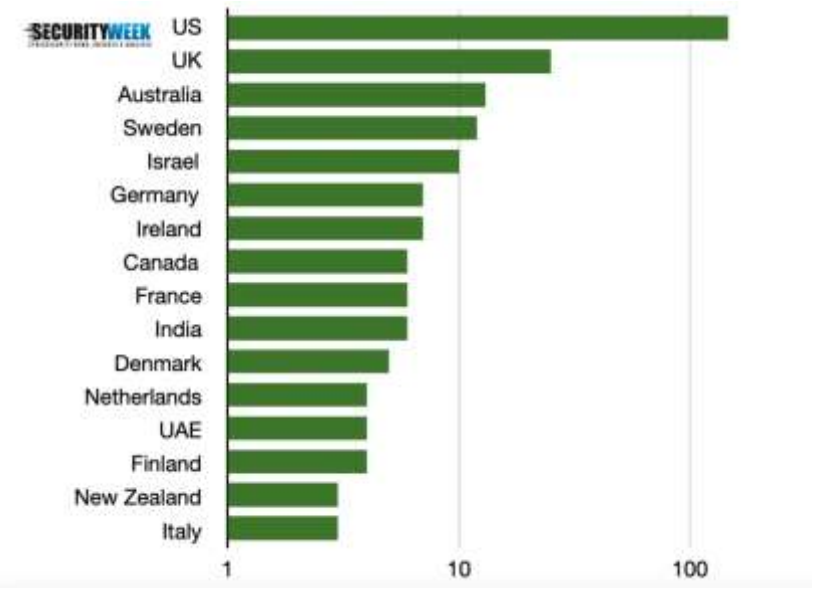
***

«SecurityWeek каталогізував 214 угод зі злиття та поглинання (M&A), пов'язаних із кібербезпекою, у період з 1 січня по 30 червня 2023 року.

Для порівняння, у 2022 році було оголошено 455 транзакцій, у тому числі 234 у першому півріччі. Найсуттєвіша різниця між першим півріччям 2022 року та першим півріччям 2023 року була в червні — минулого року був сплеск угод, а цього року — суттєве зниження, було зроблено менше двох десятків оголошень.

Більшість угод, оголошених у першій половині 2023 року, стосувалися компаній у Сполучених Штатах, що не дивно, враховуючи, що компанії в США частіше вступають у угоди злиття та поглинання в рамках стратегії розширення або виходу з ринку та, швидше за все, випустять англомовний прес-реліз.

Останні три роки за США йде Велика Британія, а такі країни, як Канада, Німеччина та Австралія, як правило, також входять до першої п'ятірки. Однак у першому півріччі 2023 року Швеція випередила Канаду та Німеччину, піднявшись на четверту позицію, маючи дюжину M&A у сфері кібербезпеки за участю шведських компаній.



З точки зору регіональних цифр, Північна Америка та Європа продовжують лідирувати, але кількість угод за участю компаній в Азії, схоже, зростає: у першій половині 2023 року було оголошено 26 угод порівняно з 29 угодами, оголошеними протягом 2022 року. З іншого боку 42 придбання стосувалися азіатських компаній З іншого боку, у 2021 році, значною мірою завдяки ізраїльським компаніям, які зараз знову спричиняють сплеск угод M&A в регіоні, поряд з компаніями з Індії, ОАЕ та Сінгапуру.

У першій половині 2023 року були доступні фінансові деталі для 30 угод на загальну суму 5,1 мільярда доларів, що значно менше, ніж розкрита вартість 51,5 мільярда доларів для 39 угод за той самий період минулого року. Також варто зазначити, що загальна розкрита вартість угоди досягла 63 мільйонів доларів на кінець 2022 року.

Найбільші угоди стосувалися приватних інвестиційних компаній, зокрема Thoma Bravo, яка придбала Magnet Forensics за 1,3 мільярда доларів, Francisco Partners придбала Sumo Logic за 1,7 мільярда доларів, а Crosspoint Capital Partners придбала Absolute Software за 870 мільйонів доларів.

Насправді компанії приватного інвестування брали участь у 20 M&A з першої половини 2023 року, що перевищує загальну кількість за рік у 2022 або 2021 роках. У чверті випадків інвестиційні компанії придбали керованих постачальників послуг безпеки (MSSP).

З усіх угод, оголошених у першому півріччі 2023 року, 82 стосувалися MSSP. Хоча ця цифра дещо вища порівняно з 66, оголошеними в першій половині 2022 року, загальна кількість придбань MSSP залишиться приблизно такою ж, як і минулого року, якщо угоди продовжаться такими ж темпами».

Сфера кібербезпеки завжди була неймовірно важливою для світу інформаційних технологій і ставала все більш критичною з розвитком технологій.

Зокрема, світ охорони здоров’я передбачає унікальний набір проблем кібербезпеки, враховуючи характер галузі та неймовірний обсяг даних. Записи здоров’я містять у собі найвразливіші деталі про людей. Немає порушень низької врожайності проти високої врожайності; скоріше, усі порушення потенційно можуть бути катастрофічними щодо конфіденційності та особистості пацієнта.

Крім того, охорона здоров’я є одним із найшвидших і потужних виробників даних, а це означає, що обсяг інформації, яка потребує захисту, неймовірно великий. За деякими оцінками, лікарні щодня створюють близько 50 петабайт даних, неймовірно великий обсяг інформації для обробки, не кажучи вже про захист. Зважаючи на те, наскільки чутливими є ці дані, потрібна інфраструктура, щоб не лише зберігати їх, але й захищати від вразливостей.

На початку цього року робоча група з кібербезпеки Міністерства охорони здоров’я та соціальних служб Сполучених Штатів випустила циркуляр із наданням ресурсів і навчанням, щоб допомогти боротися зі зростаючою хвилею кіберзагроз, характерних для охорони здоров’я. Заступник секретаря HHS Андреа Палм пояснила: «Кібератаки є однією з найбільших загроз, з якими сьогодні стикається наша система охорони здоров’я, і найкращим захистом є запобігання… Ці тренінги стануть перевагою для будь-якої великої організації, яка хоче навчити персонал основам кібербезпеки. обізнаності та пропонуються безкоштовно, гарантуючи, що ті лікарні та організації охорони здоров’я, які є найбільш вразливими до атак, можуть вжити заходів для підвищення стійкості. Це частина постійного зобов’язання HHS співпрацювати з лікарнями, Конгресом і лідерами галузі щодо захисту пацієнтів Америки».

Лише минулого тижня HCA Healthcare, одна з найбільших медичних організацій країни, повідомила про серйозний інцидент із кібербезпекою. На жаль, багато з найвідоміших лікарняних систем у всьому світі зазнали подібних проблем в останні роки, розчаровані зростаючими загрозами для своїх пацієнтів і громад. Політики, регулюючі органи охорони здоров’я та лідери організацій стурбовані, і це не дарма.

У дослідженні від грудня 2022 року, опублікованому в JAMA, дослідники виявили, що лише з 2016 по 2021 роки щорічна кількість атак програм-вимагачів на організації охорони здоров’я подвоїлася, потенційно розкривши особисту інформацію про здоров’я майже 42 мільйонів пацієнтів. Також було зазначено, що майже половина цих атак порушила надання своєчасної допомоги, створивши значну проблему для організацій охорони здоров’я та постраждалих громад.

Ключовою проблемою кіберзагроз у галузі охорони здоров’я є те, що дані не є єдиною вразливістю. Швидше, із збільшенням використання «розумного обладнання» та «підключених пристроїв» у медичних цілях з’явилися унікальні вразливості, багато з яких можуть призвести до сценаріїв «життя чи смерть». Один із найвідоміших прикладів цього було продемонстровано, коли експерти з безпеки знайшли спосіб зламати кардіостимулятор, виявивши значну вразливість, яка дозволила їм дистанційно контролювати електричні заряди, які доставляє пацієнту пристрій.

Цей інцидент змінив парадигму того, як після цього розглядалася кібербезпека охорони здоров’я: раптом занепокоєння більше не стосувалося лише даних або конфіденційності, а й того, як хакер або злочинець може дистанційно керувати рятівним пристроєм, таким як кардіостимулятор чи інсулін. помпа — пристрої, на які щодня покладаються мільйони людей у всьому світі.

З цих причин Управління з контролю за продуктами й ліками США рекомендує надзвичайно обережний підхід до медичних пристроїв та їх безпеки. Однак реальність така, що з розвитком технологій безсумнівно з’являться нові проблеми.

Ось чому кібербезпека, особливо в сфері охорони здоров’я, ймовірно, стане однією з найважливіших професійних функцій у найближчі роки. Бюро статистики праці вказує, що «аналітик інформаційної безпеки» є однією з найшвидше зростаючих професій у країні, очікується, що вона зросте майже на 35% до 2031 року. Білий дім також зробив це пріоритетом і навіть скликав національний саміт з кібернетичної праці та освіти. Минулого року: «З приблизно 700 000 відкритих вакансій у сфері кібербезпеки Америка стикається з проблемою національної безпеки, з якою потрібно боротися агресивно. [Цей саміт] також слугуватиме закликом до дії – щоб усі американці могли отримати вигоду з переваг цифрового домену та забезпечити, щоб наша країна реалізувала позитивні можливості, які перед нами відкриваються».

Дійсно, навчання наступного покоління технологів мистецтву та науці кібербезпеки матиме надзвичайно важливе значення для підтримки хребта охорони

здоров’я та стрімко зростаючої цифрової економіки в найближчі роки. Тому регулятори, політики та інноватори повинні робити все, що в їхніх силах, щоб інвестувати в цю сферу та підготуватися до кращого майбутнього». ***(Sai Balasubramanian. Healthcare Cybersecurity Specialists Will Face Unprecedented Demand In The Coming Years // Forbes (https://www.forbes.com/sites/saibala/2023/07/17/healthcare-cybersecurity-specialists-will-face-unprecedented-demand-in-the-coming-years/?sh=77c2a75f3949). 17.07.2023).***

***

«Багато лідерів уряду та приватного сектору переходять до підходу до кібербезпеки, заснованого на оцінці ризику. Ця зміна визнає, що спроможність і здатність однаково протистояти всім кіберризикам неможливі в сучасному всеохоплюючому цифровому середовищі. Однак, незважаючи на те, що люди, культура та поведінка залишаються основним ризиком в оцінках кібербезпеки та аналізі після інцидентів, ці сфери все ще потребують кращого розуміння та лікування.

У звіті Verizon про розслідування витоку даних за 2023 рік сказано, що «74% усіх зловмисностей включають людський фактор». Це менше з 82% у 2022 році, падіння, швидше за все, пов’язане з випадковістю, а не з ефективним управлінням. Викликає занепокоєння те, що хоча часто зазначається, що люди відіграють значну роль у кіберінцидентах і зломах, засобами правового захисту часто є «більше навчання», «більше відповідності» або «більше спілкування». Нам потрібна якісніша відповідь.

Ми живемо в будинку, побудованому за технологією

Ми розглядаємо кіберпроблеми, які постає перед стабільністю наших бізнес-операцій, як нову та унікальну проблему. Це не. Соціальна динаміка технологій добре зрозуміла. Наприклад, у «Федру» Платона Сократ розповідає про царя Тамуса та його занепокоєння щодо наслідків запровадження листів і писемності

серед населення. Ці інновації обіцяли зробити більш мудрими, як наші цифрові технології.

У періоди швидких технологічних інновацій організаційна зрілість відстає. Розрив між новою технологією та зрілістю для її ефективного використання є розривом можливостей. Чим швидше лідери можуть усунути розрив або організація може засвоїти та інтегрувати технологію, тим більш спроможною стає організація.

Проте наші організації – не порожні посудини. Люди оцінюють кожну нову технологію порівняно з попереднім досвідом. Вони порівнюють його з чимось знайомим і судять про це. Вони застосовують його як інструмент, який їм підходить, а не як інструмент, який міг бути призначений. Вони узгоджують технологію з переважаючою політикою, процедурами і, що важливо, культурою організації та робочого місця.

Щоб успішно запровадити нові технології, необхідно побудувати мости між існуючими соціальними та робочими практиками та технологіями. Наші уявлення про «підривні інновації» та внутрішнє та зовнішнє спонукання до швидкої трансформації є оптимістичними щодо того, як організації адаптуються до змін. Історія яскраво показує, як енергійно дає відсіч культура! Ось де починається виклик для кібербезпеки.

П'ять пропозицій про людей і кібербезпеку

Людська сторона кібербезпеки легко бути приголомшеною. Це частково тому, що йдеться не про кібербезпеку, а про організаційну культуру, лідерство та дизайн. Наступні пропозиції формулюються таким чином, що їх можна використовувати на різних рівнях керівництва. Щодо кожної пропозиції можна вжити конкретних заходів, але найефективнішою відповіддю буде їх вирішення за допомогою комплексної стратегії та планування дій. Разом вони утворюють мікрооснови для позитивної культури кібербезпеки.

1. Люди відіграють значну роль в інцидентах і зломах кібербезпеки.

Це потрібно прийняти. Люди залишатимуться центральними для роботи та організації. Однак існує потреба в багаторівневому підході до розвитку позитивної

культури інформаційної кібербезпеки, де управління, лідерська поведінка, індивідуальна поведінка та культура команди взаємопідсилюють один одного. Крім того, більш сильна орієнтація політики кібербезпеки на формування та вимірювання культурних і поведінкових чинників позитивної культури ризиків кібербезпеки також буде корисною. Мета полягає в тому, щоб працювати з людьми як частину ризику кібербезпеки, а не знецінювати людей або залишати робочу силу поза проблемою.

2. Ризик поведінки людини для кібербезпеки є незмінно високим.

З одного боку, існує тенденція стверджувати, що успішне реагування на кібербезпеку залежить від довіри, а з іншого – створювати людей і поведінку на основі реагування на кіберризики. Люди продовжуватимуть не слухати, робити помилки, нудьгувати, думати, що вони знають краще, і натискати на посилання, за якими не варто. Більш цікаве питання: «Чому вони це роблять?». Незважаючи на чітку політику, більше навчання, постійну комунікацію та стимули дотримуватись вимог, чому люди продовжують становити значну загрозу в інцидентах і порушеннях? Можливо, проблема не в людях.

Припустімо, що ми починаємо з передумови, що більшість людей хороші і хочуть чинити правильно. У такому випадку наш підхід до зниження ризиків кібербезпеки має приділяти менше часу сумнівам у індивідуальній поведінці та більше часу на розумінні керівництва та організаційного контексту, який спонукає хороших людей до поведінки, несумісної зі зниженням ризиків кібербезпеки. Наша оцінка ризику може бути зосереджена на неправильному рівні шкали.

3. Усе, що ми зараз робимо для зменшення ризику кібербезпеки, пов’язаного з поведінкою людей, не працює.

Продовжувати ігнорувати постійний факт, що значна частка порушень та інцидентів є самопровалом. Потрібно по-іншому думати про проблеми та можливості. Це може початися зі зміни наративу кібербезпеки. Наша організаційна культура культивується через щоденні мікроісторії, які ми чуємо та розповідаємо. Ці історії показують нам, що таке хороша і не дуже хороша поведінка.

Найсильніший культурний вплив на поведінку на робочому місці є місцевим. Саме розмови, які ми ведемо з однолітками та колегами, формують нашу поведінку.

Наші історії про кібербезпеку часто ґрунтуються на дотриманні вимог, пронизані страхом і пов'язані жаргоном. А для фахівців із безпеки в наших організаціях ці історії скрізь у новинах і постійно. Інтегрований підхід, який покращує загальну узгодженість повідомлень про кібербезпеку, може створити структуру, у якій можна легко вмістити внутрішні та зовнішні мікроісторії таким чином, щоб зменшити ризик.

4. Проблема поведінки людини в умовах кібербезпеки є багатогранною.

Щоб зменшити ризик, спеціалісти з кібербезпеки залежать від якості їхніх стосунків з іншими організаційними підрозділами, зокрема IT, HR, фінансами та комунікаціями.

Фахівці з кібербезпеки працюють на «ринку» відносин, де взаємозалежні ризики торгуються та управляються. Щоденна продуктивність залежить від ефективного врахування інтересів постійних працівників, співробітників за контрактом, підрядників, сторонніх постачальників, лінійних керівників, організацій зацікавлених сторін, конкурентів і спільноти. Тисяча повсякденних рішень щодо цих стосунків збираються, щоб визначити, як зменшити ризик кібербезпеки.

Робота фахівців з кібербезпеки полягає в управлінні та координації відносин для досягнення колективного результату. Отже, ефективна кібербезпека — це як переговори з іншими сторонами та функціями для покращення ефективності кібербезпеки, так і використання ресурсів для зменшення ризику.

Такий підхід може призвести до іншого розуміння ризиків і ефективності кібербезпеки та іншого набору показників успіху.

5. Існує потреба у комплексній моделі людської поведінки в кібербезпеці, яка могла б підтримувати багатовимірний підхід, який переходить від бачення людей як «проблеми» в кібербезпеці до бачення «людей як рішення».

Організації та робочі місця переживають глибокі зміни, які впливають на ризики кібербезпеки. Наприклад, скорочення персоналу, що призводить до

збільшення тимчасового тиску та вигоряння, збільшує ризик помилки та підвищує ризик кібербезпеки. Подібним чином зростання «тихого звільнення» може призвести до сплеску цинізму співробітників, зниження відданості та збільшення відчуженості. Це також може підвищити ризик кібербезпеки через як ненавмисні, так і навмисні дії.

Поведінка людини в сфері кібербезпеки є складною, але не неможливою

Наша реакція на зниження ризику не повинна бути ізольована від постійного тиску організаційних змін або постійних характеристик людської поведінки.

Існує потреба в підході, який би краще поєднував досвід роботи людей із мікроісторіями, які є місцевою основою позитивної культури кібербезпеки, з глибинними мотивами та спонуканнями, які керують і формують людську поведінку, а також із повсякденними денні розумові моделі та упереджені рішення, які безпосередньо впливають на поведінку людини на робочому місці.

Зрештою, зниження ризику кібербезпеки передбачає прийняття бажаних, передбачених і непередбачуваних наслідків об'єднання людей і технологій на робочому місці, як позитивних, так і негативних.

Запровадження цифрових технологій на робочому місці – це більше, ніж просто існуючі люди плюс нові технології. Це нова система з зовсім іншими можливостями та іншою поведінкою. Ось чому виклик кібербезпеки є динамічним, і люди завжди будуть в центрі уваги до зниження ризиків кібербезпеки». ***(David Schmidtchen. From awareness to behaviour change: The micro-foundations of cybersecurity culture // Private Media Pty Ltd. (https://www.themandarin.com.au/224389-from-awareness-to-behaviour-change-the-micro-foundations-of-cybersecurity-culture/). 10.07.2023).***

***

«…деякі з найбільших компаній кібербезпеки в сучасному світі. Це компанії, чий бізнес майже повністю присвячений кібербезпеці, а не лише програмному забезпеченню безпеки як частині їхньої ширшої бізнес-моделі.

Кожне з цих підприємств належить до однієї з трьох основних категорій: програмні рішення, постачальники послуг і гібридні підприємства безпеки, які надають як рішення, так і послуги…

№15 CyberArk — $543 мільйони річного доходу (2022)

Алон Н. Коен заснував компанію CyberArk у 1999 році. CyberArk є публічною компанією з інформаційної безпеки, яка пропонує керування ідентифікацією.

Технологія компанії широко використовується в лікарнях, енергетиці, роздрібній торгівлі, фінансових послугах і державних ринках. CyberArk гарантує, що лише авторизовані особи можуть отримати доступ до основних файлів у цих установах.

Штаб-квартира компанії знаходиться в Ньютоні, штат Массачусетс. Станом на 3 квартал 2022 року в CyberArk працює понад 2400 співробітників. CyberArk публічно торгується на NASDAQ як CYBR з 2014 року після того, як він подав заявку на первинну публічну пропозицію (IPO) до Комісії з цінних паперів і бірж.

№14 «Лабораторія Касперського» — 704 мільйони доларів річного доходу (2022)

«Лабораторія Касперського» — транснаціональна компанія з кібербезпеки зі штаб-квартирою в Москві, Росія. Євгін Касперський, Олексій Де-Мондерік, Наталя Касперська та Вадим Богданов заснували компанію в 1997 році. Станом на 2020 рік у компанії було понад 4000 співробітників.

Основним продуктом компанії є програмне забезпечення для кібербезпеки. У 2008 році «Лабораторія Касперського» створила Глобальну дослідницьку та аналітичну групу для дослідження загроз кібербезпеці. Лабораторія Касперського стала популярною після виявлення Stuxnet у 2010 році та Flame у 2012 році, які вплинули на 14 галузей промисловості в Ірані та від 1000 до 5000 машин у всьому світі відповідно.

№13 Trellix — 940 мільйонів доларів річного доходу (2022)

Trellix формально був відомий як підприємство FireEye і McAfee. Штаб-квартира компанії знаходиться в Мілпітасі, Каліфорнія, США. Компанія розпочала

свою діяльність у 2004 році як FireEye, зосередившись на віртуальних машинах для завантаження та тестування інтернет- трафіку. У 2013 році FireEye придбала приватну компанію Mandiant, яка надавала послуги реагування у випадках витоку даних.

Знову ж таки, у 2014 році FireEye придбала іншу компанію, що займається розкриттям безпеки даних, nPulse. І в 2016 році FireEye все ж придбала іншу компанію, iSIGHT, а потім компанію з автоматизації IT, Invotas. У червні 2021 року FireEye продала свою назву та продукти компанії Symphony Technology Group (STG) за 1,2 мільярда. Пізніше STG об'єднала FireEye і McAfee для запуску Trellix у 2022 році.

Компанія надає обладнання, програмне забезпечення та послуги для розслідування атак на кібербезпеку, захисту від шкідливого програмного забезпечення та аналізу ризиків IT-безпеки. Її продукти включають безпеку електронної пошти, безпеку кінцевих точок, обладнання та програмне забезпечення для кібербезпеки, інтерфейс керування та безпеку файлів.

№12 Програмне забезпечення Check Point — річний дохід 2,17 мільярда доларів (2022)

Check Point — це американо-ізраїльська багатонаціональна компанія з розробки програмного забезпечення зі штаб-квартирою в Тель-Авіві, Ізраїль, і Сан-Карлос, Каліфорнія, США. Гіл Швед, Маріус Нахт і Шломо Крамер заснували компанію в 1993 році.

Першим продуктом компанії був FireWall-1, а потім VPN-1. Check Point придбала інші IT-компанії в першому десятилітті 21-го століття, включно з мережевою безпекою Nokia.

Компанія зосереджена на своїй системі кібербезпеки п'ятого покоління (Gen V), яка спрямована на широкомасштабні та швидкі атаки на мобільні телефони.

Продукти та послуги Check Points включають безпеку мережі, безпеку даних, ThreatCloud, мобільну безпеку, безпеку кінцевих точок, керування безпекою та програмно-визначений захист тощо.

№11 Optiv Security Inc. — $2,5 млрд річного доходу (2022)

Optiv — приватна компанія з безпеки інформації зі штаб-квартирою в Денвері, штат Колорадо. 2 лютого 2015 року Accuvant і FishNet Security об'єдналися, утворивши Optiv Security, Inc. Наразі KKR & Co володіє більшою частиною компанії Optiv разом із Blackstone Group та іншими дрібними інвесторами.

Послуги Optiv включають кібероперації та стратегії, інновації та інтеграцію, керування ідентифікацією та доступом, управління ризиками, управління загрозами та кіберцифрову трансформацію.

№10 NortonLifeLock — $2,79 млрд річного доходу (2022)

NortonLifeLock — американська компанія з програмного забезпечення зі штаб-квартирою в Темпі, штат Арізона. Раніше вона була відома як Symantec Corporation. Гері Хендрікс заснував компанію 1 березня 1982 року в Саннівейлі, Каліфорнія. Станом на 2022 рік у компанії працювало 2700 співробітників.

NortonLifeLock спеціалізується на продажу програмного забезпечення для захисту інформації. Його продукти включають Norton Mobile Security, Norton Online Backup, Norton360, Norton Computer Tune Up, Norton Security і Norton Utilities.

№9 McAfee — $2,9 млрд річного доходу (2022)

McAfee — це глобальна компанія з програмного забезпечення безпеки зі штаб-квартирою в Сан-Хосе, Каліфорнія. Джон Макафі заснував компанію в 1987 році як McAfee Associates, Inc., але пізніше вона змінилася на McAfee, LLC у 2017 році. У лютому 2011 року Intel Security Division придбала McAfee. У 2017 році Intel Security і TPG Capital стали спільним підприємством McAfee.

McAfee пропонує численні продукти та послуги, які забезпечують оптимальний захист для користувачів комп'ютерів і мобільних пристроїв. Деякі з її продуктів включають McAfee Total Protection, McAfee Gamer Security і McAfee Mobile Security для Android, серед інших.

№8 Fortinet — $3,34 мільярда річного доходу (2022)

Fortinet — транснаціональна компанія, яка розробляє та продає рішення з кібербезпеки іншим компаніям. Штаб-квартира компанії знаходиться в Саннівейлі,

Каліфорнія, США. Кен Сі та Майкл Сі заснували компанію в 2000 році. До грудня 2021 року у філіях компанії було 10 195 співробітників.

Fortinet пропонує антивірусні програми, VPN, веб-фільтрацію, антишпигунське програмне забезпечення, антиспам, бездротовий контроль безпеки та систему запобігання вторгненню. Першим головним продуктом Fortinet був FortiGate, фізичний брандмауер, а потім антивірусне програмне забезпечення. Інші продукти включають Fortinet Security Fabric, FortiSwitch, FortiClient, FortiAnalyzer, FortiManager, FortiSandbox і FortiWeb.

№7 Синопсис — $4,2 мільярда річного доходу (2022)

Synopsis — це компанія з автоматизації електронного проектування зі штаб-квартирою в Маунтін-В'ю, Каліфорнія, США. Девід Грегорі та Арт де Геус заснували цю компанію в 1986 році. Станом на 2021 рік у Synopsis було 16 361 співробітників.

Нещодавно Synopsys включила тестування безпеки додатків у свої продукти та послуги. Основні послуги включають безпеку програмного забезпечення, дизайн і перевірку кремнію, інтелектуальну власність кремнію, а також безпеку та якість програмного забезпечення. У Synopsis є тренажери, які розробляють і налагоджують середовища для проектування комп'ютерних мікросхем і систем.

№6 Palo Alto Networks — $4,3 млрд річного доходу (2022)

Palo Alto Networks — багатонаціональна компанія з кібербезпеки зі штаб-квартирою в Санта-Кларі, Каліфорнія. Нір Зук заснував компанію в 2005 році. Станом на 30 квітня 2022 року в Palo Alto Networks працювало 11 870 співробітників.

Продукти та послуги компанії використовуються в понад 70 000 організаціях у 150 країнах. Вісімдесят п'ять із цих компаній належать до списку Fortune 100. Крім того, група дослідження загроз Unit 42 належить Palo Alto Networks. Palo Alto Networks відома розробкою брандмауерів і хмарного програмного забезпечення, яке забезпечує безпеку для користувачів Інтернету.

№5 Juniper Networks — $4,74 млрд річного доходу (2022)

Juniper — багатонаціональна компанія з програмного забезпечення зі штаб-квартирою в Саннівейлі, Каліфорнія. Прадіп Сіндху заснував компанію 6 лютого 1996 року. Станом на грудень 2021 року в компанії налічувався 10 191 співробітник.

Juniper Networks розробляє та продає IT-продукти, такі як маршрутизатори, комутатори, центри обробки даних та бездротові мережі. Це один з найбільших продавців основних маршрутизаторів для постачальників послуг Інтернету (ISP). Першим продуктом Juniper Networks була операційна система маршрутизатора Junos, випущена 1 липня 1998 року.

У травні 2003 року Juniper представила програмне забезпечення безпеки JProtect, яке включало моніторинг потоку, брандмауери, трансляцію мережевих адрес і фільтрацію даних. У 2014 році Juniper випустила продукти обману, які зберігали підроблені паролі та файли. Програмне забезпечення також може змінювати карти мережі, щоб заплутати хакерів.

№4 Корпорація Oracle — $42,44 млрд річного доходу (2022)

Oracle Corporation — багатонаціональна компанія з інформаційних технологій зі штаб-квартирою в Остіні, штат Техас. Ларрі Еллісон, Ед Оутс і Боб Майнер заснували компанію 16 червня 1977 року. Ларрі є найбільшим акціонером з 42,4% акцій. Станом на травень 2022 року в компанії працювало 143 тис. співробітників.

Oracle розробляє, продає та продає програмне та апаратне забезпечення. Крім того, компанія пропонує такі послуги, як консультації, навчання, хостинг і фінансові послуги, які доповнюють її продукти. Ці продукти включають Oracle Database, Oracle Cloud, сервери, робочі станції, Oracle ERP, Oracle Applications і Fusion Middleware тощо.

№3 Cisco Systems, Inc. — $51,56 млрд річного доходу (2022)

Cisco — це багатонаціональний конгломерат технологічної компанії зі штаб-квартирою в Сан-Хосе, Каліфорнія. Леонард Босак і Сенді Лернер заснували компанію 10 грудня 1984 року. Станом на 2021 рік у компанії працювало 79 500 співробітників.

Cisco розробляє, виробляє та продає мережеве обладнання, програмне забезпечення, телекомунікаційне обладнання та інші високотехнологічні послуги та продукти. Виходячи з рівня задоволеності співробітників, журнал Fortune назвав Cisco найкращою серед 100 найкращих компаній для роботи в 2021 році.

Cisco пропонує широкий спектр продуктів і послуг для малого бізнесу, корпоративного ринку та домашнього використання. Продукти та послуги Cisco охоплюють п’ять основних технологічних просторів: мережі, безпека, співпраця в центрі обробки даних та Інтернет речей.

№2 IBM — $76,2 млрд річного доходу (2022)

International Business Machines (IBM) — американська багатонаціональна технологічна компанія зі штаб-квартирою в Армонку, Нью-Йорк. Чарльз Ренлет Флінт заснував IBM 17 червня 1911 року. Станом на грудень 2021 року в компанії було 282 100 співробітників.

IBM розробляє та продає комп’ютерне програмне забезпечення, апаратне забезпечення та проміжне програмне забезпечення, а також надає хостингові та консультаційні послуги. Ця компанія пропонує продукти та послуги в таких категоріях: кібербезпека, штучний інтелект, хмарні обчислення, Інтернет речей, IT-інфраструктура та цифровий робочий простір.

№1Microsoft — $198,3 млрд річного доходу (2022)

Microsoft — багатонаціональна технологічна компанія зі штаб-квартирою в Редмонді, штат Вашингтон. Білл Гейтс і Пол Аллен заснували Microsoft Corporation 4 квітня 1975 року. Станом на 2022 рік у компанії працює 221 000 співробітників. Microsoft входить до п’ятірки великих технологічних компаній Америки разом із Google, Amazon, Meta та Apple. У 2020 році Microsoft посіла перше місце в рейтингу. 21 місце в рейтингу Fortune 500 за загальним доходом.

Спочатку Microsoft мала розробляти та продавати інтерпретатори Basic для Altair 8800. Зрештою вона стала найбільшою компанією з операційних систем для персональних комп’ютерів із MS-DOS, а потім з Windows. З 1990-х років корпорація Майкрософт суттєво зросла та здійснила кілька великих придбань, зокрема LinkedIn у грудні 2016 року та Skype Technologies у травні 2011 року.

Продукти кібербезпеки Microsoft включають Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps і Microsoft Defender Vulnerability Management…» ***(Brian Cherock. The 15 Largest Cybersecurity Companies In The World, And What They Do // History-Computer (https://history-computer.com/the-largest-cybersecurity-companies-in-the-world/). 12.07.2023).***

***

«…Головні проблеми кібербезпеки у 2023 році

Збільшення кількості кібератак

Сьогодні десь в інтернеті кожні 39 секунд відбувається нова атака, яка коштує трильйони доларів щорічно. Ці атаки можуть бути надзвичайно шкідливими для бізнесу, коштуючи непомірних доларів і відновлення ресурсів.

Віддалена робоча сила

Gartner прогнозує, що до 2025 року нестача талантів або людська невдача стануть причиною більш ніж половини значних кіберінцидентів. Кількість атак соціальної інженерії постійно зростає, оскільки люди постійно розглядаються як найбільш вразлива точка експлуатації. Опитування також показують, що співробітники обходять засоби контролю та вказівки щодо кібербезпеки організації, якщо це допомагає їм досягти робочих цілей.

Люди — слабка ланка

Велика перестановка ще більше виснажила й без того розтягнуті ресурси кібербезпеки, призвівши до відсутності сучасних інструментів безпеки або відсутності внутрішніх фахівців з безпеки або пропускної здатності для підтримки цих процесів.

Вимагацьке програмне забезпечення (ransomware)

Вимагацьке програмне забезпечення продовжує становити значну загрозу в усьому світі. Організації повинні мати рішення для резервного копіювання та

аварійного відновлення, а також плани реагування на інциденти, щоб захистити дані від атак і належним чином реагувати на інциденти.

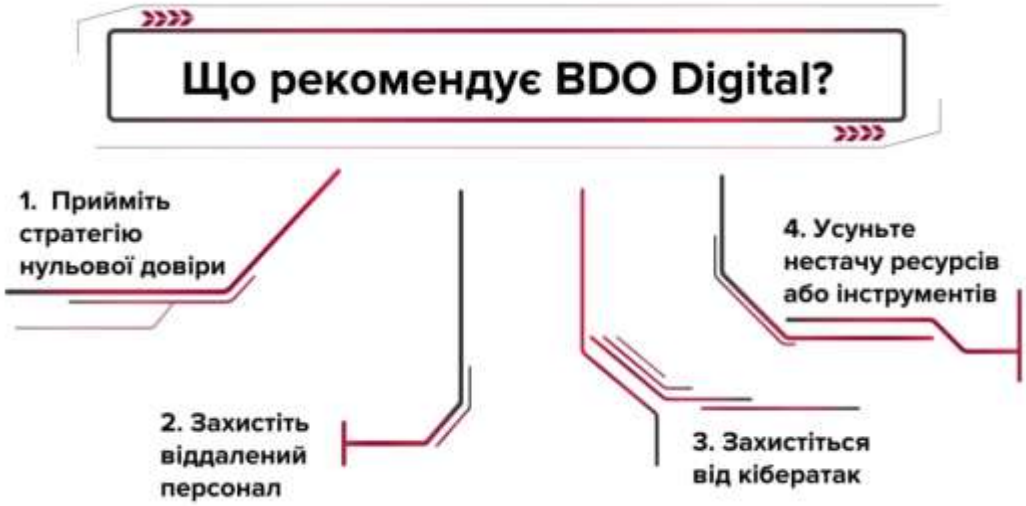
Хмарна безпека

Хмарна безпека — це спільна відповідальність між провайдером і замовником. Провайдер відповідає за безпеку інфраструктури, доступу, виправлення та конфігурації хостів / мереж, тоді як клієнт відповідає за управління користувачами та привілеями доступу, захист хмарних облікових записів, шифрування / захист даних і підтримку відповідності.

Штучний інтелект (AI)

Широке впровадження штучного інтелекту (AI) матиме як позитивні, так і негативні наслідки для кібербезпеки. Хоча ми можемо використовувати штучний інтелект для підвищення нашого кіберзахисту, хакери також вчаться на наявних інструментах штучного інтелекту для розробки більш просунутих атак і атак на традиційні системи безпеки або навіть системи, посилені штучним інтелектом.

Що рекомендує BDO Digital?



1. Прийміть стратегію нульової довіри

Впровадження стратегії нульової довіри означає перехід до широкої моделі безпеки, яка дозволить підприємствам обмежити доступ до цінних застосунків, даних і середовища компанії. Це буде зроблено таким чином, щоб не загрожувати продуктивності працівників або користувацькому досвіду.

2. Захистіть віддалений персонал

Впроваджуйте програмне забезпечення для запобігання втраті даних для моніторингу, виявлення та реагування на потенційні витоки даних, а захист кінцевих точок має бути запроваджений, щоб захистити мережу компанії від загроз, що надходять з пристроїв працівників або клієнтів.

3. Захистіться від кібератак

Багатофакторна автентифікація (MFA) є обов'язковою умовою кібербезпеки. БФА дозволяє організації надавати електронний доступ до вебсайтів або застосунків лише після надання двох або більше доказів, що підтверджують особу. Навчання з питань безпеки для працівників також має важливе значення, оскільки воно забезпечить постійну обізнаність працівників щодо будь-яких відповідних або важливих рухів кібербезпеки, наприклад, переконавшись, що всі працівники використовують найкращі практики безпеки електронною поштою.

4. Усуньте будь-яку нестачу ресурсів або інструментів

Якщо організації важко знайти інструменти або ресурси для розробки стратегії безпеки або керування нею, розгляньте можливість розробки поточної стратегії керованої безпеки та операціоналізації її. Однак уникайте просто «встановлення і забування». Безпечна стратегія повинна оновлюватись і коригуватися з часом. Щоб переконатися в цьому, подумайте про партнерство зі спеціалістом з безпеки. BDO Digital пропонує безліч внутрішніх фахівців, які можуть забезпечити постійний аналіз безпеки, що призводить до кращого прийняття рішень щодо бізнес-цілей…» ***(Що потрібно знати бізнесу про кібербезпеку у 2023 році // ТОВ «БДО» (https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/what-businesses-need-to-know-about-cybersecurity-in-2023). 17.07.2023).***

***

«Нове глобальне дослідження показує, що 70% керівників відділів кібербезпеки вважають, що всі попередження обробляються, тоді як особи, які працюють на передовій лінії, повідомляють, що обробляються лише 36%.

Звіт про готовність до кіберзагроз за 2023 рік, опублікований Swimlane і заснований на дослідженні, проведеному Dimensional Research, показує відсутність розуміння керівниками та дедалі більший дефіцит талантів, що лягає тягарем на команди безпеки, щоб запобігти порушенням, що призводять до завершення бізнесу.

Для звіту було опитано понад 1000 спеціалістів із безпеки та керівників корпоративних компаній із принаймні 5000 співробітниками та доходом 600 мільйонів доларів США. Респонденти були з Північної та Латинської Америки, Європи, Близького Сходу та Африки (EMEA) та Азіатсько-Тихоокеанського регіону (APAC). Дослідження вивчало сприйняття кібербезпеки серед професіоналів і керівників у сфері безпеки на місцях, поточні тенденції найму й утримання талантів, а також ефективність інструментів, які використовуються для вирішення найпоширеніших викликів кібербезпеки сучасності.

Згідно зі звітом, 70% керівників вважають, що всі попередження обробляються їхньою командою безпеки, тоді як лише 36% керівників, відповідальних за керування попередженнями, погоджуються з цим. Звіт показує, що лише 58% організацій фактично реагують на кожне попередження.

Незважаючи на те, що використання автоматизації для подолання цих проблем стає все більш популярним, 87% керівників вважають, що їхня команда безпеки має все необхідне для успішного впровадження. Для порівняння, 52% провідних посад стверджують, що вони мають достатньо досвіду, щоб правильно використовувати цей тип технології.

Звіт показав, що більшість респондентів вказали на збільшення труднощів у пошуку кандидатів з потрібними технічними навичками, досвідом і галузевими знаннями, причому 70% компаній повідомили, що зайняти посаду кібербезпеки займає більше часу, ніж два роки тому. На запитання, скільки часу потрібно, щоб зайняти посаду кібербезпеки, 82% організацій повідомили, що це займає три місяці або більше, а 34% повідомили, що це займає сім місяців або більше. Через ці проблеми 33% організацій вважають, що вони ніколи не матимуть повністю укомплектовану команду безпеки з відповідними навичками.

Згідно зі звітом, 95% учасників повідомили про бізнес-проблеми, що виникли внаслідок зміни команд безпеки, включаючи повільніше виявлення загроз, реагування та усунення, а також нездатність реагувати на попередження». ***(Cyber threat report reveals misalignment between execs & security analysts // BNP Media (https://www.securitymagazine.com/articles/99671-cyber-threat-report-reveals-misalignment-between-execs-and-security-analysts). 25.07.2023).***

***

«Swimlane, компанія з автоматизації безпеки з низьким кодом, сьогодні оголосила про випуск «Звіту про готовність до кіберзагроз за 2023 рік» на основі дослідження, проведеного компанією Dimensional Research. Звіт показує відсутність розуміння керівників і дедалі більший дефіцит кадрів, що лягає непосильним тягарем на команди безпеки, щоб запобігти порушенням, що призводять до припинення бізнесу.

Dimensional Research опитало 1005 професіоналів із безпеки та керівників корпоративних компаній із принаймні 5000 співробітниками та доходом 600 мільйонів доларів США. Респонденти були з Північної та Латинської Америки, Європи, Близького Сходу та Африки (EMEA) та Азіатсько-Тихоокеанського регіону (APAC). Дослідження вивчало сприйняття кібербезпеки серед професіоналів і керівників у сфері безпеки на місцях, поточні тенденції найму й утримання талантів, а також ефективність інструментів, які використовуються для вирішення найпоширеніших викликів кібербезпеки сучасності.

«Організації в різних галузях і в усьому світі намагаються найняти та утримувати кваліфікованих фахівців з кібербезпеки, які можуть ефективно керувати сучасною системою загроз», — сказав Джеймс Брір, генеральний директор Swimlane. «Це, на додаток до стрімко розвивається нормативно-правового ландшафту та складних нових загроз, створених генеративним штучним інтелектом, підкреслює необхідність для організацій масштабувати свій захист, поки не стало надто пізно. Ми сподіваємося, що наше дослідження послужить

каталізатором для дискусій, які прокладуть шлях до нової ери кібербезпеки, яка встановлює баланс між людським досвідом і технологічним прогресом».

Невідповідність безпеки зверху вниз

Незважаючи на посилення дискусій щодо кібербезпеки на рівні керівників і залів засідань, виникло різке зіткнення між керівниками, які вважають, що кожне попередження системи безпеки розглядається, і командами на місцях, які реагують на попередження. Сімдесят відсотків керівників вважають, що всі сповіщення обробляються їхньою командою безпеки, тоді як лише 36% керівників, відповідальних за керування сповіщеннями, погоджуються з цим. Правда полягає в тому, що лише 58% організацій фактично реагують на кожне попередження.

Незважаючи на те, що використання автоматизації стає все більш популярним для подолання цих проблем, помітна розбіжність також існує в розумінні набору навичок команди безпеки та наявних ресурсів для впровадження важких інструментів автоматизації сценаріїв. 87% керівників вважають, що їх команда безпеки володіє всім необхідним для успішного впровадження. Для порівняння, лише 52% провідних посад стверджують, що вони мають достатній досвід, щоб правильно використовувати цей тип технології.

Боротьба за наймання й утримання талантів збільшує ризики

Переважна більшість респондентів зазначили, що пошук кандидатів із відповідними технічними навичками, досвідом і галузевими знаннями ускладнюється. Сімдесят відсотків компаній повідомили, що зараз займає більше часу, щоб зайняти посаду кібербезпеки, ніж два роки тому. На запитання, скільки часу потрібно, щоб зайняти посаду кібербезпеки, 82% організацій повідомили, що це займає три місяці або більше, а 34% повідомили, що це займає сім місяців або більше. Ці проблеми змусили одну третину (33%) організацій вважати, що вони ніколи не матимуть повністю укомплектовану команду безпеки з відповідними навичками.

Дослідження також показало, що загрозливий рівень плинності кадрів і виснаження становить значний ризик для бізнесу, ставлячи під загрозу його операційну стабільність і стійкість. Понад дев’ять із 10 учасників (95%)

повідомляють про бізнес-проблеми, спричинені зміною команд безпеки, включаючи повільніше виявлення загроз, реагування та усунення, а також нездатність реагувати на попередження.

Наслідки автоматизації кібербезпеки

Результати дослідження підкреслили, що люди самі не можуть вирішити проблеми, які мучать сучасні команди з кібербезпеки. Організації, які успішно справляються з цими викликами, підвищують кваліфікацію людей із команди безпеки (SecOps) за допомогою стратегічних інвестицій у технології. Понад три чверті (78%) організацій, які обробляють кожне сповіщення, заявили, що використовують автоматизацію безпеки з низьким кодом у своєму стеку безпеки. Дев'яносто вісім відсотків учасників сказали, що використання рішень автоматизації безпеки, які охоплюють принципи низького коду, має переваги, такі як можливість масштабувати рішення за допомогою досвіду команди з меншою залежністю від навичок програмування.

За словами Gartner®, «технології SOAR є звичним явищем, щоб пропонувати функціональні можливості, схожі на низький код. Це робить покращення програмування та робочого процесу більш доступними для всіх членів групи безпеки, навіть якщо вони не мають великого досвіду програмування. Хоча SOAR продовжує пропонувати багато функцій для «досвідчених користувачів», ці особи можуть нести ширшу відповідальність за автоматизацію в усій організації. Досвідчені користувачі можуть розробляти власні інтеграції та часто повторно використовувати існуючий код/сценарії. Потім SOAR використовується для створення більш повторюваних ігор, що дозволяє організаціям використовувати цей код на основі будівельних блоків, які вже існують у технології».

Зобов'язання Swimlane допомогти

Щоб допомогти прокласти шлях організаціям, які борються з проблемами, викладеними у звіті, Swimlane сьогодні оголосила про доступність своєї автоматизованої готовності та зрілості оркестрованих ресурсів (ARMOR) Framework. Цей перший у своєму роді стандарт зрілості автоматизації безпеки

допоможе організаціям усіх розмірів і галузей зрозуміти, запровадити та вдосконалити автоматизацію безпеки для кращих результатів.

Онлайн-опитування є безкоштовним для будь-якої організації та вимагає приблизно 10 хвилин. Після подання консультант з автоматизації безпеки запланує безкоштовний перегляд спеціального звіту з детальним описом поточної зрілості автоматизації безпеки та рекомендаціями щодо вдосконалення своїх стратегій, щоб узгодити їх з найкращими галузевими практиками…» ***(Cyber Threat Readiness Report Reveals Alarming Misalignment Between Execs and Security Analysts // Business Wire (https://www.businesswire.com/news/home/20230725291049/en/Cyber-Threat-Readiness-Report-Reveals-Alarming-Misalignment-Between-Execs-and-Security-Analysts). 25.07.2023).***

***

«Технології мають вирішальне значення практично в кожній частині вашого життя в сучасному цифровому суспільстві. Це призвело до глобальних технологічних вимог, які збільшили можливості кар'єрного росту в цій галузі. Серед популярних варіантів кар’єри два варіанти кар’єри, які з’явилися на вершині, – це кібербезпека та наука про дані.

Згідно з останніми звітами, глобальний ринок кібербезпеки досягне 424,97 мільярда доларів США до 2030 року, а індустрія обробки даних, за прогнозами, зростатиме на 30,1% на рік між 2021 та 2028 роками. Таким чином, обидві кар’єри обіцяють зростання, а отже, вибір правильної кар’єри може бути важко.

Що таке Data Science?

Наука про дані — це робота з великими обсягами даних для отримання значущої інформації. Це як детектив, який шукає закономірності та рішення серед купи підказок. Ви аналізуєте дані за допомогою математики, статистики та комп’ютерних здібностей, щоб виявити приховані ідеї. Після цього ви надаєте цю інформацію у формі, яку інші можуть зрозуміти, дозволяючи їм приймати кращі рішення.

Важливість науки про дані

Він витягує інформацію з великих даних.

Розширена аналітика оптимізує ефективність і використання ресурсів.

Data Science покращує процес прийняття рішень, стратегію та дохід.

Data Science стимулює інновації та зростання бізнесу в цифрову еру.

Що таке кібербезпека?

Кібербезпека – це захист комп'ютерів, мереж і даних від зловмисників. Це як щит, який захищає ваші цифрові дані. Кібербезпека запобігає несанкціонованому доступу, виявляє та реагує на кібератаки за допомогою методів і технологій.

Важливість кібербезпеки

Згладжує віддалену роботу

Спрощує доступ до даних

Захищає від онлайн-загроз

Підвищує довіру споживачів до компанії

Різниця між кібербезпекою та наукою про дані

Обговорюючи кібербезпеку та науку про дані, існує багато способів, у яких вони відрізняються. Ось вони:

1. Зосередьтеся

Кібербезпека: Кібербезпека спрямована на захист комп'ютерів, мереж і даних від несанкціонованого доступу. Це частина впровадження профілактичних заходів, виявлення вразливостей і реагування на події безпеки.

Наука про дані: Наука про дані вивчає дані, щоб отримати розуміння та покращити прийняття рішень. Це відноситься до різних підходів і процедур для збору, аналізу та інтерпретації даних, щоб надати практичну інформацію та допомогти процесам прийняття рішень.

2. Цілі

Кібербезпека: Основна мета кібербезпеки — забезпечити конфіденційність, цілісність і доступність інформаційних систем і даних. Його мета — захистити цифрові активи та обмежити несанкціонований доступ. Його метою також є зменшення можливих ризиків і небезпек.

Наука про дані. Наука про дані спрямована на пошук закономірностей, тенденцій і кореляцій у даних, щоб отримати уявлення та зробити прогнози чи судження на основі даних. Його метою є отримання знань із даних для вирішення складних проблем, оптимізації процедур і сприяння інноваціям.

3. Набори навичок

Кібербезпека: спеціалісти з кібербезпеки повинні бути знайомі з комп'ютерними мережами, ідеями інформаційної безпеки, технологіями шифрування, методологією оцінки вразливості та процесами реагування на інциденти. Вони повинні бути знайомі з мережевою безпекою, шифруванням, етичним хакерством і безпекою.

Наука про дані: вчені з обробки даних повинні вміти проводити статистичний аналіз, програмувати та машинне навчання. Вони повинні володіти статистичним аналізом, машинним навчанням, візуалізацією даних і такими мовами програмування, як Python або R.

4. Додатки

Кібербезпека: кібербезпека захищає конфіденційні дані в різних галузях і на підприємствах, зокрема фінансові дані, особисті записи, інтелектуальну власність і урядові мережі. Організації, уряди та окремі особи повинні захищати свої цифрові активи від кіберзагроз.

Наука про дані: Наука про дані використовується в різних секторах, таких як бізнес-аналітика, охорона здоров'я, фінанси, маркетинг і соціальні науки. Він використовується для виявлення тенденцій у поведінці клієнтів, покращення операційних процесів, створення прогнозних моделей і покращення процесу прийняття рішень на основі фактичних даних…» ***(Pradip Mohapatra. Cyber Security or Data Science: Pick the Best Career Option // Datafloq (https://datafloq.com/read/cyber-security-or-data-science-pick-the-best-career-option/). 25.07.2023).***

***

«У цифровому середовищі, що постійно розвивається, підприємства все більше покладаються на технології для ефективної роботи. З цією довірою виникає нагальна потреба захистити конфіденційні дані та активи від кіберзагроз. Занепокоєння щодо кібербезпеки в певній галузі виникають через унікальні проблеми та вразливі місця, з якими стикаються різні сектори. Від фінансових установ і постачальників медичних послуг до виробництва та платформ електронної комерції кожна галузь має бути пильною щодо кібератак. У цій статті ми досліджуємо різноманітні проблеми та пропонуємо експертну думку, яка допоможе вам захистити вашу організацію від можливих порушень.

1. Зростаючий спектр кібератак

Кібератаки продовжують зростати за частотою та складністю, створюючи значні ризики для галузей у всьому світі. Оскільки хакери адаптують свої стратегії, компанії повинні бути на крок попереду, впроваджуючи надійні заходи кібербезпеки.

2. Виявлення вразливостей, характерних для галузі

Кожна галузь стикається з різними вразливими місцями та вимогами відповідності. Розуміння цих факторів має вирішальне значення для розробки ефективних стратегій кібербезпеки, адаптованих до конкретних потреб вашого бізнесу.

3. Відповідність і правила кібербезпеки

Дотримання галузевих правил кібербезпеки має важливе значення не лише для дотримання законодавства, але й для захисту конфіденційних даних. Недотримання цих стандартів може призвести до серйозних штрафів і шкоди репутації.

4. Роль штучного інтелекту в кібербезпеці

Штучний інтелект (ШІ) революціонізує ландшафт кібербезпеки, допомагаючи виявляти загрози, реагувати на інциденти та виявляти аномалії. Застосування технологій штучного інтелекту може підвищити здатність компанії перешкоджати потенційним атакам.

5. Спеціальні для галузі системи кібербезпеки

Різні галузі розробили власні рамки кібербезпеки, щоб вирішити свої унікальні проблеми. Ознайомтеся з цими рамками, щоб прийняти найбільш релевантні практики для свого бізнесу.

6. Захист фінансових установ від кіберзагроз

Фінансовий сектор є основною мішенню для кіберзлочинців через величезну кількість конфіденційної фінансової інформації, з якою він працює. Ознайомтеся з проблемами, з якими стикаються банки та фінансові установи, а також найкращими методами зменшення ризиків.

7. Сектор охорони здоров'я: захист даних пацієнтів

Індустрія охорони здоров’я бореться із захистом даних пацієнтів і електронних медичних записів. Дізнайтеся про гострі проблеми кібербезпеки, з якими стикаються постачальники медичних послуг, і про те, як забезпечити конфіденційність пацієнтів.

8. Кібербезпека в електронній комерції: захист онлайн-транзакцій

Оскільки індустрія електронної комерції процвітає, кіберзлочинці все частіше націлюються на онлайн-платформи, щоб викрасти платіжну інформацію. Відкрийте для себе основні стратегії кібербезпеки для компаній електронної комерції.

9. Виробничий сектор: захист від крадіжки інтелектуальної власності

Виробники стикаються з кіберзагрозами, які можуть порушити ланцюги поставок і поставити під загрозу інтелектуальну власність. Дізнайтеся, як захистити свій виробничий бізнес від кібершпигунства.

10. Зростаюча загроза атак програм-вимагачів

Атаки програм-вимагачів можуть завдати шкоди бізнесу, шифруючи важливі дані та вимагаючи викуп за розшифровку. Дізнайтеся, як захиститися від програм-вимагачів і забезпечити безперервність бізнесу.

11. Виклики хмарній безпеці

Перехід до хмарних інфраструктур створює нові виклики кібербезпеці. Зрозумійте ризики, пов’язані з хмарними обчисленнями, і те, як захистити свої дані в хмарі.

12. Уразливості Інтернету речей (IoT).

У зв’язку з поширенням пристроїв Інтернету речей компанії повинні усунути ризики безпеці, створені цими підключеними пристроями. Відкрийте для себе ефективні стратегії захисту вашої екосистеми IoT.

13. Захист критичної інфраструктури від кіберзагроз

Критична інфраструктура, така як електромережі та транспортні системи, чутлива до кібератак із потенційно катастрофічними наслідками. Дізнайтеся про кроки, вжиті для захисту цих життєво важливих систем.

14. Внутрішні загрози: небезпека всередині

Інсайдерські загрози, навмисні чи ненавмисні, становлять значний ризик для організацій. Досліджуйте способи виявлення та запобігання інсайдерським атакам для підтримки цілісності даних.

15. Створення кібер-обізнаної робочої сили

Ваші співробітники – ваша перша лінія захисту від кіберзагроз. Навчіть і навчіть свою робочу силу розпізнавати потенційні атаки та ефективно реагувати на них.

16. Роль страхування кібербезпеки

Страхування кібербезпеки може забезпечити фінансовий захист у разі витоку даних. Оцініть переваги та міркування інвестування в кіберстрахування.

17. Реагування на інциденти та готовність до кібербезпеки

Наявність чітко визначеного плану реагування на інцидент має вирішальне значення для мінімізації впливу кібератаки. Дізнайтеся, як розробити надійну стратегію реагування.

18. Аудити та оцінки кібербезпеки

Регулярні перевірки кібербезпеки допомагають виявити слабкі місця та забезпечити дотримання галузевих норм. Дізнайтеся про важливість проведення ретельних оцінок безпеки.

19. Захист інтелектуальної власності в епоху цифрових технологій

Захист інтелектуальної власності життєво важливий для компаній у всіх галузях. Впроваджуйте заходи для захисту ваших комерційних таємниць та інновацій.

20. Практики безпечної розробки програмного забезпечення

Розробка безпечного програмного забезпечення має першорядне значення для запобігання вразливостям, якими можуть скористатися кіберзловмисники. Ознайомтеся з найкращими методами розробки безпечного програмного забезпечення.

21. Технологія блокчейн і кібербезпека

Технологія блокчейн пропонує невід'ємні переваги безпеки. Зрозумійте, як інтеграція блокчейну може посилити зусилля вашої організації з кібербезпеки.

22. Атаки соціальної інженерії та запобігання

Соціальна інженерія залишається поширеною тактикою, яку використовують хакери. Навчіться розпізнавати та перешкоджати спробам соціальної інженерії.

23. Роль тестування на проникнення в кібербезпеці

Тестування на проникнення є важливою практикою для виявлення та усунення вразливостей у ваших системах до того, як ними скористаються кіберзлочинці.

24. Автоматизація кібербезпеки та її переваги

Автоматизація певних завдань кібербезпеки може збільшити ефективність і час відповіді. Дослідіть переваги автоматизації кібербезпеки.

25. Майбутнє галузевої кібербезпеки

З розвитком технологій зростатимуть і кіберзагрози. Отримайте уявлення про майбутнє кібербезпеки та про те, як випереджати нові ризики.

Проблеми кібербезпеки в галузі

Проблеми кібербезпеки значно відрізняються залежно від галузі, у якій ви працюєте. Розуміння цих викликів має вирішальне значення для розробки ефективних заходів безпеки». ***(Industry-Specific Cybersecurity Concerns: Safeguarding Your Business in the Digital Age // News Track Live (https://english.newstracklive.com/news/industry-specific-cybersecurity-concerns-safeguarding-your-business-in-the-digital-age-sc54-nu371-ta371-1288661-1.html). 30.07.2023).***

***

«28 червня 2023 року Департамент фінансових послуг Нью-Йорка («NYDFS») опублікував оновлену запропоновану Другу поправку («Поправка») до свого Регламенту про кібербезпеку, 23 NYCRR Part 500. 9 листопада 2022 року NYDFS опублікував перший проект запропонованої поправки та отримав коментарі від зацікавлених сторін протягом 60-денного періоду. Оновлена запропонована поправка підлягає додатковому 45-денному періоду коментарів.

У результаті початкового 60-денного періоду коментарів оновлена Поправка містить низку змін, зокрема такі:

визначення NYDFS роз'яснив порогові значення для розрахунку, коли охоплені організації кваліфікуються як «компанії класу А», до яких пред'являтимуться підвищені вимоги. «Компанія класу А» — це суб'єкт господарювання, що має принаймні 20 мільйонів доларів США валового річного доходу за кожний з останніх двох фінансових років від комерційної діяльності суб'єкта господарювання та його філій у Нью-Йорку та: (1) понад 2000 працівників у середньому за останній два фінансові роки як для організації, так і для її філій; або (2) понад 1 000 000 000 доларів США валового річного доходу за кожний з останніх двох фінансових років від усіх ділових операцій організації та її філій. В оновленій запропонованій поправці пояснюється, що під час розрахунку кількості працівників і валового річного доходу «філії» включають лише ті, які спільно використовують інформаційні системи, ресурси кібербезпеки або всю чи будь-яку частину програми кібербезпеки з відповідною охопленою організацією.

NYDFS уточнив, що, хоча відповідно до поправок від компаній класу А все ще вимагатиметься проводити «незалежний аудит» своїх програм кібербезпеки принаймні раз на рік, такі «незалежні аудити» включають ті, які проводяться внутрішніми аудиторами, які можуть приймати рішення (крім зовнішніх). аудитори).

NYDFS звузила запропоноване раніше визначення «привілейованого облікового запису» таким чином, що тепер воно застосовується до «будь-якого авторизованого облікового запису користувача або облікового запису служби, які можуть використовуватися для виконання важливих для безпеки функцій, які звичайні користувачі не мають права виконувати, включаючи, але не обмежуючись цим, можливість додавати, змінювати або видаляти інші облікові записи або вносити зміни в конфігурацію інформаційних систем, щоб зробити їх більш-менш безпечними». Запропонована поправка все одно вимагатиме від охоплених суб'єктів дотримуватись низки нових зобов'язань щодо контролю доступу щодо привілейованих облікових записів і повідомляти NYDFS протягом 72 годин після того, як їм стане відомо про подію кібербезпеки, коли неавторизований користувач отримав доступ до привілейованого облікового запису.

NYDFS пояснив, що якщо програма кібербезпеки або частина програми кібербезпеки прийнята від афілійованої особи, «старшим керівним органом» (наприклад, рада або еквівалентний керівний орган) може бути афілійована особа. Як описано нижче, відповідно до поправок вищі керівні органи матимуть нові наглядові обов'язки.

Вимоги до управління

Вищі керівні органи: NYDFS звузила запропоновані раніше обов'язки для вищих керівних органів, скасувавши вимогу «надавати вказівки керівництву щодо управління ризиками кібербезпеки відповідної організації». Оновлені поправки та додаткові вказівки NYDFS пояснюють, що основним обов'язком вищого керівного органу є ефективний нагляд за управлінням ризиками кібербезпеки організації, а не участь у повсякденних операціях управління. Крім того, NYDFS пом'якшила запропоновану раніше вимогу про те, щоб вищий керівний орган «володів достатнім досвідом і знаннями або отримував поради від осіб з достатніми досвідом і знаннями для здійснення ефективного нагляду за управлінням ризиками кібербезпеки», замінивши її вимогою «мати достатнє розуміння питань, пов'язаних з кібербезпекою, для здійснення такого нагляду, який може включати використання радників».

Оцінка ризиків: NYDFS повністю вилучив запропоновану раніше вимогу відповідно до Розділу 500.9(d) про те, що принаймні раз на три роки компанії класу A залучають зовнішніх експертів для проведення необхідної оцінки ризиків.

План реагування на інциденти (IRP) і план забезпечення безперервності роботи та аварійного відновлення (BCDRP):

NYDFS додав пропоновану вимогу, згідно з якою план реагування на інцидент відповідної організації передбачає підготовку «аналізу першопричини, який описує, як і чому сталася подія, який вплив вона мала на бізнес і що буде зроблено, щоб запобігти повторенню». NYDFS уточнив, що покрита план BCDR суб'єкта, який вимагається згідно із запропонованими поправками, має бути розроблений для забезпечення доступності та функціональності інформаційних систем та матеріальних послуг охопленого суб'єкта, а також захисту персоналу, активів і непублічної особистої інформації у випадку, пов'язаного з кібербезпекою. порушення нормальної господарської діяльності.

NYDFS пояснила, що суб'єктам, які охоплюються, потрібно щорічно тестувати як свої IRP, так і BCDRP за участю всього персоналу, який має важливе значення для реагування, включаючи вищих посадових осіб і керівників найвищого рангу відповідної організації.

Резервне копіювання: Що стосується запропонованих вимог щодо підтримки та тестування резервних копій, NYDFS (1) пояснив, що охоплена організація повинна щорічно перевіряти свою здатність відновлювати свої «критичні дані та інформаційні системи» з резервних копій; і (2) обмежив раніше запропоновану вимогу щодо того, щоб охоплені організації зберігали резервні копії до тих, які «необхідні для відновлення суттєвих операцій».

Заходи безпеки

Автоматичний блокувальник паролів: NYDFS пояснив, що вимога до компаній класу A щодо впровадження «автоматизованого методу блокування часто використовуваних паролів» стосується лише облікових записів в інформаційних системах, які «належать або контролюються компаніями класу A», а для всіх інших облікових записів лише там, де «можливо».

Багатофакторна автентифікація («MFA»): NYDFS значно розширила обсяг запропонованих вимог MFA, щоб вони тепер узгоджувалися з вимогами MFA відповідно до Правил безпеки FTC. У той час як початкова запропонована поправка вимагала MFA лише для певних привілейованих облікових записів і для віддаленого доступу до охоплених систем організації та сторонніх програм, оновлена запропонована поправка загалом вимагає MFA для будь-якого доступу до систем організації, незалежно від того, чи є цей доступ віддаленим, якщо суб'єкт, на який поширюється дія, не відповідає вимогам обмеженого виключення (у цьому випадку суб'єкт повинен відповідати спочатку запропонованим вимогам MFA). Як альтернатива, головний спеціаліст з інформаційної безпеки («CISO») охопленої організації може письмово схвалити використання розумно еквівалентних або більш безпечних компенсаційних засобів контролю, хоча такі засоби контролю потрібно буде переглядати принаймні щорічно.

Повідомлення та сертифікати до NYDFS

Звітування про події кібербезпеки: NYDFS скасувала запропоновану раніше вимогу про те, щоб суб'єкти, які покриваються, повідомляли NYDFS протягом 72 годин, якщо на них вплинула подія кібербезпеки у стороннього постачальника послуг. Натомість NYDFS пояснила, що інші порогові значення для звітування про події кібербезпеки (наприклад, подія, яка має обґрунтовану ймовірність завдати суттєвої шкоди суттєвій частині нормальної діяльності суб'єкта) дотримуються незалежно від того, сталася подія в охопленому суб'єкті чи його постачальник послуг. Крім того, NYDFS скасувала запропоновану раніше вимогу оновлювати NYDFS протягом 90 днів після повідомлення про подію кібербезпеки та замінила її зобов'язанням негайно надавати інформацію на запит NYDFS.

Щорічна сертифікація відповідності: наразі компанії зобов'язані щорічно сертифікувати свою відповідність Правилам кібербезпеки NYDFS за попередній календарний рік. В оновленій запропонованій поправці NYDFS запропонувала звузити сферу сертифікації до відповідності матеріалів. Крім того, відповідно до початкової запропонованої поправки, NYDFS додав альтернативний варіант до щорічної сертифікації відповідності, який дозволить охопленим організаціям

подати письмове підтвердження того, що вони не повністю відповідають усім вимогам. В оновленій версії запропонованої поправки NYDFS пом'якшила вимогу щодо письмового підтвердження, скасувавши зобов'язання ідентифікувати «всі області, системи та процеси, які потребують суттєвого вдосконалення, оновлення або перепроектування».

Крім того, згідно з початковою версією Поправки, хоча суб'єкти, на які поширюється дія, мали виконати деякі нові вимоги протягом 180 днів після дати набрання чинності Поправкою, для інших вимог діяли перехідні періоди в один рік, 18 місяців або два роки., відповідно. Згідно з оновленою версією Поправки, для більшої кількості нових вимог поширюватимуться більш тривалі перехідні періоди. Нові вимоги МЗС, наприклад, будуть залежати від дворічного перехідного періоду…» ***(NYDFS Proposes Updated Second Amendment to Its Cybersecurity Regulation // Hunton Andrews Kurth LLP. (https://www.huntonprivacyblog.com/2023/07/05/nydfs-proposes-updated-second-amendment-to-its-cybersecurity-regulation/#page=1). 05.07.2023).***

***

«13 июля 2023 г. Белый дом опубликовал первую версию своего Плана реализации национальной стратегии кибербезопасности («План реализации»), который будет обновляться ежегодно. Две всеобъемлющие цели Плана реализации заключаются в том, чтобы удовлетворить потребность в более способных участниках киберпространства, чтобы нести большую ответственность за кибербезопасность, и увеличить стимулы для инвестиций в долгосрочную устойчивость. План реализации построен вокруг пяти столпов, изложенных в Национальной стратегии кибербезопасности Белого дома ранее в этом году, а именно: (1) защита критической инфраструктуры; (2) разрушить и ликвидировать участников угроз; (3) формирование рыночных сил для обеспечения безопасности и устойчивости; (4) инвестировать в устойчивое будущее; и (5) наладить международное партнерство для достижения общих целей. План реализации определяет стратегические цели и высокоэффективные инициативы в области

кибербезопасности по каждому компоненту и назначает федеральное агентство, ответственное за руководство инициативой для достижения каждой цели. Ниже приводится краткое описание некоторых ключевых инициатив, включенных в План реализации, которые непосредственно повлияют на организации критической инфраструктуры, включая здравоохранение, энергетику, производство, информационные технологии и финансовые услуги.

Столп первый: защита критической инфраструктуры

Первый компонент Плана реализации сосредоточен на инициативах, направленных на поддержку национальной и общественной безопасности. Он включает в себя инициативу Совета национальной безопасности (NSC) по установлению требований к кибербезопасности в критических секторах инфраструктуры, инициативу Национального института стандартов и технологий (NIST) по расширению использования агентствами структур и международных стандартов (таких как NIST Cybersecurity Framework (CSF)), а также инициатива Агентства кибербезопасности и безопасности инфраструктуры (CISA) по расширению государственно-частного партнерства. Примечательно, что он также включает инициативу CISA по выпуску окончательного правила в соответствии с Законом об отчетности о кибер-инцидентах для критически важной инфраструктуры (CIRCIA). …CIRCIA поручает CISA опубликовать уведомление о предлагаемом нормотворчестве в течение 24 месяцев с даты принятия CIRCIA, а окончательное правило должно быть выпущено не позднее, чем через 18 месяцев после публикации предлагаемого нормотворчества. Согласно Плану реализации, это должно быть завершено к 30 сентября 2025 года.

Столп второй: разрушить и ликвидировать участников угрозы

Второй компонент плана реализации включает ряд законодательных и нормативных инициатив с короткими сроками, направленных на борьбу с киберпреступностью и ее предотвращение. К ним относятся инициатива Министерства обороны (DOD) опубликовать обновленную киберстратегию к первому кварталу 2024 финансового года (1 квартал 24 финансового года) (т. е. с 1 октября по 31 декабря 2023 г.); инициатива Министерства юстиции (DOJ) по работе

с межведомственными партнерами по предложению законодательства по пресечению и сдерживанию киберпреступности к четвертому кварталу 2023 финансового года (т. е. с 1 июля по 30 сентября 2023 г.); а также инициатива Министерства торговли опубликовать Уведомление о предлагаемом нормотворчестве в отношении стандартов и процедур требований для поставщиков и реселлеров инфраструктуры как услуги (IaaS) также к четвертому кварталу 2023 ФГ. (Федеральный финансовый год длится с 1 октября по 30 сентября.)

Столп третий: формирование рыночных сил для обеспечения безопасности и устойчивости

Возможно, наиболее важно, что третий столп включает в себя стратегическую цель «переложить ответственность за небезопасные программные продукты и услуги» с директивой для Управления национального кибер-директора (ONCD) о проведении симпозиума для «изучения подходов к разработке долгосрочной стратегии». гибкая и устойчивая система ответственности за программное обеспечение». Как указано в Плане реализации, «чтобы начать формировать стандарты заботы о безопасной разработке программного обеспечения», администрация «будет стимулировать разработку адаптируемой структуры безопасной гавани для защиты от ответственности компаний, которые безопасно разрабатывают и поддерживают свои программные продукты и услуги.» Дата завершения этой инициативы — 2 квартал 2024 финансового года.

Другие стратегические цели и инициативы в области безопасности третьего компонента включают:

Управление разработкой безопасных устройств IoT. Эта стратегическая цель включает в себя инициативу Административно-бюджетного управления (OMB) по внедрению требований Федерального регламента закупок (FAR) в соответствии с Законом об улучшении кибербезопасности Интернета вещей от 2020 года... Дата завершения — 4 квартал 2023 финансового года.

Использование Закона о ложных претензиях для улучшения кибербезопасности поставщиков. В рамках этой инициативы Министерство юстиции расширит усилия по «выявлению, преследованию и предотвращению

заведомо несоблюдения требований кибербезопасности в федеральных контрактах и грантах[.]». Закон о ложных претензиях может возбуждать гражданские иски против государственных грантополучателей и подрядчиков, «которые не выполняют обязательства по кибербезопасности», например, «предоставляя некачественные продукты кибербезопасности, сознательно искажая свои методы или протоколы кибербезопасности или сознательно нарушая обязательства по мониторингу и отчетности о киберинцидентах и нарушения». Дата завершения — 4 квартал 2025 финансового года.

Изучение поддержки федерального киберстрахования. В рамках этой инициативы Федерального страхового управления Министерства финансов в сотрудничестве с CISA и ONCD «оценит необходимость федерального страхового реагирования на катастрофические кибер-события», которые «поддержат существующий рынок киберстрахования». Дата завершения – 1 квартал 2024 года.

Столп четвертый: инвестируйте в устойчивое будущее

Заметной стратегической целью четвертого компонента является «защита технической основы Интернета». Инициативы в рамках четвертого компонента включают инициативу OMB по внедрению передовых методов сетевой безопасности, включая определение приоритетов шифрования запросов системы доменных имен (DNS), с датой завершения во 2 квартале 2024 финансового года… Эта основа также включает инициативу ONCD по содействию внедрению «языков программирования, безопасных для памяти» в рамках Инициативы по безопасности программного обеспечения с открытым исходным кодом. (OS3I) (дата завершения 1 квартал 24 финансового года) и инициатива NIST по устранению пробелов в безопасности пограничного протокола (BGP) и IPv6 с помощью международных стандартов (дата завершения 2 квартал 24 финансового года). ONCD также возглавит инициативу по разработке национальной стратегии в области кибербезопасности и образования (дата завершения — 2 квартал 2024 финансового года).

Пятый столп: налаживание международного партнерства для достижения общих целей

Пятый компонент Плана реализации включает в себя стратегические цели по публикации Международной стратегии киберпространства и цифровой политики, расширению киберпотенциала международных партнеров за счет оперативного сотрудничества правоохранительных органов и созданию гибких механизмов иностранной помощи для быстрого реагирования на киберинциденты. Он также включает в себя инициативу Министерства обороны США, Министерства юстиции и ФБР по «привлечению к ответственности безответственных государств, когда они не выполняют свои обязательства».

Широкие инициативы

План реализации включает более 65 инициатив, лишь некоторые из которых освещены в этом посте. Хотя План реализации в настоящее время не устанавливает каких-либо новых или обязательных требований к предприятиям, он представляет собой полезную дорожную карту для понимания приоритетов федерального правительства в области кибербезопасности, а также графиков ведомств для завершения конкретных законодательных предложений и нормотворчества, а также политик правоприменения, все из которых имеют значительное влияние бизнеса на кибербезопасность. Организации, затронутые этими инициативами, в том числе поставщики финансовых услуг, энергетики, здравоохранения, программного обеспечения и технологий, должны оценить влияние Плана на их операции в области кибербезопасности, особенно в том, что касается соблюдения нормативных требований и любых потенциальных безопасных убежищ. EBG тесно сотрудничает с организациями в рамках конфиденциальности между адвокатом и клиентом для проведения оценки рисков и выявления признанных методов обеспечения безопасности, которые могут укрепить практическую безопасность и улучшить соответствие требованиям». ***(Brian G. Cesaratto & Alexander J. Franchilli. White House Releases National Cybersecurity Strategy Implementation Plan // Epstein Becker & Green, P.C. (https://www.workforcebulletin.com/2023/07/14/white-house-releases-national-cybersecurity-strategy-implementation-plan/). 14.07.2023).***

***

«Средняя стоимость утечки данных в 2022 году составила 4,35 миллиона долларов, а в 2023 году ожидается, что она достигнет 5 миллионов долларов. Исследовательская компания Cyber Ventures прогнозирует, что к 2025 году киберпреступления обойдутся миру в 10,5 триллиона долларов. По данным Комиссии по ценным бумагам и биржам (SEC), «потенциальные затраты и ущерб, которые могут возникнуть в результате инцидента кибербезопасности, значительны. Многие небольшие компании стали объектами кибератак, настолько серьезных, что в результате они прекратили свою деятельность».

Чтобы снизить риск и повысить устойчивость к злонамеренной киберактивности, правительства и частный сектор должны разработать свои соответствующие подходы к управлению рисками кибербезопасности. Обе стороны должны более стратегически использовать свои возможности и разработать рамки для определения приоритетности инвестиций в соответствии с киберугрозами.

Призыв к действию

В марте 2023 года Белый дом опубликовал долгожданную Национальную стратегию кибербезопасности. Намечая курс на это «решающее десятилетие», Стратегия признает, что различные участники цифровой экосистемы обладают сравнительными преимуществами, когда речь идет о снижении рисков, наблюдении за злонамеренной киберактивностью, обобщении информации об угрозах и выработке действенных рекомендаций, пресечении действий субъектов угроз и повышении устойчивости. В связи с этим Стратегия требует большего от правительства и частного сектора.

Два всеобъемлющих принципа лежат в основе Национальной стратегии кибербезопасности. Во-первых, «наиболее способные и занимающие наилучшие позиции в киберпространстве должны лучше распоряжаться цифровой экосистемой». Во-вторых, «экономика и общество должны стимулировать принятие решений, чтобы сделать киберпространство более устойчивым и защищенным в долгосрочной перспективе». Согласование политики и бизнес-

решений с этими принципами, несомненно, повысит нашу национальную позицию в области кибербезопасности.Более безопасный и устойчивый кибердомен также полезен для бизнеса — инвестиции в безопасность стоят денег, но устранение нарушений стоит дороже.

Инвестиции, необходимые для принятия на себя дополнительной ответственности за безопасность, могут быть сопряжены с краткосрочными затратами, но они также повысят доверие общественности к надежности критической инфраструктуры и технологий, повысят производительность и прибыль и сделают возможным более прочное и более стратегическое партнерство между федеральным правительством и государством. частный сектор. Короче говоря, частный сектор и правительство хорошо обслуживаются, встраивая кибербезопасность во все аспекты операций и управления.

Смена парадигмы для правительства

Исторически сложилось так, что федеральное правительство полагалось на добровольные рамки для поощрения принятия частным сектором строгих стандартов кибербезопасности. Однако киберинциденты, такие как атака цепочки поставок SolarWinds и атака программы-вымогателя Colonial Pipeline, выявили ограничения чисто добровольной модели и подчеркнули каскадные последствия киберинцидентов. Еще до публикации Национальной стратегии кибербезопасности громкие кибератаки в 2020 и 2021 годах вынудили федеральное правительство пересмотреть свою зависимость от добровольных мер по повышению кибербезопасности критически важной инфраструктуры и технологических компаний.

Признавая необходимость повышения коллективной видимости вредоносной активности в домашних сетях, Конгресс США принял Закон об отчетности о кибер-инцидентах для критически важной инфраструктуры от 2021 года, который предписывает подпадающим под действие организациям сообщать об определенных кибер-инцидентах в Агентство по кибербезопасности и безопасности инфраструктуры (CISA) в рамках 72 часа. Этот закон получил поддержку частного сектора, потому что он позволил федеральному правительству

быстрее пресекать злонамеренные кибер-кампании и предоставлять критическое представление о тактике наших противников.

Между тем, исполнительная власть предпринимала активные усилия по поощрению внедрения более надежных методов обеспечения кибербезопасности. Заместитель советника по национальной безопасности по кибербезопасности и новым технологиям Энн Нойбергер в июне 2021 года написала открытое письмо руководителям корпораций и бизнес-лидерам, призвав их внедрить пять передовых методов из указа 14028, включая использование сторонних тестеров на проникновение и устранение инцидентов. планы реагирования.

В июле 2021 года президент Байден подписал Меморандум о национальной безопасности о повышении кибербезопасности для систем управления критически важной инфраструктурой, поручив Министерству внутренней безопасности (DHS) и Министерству торговли разработать цели по обеспечению кибербезопасности для критически важной инфраструктуры. Два департамента выпустили первую версию базовых межотраслевых целей в области кибербезопасности (CPG) в октябре 2022 года и с тех пор обновили их. С момента своего выпуска CPG информировали о новых федеральных требованиях к кибербезопасности, среди прочего, для наземного транспорта и авиации.

В феврале 2023 года директор CISA Джен Истерли и исполнительный помощник директора по кибербезопасности Эрик Гольдштейн опубликовали в журнале Foreign Affairs статью, в которой утверждалось, что «в каждом бизнесе ответственность за кибербезопасность должна быть возложена с ИТ-отдела на совет директоров, генеральный директор и высший исполнительный уровень». С этой целью директор Истерли и исполнительный помощник директора Гольдштейн заявили, что «каждый поставщик технологий должен начать с создания продуктов, которые являются «безопасными по умолчанию» и «безопасными по замыслу». С тех пор они выступают за принятие этих принципов.

Соответственно, в марте 2022 года Комиссия по ценным бумагам и биржам (SEC) опубликовала предлагаемое правило по управлению и управлению рисками

кибербезопасности. Новые правила SEC направлены на содержательное взаимодействие высшего руководства и совета директоров.

Среди прочего, предлагаемое правило разъясняет требования к раскрытию информации, связанные с политиками и процедурами владельца регистрации по выявлению и управлению рисками кибербезопасности, структурой управления кибербезопасностью, ролью руководства в устранении и снижении рисков кибербезопасности, а также тем, входит ли лицо, обладающее опытом в области кибербезопасности, в совет директоров владельца регистрации.

Эти требования подчеркивают важность продвижения усилий по управлению рисками и управлению в рамках всего совета директоров, чтобы гарантировать, что ресурсы и инвестиции применяются к тем киберрискам, которые имеют наиболее существенное финансовое, деловое и операционное влияние.

Национальная стратегия кибербезопасности основывается на работе администрации на сегодняшний день. В то время как федеральный подход к кибербезопасности развивается — и эта эволюция может привести к появлению новых стандартов — он также будет способствовать улучшению методов кибербезопасности для критически важных инфраструктурных и технологических компаний, снижая риск кибератак, которые наносят ущерб производительности, общественному доверию и, в конечном итоге, прибыли.

Со своей стороны, правительство обязано своим партнерам из частного сектора продемонстрировать ценность безопасности новых требований кибербезопасности и государственно-частного партнерства. Поскольку Стратегия требует большего от частного сектора, она берет на себя смелые обязательства от имени правительства. Он предусматривает широкомасштабное судебное давление для борьбы с вредоносной киберактивностью — от международной координации программ-вымогателей и агрессивного преследования киберпреступников до срыва злонамеренных киберкампаний и уничтожения инфраструктуры злоумышленников.

Правительство уже делает многое из этого — ранее в этом году ФБР проникло в группу вымогателей Hive, захватило ключи дешифрования и раздало их

жертвам. В апреле ФБР и его международные партнеры закрыли Genesis, интернет-магазин взломанных и украденных данных. Вместе эти действия демонстрируют, как правительство может использовать свои уникальные ресурсы и полномочия для снижения риска для своих партнеров и общества.

Кроме того, поскольку правительство создает новые стандарты для частного сектора, оно должно обеспечить гармонизацию любых дополнительных нагрузок на всех уровнях государственного управления. Затраты на соответствие требованиям не должны умалять инвестиций в безопасность. Стратегия обязуется гармонизировать правила через Управление национального кибер-директора и Управление управления и бюджета, подобно тому, как Совет по отчетности о кибер-инцидентах в DHS работает над устранением противоречий различных требований к отчетности о кибер-инцидентах. Однако эти усилия по гармонизации преодолевают сложности регулирующих органов независимых агентств.

Наконец, правительство должно разработать основу для лучшей оценки взаимозависимостей между владельцами и операторами критически важной инфраструктуры и потенциальных каскадных последствий киберинцидентов. Надежная основа для такого анализа будет способствовать стратегическим инвестициям в безопасность и повышению отказоустойчивости. Агентство кибербезопасности и безопасности инфраструктуры (CISA) как раз занимается этим.

Работать умнее

Экосистема кибербезопасности (люди, процессы, технологии) в значительной степени сосредоточена на устранении угроз технического уровня, используемых для снижения риска. Хотя экосистема кибербезопасности продолжает развиваться, ей по-прежнему не хватает возможности контекстуализировать киберугрозы и инциденты для бизнеса, операционных и финансовых рисков. На «существенное» определение влияет влияние инцидента на бизнес, операции и финансовое положение компании.

Ниже приводится перечень типов деловых и финансовых факторов, которые следует учитывать при определении существенности инцидента. Типы затрат и

неблагоприятных последствий, которые компании могут понести или испытать в результате инцидента кибербезопасности, включают следующее:

• Затраты из-за приостановки деятельности, сокращения производства и задержек с выпуском продукции.

• Платежи для удовлетворения требований о выкупе и других вымогательствах.

• Затраты на восстановление, такие как ответственность за украденные активы или информацию, устранение повреждений системы и поощрения клиентов или деловых партнеров в попытке сохранить отношения после атаки.

• Увеличение затрат на защиту от кибербезопасности, которые могут включать увеличение страховых взносов и затрат на проведение организационных изменений, развертывание дополнительного персонала и технологий защиты, обучение сотрудников и привлечение сторонних экспертов и консультантов.

• Потеря доходов в результате кражи интеллектуальной собственности и несанкционированного использования конфиденциальной информации или невозможности удержать или привлечь клиентов после атаки.

• Судебные и юридические риски, включая регулятивные действия со стороны государственных и федеральных органов власти, а также органов власти за пределами США.

• Ущерб сотрудникам и клиентам, нарушение законов о конфиденциальности и ущерб репутации, отрицательно влияющий на доверие клиентов или инвесторов.

• Ущерб конкурентоспособности компании, курсу акций и долгосрочной акционерной стоимости.

Управление киберрисками — это командный вид спорта, который требует, чтобы все предприятие обеспечивало устойчивость бизнеса. Что требуется, так это более инклюзивное сообщение и сотрудничество, в котором участвуют все лидеры управления рисками предприятия.

Технологии быстро меняются, как и киберугрозы. Статический анализ сегодняшних рисков менее полезен, чем организация регулярного потока информации для совета директоров, который поддерживает решения об

инвестициях в кибербезопасность на основе деловых, операционных и финансовых соображений. Поскольку совет директоров регулярно следит за кибербезопасностью как за аспектом рутинного управления, директора будут готовы соответствовать новым требованиям SEC.

Киберриск — это дискуссия для директоров и должностных лиц

Крис Хетнер, бывший старший советник по кибербезопасности председателя Комиссии по ценным бумагам и биржам США и председатель Центра повышения квалификации советов директоров Nasdaq, говорит: «Для советов директоров крайне важно постоянно включать обсуждения по управлению киберрисками, связанные с наиболее эффективным способом сокращения финансовых и деловых воздействие, связанное с кибер-риском. Разговор ведется не только о директоре по информационным технологиям (CIO) и директоре по информационной безопасности (CISO). Это более широкое обсуждение на высшем уровне, которое должны вести финансовый директор (CFO) и главный юрисконсульт».

Хетнер говорит, что советы больше не могут игнорировать кибербезопасность, отмечая: «По умолчанию руководители склонны полагаться на периодические тактические и технические отчеты для обоснования технических решений, которые могут решить проблемы с технической безопасностью». Он добавляет: «Слишком часто кибербезопасность теряется при переводе, когда речь идет о членах совета директоров и высшем руководстве. Это оставляет руководство неуверенным в том, что именно они финансируют и где остаются остаточные пробелы».

Hetner и NACD недавно поддержали запуск службы, в рамках которой советы директоров получают поддержку для более эффективного осуществления надзора, связанного с подверженностью кибер-рискам. X -Analytics и Служба отчетности о кибер-рисках NACD — это годовая подписка, предоставляющая ежеквартальные отчеты совета директоров, в которых освещаются финансовые риски, связанные с кибер-риском организации. Платформа использует ту же аналитику, которую используют лидеры индустрии киберстрахования.

Эта новая услуга NACD способствует более широкому обсуждению в высшем руководстве вопросов, связанных с киберрисками, и помогает советам директоров участвовать в дискуссиях, выходящих за рамки технических аспектов кибербезопасности.

В заключение, инвестиции в кибербезопасность стоят денег. Недооценка инвестиций в кибербезопасность стоит дороже». ***(Eric Swalwell. Why we need business, operational and financial resilience to optimize cybersecurity // World Economic Forum (https://www.weforum.org/agenda/2023/07/why-we-need-business-operational-and-financial-resilience-to-optimize-cybersecurity/). 11.07.2023).***

***

«Апеляційний суд США в середу тимчасово заблокував план адміністрації Байдена щодо покращення кібербезпеки для громадських систем водопостачання після того, як очолювані республіканцями штати поскаржилися, що це призведе до обтяжливих витрат на малих і сільських постачальників води.

8-й окружний апеляційний суд США в Сент-Луїсі тимчасово призупинив дію плану кібербезпеки Агентства США з охорони навколишнього середовища (EPA), поки триває судовий оскарження, подане генеральними прокурорами штатів Міссурі, Арканзас і Айова.

У плані EPA, оголошеному 3 березня, який він назвав «керівництвом», що означає, що він не був зобов’язуючим, рекомендовано низку нових правил, що передбачають більшу відповідальність за безпеку водних об’єктів на державному рівні. Агентство випустило план після кількох резонансних хакерських інцидентів за останні роки.

Генеральний прокурор Арканзасу Тім Гріффін заявив у заяві в середу, що він задоволений рішенням суду та вважає, що EPA не має повноважень нав’язувати правила.

Представник Національної сільської асоціації водопостачання, яка разом із Американською асоціацією водопостачання втрутилася в судовий процес щодо

оскарження плану EPA, заявив у заяві, що вона підтримує посилену кібербезпеку, але план EPA буде надто обтяжливим для невеликих систем водопостачання.

EPA не відразу відповіло на запит про коментар.

Експерти з безпеки кажуть, що водний сектор уже давно вважався вразливим до кібератак, які могли спричинити дефіцит або небезпечно збільшити концентрацію хімікатів, які зазвичай використовуються для очищення питної води.

У березні 2019 року звільнений співробітник водного підприємства в Канзасі використовував свої старі комп'ютерні облікові дані, щоб дистанційно вимкнути системи, заявив представник адміністрації Байдена, коли було оголошено про план.

Штати під керівництвом республіканців подали позов у квітні, заявивши, що EPA не має повноважень накладати обов'язки щодо оцінки кібербезпеки на штати та місцевих постачальників води.

У позові говориться, що меморандум створює дорогі юридичні зобов'язання, хоча EPA назвало його лише вказівкою». ***(Clark Mindock. Biden administration water cybersecurity plan temporarily blocked // Reuters (https://www.reuters.com/legal/biden-administration-water-cybersecurity-plan-temporarily-blocked-2023-07-12/). 13.07.2023).***

***

«У вівторок Білий дім разом із такими компаніями, як Amazon.com Inc (AMZN.O), Alphabet Google (GOOGL.O) і Best Buy (BBY.N) оголосить про ініціативу, яка дозволить американцям ідентифікувати пристрої, які менш вразливі до кібератак.

Нова програма сертифікації та маркування підніме планку кібербезпеки розумних пристроїв, таких як холодильники, мікрохвильові печі, телевізори, системи клімат-контролю та фітнес-трекери, йдеться в заяві Білого дому.

Роздрібні торговці та виробники нанесуть на свої пристрої логотип «US Cyber Trust Mark», і програма запрацює в 2024 році.

Ініціатива розроблена для того, щоб переконатися, що «наші мережі та їх використання є більш безпечними, тому що це дуже важливо для економічної та

національної безпеки», - сказав високопоставлений чиновник адміністрації, який не побажав залишитися ім'ям.

Федеральна комісія зі зв’язку шукатиме коментарі громадськості, перш ніж розгортати програму маркування та зареєструвати національну торгову марку в Управлінні патентів і торгових марок США, повідомили в Білому домі.

Інші роздрібні продавці та виробники, які беруть участь у програмі, включають LG Electronics USA, Logitech (LOGN.S), Cisco Systems (CSCO.O) і Samsung (005930.KS).

У березні Білий дім запустив свою національну кіберстратегію, яка закликала виробників програмного забезпечення та компанії взяти на себе набагато більшу відповідальність за те, щоб їхні системи не могли бути зламані.

Це також прискорило зусилля таких відомств, як Федеральне бюро розслідувань і Міністерство оборони, щоб перешкоджати діяльності хакерів і груп програм-вимагачів у всьому світі.

Минулого тижня корпорація Майкрософт (MSFT.O) та офіційний представник США заявили, що з травня пов’язані з державою Китаю хакери таємно отримали доступ до облікових записів електронної пошти приблизно 25 організацій, у тому числі щонайменше двох урядових установ США». ***(White House partners with Amazon, Google, Best Buy to secure devices from cyberattacks // Reuters (https://www.reuters.com/technology/white-house-partners-with-amazon-google-best-buy-secure-devices-cyberattacks-2023-07-18/). 19.07.2023).***

***

«Двопартійне законодавство щодо вдосконалення заходів кібербезпеки в усіх федеральних урядах просунулося в Сенаті Сполучених Штатів.

Федеральний закон про модернізацію інформаційної безпеки від 2023 року в середу пройшов оцінку Комітету Сенату з внутрішньої безпеки та урядових справ, і тепер він буде обговорюватися законодавцями у верхній палаті.

Довгоочікуваний законопроект про реформу спрямований на покращення координації між Адміністративно-бюджетним управлінням, Агентством з

кібербезпеки та безпеки інфраструктури, Офісом національного кібердиректора, а також іншими федеральними агентствами та підрядниками.

Якщо він буде прийнятий, він також кодифікує роль федерального головного офіцера з інформаційної безпеки, який працюватиме в Офісі федерального інформаційного директора.

Законодавство надає CISA додаткові повноваження для реагування на кіберзломи у федеральних цивільних мережах, а також кодифікує аспекти виконавчого наказу президента Байдена щодо покращення кібербезпеки нації.

Голова HSGAC Гері Пітерс, штат Мічиган, і сенатор Джош Хоулі, штат Мічиган, є авторами законопроекту Сенату. Супутнє законодавство ведеться через Палату представників Джеймсом Комером, R-Ky., Джеймі Раскіном, D-Med., Головою та високопоставленим членом Комітету з нагляду та підзвітності, та Ненсі Мейс, RS.C. і Джеррі Конноллі, D-VA.

Коментуючи законопроект, сенатор Пітерс сказав: «Цей двопартійний, двопалатний законопроект модернізує федеральні стандарти кібербезпеки та забезпечить безпеку державних систем та інформації, яку вони зберігають».

Сенатор Хоулі сказав: «Мене надихає те, що Конгрес вживає двопартійних заходів для покращення та модернізації кібербезпеки федерального уряду. Оскільки кібератаки продовжують виявляти вразливість федеральних технологій, особливо з боку іноземних супротивників, таких як КПК, нам вкрай необхідно зміцнювати наші мережі кібербезпеки та захищати нашу національну безпеку». ***(John Hewitt Jones. FISMA reform bill advances in Senate // FedScoop (https://fedscoop.com/fisma-reform-bill-advances-in-senate/?utm_source=flipboard&utm_content=other). 26.07.2023).***

***

«Цього тижня Комісія з цінних паперів і бірж США (SEC) оголосила нове правило, яке вимагає від публічних компаній розкривати будь-які порушення безпеки протягом чотирьох днів.

Обмеження часу встановлюється спеціально для будь-яких порушень, які можуть вплинути на прибутки компанії. Однак затримки будуть дозволені для всього, що становить загрозу громадській або національній безпеці.

Щоб захистити інвесторів, нові правила також вимагають від публічних компаній ділитися інформацією про управління ризиками кібербезпеки та будь-яким досвідом у сфері кібербезпеки, який мають їхні керівники.

Ця зміна сталася після нещодавніх новин про те, що витік даних на шляху до встановлення у 2023 році нового рекорду: лише за перше півріччя цього року кількість жертв зросла на 153%.

Ці нові правила спрямовані на забезпечення прозорості щодо «зростаючого ризику» витоку даних і, сподіваємось, підштовхнуть компанії до посилення кіберзахисту.

До цього часу не існувало федерального закону про розкриття порушень. Закон зобов’язав повідомляти про них лише постачальників медичних послуг та деяких операторів критичної інфраструктури.

SEC зазначила, що якщо компанія «втратить фабрику через пожежу або мільйони файлів через інцидент кібербезпеки», це вплине на інвесторів.

Правило стверджує, що чотириденне вікно звітності офіційно не починається, доки компанія не підтвердить порушення як істотне. Однак генеральний прокурор США заявив, що затримку можна продовжити понад 60 днів за надзвичайних обставин, таких як «суттєвий ризик для національної або громадської безпеки».

Правило було вперше запропоновано ще в березні 2022 року, коли SEC виявила, що зростання кількості порушень корпоративної мережі та інцидентів кібербезпеки призвело до збільшення витрат для інвесторів. Це значною мірою пояснюється зростанням цифрових операцій і віддаленої роботи.

Генеральний директор Tenable Аміт Йоран, провідний діяч у сфері кібербезпеки, високо оцінив нове правило у своїй заяві:

«Протягом тривалого часу найбільші та найпотужніші компанії США розглядали кібербезпеку як те, що приємно мати, а не як те, що потрібно мати.

Тепер абсолютно ясно, що керівники компаній повинні підвищити рівень кібербезпеки в своїх організаціях».

Однак не скрізь нова вимога сприймається цілком позитивно чи впевнено. Занепокоєна тим, що хакери можуть отримати вигоду з інформації про те, як компанії керують своїми кіберризиками, комісар республіканців Хестер Пірс заявила, що це правило виходить за межі повноважень Комітету з цінних паперів і цінних паперів і «схоже, розроблене, щоб краще задовольнити потреби потенційних хакерів».

Далі в його заяві говориться, що спокуса SEC «мікрокерувати» діяльністю компанії, швидше за все, зросте після цієї останньої вимоги.

Нове правило SEC включає програми сторонніх розробників і визнає, що компанії все більше покладаються на зовнішні хмарні служби для даних і зберігання. Частково це пояснюється зростанням витрат, з якими стикаються компанії, коли мають справу з інцидентами кібербезпеки.

У новій доповіді IBM Security дослідники виявили, що компанії платять у середньому 4,5 мільйона доларів за усунення порушень. Це на 15% більше, ніж за останні три роки. І рахунки за це сплачують не підприємства, оскільки багато з цих витрат перекладаються на споживачів.

Фактично, схоже, що споживачі постраждають найбільше, якщо станеться порушення, кількість жертв кібербезпеки зросла з 62 мільйонів до 157 мільйонів тільки в першій половині цього року. Це може включати будь-що: від злому облікового запису в соціальних мережах або зламу банківської інформації.

Окрім зниження ризику для інвесторів, є надія, що також буде спостерігатися зменшення кількості споживачів, які постраждали від інцидентів, якщо рішення SEC спрацює, як очікувалося». ***(Ellis Di Cataldo. Companies Must Disclose Security Breaches Within Four Days Under New Rule // Marketing VF Ltd. (https://tech.co/news/companies-disclose-breach-4-days?utm_source=flipboard&utm_content=other). 27.07.2023).***

***

«Раніше цього місяця Білий дім оприлюднив План реалізації національної стратегії кібербезпеки, в якому викладено конкретні «ініціативи високого впливу», які федеральний уряд впроваджуватиме для досягнення своїх цілей у сфері кібербезпеки.

Огляд національного плану реалізації кібербезпеки

Ініціатива № 3.5.2 Плану впровадження має назву: «Використання Закону про неправдиві твердження для покращення кібербезпеки постачальників». Зокрема, в ініціативі йдеться про те, що Міністерство юстиції (DOJ) «розширить зусилля з виявлення, переслідування та запобігання свідомим порушенням вимог щодо кібербезпеки у федеральних контрактах і грантах».

Це частина Ініціативи цивільного кібершахрайства (CCFI), яку Міністерство юстиції запустило в жовтні 2021 року, щоб «притягнути до відповідальності юридичні чи фізичні особи, які піддають ризику інформаційні системи США, свідомо надаючи неякісні продукти чи послуги кібербезпеки, свідомо спотворюючи свою практику кібербезпеки або протоколів або свідоме порушення зобов'язань щодо моніторингу та звітування про кіберінциденти та порушення».

Примусове виконання згідно з CCFI

З моменту запуску Міністерство юстиції оголосило про кілька врегулювань згідно із Законом про неправдиві претензії (FCA). Наприклад, у березні 2022 року Міністерство юстиції оголосило, що компанія Comprehensive Health Services LLC (CHS) заплатила 930 000 доларів США за вирішення звинувачень у тому, що вона виставила Державному департаменту рахунок приблизно 485 000 доларів США за зберігання медичних записів у безпечній системі електронних медичних записів, хоча Міністерство юстиції стверджувало, що багато медичних записів фактично було збережено на внутрішньому мережевому диску, доступному для немедичного персоналу, що є прямим порушенням урядового контракту CHS.

Ініціатива також успішно заохотила інформаторів, відомих як зв'язки, порушувати справи від імені уряду щодо очевидних збоїв у сфері кібербезпеки компаніями, які отримують федеральні кошти. У справі, яка, мабуть, найбільше спостерігають у цій сфері, колишній офіцер із комплаєнсу в Aerojet Rocketdyne Inc.

порушив справу, стверджуючи, що Aerojet знала, що її програма кібербезпеки не відповідає нормам Міністерства оборони та NASA, які були частиною контрактів Aerojet з цими агентствами. Справа перейшла до розгляду в порядку спрощеного судочинства, де окружний суд відхилив клопотання Aerojet після того, як Міністерство юстиції подав заяву про зацікавленість, критикуючи аргументи Aerojet. У липні 2022 року Міністерство юстиції оголосило, що Aerojet погодилася заплатити 9 мільйонів доларів, щоб врегулювати звинувачення в угоді, яка була укладена на другий день суду.

Очікуйте більше костюмів проти кібербезпеки для інформаторів

Історично відносини були рушійною силою правозастосування згідно з FCA, зазвичай подаючи від 500 до 600 позовів від імені уряду на рік. Оскільки цивільні кіберзастосування стають все більш поширеними в новинах, а серед потенційних інформаторів зростає обізнаність, державні підрядники та постачальники медичних послуг повинні стежити за зростанням таких випадків. І незмінна увага уряду до кіберзастосування як до «ініціативи високого впливу» підкреслює потребу в тому, щоб компанії, які отримують федеральні кошти, розуміли та дотримувалися вимог кібербезпеки у відповідних нормах, контрактах і сертифікатах, наданих уряду, включаючи забезпечення будь-яких постачальників зберігання інформації від імені компаній також відповідає вимогам…» ***(Taylor Sample. Expect More Cyber-Enforcement under the False Claims Act // Bass, Berry & Sims PLC (https://www.insidethefalseclaimsact.com/cyber-enforcement-false-claims-act/). 28.07.2023).***

***

Країни ЄС та Великобританія

«Швидкість атак на ланцюг постачання програмного забезпечення дивним чином не відстає від швидкості, з якою програмне забезпечення пожирає світ. З 2019 по 2022 рік середньорічний приріст атак перевищив 700%.

На початку цього року ми навіть побачили перший офіційний випадок послідовного ланцюжкового ефекту однієї атаки на ланцюг поставок програмного забезпечення, яка безпосередньо призводить до іншої. Зловмисники використовують складніші способи зловживання екосистемами з відкритим кодом, як-от GitHub, для розміщення, здавалося б, нешкідливих файлів, імена та формати яких не викликають очевидних попереджень і спочатку очищуються більшістю антивірусних продуктів.

Однак одна річ, яка не встигає за зростаючими загрозами, це політика. Уряди в усьому світі намагаються визначити правила, які принесуть більше користі, ніж шкоди індустрії програмного забезпечення. У всьому світі існує безліч нормативних актів, але немає загальної глобальної стратегії, яка б об'єднала все це воєдино. Враховуючи, що програмне забезпечення є глобальною індустрією, існує ризик того, що незабаром ми можемо побачити низку балканізованих територій, які виробляють незрозумілу політику.

Відсутність зв'язку зі спільнотою відкритих вихідних кодів, зокрема, є великою виною цьому. З відкритим вихідним кодом, який містить 80-90% усього коду сучасних програм (з причин, зокрема підвищення продуктивності та економічності), уряди повинні подбати про захист екосистеми, яка стає все більш привабливою мішенню для зловмисних атак.

Але те, як ЄС вирішує питання відкритого коду, дуже відрізняється від того, як Великобританія чи США мають справу з ним. І саме підхід ЄС, можливо, має найбільший потенціал для шкоди екосистемі з відкритим кодом. Отже, давайте детальніше розглянемо Директиву ЄС про відповідальність за товар (PLD).

Чи справді слід притягувати до відповідальності всю комерційну діяльність, опосередковано пов'язану з відкритим кодом?

З тих чи інших причин цей вкрай необхідний діалог між ЄС і спільнотою відкритого коду, здається, не відбувся. Результатом є якась небезпечна мова в PLD, яка може означати наближення темних віків для відкритого коду – еру закритого коду, якщо хочете.

Чесно кажучи, PLD отримав похвалу за спробу встановити кращі стандарти для програмного забезпечення та спеціальні критерії для програмного забезпечення з відкритим кодом. Це слушно вимагає від постачальників і виробників програмного забезпечення всеосяжного розуміння складу свого програмного забезпечення (наприклад, використання номенклатури матеріалів програмного забезпечення).

Він йде ще далі, запитуючи можливість відкликати програмне забезпечення, уражене вразливістю. Це природно означає, що постачальникам доведеться активно керувати всім ланцюгом поставок. Більшої відповідальності для компаній, які роблять неправильний вибір, — це те, чого нам не вистачало в політиці протягом тривалого часу.

На жаль, PLD нейтралізує ці позитиви досить неоднозначною мовою, яку можна розглядати як ненавмисне націлювання на розповсюджувачів програмного забезпечення з відкритим кодом, таких як Maven Central, PyPi, npm і навіть GitHub.

На перший погляд, здається, що PLD звільняє відкрите програмне забезпечення: «Щоб не перешкоджати інноваціям або дослідженням, безкоштовне програмне забезпечення з відкритим кодом, розроблене або надане поза межами комерційної діяльності, не повинно охоплюватися цим Регламентом». Одразу найбільша проблема полягає в тому, що немає чіткого визначення того, що таке комерційна діяльність.

Текст намагається розрізнити комерційне та некомерційне використання відкритого коду: «У контексті програмного забезпечення комерційна діяльність може характеризуватися не лише стягненням ціни за продукт, але також стягненням ціни за послуги технічної підтримки, шляхом надання програмної платформи, за допомогою якої виробник монетизує інші послуги, або шляхом використання персональних даних з інших причин, ніж виключно для підвищення безпеки, сумісності або взаємодії програмного забезпечення».

Проблема полягає в тому, що якщо ви є розробником постачальника, який отримує комерційну вигоду від OSS, ви також підпадаєте під дію PLD. Далі в тексті йдеться про те, що розповсюджувачі програмного забезпечення несуть пряму

відповідальність і порушують запропоноване положення, якщо їхні проекти використовуються в комерційних цілях.

Ви можете уявити багато сценаріїв, коли, здавалося б, невинні виробники з відкритим кодом можуть потрапити в шторм. GitHub сам по собі не є «продуктом», але його компоненти використовуються в програмному забезпеченні, яке продається в комерційних цілях. Таку саму думку можна застосувати до інших сховищ, таких як Maven Central, npm, PyPi та незліченна кількість інших.

Уявіть собі, що Etsy притягують до відповідальності за те, що хтось продає прокладку головки, яку виробник автомобілів вирішив використати в якомусь божевільному проекті, що призвело до того, що прокладка вибухнула. Це смішно у світі фізичних товарів – це ще смішніше у світі програмного забезпечення.

Досить звинувачувати не тих людей, і вони можуть просто взяти під заставу

Коли у 2021 році було виявлено вразливість Log4Shell, для виправлення компонента знадобилося 24 години. Проте до цього дня 30-40% усіх завантажень продовжують бути вразливою версією. У ширшому плані ми бачимо, що у 96% випадків завантаження компонента доступна безпечніша або краща версія цього програмного забезпечення. За логікою PLD, виробник компонента – не завжди постачальник програмного забезпечення, який вирішив включити його – може нести відповідальність, що мало сенсу.

Як наслідок, існує цілком реальна ймовірність того, що багато проектів з відкритим кодом незабаром стануть недоступними в ЄС через те, що їх притягнуть до відповідальності за дії споживачів. Це не ситуація, пов’язана з GDPR, де відмова від цього законодавства означала ризик старіння вашого бізнесу; Виробники та супроводжувачі з відкритим кодом (багато з яких роблять безкоштовний внесок) можуть і будуть відмовлятися від надання своїх матеріалів у Європі, якщо вони вважають ризик більшим, ніж винагорода. Це було б катастрофічним як для ЄС, так і для екосистеми в цілому.

Звичайно, я не єдиний, хто тут б’є на сполох. Eclipse Foundation та 12 інших організацій з відкритим кодом вже подали відкритий лист до Європейської комісії

на початку цього року. У ньому вони різко попереджали про потенційно негативний вплив PLD на виражені цілі ЄС щодо інновацій, цифрового суверенітету та майбутнього процвітання.

Видалення кваліфікатора «комерційна діяльність» із винятків щодо відкритого коду як у PLD, так і в Законі про кібернетостійкість (CRA) забезпечить більшу ясність для комерційних організацій, які безкоштовно підтримують проекти з відкритим кодом, і все ще вимагатиме від компаній, які безпосередньо монетизують програмне забезпечення з відкритим кодом. відповідати політиці.

Нам потрібна краща, послідовніша активність у відкритому коді

Чи змінить Європейський парламент формулювання PLD? Її плани незрозумілі, але бездіяльність буде катастрофічною.

Поточна пропозиція виходить за межі, більш чітко визначені законодавством інших частин світу, які представили більш продумані підходи до ролі та цінності програмного забезпечення з відкритим кодом.

Наприклад, історичний підхід Великої Британії до управління ланцюгом постачання програмного забезпечення з відкритим кодом найкраще можна описати як невтішний. Але на початку цього року компанія показала багатообіцяючі пропозиції щодо відмовостійкості та безпеки програмного забезпечення від організацій. Це перший випадок, коли уряд Великої Британії настільки прозоро й ретельно визнав небезпеку поганої видимості потенційно скомпрометованих компонентів з відкритим кодом, як це видно з таких резонансних інцидентів, як атаки на SolarWinds і Kaseya, інцидент Log4Shell і нещодавні збої в NHS. IT системи.

Він справедливо закликає до «підходу всього суспільства», який вимагатиме не лише уряду, а й участі керівників C-Suite, розробників і постачальників програмного забезпечення, а також тих, хто його закуповує та використовує. Як виглядатиме остаточний запропонований закон, залишається незрозумілим, але слід похвалити уряд Великобританії за початок цього діалогу. Набагато важче виправити політику після того, як речі вже запущені.

США так само запустили власну національну стратегію кібербезпеки, яка звернулася за вказівками до представників галузі, включно з моєю. Eclipse Foundation та Internet Systems Consortium у своєму листі до Європейського парламенту щодо PLD рекомендували розглядати конкретні та директивні вказівки США як орієнтир. Зокрема, підкреслюється, що «відповідальність має бути покладена на зацікавлені сторони, які найбільше здатні вжити заходів для запобігання поганим результатам, а не… на розробника з відкритим кодом компонента, інтегрованого в комерційний проект».

Політика щодо відкритого коду має бути не просто конкретною та чіткою. Це має бути послідовним у всьому світі, якщо ми хочемо уникнути плутанини, яка відлякує людей від внеску у відкриту екосистему, яка принесла інновації та ефективність у стільки частин світу програмного забезпечення.

Є надія, що спільнота з відкритим кодом зможе об'єднатися для досягнення суттєвих змін. На цьогорічному KubeCon + CloudNativeCon голова Linux Foundation Europe Габріель Колумбро закликав спільноту «виправити недоліки в запланованому ЄС Законі про кібервідбійність». З більшою кількістю заходів, таких як KubeCon, які демонструють зростання та вплив відкритого коду, ми повинні використовувати ці події як платформи для мотивації та прямого спілкування з спільнотою відкритого коду щодо критичних тем, таких як PLD.

Можна лише припустити, що PLD стимулює ще більше усвідомлення необхідності змін». ***(Brian Fox. The EU's Product Liability Directive could kill open source // Future US, Inc. (https://www.techradar.com/pro/the-eus-product-liability-directive-could-kill-open-source?utm_source=flipboard&utm_content=other). 10.07.2023).***

***

«Сегодня было опубликовано открытое письмо, подписанное ведущими экспертами по кибербезопасности по всей стране, в котором подчеркиваются «тревожные недоразумения и заблуждения» вокруг законопроекта о безопасности в Интернете.

Положение законопроекта о безопасности в Интернете о сканировании сообщений, которыми обмениваются через такие приложения, как WhatsApp и Signal, находится в центре интенсивных дебатов из-за его потенциального крупномасштабного воздействия на права человека. Ученые из Национального исследовательского центра Великобритании по вопросам конфиденциальности, снижения вреда и враждебного влияния в Интернете (REPHRAIN) призвали правительство и парламент изучить независимую научную оценку инструментов, предложенных для проведения такого сканирования в рамках правительственного фонда Safety Tech Challenge Fund.

Благодаря сквозному шифрованию (E2EE) никакие третьи стороны, включая поставщиков услуг, таких как WhatsApp и Signal, не могут читать сообщения, когда они перемещаются между отправителем и получателем.

Оценка пришла к выводу, что, хотя ни один из инструментов не предлагает ослабить или взломать протокол E2EE, с точки зрения прав человека, конфиденциальность сообщений пользователей службы E2EE не может быть гарантирована, когда весь контент, предназначенный для отправки в частном порядке в рамках службы E2EE, отслеживается. предварительное шифрование.

Министр внутренних дел в статье для The Telegraph на прошлой неделе отметил, что программа «продемонстрировала, что технически возможно выявлять сексуальное насилие над детьми в средах, использующих шифрование».

«Проблема в том, что обсуждаемая технология не подходит в качестве решения», — сказал Авайс Рашид, профессор кибербезопасности Бристольского университета и директор центра REPHRAIN, который работал над разработкой автоматизированных инструментов для обнаружения материалов о жестоком обращении с детьми в Интернете. а также внедрение конфиденциальности в программные системы в течение 15 лет.

«Наша оценка показывает, что рассматриваемые решения будут нарушать конфиденциальность в целом и не имеют встроенных средств защиты, чтобы предотвратить перепрофилирование таких технологий для мониторинга любых личных сообщений.

«Нет также никаких механизмов обеспечения прозрачности и подотчетности того, кто будет получать эти данные и для каких целей они будут использоваться.

«Парламент должен учитывать независимые научные данные по этому поводу. В противном случае законопроект о безопасности в Интернете рискует предоставить карт-бланш для мониторинга личных сообщений и возможности для беспрепятственного наблюдения в общественном масштабе».

Оценка также показала, что большие проблемы связаны с отсутствием задокументированных, этически ответственных эталонных наборов данных для разработки и оценки таких инструментов, а также с отсутствием подробной экспериментальной информации из-за проприетарного характера таких инструментов.

Доктор Клаудия Пирсман, научный сотрудник Бристольского университета и Центра REPHRAIN, которая руководила оценкой, сказала: «Группа оценки REPHRAIN, состоящая из экспертов в области онлайн-защиты детей, конфиденциальности и безопасности, технологий искусственного интеллекта и прав человека, решительно поддерживает разработку автоматизированных инструментов для борьбы с сексуальным насилием и эксплуатацией детей в Интернете. Мы сотрудничаем с правоохранительными органами по всему миру уже более 10 лет, разрабатывая новые решения для поддержки их онлайн-расследований по защите детей в нечастных онлайн-средах, таких как одноранговые сети и социальные сети; и автономный анализ изъятого оборудования подозреваемых.

«Однако наша недавняя оценка инструментов, финансируемых Фондом Safety Tech Challenge Fund, показала, что установление справедливого баланса между правами законопослушных пользователей, потенциальных жертв CSAM и предполагаемых преступников становится ключевой проблемой, когда такие инструменты используются в контексте крупномасштабного мониторинга личных сообщений людей в средах сквозного шифрования.

«Научные дебаты только начинаются о том, как принципы ответственного и этичного ИИ, такие как последствия для прав человека, безопасность,

объяснимость, прозрачность, непредвзятость, подотчетность и спорность, должны быть реализованы в очень чувствительной и важной области, такой как защита детей в Интернете. Например, ни один из существующих инструментов обнаружения CSAM в настоящее время не может обнаруживать жертв всех этнических, возрастных и гендерных групп из-за отсутствия разнообразия в текущих обучающих наборах данных. Поэтому мы утверждаем, что необходимо разработать согласованный международный стандарт для эталонных наборов данных и оценки инструментов CSAM, учитывающий такие принципы и разделяемый организациями по защите детей, частным сектором и исследователями, тем самым защищая всех детей и законопослушных пользователей». ***(Online Safety Bill undermines privacy online, say UK's top cyber security experts // University of Bristol (https://www.bristol.ac.uk/news/2023/july/online-safety-bill.html). 05.07.2023).***

***

«Принаймні останній рік інфляція та загроза рецесії витали в повітрі. Зростання для бізнесу було делікатним актом, і це вдвічі вірно для правильної стратегії кібербезпеки. Кіберзлочинність зростає. Згідно з опитуванням уряду Великої Британії щодо порушень кібербезпеки за 2023 рік, понад чверть компаній зізналися, що зазнавали кібератак за останні 12 місяців, причому цей показник значно вищий для середнього бізнесу (59%) і великих компаній (69%). Сукупний вплив цієї підвищеної загрози та економічної невизначеності спричиняє відчутні відмінності на ринку кібербезпеки, а отже, і в тому, як компанії борються з кіберзлочинністю. Ось чому все більше організацій обирають макроплатформи, щоб захистити себе від кіберзлочинців, замість того, щоб шукати очікувані найкращі у своєму класі рішення. Давайте більш детально розглянемо, чому ці платформи стали популярними серед бізнесу.

Оптимізація витрат означає, що маятник рухається в бік платформ безпеки

Узагальнюючи, макротенденція, яку ми спостерігали на ринку кібербезпеки, полягає в тому, що підприємства коливаються між двома різними стратегіями кібербезпеки. З одного боку, найкращі у своєму класі платформи займаються певними сферами кібербезпеки. Хоча вони можуть бути ефективними, вони також можуть мати ускладнюючий ефект, оскільки організаціям потрібно закуповувати, інтегрувати та вимірювати численні рішення для створення надійного захисту від кіберзлочинців. Це, у свою чергу, виявляється трудомістким і дорогим завданням.

Натомість, перед обличчям збільшення попиту на оптимізацію витрат, CISO відчувають тиск, змушуючи робити більше з меншими витратами. Таким чином, платформи пропонують набір рішень від однієї компанії, які обслуговують різні операції кіберзахисту. Вибір набору інструментів може запропонувати ефективний комплексний захист від кіберзагроз і забезпечити бюджетні обмеження за рахунок багаторічної оптимізації витрат; значно скорочуючи витрати в довгостроковій перспективі. Пізніше це можна доповнити додатковими найкращими у своєму класі рішеннями для задоволення будь-яких подальших вимог.

Є ще одна важлива причина, чому простіші, легкі в інтеграції та економічно ефективні рішення можуть найкраще працювати для CISO та спеціалістів з кібербезпеки. Керівники та члени правління відчувають відчутне виснаження, коли справа доходить до кібербезпеки. Перш за все вони хочуть розірвати нескінченний цикл придбання нового рішення, його інтеграції та заміни або оновлення лише через кілька років. Що зумовлює це?

Оцінка ризику на основі інтерв'ю більше не працює. що далі

Стандартна «оцінка ризиків на основі інтерв'ю», яка часто використовується для оцінки готовності бізнесу до кібербезпеки, більше не підходить для цілей. Священний Грааль кібербезпеки полягає у створенні автоматизованих системних оцінок зрілості в режимі реального часу, які завершують виснажливий цикл інвестування та оновлення. Але наразі надзвичайно важко точно визначити, які інструменти було використано, наскільки вони ефективні та чи виправдовує їхня ефективність вартість. Отже, компанії знаходять гіперпостачальників, а

макроплатформи пропонують найчіткіший шлях для досягнення цієї мети в короткостроковій перспективі.

Ось у чому полягає головоломка: як підприємства можуть переконатися, що вони використовують правильні інструменти та вимірювання, щоб підвищити свою безпеку таким чином, щоб резонувати з правлінням? Досягнення такого виду видимості звітності не є універсальною пропозицією, і в кінцевому підсумку CISO повинні шукати партнерства з експертами, здатними спиратися на ширший галузевий контекст і пристосовуватись до їхніх потреб та історії.

Автоматизація відіграє ключову роль

Першим кроком до представлення планів правлінню та вибору платформи є створення видимості, звітування та системне оцінювання. Нестача кваліфікації може бути предметом занепокоєння, який багато обговорюється, але автоматизація може допомогти пом'якшити проблему, особливо в періоди скорочення бюджету, коли звільнення є звичайним явищем. По-друге, автоматизація може звільнити команди з кібербезпеки від обов'язкових трудомістких повторюваних завдань, водночас масштабуючи зусилля бізнесу щодо безпеки. У поєднанні зі штучним інтелектом і машинним навчанням (ML) він також може відігравати важливу роль у розробці планів кіберстійкості. У результаті автоматизація може ще більше посилити стратегію кібербезпеки компанії, зробивши її набагато гнучкішою та гнучкою. Після того, як видимість буде встановлено, належний досвід може встановити зв'язки між точками даних, щоб пов'язати кібербезпеку з бізнес-результатами та KPI, які ради можуть переварити.

Ефективна стратегія кібербезпеки починається з вас

Зрозуміло, що нещодавня економічна невизначеність спричинила консолідацію на ринку. CISO, які перебувають під фінансовим тиском, змушені робити більше з меншими витратами, а перехід на макроплатформи забезпечує життєво важливу економію бюджету завдяки багаторічній оптимізації витрат, забезпечуючи при цьому високі стандарти захисту.

Першим кроком до вибору макроплатформи, яка задовольняє як кібернетичні потреби, так і потреби економії коштів, є створення видимості. Лише встановивши

правильні вимірювання та ключові показники ефективності, CISO можуть успішно представити кіберінвестиції в термінах, зрозумілих правлінню, наприклад, їх зв’язок із доходом і корпоративною репутацією.

Автоматизація відіграє центральну роль. Це не тільки може допомогти командам робити більше з меншими витратами, але також може покращити здатність команди вимірювати позитивні результати та витонченість відповідей на загрози. Разом з поглибленою співпрацею з експертами в екосистемі кібербезпеки, які можуть допомогти орієнтуватися в змінах, надати контекст і визначити нових постачальників для інтеграції в їх інфраструктуру кібербезпеки. Це перший крок до більш цілісного та чіткішого погляду на кібербезпеку, який допоможе CISO заощадити витрати, а також задовольнити потреби організації в безпеці». ***(Tony Buffomante. We’re spending too much on cybersecurity // Future US, Inc. (https://www.techradar.com/pro/were-spending-too-much-on-cybersecurity?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 26.07.2023).***

***

«Близько 64% болгар вважають, що вони не поінформовані про проблеми кібербезпеки, показує перше національно-репрезентативне дослідження кібербезпеки в країні, проведене Дослідницьким центром Trend. Результати представила співзасновник Trend Евеліна Славкова в Національному прес-клубі ВТА у Софії у вівторок.

Близько 42% оцінили себе як дещо не поінформовані, а 22% – як зовсім не поінформовані. Близько 30% вважають себе обізнаними і 3% не оцінили свої знання з цього питання.

Дослідження проводилося на замовлення Союзу приватного економічного підприємництва.

Близько 21% сказали, що користуються Інтернетом майже весь день, 40% кілька разів на день, 14% один раз на день, а 14% сказали, що ніколи не

користуються Інтернетом. Трохи більше 50% заявили, що вони почуваються в безпеці, коли користуються Інтернетом, і близько 38% не впевнені.

Загалом 5% сказали, що вони стали жертвами кіберзлочинців, тоді як 88% відповіли негативно. Приблизно 41% поділилися особистою інформацією в Інтернеті, а 54% – ні. 53% витратили б час і зусилля, щоб покращити свою обізнаність у питанні. 48% респондентів висловили переконання, що батьки несуть найбільшу відповідальність за безпеку дітей у кіберпросторі.

На думку 25% респондентів, краща освіта та обізнаність громадян покращить запобігання кіберзлочинності в Болгарії. 39% висловили переконання, що рішенням є суворі закони та ефективне застосування санкцій, 12% зазначили, що існує потреба у збільшенні інвестицій у кібербезпеку на національному рівні, а 13% стверджували, що існує потреба у покращенні співпраці між установами, бізнесом. і суспільство.

«Ми живемо в дуже дивний час, коли скрізь панує небезпека, і ми змушені говорити про енергетичну та продовольчу безпеку, але зараз також дуже серйозно про кібербезпеку», – зазначив голова Союзу приватного економічного підприємництва Кузман Ілієв. Він додав, що більшість болгар не знають про установи, які борються з кіберзлочинністю.

Величезна кількість громадян так чи інакше стають жертвами кіберзлочинності, зазначив уповноважений Володимир Дімітров, начальник відділу боротьби з кіберзлочинністю ГУБОЗ. За його словами, значна частина громадян стають жертвами цього виду злочину через брак інформації або необізнаність. За його словами, щодня надходить близько 30 повідомлень про кіберзлочини». ***(Momchil Rusev. 4% of Bulgarians Feel Uninformed about Cyber Security Issues - Trend Poll // Bulgarian News Agency (https://www.bta.bg/en/news/bulgaria/496088-some-64-of-bulgarians-feel-uninformed-about-cyber-security-issues-trend-resea). 25.07.2023).***

***

«Прагнучи підвищити безпеку цифрових продуктів, таких як смарт-телевізори, домашні камери, підключені іграшки та розумні холодильники, перш ніж вони вийдуть на ринок, представники країн-членів ЄС погодили спільну позицію щодо запропонованого Закону про захист від кібернетичної інформації. Це законодавство встановлює широкі вимоги до кібербезпеки для продуктів із цифровими компонентами.

Державний секретар з цифровізації та штучного інтелекту Кармe Артігас Бругал привітав цю подію як важливу віху в просуванні зобов'язань ЄС щодо безпечного єдиного цифрового ринку. Вона підкреслила необхідність того, щоб IoT та інші підключені пристрої відповідали основним стандартам кібербезпеки, пропонуючи тим самим ефективний захист для компаній і споживачів від кіберзагроз.

Цей проект розпорядження встановлює обов'язкові вимоги кібербезпеки для проектування, розробки та виробництва апаратних і програмних продуктів. Мета полягає в тому, щоб запобігти будь-яким дублюванням вимог, які можуть виникнути через різне законодавство в країнах-членах ЄС. Він широко застосовуватиметься до будь-яких продуктів, які прямо чи опосередковано підключаються до іншого пристрою чи мережі, за деякими винятками для продуктів, на які вже діють чинні правила ЄС, як-от медичні пристрої, авіація чи автомобілі.

Відповідно до початкової пропозиції Комісії, спільна позиція Ради підкреслює важливість відповідальності виробника у забезпеченні відповідності продукції вимогам безпеки. Він також підкреслює необхідність прозорості функцій безпеки апаратних і програмних продуктів і встановлює систему нагляду за ринком для забезпечення дотримання правил.

Проте Рада запропонувала кілька поправок, зокрема зміни зобов'язань щодо звітування про вразливості чи інциденти та положення щодо визначення терміну служби продукту виробниками. Також запропоновано додаткові заходи підтримки малих та мікропідприємств та спрощену декларацію про відповідність.

Після узгодження спільної позиції Ради Іспанія розпочне переговори з Європейським парламентом щодо остаточної версії запропонованого законодавства.

Цей Закон про захист від кібербезпеки знаменує собою ключовий крок на шляху ЄС до всебічної кібербезпеки. Раніше Рада підкреслювала важливість такого законодавства у своїх висновках щодо кібербезпеки підключених пристроїв у грудні 2020 року, і Закон доповнює існуючу систему кібербезпеки ЄС, яка включає Директиву про безпеку мережевих та інформаційних систем». ***(Директива NIS) та Акт ЄС про кібербезпеку. (EU Agrees on Common Position for Cyber Resilience Act to Enhance Security of Digital Products // ISBuzz Pty Ltd (https://informationsecuritybuzz.com/eu-agrees-on-common-position-for-cyber-resilience-act-to-enhance-security-of-digital-products/). 25.07.2023).***

***

Австралія та Нова Зеландія

«… Збільшення кібератак в Австралії продовжується в 2023 році, і це може бути з кількох причин, зокрема:

збільшення залежності бізнесу від нових технологій, що робить можливості для атак більш імовірними;

фінансова мотивація кіберзлочинців;

підвищена доступність інструментів і ресурсів для здійснення успішних атак;

невиправлені вразливості в програмному забезпеченні та системах;

людські помилки та недостатня обізнаність щодо кібербезпеки;

ландшафт загроз, що швидко розвивається, за допомогою якого кіберзлочинці знаходять нові способи використання існуючих вразливостей або обходу нових заходів безпеки.

Важко сказати, чи сталося більше інцидентів з даними, чи загрозливі суб’єкти просто вдосконалюються в тому, що вони роблять, і, можливо, справжня відповідь лежить десь посередині.

Усунення ризиків і поширеності кібератак і інцидентів з даними вимагає багатостороннього підходу, що включає надійні заходи кібербезпеки, безперервну освіту та обізнаність на особистому та організаційному рівнях, вдосконалення практик розробки програмного забезпечення в приватному секторі та спільнотах із відкритим кодом, а також поглиблену співпрацю та співробітництво між державним і приватним секторами, як на внутрішньому, так і на міжнародному рівнях.

Що змінюється з обізнаністю про кібербезпеку в Австралії?

Останніми роками уряд Австралії та різні організації вжили значних заходів для підвищення обізнаності та освіти з кібербезпеки по всій країні.

Деякі помітні зміни включають:

Австралійський центр кібербезпеки, заснований у 2014 році, є ініціативою уряду Співдружності, який є центральним центром інформації, порад і вказівок щодо кібербезпеки в Австралії.

У жовтні 2022 року Австралійський інститут директорів компаній і Спільний дослідницький центр кібербезпеки запустили Принципи управління кібербезпекою. Принципи пропонують основу для допомоги директорам австралійських компаній у нагляді за ризиками кібербезпеки та взаємодії з керівництвом.

Австралійська стратегія кібербезпеки на 2023-2030 рр., яка є планом посилення можливостей країни в галузі кібербезпеки, посилення захисту критичної інфраструктури та сприяння міжнародній співпраці.

Уряд Австралії створив Національне управління кібербезпеки, а з 3 липня 2023 року призначив маршала авіації Даррена Голді AM CSC першим національним координатором Австралії з кібербезпеки. Координатор керуватиме національною політикою кібербезпеки, координацією реагування на великі кіберінциденти, загальнодержавними зусиллями з підготовки до кіберінцидентів і зміцненням потенціалу Співдружності у сфері кібербезпеки.

Очікування спільноти також змінюються, і з огляду на частіші випадки кіберзлочинності жертви очікують, що державні та приватні організації візьмуть на себе більшу відповідальність за безпечний збір та обробку особистої інформації.

Крім того, власники пропонують більш ефективне та краще сповіщення у випадку порушення даних, що впливає на ці особисті дані.

Як змінюються зобов'язання щодо дотримання нормативних вимог для компаній?

Зобов’язання щодо регулювання та відповідності зростають. Лише за останні роки було запроваджено низку схем сповіщення про порушення даних, зокрема на рівні федерального уряду в Австралії, але це також відбувається в усьому світі.

Деякі з австралійських схем сповіщення включають:

Схема витоку даних, що підлягає сповіщенню, положення про сповіщення в частині Закону про корпорації 2001 (Cth), яка вимагає від власників ліцензії на фінансові послуги Австралії повідомляти ASIC про порушення або невиконання своїх ліцензійних зобов’язань; і (Cth) відповідальні суб’єкти активів критичної інфраструктури зобов’язані Відповідно до Закону про безпеку критичної інфраструктури від 2018 року повідомляти про інциденти кібербезпеки в Австралійський центр кібербезпеки (ACSC) протягом 12 годин про інциденти зі «значним впливом» і протягом 72 годин про всі інші інциденти. Деякі відповідальні організації також зобов’язані створити, підтримувати та дотримуватися Програми управління ризиками критичної інфраструктури для кожного зі своїх активів критичної інфраструктури.

Чи застосовуються зобов’язання щодо відповідності на міжнародному рівні?

За межами Австралії також існують подібні схеми повідомлень про порушення даних, кібербезпеки або критичної інфраструктури. Якщо ваша організація працює за межами Австралії, під час оцінки сповіщень про відповідність вам потрібно враховувати кілька схем». ***(Steven Hunwicks. Cyber attacks, governance and compliance // HopgoodGanim Lawyers (https://www.hopgoodganim.com.au/page/knowledge-centre/blog/cyber-attacks-governance-and-compliance). 11.07.2023).***

***

«Нова Зеландія засновує нове агентство для посилення готовності до кібербезпеки та реагування, а також полегшення людей і організацій для отримання допомоги.

Загрози кібербезпеці, з якими стикається Нова Зеландія, стають все більш масштабними та складними, тому Новозеландська група реагування на надзвичайні ситуації з комп'ютерами (CERT NZ) співпрацюватиме з Національним центром кібербезпеки (NCSC).

Наявність єдиного агентства для надання авторитетних порад і реагування на інциденти з усіма рівнями загрози є найкращою міжнародною практикою, яка забезпечить Новій Зеландії хороші можливості для використання можливостей цифрової економіки та надання безпечних державних послуг для Ківі.

З 2018 року уряд інвестував 94 мільйони доларів у покращення можливостей кібербезпеки. Ми постачаємо провідні у світі продукти захисту, такі як мережі без зловмисного програмного забезпечення для захисту постачальників послуг Інтернету та приватних мереж.

Але є ще багато чого зробити, оскільки в першому кварталі року CERT NZ було повідомлено про 5,8 мільйона доларів прямих фінансових збитків від кіберінцидентів. За весь минулий рік NCSC запобігла збитку економіці на 33 мільйони доларів.

Створення спеціального нового провідного операційного агентства гарантує, що Aotearoa має найкращі можливості для боротьби з хакерами, які, як ми знаємо, завдають реальної шкоди людям і економіці.

Оперативна інтеграція CERT NZ в NCSC почнеться 31 серпня і відбуватиметься поетапно протягом кількох років. Тимчасово всі поточні послуги будуть підтримуватися.

Незалежний консультативний комітет з кібербезпеки (CSAC), створений у грудні 2021 року, рекомендував створити єдину точку входу для реагування на інциденти кібербезпеки для перевірки стійкості Нової Зеландії до кіберзагроз.

Провідна оперативна агенція з кібербезпеки включатиме функції консультування та реагування, які зараз надаються громадськості та підприємствам

CERT NZ, а також підтримку, яку надає NCSC для організацій, що мають національне значення.

Відбувається процес передачі персоналу, обов'язків і фінансування CERT NZ до NCSC. Інтегроване агентство розгляне, як воно може краще використовувати свій розширений діапазон і масштаб, щоб розробити вдосконалену модель роботи, яка набуде чинності в 2024 році.

CERT NZ було створено в 2017 році як громадське агентство з кібербезпеки для уряду, щоб підтримувати широкий спектр підприємств, організацій і окремих осіб, які постраждали або можуть постраждати від інцидентів кібербезпеки». ***(Kip Brook. NZ strengthening cyber security // Make Lemonade NZ (https://www.makelemonade.nz/2023/07/27/nz-strengthening-cyber-security/?utm_source=flipboard&utm_content=other). 27.07.2023).***

***

Китай

«Зіштовхнувшись із постійно зростаючими складними ризиками та викликами національній безпеці як усередині країни, так і на міжнародній арені, вище керівництво Китаю проаналізувало роботу з кібербезпеки за останні п'ять років, наголошуючи на дотриманні кількох принципів, таких як керівництво партією у справах кіберпростору та посилення спроможності до забезпечити кібербезпеку країни, що, на думку експертів, надає чітку дорожню карту для посилення сили Китаю в кіберпросторі, коли він став головним полем битви для суперництва між великими державами.

Голова Китаю Сі Цзіньпін наголосив на необхідності ретельного виконання важливих вказівок ЦК Комуністичної партії Китаю (КПК) щодо зміцнення сили Китаю в кіберпросторі, а також енергійного просування високоякісного розвитку роботи з кібербезпеки та інформатизації, Сіньхуа Інформаційне агентство повідомляє в суботу.

Сі, також генеральний секретар ЦК КПК і голова Центральної військової комісії, зробив зауваження в нещодавній інструкції з кібербезпеки та роботи з інформатизації.

Сі сказав, що важлива роль роботи з кібербезпеки та інформатизації стає дедалі помітнішою в нову епоху, наголосивши на дотриманні кількох принципів, включаючи партію, що керує справами кіберпростору, розвиває справи кіберпростору для людей і йде шляхом управління Інтернетом разом з Китаєм. характеристики.

Він також підкреслив необхідність координації розвитку та безпеки, зміцнення спроможності забезпечувати кібербезпеку країни та сприяти побудові спільноти спільного майбутнього в кіберпросторі.

З п'ятниці по суботу в Пекіні проходила національна нарада з питань роботи з кібербезпеки та інформатизації. Деякі ЗМІ відзначили, що це була друга загальнонаціональна робоча зустріч з кібербезпеки та інформатизації протягом п’яти років після першої, що відбулася у квітні 2018 року, на якій були сформульовані стратегічні домовленості для роботи в нову еру.

Основним моментом останньої зустрічі є те, що вона висунула «дотримання кількох принципів», які допоможуть сформувати більш комплексні теоретичні вказівки щодо того, як посилити силу країни в кіберпросторі на основі досвіду, накопиченого за останні десятиліття, і роз’яснити деякі конкретні вимоги. для подальшої роботи відповідно до звіту на 20-му національному з’їзді КПК, в якому зазначено, що кібербезпека є ключовим напрямком системи національної безпеки, відзначили експерти.

Комплексні ризики

Висвітлюючи дводенну зустріч, деякі західні ЗМІ зосередилися на заклику вищого лідера Китаю «побудувати міцний бар’єр безпеки» навколо Інтернету країни, наголошуючи на пріоритеті забезпечення безпеки з концепцією охоплення як традиційних, так і нетрадиційних сфер.

«Кібербезпека — це не лише безпека кіберкомунікацій, але й безпека даних, на додаток до високого рівня залежності від цифрових технологій, які можуть

принести більше потенційних ризиків», — Тан Лан, директор Центру безпеки та управління кіберпростором. Дослідження в Китайських інститутах сучасних міжнародних відносин, повідомляє Global Times у неділю.

Наразі кіберпростір став основним полем бою для суперництва між великими державами, включаючи кібератаки проти кіберзахисту, технічні стандарти та технічний контроль, які роблять проблеми кібербезпеки більш складними та помітними, сказав Тан.

Хоча багато критично важливих інфраструктур, таких як високошвидкісна залізниця та фінансові транзакції, залежать від цифрових технологій та інформатизації, важливість безпеки мережі та даних була поставлена в центр уваги, особливо коли нові технології, такі як штучний інтелект, принесли нові виклики кібербезпеці, сказали експерти.

Після 18-го Національного з'їзду КПК у 2012 році Китай прискорив свої зусилля щодо підвищення самозабезпеченості та посилення науково-технічної діяльності, одночасно зміцнюючи законодавче управління кіберпростором, сказав Сі Цзіньпін, додавши, що були зроблені нові кроки у зміцненні сили Китаю в кіберпростір.

«Безпека технологій є надзвичайно важливою, оскільки китайські компанії стикаються з вузькими місцями в деяких секторах високих технологій. Наприклад, хоча ми використовуємо технології GPT з відкритим кодом, ми все ще відстаємо в деяких апаратних засобах і чіпсетах, а деякі основні технології все ще знаходяться в руках інших країни», - сказав Чжу Вей, віце-директор Дослідницького центру комунікаційного права при Китайському університеті політичних наук і права, Global Times у неділю.

Також Чжу сказав, що деякі транскордонні транзакції даних, пов'язані з критичною оборонною інфраструктурою та засобами існування людей, є важливими складовими кібербезпеки та національної безпеки.

Що стосується кібербезпеки, Сі підкреслив, що «без забезпечення кібербезпеки ми не можемо захистити національну безпеку; без сприяння застосуванню IT ми не можемо реалізувати модернізацію».

«На міжнародній арені, оскільки ми зараз бачимо кібератаки в російсько-українських конфліктах, а також з боку США і НАТО, Китай може стати головною ціллю кібератак США, оскільки він вважає нас «кіберзагрозою» №1», Тан сказав, зазначивши, що ці геополітичні фактори створюють нові виклики для ліній кіберзахисту, особливо коли в деяких фундаментальних технологіях домінує Захід під проводом США.

Керівництво Сі

У своїй інструкції Сі сказав, що необхідно докласти рішучих зусиль для просування високоякісного розвитку заходів з кібербезпеки та інформатизації та досягти нових досягнень у зміцненні потужності Китаю в кіберпросторі, таким чином зробивши новий внесок у розбудову сучасної соціалістичної країни в усіх відношеннях і просування національного омолодження по всіх фронтах.

У вівторок у Народному видавництві була опублікована книга Сі Цзіньпіна про зміцнення Китаю в кіберпросторі, яка містить короткий виклад досвіду КПК щодо регулювання кіберпростору та керівництво для розвитку кібербезпеки та інформатизації.

Під керівництвом Сі Цзіньпіна було прийнято та втілено в життя низку важливих рішень і заходів, пов’язаних із кіберрозвитком.

Наприклад, протягом останніх кількох років було розпочато спеціальну кампанію під назвою «Операція Qinglang» для створення більш здорової інтернет-екосистеми в Китаї, під егідою якої було проведено ряд заходів.

Нещодавно найвищі органи громадської безпеки та кібербезпеки Китаю запустили кампанію боротьби з чутками в Інтернеті, починаючи з суботи по 21 липня, намагаючись створити гармонійне та чисте онлайн-середовище. Він уже покарав 373 акаунти за поширення неправдивої інформації, спрямованої на фондовий ринок Китаю та політику соціального забезпечення.

Тим часом Китай прискорив зусилля для просування кіберзаконодавства, оприлюднивши понад 140 законів про кіберпростір з 1994 року, сформувавши кіберзаконодавчу базу на основі Конституції, що підтримується законами, постановами та правилами, затвердженими традиційним законодавством і

підкріпленими спеціалізовані кіберзакони, згідно з документом під назвою «Китайське правове управління кіберпростором у нову еру», опублікованому урядом Китаю в березні.

Цай Ці, член Постійного комітету Політбюро ЦК КПК і член Секретаріату ЦК КПК, сказав під час зустрічі, що Китаю необхідно зміцнити позитивну рекламу в Інтернеті та керівництво, захищатися від мережевих ідеологічних ризики, підвищити ефективність комплексного управління мережею, сформувати здорову мережеву екологію та міцно взяти лідерство в ідеологічній роботі мережі…» ***(Xi instructs on cybersecurity work, highlights principles to boost cyberspace strength // Global Times (https://www.globaltimes.cn/page/202307/1294455.shtml). 16.07.2023).***

***

«Китай випустив рекомендації щодо сприяння здоровому розвитку сектору страхування кібербезпеки.

Керівництво було опубліковано спільно Міністерством промисловості та інформаційних технологій та Національною адміністрацією фінансового регулювання.

Як новий вид страхової послуги, страхування кібербезпеки покращить здатність підприємств справлятися з проблемами кібербезпеки, таким чином сприяючи цифровій трансформації малих і середніх підприємств країни.

Країна й надалі вдосконалюватиме допоміжні політики та нормативні акти, сприятиме застосуванню страхування кібербезпеки серед підприємств і вирощуватиме більше високоякісних страховиків кібербезпеки, йдеться в керівних принципах.

Також буде докладено зусиль для заохочення страхових компаній до розробки більш диверсифікованих типів послуг страхування кібербезпеки для задоволення різних потреб управління ризиками кібербезпеки, додається в ньому». ***(China unveils guideline on cybersecurity insurance development // China.org.cn (http://www.china.org.cn/china/2023-07/17/content_92729713.htm). 17.07.2023).***

***

«Президент Китаю Сі Цзіньпін заявив, що Китай повинен побудувати «твердий» бар'єр безпеки навколо свого Інтернету під наглядом правлячої Комуністичної партії, у своєму останньому заклику захистити онлайн-дані та інформацію.

Китай повинен наполягати на управлінні, експлуатації та забезпеченні доступу до Інтернету відповідно до закону, сказав Сі в інструкціях, переданих офіційним особам, які взяли участь у дводенній зустрічі з кібербезпеки в Пекіні, яка завершилася в суботу.

«Ми повинні дотримуватися партійного управління Інтернетом і дотримуватися (принципу) змусити Інтернет працювати на людей», — цитує слова Сі Цзіньпі державне інформаційне агентство Сіньхуа.

В останнє десятиліття Сі зробив збереження безпеки пріоритетом, і його концепція безпеки охоплює все: від політики та економіки до навколишнього середовища та кіберпростору.

У 2015 році Китай прийняв закон про національну безпеку з ширшою сферою дії, включаючи його кіберпростір. Через рік був прийнятий закон, який містив вимоги щодо перевірки безпеки та зберігання даних на серверах у Китаї.

У 2021 році Китай запровадив правила щодо так званої критичної інформаційної інфраструктури.

Цього року законодавці оновили антишпигунське законодавство, заборонивши передачу інформації, пов'язаної з національною безпекою, і розширили визначення шпигунства.

Навігація щільною мережею китайських правил і законів щодо даних та інформації в Інтернеті не без ризику для компаній.

У квітні американська консалтингова компанія Bain & Co повідомила, що поліція відвідала її офіс у Шанхаї та опитала деяких співробітників. Financial Times з посиланням на людей, поінформованих про несподіваний візит, повідомила, що поліція також вилучила комп'ютери та телефони.

Минулого року регулюючі органи наказали найбільшому китайському постачальнику фінансових даних Wind Information Co припинити надавати офшорним користувачам певні дані, повідомили Reuters тоді джерела.

У 2021 році влада розпочала розслідування щодо кібербезпеки гіганта Didi Global через два дні після того, як він став публічним у Сполучених Штатах». ***(Xi Jinping calls for 'solid' security barrier around China's internet // Reuters (https://www.reuters.com/world/china/xi-calls-solid-security-barrier-around-chinas-internet-2023-07-15/). 15.07.2023).***

***

Індія

«Постійний комітет з фінансів запропонував створити централізований і уповноважений «орган кіберзахисту», зокрема для екосистеми фінансових послуг, подібний до Генерального директорату цивільної авіації (DGCA), щоб боротися зі зростанням кількості злочинів «білих комірців» у кіберпросторі.

Комітет, очолюваний Джаянтом Сінхою, заснував свої рекомендації на основі широких обговорень з галузевими органами, корпораціями та банківськими органами. Внески надходили від Резервного банку Індії (RBI), Національної платіжної корпорації Індії (NPCI), CERT-In і приватних компаній, таких як RazorPay і Flipkart.

Комітет також рекомендував запровадити систему білих списків для цифрових кредитних агентств та інших фінансових посередників. Комітет вважає, що цей захід буде боротися з незаконною практикою та просуватиме стандартизований кодекс поведінки в секторі цифрового кредитування.

На думку комітету, запровадження системи білого списку вимагатиме ретельної оцінки цифрових кредитних агентств для забезпечення відповідності нормативним вимогам, операційної прозорості та дотримання етичних норм. «Це усуне з ринку шахрайські або недобросовісні агентства цифрового кредитування та

заохотить позичальників від хижацької практики кредитування та іншої незаконної діяльності», — йдеться у звіті комітету.

Комітет також порадив регулювати сторонніх постачальників послуг, включаючи великі технологічні та телекомунікаційні компанії. Магазинам додатків, таким як iStore від Apple і Play Store від Google, рекомендовано ділитися повними метаданими про всі додатки з відповідними органами для перевірки безпеки.

«Це сховище даних дасть регуляторам можливість проводити поглиблений аналіз, виявляти потенційні вразливості безпеки та вживати відповідних заходів для зміцнення цифрового ландшафту», — йдеться у рекомендаціях комітету.

Комісія була створена для розслідування випадків ескалації кібератак і розробки методів їх пом'якшення. Згідно з інформацією, наданою CERT-In, організація спостерігала та керувала 1,15 мільйонами інцидентів кібербезпеки у 2020 році, 1,4 мільйона у 2021 році та 1,39 мільйона у 2022 році.

Зі зростанням кібератак зростає й фінансове шахрайство. У 23 фінансовому році було зареєстровано 1,99 мільйона випадків шахрайства на суму 2537,35 рупій. крор, що на 87 відсотків більше від 1357,06 рупій. крор, заявлених у 22 фінансовому році, і значно більше, ніж рупій. 542,7 крор, повідомлених у 21 фінансовому році. Більшість шахрайств із платежами відбувається у формі фішингових атак.

Комітет також зазначив, що поточний механізм компенсації є складним і трудомістким і покладає на потерпілих обов'язок довести зв'язок між інцидентом кіберзлочинності та фінансовими втратами.

«Комітет твердо вірить у створення автоматичної системи компенсації, розробленої RBI. Виключною відповідальністю фінансових установ має бути своєчасне виплату компенсації постраждалому клієнту…», – йдеться у звіті.

Комітет також наголосив на необхідності посилення можливостей правозастосування та співпраці з міжнародними партнерами для впровадження передового досвіду.

Ключові рекомендації

Створити централізований «орган кіберзахисту»

Регулювати сторонніх постачальників послуг, зокрема великі технологічні та телекомунікаційні компанії

Впровадити структуру білого списку для цифрових кредитних агентств

Співпрацюйте з фінансовими установами, щоб покращити час безперебійної роботи служби та вирішити проблеми, що виникають у разі простою

Прийміть проактивний підхід до глобальних правил кібербезпеки». ***(Parliamentary Panel recommends DGCA-like authority for cybersecurity // Business Standard Private Ltd. (https://www.business-standard.com/economy/news/government-panel-recommends-a-centralised-authority-for-cyber-security-123072701065_1.html). 27.07.2023).***

***

«Організації в Індії отримали приріст продуктивності та інші бізнес-вигоди від впровадження цифрових технологій, але, як і в інших країнах, відповідне зростання кіберзагроз ставить під загрозу їхні зусилля з оцифрування.

Згідно з дослідженням Check Point Software, індійські підприємства стикалися в середньому з 1787 кібератаками на тиждень протягом останніх шести місяців проти середнього глобального показника 983, тоді як окреме дослідження TeamLease, платформи технологічних професійних послуг, показало, що організації в сфері охорони здоров'я, освіта, дослідження та уряд були найбільш вразливими до кібератак.

Як і в більшості країн, найпоширенішими загрозами в Індії були програми-вимагачі, які вразили 73% індійських компаній у 2022 році, що вище середнього світового показника в 66%, згідно з нещодавнім опитуванням Sophos. Найбільш цільовими галузями були уряд, освіта, фінансові послуги та виробництво.

Сантош Інгалкар, керівник відділу операцій логістичної компанії KSH Distriparks, сказав, що кібератаки на життєво важливу інфраструктуру, витоки

даних, атаки зловмисного програмного забезпечення та фішингові електронні листи є основною небезпекою.

«Кібератаки на ключові інфраструктури, такі як оборонний, енергетичний і фінансовий сектори, мають серйозні наслідки. Пошкодження, які виникають, можуть призвести до крадіжки даних і проблем із безпекою. Такі напади можуть паралізувати або затримати життєво важливі функції, що призведе до економічних і корпоративних втрат. Такі ризики вже спостерігалися в нашому бізнесі, і ми визнаємо це можливою катастрофою», – додав він.

Бупендра Соланкі, директор з інформаційних технологій Sakra World Hospital, сказав, що сектор охорони здоров'я особливо вразливий, оскільки кіберзлочинці знають, що постачальники медичних послуг зберігають конфіденційні дані клієнтів, і будуть платити за забезпечення безпеки та конфіденційності даних, що робить їх привабливими цілями для хакерів, мотивованих фінансовою вигодою.

Інгалкар зазначив, що ще одним крихким сегментом є малі та середні підприємства. «Малі підприємства мають менше капіталу і більше зосереджені на виробництві та наданні послуг. Ці галузі приділяють менше уваги IT-інфраструктурі та кібербезпеці, що робить їх більш уразливими до кібератак і легкими мішенями для кіберхакерів».

Джонас Уокер, директор відділу аналізу загроз у Fortinet, сказав, що оцифровка роздрібної торгівлі та зростання електронної комерції роблять ці сектори сприйнятливими до витоку даних платіжних карток, атак на ланцюги поставок і атак, спрямованих на інформацію про клієнтів. «Освітні заклади також зберігають велику кількість особистої інформації, включаючи дані студентів і викладачів, що робить їх привабливими мішенями для витоку даних і крадіжки особистих даних», — додав він.

Але підприємства в Індії не збираються дозволяти поганим діячам добиватися свого. Наприклад, лікарня Sakra World Hospital сегментувала свої мережі та запровадила доступ на основі ролей, виявлення кінцевих точок і реагування, а також можливості нульової довіри для своєї внутрішньої мережі. Він

також проводить оцінку вразливості та тести на проникнення для захисту своїх зовнішніх активів.

«Нульова довіра також повинна бути реалізована на ваших зовнішніх пристроях безпеки», — додав він. Система сповіщень має бути надійною та оперативною, щоб можна було негайно вжити заходів для пом’якшення будь-якого ризику кібербезпеки».

Для KSH Distriparks шифрування даних є важливим. Інгалкар сказав, що хмарні провайдери часто забезпечують шифрування даних у стані спокою та під час передачі, тому навіть якщо неавторизовані особи отримають доступ до даних, вони не зможуть прочитати або використовувати їх без ключів шифрування.

Інгалкар сказав, що його компанія також розгортає інструменти моніторингу та аналізу журналів, які відстежують та аналізують дії в IT-середовищі, щоб виявити прогалини та аномалії безпеки, а також забезпечити швидке реагування та пом’якшення. Оскільки люди часто є найслабшою ланкою в кібербезпеці, компанія також вклала значні кошти в підвищення обізнаності щодо безпеки та навчання співробітників і біометричну автентифікацію.

На тлі зростання кіберзагроз для критичної інфраструктури уряд Індії вжив рішучих заходів для зміцнення кібербезпеки країни через Національний центр захисту критичної інформаційної інфраструктури та Національний координаційний центр кібернетичної інформації.

Він також сформулював нову політику щодо кібербезпеки на тлі зростаючої кількості атак шкідливих програм на критичні сектори. Національна нормативна база кібербезпеки 2023 особливо спрямована на допомогу таким критичним секторам, як банківський, енергетичний та інші, озброївши їх стратегічними вказівками щодо проблем кібербезпеки.

Згідно з індексом готовності до кібербезпеки Cisco, близько 24% організацій в Індії мають «зрілий» рівень готовності з точки зору їх стійкості до подолання кіберзагроз. Це, якщо порівнювати із середнім глобальним показником у 15%, свідчить про кращий стан кібербезпеки Індії. Оскільки 90% підприємств очікують,

що інцидент із безпекою порушить їхній бізнес протягом наступних 12–24 місяців, ця еволюція повинна продовжуватись у належному темпі.

На цьому тлі Вокер із Fortinet закликав організації в Індії розробити комплексну стратегію кібербезпеки, яка б відповідала їхнім потребам. За його словами, регулярні оцінки безпеки, інформування про нові загрози та адаптація заходів безпеки є ключовими для ефективного пом'якшення ризиків.

Джон Шиєр, головний технологічний директор із комерційних питань у Sophos, сказав, що організації в Індії продовжуватимуть стикатися з проблемами, пов'язаними з успадкованими проблемами кібербезпеки, додавши, що трьома основними причинами атак в Індії минулого року були використані вразливості, скомпрометовані облікові дані та фішинг.

«Таким чином, підвищення стійкості систем шляхом своєчасного встановлення виправлень і зміцнення доступу за допомогою надійних механізмів автентифікації значно зменшить ризики, з якими зараз стикаються організації. Крім того, керовані послуги виявлення та реагування важливі для організацій, які не можуть забезпечити постійний проактивний моніторинг свого середовища на предмет підозрілих сигналів, а також швидке розслідування та реагування на потенційні порушення». ***(Pratima Harigunani. How Indian organisations are keeping pace with cyber security // TechTarget (https://www.computerweekly.com/news/366546093/How-Indian-organisations-are-keeping-pace-with-cyber-security?utm_source=flipboard&utm_content=other). 28.07.2023).***

***

Інші країни

«Согласно отраслевому отчету, у тайваньских предприятий есть значительные возможности для совершенствования, когда речь идет о решении «серьезных» проблем кибербезопасности, с которыми они сталкиваются.

Фирма по кибербезопасности Palo Alto Networks опубликовала отчет во вторник (4 июля), в котором показано, что из более чем 100 опрошенных тайваньских компаний более 60% тратят неделю или больше, чтобы отреагировать на инциденты кибербезопасности, и только 20% ответили в течение одного дня. Кроме того, 40% компаний обсуждали кибербезопасность на уровне совета директоров только один или два раза в год, и только 23% обсуждали ее ежемесячно.

Несмотря на это, в отчете говорится, что 75% предприятий увеличивают свои ежегодные бюджеты на кибербезопасность, что, по словам тайваньского регионального менеджера Пало-Альто Джеймса Ю (尤惠生), свидетельствует о росте осведомленности о кибербезопасности…

В отчете также отмечается относительно низкий уровень уверенности предприятий в том, что их сотрудники смогут адекватно решать проблемы кибербезопасности: чуть менее половины респондентов заявили, что, по их мнению, способности их сотрудников в этой области являются сильными или очень сильными. Чуть более 60% предприятий заявили, что они очень или очень сильно уверены в своих процессах и технологиях, когда речь идет о борьбе с угрозами кибербезопасности.

Глава отдела системной инженерии Пало-Альто Николас Сяо (蕭松瀛) сказал, что хакеры все чаще используют искусственный интеллект, а атаки на киберинфраструктуру все чаще автоматизируются. Тем не менее, 63% респондентов заявили, что считают, что чат-бот ChatGPT с искусственным интеллектом окажет положительное влияние на их процессы обслуживания клиентов и создание контента, несмотря на то, что только 52% тех же респондентов сообщили, что они знакомы с ChatGPT и его возможностями…

В мае два крупных интернет-магазина, работающих на тайваньском рынке, были оштрафованы на сумму от 100 000 тайваньских долларов (3 215 долларов США) до 200 000 тайваньских долларов за неспособность защитить личные данные своих клиентов. Отвечая на вопрос об использовании штрафов для наказания

компаний за нарушения кибербезопасности, Сяо сказал, что, несмотря на довольно низкий финансовый штраф, будут и другие последствия.

«Это не значит, что после того, как вы заплатите штраф, все будет позади, компании будут знать о влиянии, которое это оказывает на их доверие, и это продлится какое-то время», — сказал Сяо.

По словам Сяо, тайваньские предприятия больше всего обеспокоены атаками программ-вымогателей, которые нацелены на техническую инфраструктуру бизнеса и выводят ее из строя, а восстанавливают только после оплаты. Между тем, 67% респондентов заявили, что они обеспокоены атаками вредоносных программ (включая программы-вымогатели) в целом, а 57% заявили, что их беспокоят атаки программ-вымогателей конкретно.

Всего четыре дня назад тайваньская ведущая в мире компания по производству чипов TSMC столкнулась с угрозой кибербезопасности из-за атаки программы-вымогателя, требующей 70 миллионов долларов США, согласно Tech Radar. Представитель TSMC заявил в понедельник (3 июля), что жертвой атаки стала не сама компания, а один из ее поставщиков, и что данные клиентов не были взломаны…» ***(Jono Thomson. Significant room for improved cyber security in Taiwan businesses // Taiwan News (https://www.taiwannews.com.tw/en/news/4935822). 04.07.2023).***

***

«Избирательная комиссия Пакистана (ECP) выпустила предупреждение о кибербезопасности после того, как ее сотрудники начали получать электронные письма от неизвестных отправителей.

В письме, опубликованном 6 июля, ECP предупредила своих сотрудников, что атака программы-вымогателя была «попыткой украсть информацию» с помощью фишинговых методов.

Письмо, написанное специалистом по информационной безопасности ECP Навидом Ахмедом Кандиром, содержало скриншот электронного письма,

отправленного официальному лицу ECP, в котором получателю предлагалось открыть прикрепленный файл RAR под названием «Кабинет».

Ссылаясь на электронное письмо, ECP заявила, что «кто-то […] рассылает электронное письмо всем» официальным лицам ECP.

Служба по наблюдению за выборами попросила своих сотрудников не открывать электронное письмо, игнорировать его и сообщать о нем как о спаме.

Предполагаемое фишинговое электронное письмо информировало получателя о письме от 5 июля, которое было прикреплено к электронному письму.

Он «предупредил» получателя, что «данные для вышеуказанного не представлены», и попросил их предоставить их до 11 июля. В электронном письме также был указан буквенно-цифровой пятизначный код доступа без указания его цели.

Не удалось подтвердить, получили ли хакеры/спаммеры доступ к каким-либо важным данным о политических партиях, поскольку страна готовится к всеобщим выборам через несколько месяцев». ***(ECP issues cyber security alert after ransomware attack targets employees // Business Recorder (https://www.brecorder.com/news/40251484/ecp-issues-cyber-security-alert-after-ransomware-attack-targets-employees). 07.07.2023).***

***

«…На Филиппинах и в других странах Юго-Восточной Азии, будь то обычные люди, журналисты или активисты, онлайн-угрозы, от доксинга до блокировки доменов и цифровой слежки, растут, что подчеркивает нехватку ресурсов и опыта для борьбы с ними, говорят эксперты.

За такими онлайн-угрозами в таких странах, как Камбоджа, Таиланд, Мьянма и Филиппины, часто стоят правительства, заявила базирующаяся в Бангкоке группа цифровых прав DigitalReach, глобальное явление, получившее название цифрового авторитаризма.

«В Юго-Восточной Азии стало тенденцией, когда репрессивное правительство знает, насколько важно цифровое пространство для гражданского

общества, и считает, что контроль над ним является частью работы государства», — сказал Сутаван Чанпрасерт, основатель DigitalReach, Фонду Thomson Reuters.

В прошлом месяце два тайских активиста подали в суд на правительство за то, что они якобы использовали шпионское ПО Pegasus для мониторинга своих мобильных устройств.

Взлом Bulatlat пять лет назад, который, по словам газеты, был «целенаправленным, преднамеренным и хорошо организованным», стал первой известной распределенной атакой типа «отказ в обслуживании» (DDoS) против филиппинской медиа-организации.

Хакеры, участвующие в DDoS-атаках, направляют большие объемы интернет-трафика на целевые серверы в относительно простой попытке отключить их.

Не имея технических знаний, чтобы выследить хакеров и отреагировать на атаку, старшие сотрудники Bulatlat позвонили на горячую линию цифровой безопасности, управляемую Access Now, международной группой по защите цифровых прав.

Access Now связал их со шведским фондом Qurium Media Foundation, где специалисты по цифровой криминалистике смогли отследить вторжение до двух филиппинских ИТ-компаний.

Компании, которые также были связаны с DDoS-атаками на три других независимых новостных веб-сайта на Филиппинах, договорились о финансовом урегулировании гражданского дела, возбужденного против них.

Как остановить хакеров?

Однако для борцов за цифровые права это был относительно редкий пример успешного привлечения хакеров к ответственности.

Филиппины занимают второе место — после Монголии — среди стран, наиболее пострадавших от веб-угроз в мире, согласно отчету глобальной компании по кибербезопасности «Лаборатории Касперского» за 2022 год.

Но, по данным Департамента информационных и коммуникационных технологий, в стране всего 300 практикующих экспертов по кибербезопасности, а в идеале их должно быть 200 000.

Страна с 85 миллионами интернет-пользователей, или более 70% населения, должна больше инвестировать в меры кибербезопасности и сделать этот вопрос ключевым приоритетом, говорится в отчете некоммерческой организации The Asia Foundation за 2022 год.

Растущая обеспокоенность онлайн-угрозами побудила группы гражданского общества в регионе искать новые способы реагирования.

Некоторые из них предлагают обучение цифровой безопасности для лиц, подвергающихся риску, по таким мерам безопасности, как цифровое шифрование, виртуальные частные сети (VPN) и безопасные приложения.

Но Сутаван сказал, что, хотя обучение цифровой безопасности работает на индивидуальном уровне, в Юго-Восточной Азии необходимо принять более коллективный подход.

Это включает в себя наличие местных координаторов, которым доверяют диссиденты, с которыми они могут поделиться своим опытом на своих местных языках, и проведение дополнительных технических исследований для анализа угроз в каждой стране.

Более тесное трансграничное сотрудничество, как в случае с Булатлатом, также считается жизненно важным для сохранения свободы интернета.

В то время как существуют «очень ощутимые угрозы цифровой безопасности» для журналистов и активистов, Марлон Номбрадо из группы цифровых прав Out of the Box сказал, что обычные граждане также страдают, например, в форме фишинга, доксинга или неправомерного использования личных данных.

В январе прошлого года его группа обучила 20 женщин из бедного городского сообщества в Маниле цифровым правам и интернет-безопасности, в том числе тому, как предотвращать и реагировать на так называемый доксинг — злонамеренное размещение личной информации в социальных сетях.

В отличие от цифрового авторитаризма, направленного против инакомыслящих и журналистов, Номбрадо сказал, что борьба со злоупотреблениями в Интернете во всех слоях общества заключается в защите основных прав и свобод…» ***(Mariejo Ramos. Activists fight back as online threats rise // Philstar Global Corporation (https://interaksyon.philstar.com/trends-spotlights/2023/07/12/255588/activists-fight-back-online-threats-rise/?utm_source=flipboard&utm_content=philstarnews%2Fmagazine%2FInteraksyon.com). 12.07.2023).***

***

«…Кібербезпека – це практика захисту комп'ютерних систем, мереж і даних від зловмисних атак, несанкціонованого доступу та пошкодження для забезпечення конфіденційності, цілісності та доступності. По суті, це схоже на будівництво міцної фортеці навколо наших цифрових активів, захищаючи їх від кіберзлочинців, які прагнуть використовувати вразливі місця для отримання фінансової вигоди, політичних мотивів або навіть просто для захоплення викликання збоїв.

У Нігерії в міру того, як цифровий ландшафт стрімко розширюється, зростає гострота прийняття та розуміння кібербезпеки. Існує кілька ключових причин, чому вивчення кібербезпеки має велике значення в контексті Нігерії:

Захист особистих даних: у нашому взаємопов'язаному світі ми ділимося величезною кількістю особистої інформації в Інтернеті, від фінансових деталей до конфіденційних медичних записів. Навчання з кібербезпеки дає людям змогу розпізнавати потенційні ризики та застосовувати найкращі методи захисту своїх особистих даних від потрапляння в чужі руки. Варто відзначити, що 14 червня 2023 року президент Бола Тінубу зробив важливий крок, підписавши Закон про захист даних 2023 року. Основна мета цього Закону — забезпечити захист основних прав, свобод та інтересів суб'єктів даних, як це закріплено в Конституції Нігерії 1999 року. Серед положень Закону вводиться Нігерійська комісія із захисту даних

(Комісія) замість попереднього Нігерійського бюро із захисту даних (NDPB), яке було створено під час перебування на посаді колишнього президента Бухарі.

Закон стосується кількох важливих аспектів захисту даних, включаючи обробку персональних даних, захист прав суб'єктів даних, формування та функціонування Комісії із захисту даних, заходи безпеки даних, правила транскордонної передачі даних та управління порушення даних.

Захист національної безпеки: взаємозв'язок державних систем і критичної інфраструктури наражає Нігерію на кіберзагрози, які можуть поставити під загрозу національну безпеку. Вивчення кібербезпеки дозволяє фахівцям захищатися від таких атак, запобігаючи потенційним збоям у роботі основних послуг і забезпечуючи безпеку країни. Під час нещодавно завершеної дводенної конференції Cyber Secure Nigeria 2023 року в Абуджі радник з національної безпеки (NSA) Маллам Нуху Рібаду підкреслив життєво важливу роль сталої системи кібербезпеки в досягненні Цілей сталого розвитку (ЦСР) Порядок денний до 2030 року. Він наголосив на зобов'язанні уряду захистити кіберпростір Нігерії, який стикається зі зростаючою хвилею атак з боку кіберзлочинців.

Рібаду зазначив, що в Нігерії вживаються зусилля для зміцнення ландшафту кібербезпеки, приділяючи особливу увагу внесенню змін до Закону про заборону та попередження кіберзлочинів 2015 року. Крім того, уряд активно розглядає цінні внески зацікавлених сторін, таких як штучний інтелект (ШІ) та віртуальні активи, як частину процесу внесення поправок для ефективного протидії виникаючим кіберзагрозам. Ці заходи демонструють відданість уряду справі забезпечення безпеки та цілісності цифрової екосистеми Нігерії.

Економічна стійкість. Економіка Нігерії все більше залежить від цифрових технологій, де зростає кількість компаній, які здійснюють транзакції онлайн. Кібератаки, спрямовані на компанії, призводять не лише до фінансових втрат, але й підривають довіру споживачів. Інвестуючи в освіту з кібербезпеки, підприємства можуть захистити свої активи та забезпечити безперервність своєї діяльності. Значна кількість людей і власників бізнесу не знають про потенційні ризики, з якими вони стикаються в цифровій сфері. Багато хто недбало ставиться до своєї

картки та банківської інформації, тоді як деякі малі підприємства нехтують інвестуванням навіть у базову інфраструктуру кібербезпеки, таку як антивірусний захист своїх комп'ютерів. Ця відсутність запобіжних заходів часто призводить до того, що співробітники несвідомо отримують доступ до скомпрометованих сайтів і ненавмисно запроваджують шкідливе програмне забезпечення до їхньої мережі.

Вирішуючи цю проблему, у звіті Global Cybersecurity Outlook 2023 наголошується на необхідності розширення резерву спеціалістів із кібербезпеки для ефективної боротьби з цими загрозами. Незважаючи на те, що в усьому світі існує кілька успішних програм навичок кібербезпеки, проблема полягає в тому, щоб розширити їх для обробки більшої кількості. Щоб подолати цю перешкоду, у звіті наголошується на важливості розширення міжгалузевої співпраці та державно-приватного партнерства.

У звіті, підготовленому у співпраці з Accenture, наголошується, що підвищення обізнаності та готовності в організаціях може допомогти знайти баланс між прийняттям цінності нових технологій та пом'якшенням кіберризиків, які їх супроводжують.

Геополітичні зміни також впливають на правове, нормативне та технологічне середовище. У відповідь на ескалацію глобальної нестабільності, яка підвищує кіберризик, звіт закликає до відновлення співпраці між усіма зацікавленими сторонами, як з державного, так і з приватного секторів, які відповідають за нашу спільну цифрову інфраструктуру. Спільні зусилля спрямовані на розбудову безпеки, стійкості та довіри в цифровому просторі.

Крім того, питання кібербезпеки зараз впливають на стратегічні бізнес-рішення. Згідно з дослідженням Cybersecurity Outlook 2023, 50 відсотків учасників повідомили, що кібербезпека відіграє значну роль під час оцінки країн для інвестицій та бізнес-підприємств. Це демонструє зростаюче значення кібербезпеки у формуванні бізнес-стратегій і операцій.

Протидія кіберзлочинності: кіберзлочинці часто використовують прогалини в кібербезпеці для здійснення шахрайських дій, таких як фішинг, атаки програм-вимагачів і викрадення особистих даних. Найбільше в Нігерії постраждали банки:

університети та навіть державні установи, такі як Національна комісія з питань народонаселення та Незалежна національна виборча комісія, останнім часом зазнають тих чи інших типів атак.

Вивчення кібербезпеки надає правоохоронним органам необхідні навички для розслідування та затримання цих злочинців, сприяючи безпечнішому онлайн-середовищу для всіх.

Сприяння інноваціям: міцна основа кібербезпеки плекає культуру інновацій і технологічного прогресу. Коли люди та організації відчувають впевненість у своїй безпеці в Інтернеті, вони, швидше за все, досліджуватимуть нові ідеї та прийматимуть цифрову трансформацію, що веде до технологічного прогресу в різних секторах.

Щоб звернути увагу на важливість вивчення кібербезпеки, необхідно вживати ініціативи на різних рівнях. Деякі пропозиції:

Освіта та обізнаність: Кампанії з підвищення обізнаності про кібербезпеку слід проводити в навчальних закладах, на підприємствах і в державних організаціях. Нетехнічний персонал також слід заохочувати до участі в навчальних програмах з кібербезпеки, адаптованих до їхніх потреб.

Урядова підтримка: Уряд Нігерії має визначити пріоритетність ініціатив у сфері кібербезпеки та виділити ресурси для створення надійної інфраструктури кібербезпеки. Спільні зусилля з міжнародними партнерами можуть допомогти в обміні знаннями та передовим досвідом.

Державно-приватне партнерство: співпраця між державним і приватним секторами може зміцнити потенціал країни у сфері кібербезпеки. Приватні компанії можуть інвестувати в навчання своїх співробітників, тоді як держава забезпечує необхідну структуру та підтримку.

Постійне навчання: у міру розвитку кіберзагроз; знання та навички фахівців з кібербезпеки повинні йти в ногу. Постійне навчання на семінарах, конференціях і сертифікаціях покращить їх здатність ефективно протистояти складним кібератакам.

Підсумовуючи, освіта з кібербезпеки є не розкішшю, а необхідністю в сучасну цифрову епоху, особливо в Нігерії, де переваги технологій йдуть рука об руку з ризиками кіберзагроз. Ставлячи пріоритетом освіту з кібербезпеки та впроваджуючи профілактичні заходи, ми можемо зміцнити наш цифровий ландшафт, забезпечивши безпечне та процвітаюче майбутнє для всіх нігерійців...» ***(Brian Nduka. Protecting the digital realm: The vital importance of studying cybersecurity in Nigeria // GUARDIAN Newspapers (https://guardian.ng/technology/protecting-the-digital-realm-the-vital-importance-of-studying-cybersecurity-in-nigeria/). 17.07.2023).***

***

«Парламент Йорданії в четвер схвалив законопроект про кіберзлочинність, незважаючи на попередження правозахисних груп і громадянського суспільства, що він обмежить свободу слова в королівстві.

Законопроект був схвалений палатою представників після відкритого засідання, деякі із запропонованих покарань зменшені порівняно з початковим проектом, хоча тюремне ув'язнення залишається можливим для тих, хто порушує закон.

Законопроект також має бути схвалений сенатом, перш ніж його ратифікує король Абдалла II і опублікує в офіційному бюлетені.

Це сталося після того, як у понеділок 14 неурядових організацій виступили із заявою, в якій описали новий законопроект як «драконівський» і сказали, що він «прокладе шлях до тривожного сплеску онлайн-цензури».

Організації, в тому числі Human Rights Watch і група цифрових громадянських прав Access Now, попередили, що це «поставить під загрозу цифрові права, включаючи свободу вираження думок і право на інформацію».

Законопроект передбачає, що особам, яких визнають «поширенням неправдивих новин» в Інтернеті, загрожує покарання у вигляді тюремного ув'язнення не менше трьох місяців і штрафів у розмірі від 5000 до 20 000 йорданських динарів (близько 7000-28 000 доларів).

«Хибні новини» визначаються як усе, що «впливає на соціальний мир і національну безпеку».

Прем'єр-міністр Бішер аль-Хасауна заявив під час засідання в четвер, що "уряд не представляє нічого, що порушувало б чи суперечило б конституції", яка гарантує свободу слова.

Уряд «цілком відкритий до будь-якої форми критики», додав він.

Уряд Йорданії направив проект закону до парламенту для обговорення з метою внесення змін до закону про кіберзлочинність 2015 року.

У понеділок десятки журналістів влаштували акцію протесту перед своєю профспілкою, щоб висловити свої заперечення проти законопроекту.

У неділю група йорданських активістів, журналістів і політичних діячів розпочала онлайн-кампанію, відхиляючи проект закону та описуючи його як «некролог свободам».

Минулого тижня сотні політиків і журналістів підписали заяву із закликом скасувати закон, назвавши його «найбільшою загрозою для громадськості та свободи преси». ***(Jordan approves cybercrime bill despite rights groups // Al-Monitor, LLC. (https://www.al-monitor.com/originals/2023/07/jordan-approves-cybercrime-bill-despite-rights-groups?utm_source=flipboard&utm_content=AlMonitor%2Fmagazine%2FAl-Monitor). 27.07.2023).***

***

«Уряд Кенії успішно відновив роботу платформи e-Citizen після кібератаки, яка порушила її роботу.

У четвер Міністерство внутрішніх справ підтвердило, що платформа, яка пропонує понад 5000 послуг, наразі повністю запрацювала.

Сервіс на порталі був недоступний з 23 липня 2023 року.

«Ми хочемо повідомити широку громадськість, що послуги через e-Citizen Платформа (ecitizen.go.ke) відновила роботу», – йдеться у повідомленні.

У заяві міністерства зазначено, що короткий збій став результатом спроби кібератаки на платформу з використанням методу розподіленої відмови в обслуговуванні (DDoS).

Це передбачало перевантаження цільової системи величезним обсягом трафіку з кількох джерел одночасно.

У заяві додається, що в результаті злому «платформа була перевантажена і стала недоступною для справжніх користувачів, що спричинило перешкоди в роботі сервісів».

Уряд стверджує, що жодні дані не були скомпрометовані або втрачені під час інциденту, в результаті якого постраждали кілька компаній.

Раніше секретар кабінету міністрів ІКТ Еліуд Овало також підтвердив, що платформа зазнала кібератаки, яка порушила її роботу.

Овало розкрив, що хакери, відомі як «Анонімний Судан», відповідальні за атаку.

Платформа eCitizen надає понад 5000 державних послуг від різних міністерств, окружних урядів і агенцій.

Основна мета платформи – спростити та оцифрувати державні послуги, забезпечивши більшу доступність та зручність для користувачів.

Використовуючи технологію, платформа eCitizen прагне підвищити ефективність, прозорість і взаємодію з державними службами, що зрештою принесе користь народу Кенії». ***(DAVIS AYEGA. Govt restores e-Citizen portal after cybersecurity breach // Capital Digital Media (https://www.capitalfm.co.ke/news/2023/07/govt-restores-e-citizen-portal-after-cybersecurity-breach/?utm_source=flipboard&utm_content=other). 27.07.2023).***

***

«П’ятирічний національний план кібербезпеки, який викладає загальну стратегію уряду у боротьбі на новому полі бою, де Філіппіни можуть бути нарівні з потенційними іноземними противниками, очікує на схвалення президентом Фердінандом Маркосом-молодшим.

Стратегія охоплюватиме захист цілей, вразливих до кібератак, які можуть завдати шкоди економіці та національній безпеці ще до того, як по Філіппінах буде випущена перша ворожа ракета, заявив міністр інформаційних і комунікаційних технологій Іван Джон Уй під час форуму з управління та безпеки минулого тижня.

За його словами, Кабміну нещодавно представили «Національний план кібербезпеки (2023-2028)».

«Це фактично визначає зони, де необхідно захистити критичну інфраструктуру, і яке саме об'єднання агенцій, які займатимуться цим з цивільної та військової сторони, а також те, як ми всі працюватимемо разом, щоб координувати всі зусилля в захищаючи нашу країну», – сказав Уй під час форуму в середу.

«Як більшість із нас бачили сьогодні, під час війни перша атака не здійснюється кулею чи ракетою», — сказав він. «Коли ви запускаєте кібератаку та закриваєте всю фінансову систему країни, збиток від впливу є у багато разів більшим».

«Чудовий еквалайзер»

«Саме це те, що ми шукаємо — як нам потрібно приділити увагу безпеці нашого кіберпростору», — додав він.

Виступаючи на тому ж форумі, начальник штабу збройних сил Філіппін генерал Ромео Браунер-молодший сказав, що у військових також є плани щодо розвитку можливостей ведення кібервійни.

«Це одна з можливостей, за якою ми могли б досягти успіху в Збройних силах Філіппін, і ми могли б бути на рівні навіть із сучасними країнами», — сказав він.

Коли 21 липня він очолив AFP, Браунер сказав, що кіберпростір є «чудовим вирівнювачем».

«Незалежно від того, велика ви нація чи маленька нація — ви можете воювати в цьому кібердоміні. Немає потреби у великій техніці, щоб воювати в кіберсфері. Я вважаю, що у нас є великий потенціал тут, на Філіппінах», — сказав він журналістам.

Керівник AFP нагадав, що вірус «I Love You» — хробак, який заразив мільйони комп'ютерів у всьому світі в 2000 році, завдавши збитків на мільярди доларів — був створений філіппінцем. «Тож нам не бракує потенціалу та таланту, коли йдеться про кібербезпеку», — сказав він.

Американська компанія з кібербезпеки Insikt Group у 2021 році повідомила, що AFP, зокрема Військово-морські сили Філіппін, Міністерство закордонних справ і адміністрація президента, нібито стали мішенню хакерів, спонсорованих державою Китаю.

У ньому говориться, що Китай має «стратегічний і тактичний інтерес» до уряду Південно-Східної Азії та організацій приватного сектора.

Мета шпигунства

Марк Манантан, директор із кібербезпеки та критичних технологій аналітичного центру Pacific Forum, що базується на Гаваях, сказав, що Філіппіни залишаються мішенню хакерських груп, підтримуваних Китаєм.

«Більшість операцій пов'язані зі шпигунством з метою збору геополітичної розвідки щодо питань, пов'язаних із Південно-Китайським морем, але все частіше це відбувається з підвищеною увагою до потенційних непередбачених обставин на Тайвані», — сказав він Inquirer.

Кібершпигунство, за його словами, є «ефективним інструментом для збору геополітичної розвідки, що дає країнам передову перевагу в переговорах з іншими національними державами або, у разі війни, превентивну стратегію виведення з ладу критичної національної інфраструктури супротивника».

Між Філіппінами та Китаєм триває десятиліття морська суперечка в Південно-Китайському морі.

Пекін проігнорував арбітражне рішення 2016 року, яке скасувало широкі претензії Китаю на більшу частину критичного водного шляху та підтримало суверенітет Філіппін над його 370-кілометровою виключною економічною зоною, яка включає Західне Філіппінське море.

Китай направив сотні кораблів морської збройної армії для нападу на частини філіппінських вод, що філіппінські військові та берегова охорона вважають

способом остаточного контролю та окупації цих територій, які включають багатий ресурсами Ректо (Рід) Банк поблизу Палаван.

Навчання за підтримки США

Військові тренуються з такими країнами, як Сполучені Штати, щоб захистити свій кібердомен. Тепер кіберзахист є новим компонентом цьогорічних «Балікатан» — найбільших військових навчань між двома союзниками — для зміцнення кібербезпеки країни.

Канада, Австралія та Японія також прагнули до тіснішої співпраці з Філіппінами у сфері кібербезпеки.

«Національний план кібербезпеки» вперше був оприлюднений у 2017 році, через рік після створення Департаменту інформаційно-комунікаційних технологій, який був виділений із колишнього Департаменту транспорту та зв'язку.

Окрім захисту критичної інфраструктури країни, урядових і військових мереж, план також охоплював підприємства та їхні ланцюжки поставок, а також кожного філіппінця, який користується Інтернетом.

Його цілі включають забезпечення безперервної роботи важливих інфраструктур, державних і військових мереж, підвищення здатності Філіппін реагувати на кіберзагрози, координацію з правоохоронними органами та створення суспільства, освіченого кібербезпекою.

Навчання з кіберзахисту, що моделюють реагування на кібератаки, були частиною 12-денних військових навчань, які відбулися в листопаді 2022 року для перевірки готовності та сумісності армії, ВВС і ВМС». ***(Frances Mangosing. PH draws up 5-year cybersecurity plan // inquirer.net (https://newsinfo.inquirer.net/1809372/ph-draws-up-5-year-cybersecurity-plan). 30.07.2023).***

***

«Элитный иранский Корпус стражей исламской революции активизирует усилия по взлому учетных записей американских и западных лидеров, ученых и журналистов, занимающихся ядерной стратегией и Ближним Востоком, возможно, в рамках усилий по отслеживанию бывших американских чиновников, которым Тегеран угрожал убийством.

Атаки, описанные калифорнийской охранной фирмой Proofpoint и рядом бывших американских чиновников, подозреваемых в том, что они являются мишенями, были осуществлены хакерской группой Charming Kitten, связанной с КСИР, и, как считается, поддерживают Тегеран в его обостряющемся противостоянии с США и Европой из-за Ирана. ядерная программа и военная поддержка России в войне на Украине.

Джошуа Миллер, старший исследователь угроз Proofpoint, и эти бывшие официальные лица США сообщили Semafor, что КСИР стремится лучше понять и предсказать принятие решений и дипломатию Запада, направленную на сдерживание ядерной программы Ирана. Администрация Байдена заявила, что готова возобновить официальные переговоры, хотя Израиль заявил, что готов применить военную силу для уничтожения иранских ядерных объектов.

Но в то время как ранее иранские хакерские усилия были в основном направлены на сбор разведданных и шпионаж, Миллер говорит, что есть доказательства того, что усилия Charming Kitten теперь также направлены на поддержку глобальных террористических операций КСИР, включая похищения людей и убийства.

Иран публично пообещал убить ряд официальных лиц эпохи Трампа, в том числе бывшего госсекретаря Майка Помпео и бывшего советника по национальной безопасности Джона Болтона, которых он обвиняет в ударе беспилотника в 2020 году, в результате которого погиб генерал-майор Касем Сулеймани, командующий Вооруженными силами Ирана. Международная деятельность КСИР. Министерство юстиции в прошлом году предъявил обвинения лидерам КСИР в предполагаемом заговоре с целью убийства Болтона в Вашингтоне.

Миллер сказал Semafor в интервью в понедельник, что взлом учетных записей бывших американских чиновников может помочь КСИР отследить их цели.

«Наша оценка такова, что… наблюдение за кем-то, кто находится рядом с целью вашего убийства, имеет смысл с точки зрения планирования разведки», — сказал он. «Мы осторожны, чтобы сказать, что мы не видим окончательного доказательства. Но мы видели достаточно, что мы были готовы опубликовать»…» ***(Jay Solomon. Iran is on a hacking spree. The reason why may be ominous // Semafor Inc. (https://www.semafor.com/article/07/10/2023/iran-is-on-a-hacking-spree-the-reason-why-may-be-ominous?utm_source=flipboard&utm_content=user%2FSemafor). 11.07.2023).***

***

«Microsoft заявляет, что до сих пор не знает, как китайские хакеры украли ключ подписи потребителя неактивной учетной записи Microsoft (MSA), который использовался для взлома учетных записей Exchange Online и Azure AD двух десятков организаций, включая государственные учреждения.

«Метод, с помощью которого злоумышленник получил ключ, является предметом продолжающегося расследования», — признала Microsoft в новом бюллетене, опубликованном сегодня.

Об инциденте сообщили правительственные чиновники США после обнаружения несанкционированного доступа к почтовым службам Exchange Online нескольких государственных учреждений.

Microsoft начала расследование атак 16 июня и обнаружила, что китайская группа кибершпионажа, которую она отслеживает как Storm-0558, взломала учетные записи электронной почты примерно 25 организаций (по сообщениям, включая Государственный департамент США и Департамент торговли).

Злоумышленники использовали украденный корпоративный ключ подписи Azure AD для подделки новых токенов аутентификации, воспользовавшись

уязвимостью API GetAccessTokenForResource, предоставив им доступ к корпоративной почте целей.

Storm-0558 может использовать сценарии PowerShell и Python для создания новых токенов доступа через вызовы API REST для службы OWA Exchange Store для кражи электронных писем и вложений. Однако Редмонд не подтвердил, использовали ли они этот подход в прошлом месяце при атаках кражи данных Exchange Online.

«Наша телеметрия и расследования показывают, что действия после взлома были ограничены доступом к электронной почте и эксфильтрацией для целевых пользователей», — добавили сегодня Microsoft.

Компания заблокировала использование украденного закрытого ключа подписи для всех пострадавших клиентов 3 июля и сообщила, что инфраструктура воспроизведения токенов злоумышленников была отключена днем позже.

Ключи подписи MSA отозваны, чтобы заблокировать подделку токена Azure AD

27 июня Microsoft также отозвала все действительные ключи подписи MSA, чтобы заблокировать все попытки создания новых токенов доступа, и переместила вновь созданные в хранилище ключей, которое она использует для своих корпоративных систем.

«Никаких действий актера, связанных с ключом, не наблюдалось с тех пор, как Microsoft признала недействительным ключ подписи MSA, полученный актером», — заявили в Microsoft.

Тем не менее, несмотря на то, что после отзыва всех активных ключей подписи MSA и устранения уязвимости API Редмонд больше не обнаруживал какой-либо вредоносной активности Storm-0558, связанной с ключами, в сегодняшнем бюллетене говорится, что злоумышленники теперь переключились на другие методы.

«Никаких действий субъекта, связанных с ключом, не наблюдалось с тех пор, как Microsoft признала недействительным ключ подписи MSA, полученный субъектом. Кроме того, мы наблюдали переход Storm-0558 на другие методы, что

указывает на то, что субъект не может использовать или получить доступ к каким-либо ключам подписи», - заявила Microsoft.

Во вторник Microsoft также сообщила, что российская киберпреступная группа RomCom использовала уязвимость Office «нулевого дня», которая еще не исправлена, в недавних фишинговых атаках против организаций, присутствовавших на саммите НАТО в Вильнюсе, Литва.

Операторы RomCom использовали вредоносные документы, выдающие себя за Всемирный конгресс украинцев, для продвижения и развертывания полезной нагрузки вредоносных программ, таких как загрузчик MagicSpell и бэкдор RomCom». ***(Sergiu Gatlan. Microsoft still unsure how hackers stole Azure AD signing key // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/microsoft/microsoft-still-unsure-how-hackers-stole-azure-ad-signing-key/?utm_source=flipboard&utm_content=KevinCarrol78tk%2Fmagazine%2Fsysadmin). 14.07.2023).***

***

«У понеділок, 10 липня, внаслідок DDoS-атаки було порушено роботу деяких сайтів і транспортного мобільного застосунку в литовському Вільнюсі, де завтра розпочнеться саміт НАТО.

Про це заявив керівник Національного центру кібербезпеки (НЦКБ) Людас Алішаускас, повідомляє «Європейська правда» з посиланням на LRT.

«Наразі знову відбуваються DDoS-атаки на нашу країну, цілеспрямовані DDoS-атаки», – сказав він, додавши, що через атаки не працюють система m.Ticket і сайт GoVilnius.lt.

Алішаускас підкреслив, що установам необхідно готуватися до кіберзагроз і зважувати ризики.

«Сьогодні ми змушені констатувати, що багато керівників компаній, причому я говорю як про приватний, так і про державний сектор, трохи відсувають ризик

кіберзагроз на другий план, і тоді залишаються тільки симптоми: у нас один інцидент, у нас інший», – додав він.

Наразі центр кібербезпеки працює в посиленому складі у співпраці зі спецслужбами і поліцією, а також з іноземними партнерами партнерами.

Раніше повідомялося, що напередодні саміту НАТО у Литві 11-12 липня зафіксували дві кібератаки, через які на регіональній радіостанції та в торговому центрі транслювалася дезінформація після злому музичного потокового сервісу». ***(Через кібератаку стався збій у транспортній системі Вільнюса // Європейська правда (https://www.eurointegration.com.ua/news/2023/07/10/7165422/). 10.07.2023).***

***

«Нова голова німецького Федерального відомства з безпеки у сфері інформаційної техніки (BSI) Клаудіа Платтнер (Claudia Plattner) попередила про все вищу небезпеку для Німеччини у зв'язку з російськими кібератаками.

Як сказала керівниця відомства в інтерв'ю газеті Süddeutsche Zeitung, що було опубліковано у середу, 5 липня, ФРН, будучи європейською державою і прихильницею України, є «привабливою мішенню» для хакерських груп, якими керують з Москви.

Загалом загрози в мережі є «великими як ніколи», впевнена Платтнер, при цьому «цілями є: шпигунство, дестабілізація і (кампанія. - Ред.) впливу». За її словами, збільшення кількості атак також спостерігається з боку Китаю та Ірану.

«Зупинити і відбити атаки»

У представників органів безпеки Німеччини зростає стурбованість, що проросійські активісти, кіберзлочинці та хакерські групи, координовані російськими спецслужбами, об'єднуються для атак на західні системи, зазначає Süddeutsche Zeitung. Клаудіа Платтнер закликала до поліпшення захисту критичної інфраструктури. Так, навесні 2022 року у ФРН вийшли з ладу 5800 вітряних турбін унаслідок, ймовірно, російської атаки на супутникову мережу, при цьому низка експертів розцінила це як своєрідне попередження владі Німеччини.

Глава BSI закликала шукати способи «зупинити і відбити» атаки. Міністерка внутрішніх справ ФРН Ненсі Фезер (Nancy Faeser) хоче надати Федеральному відомству у кримінальних справах (BKA) більше повноважень, зокрема, воно повинно отримати право "активно" протистояти таким нападам - тобто проникати на сервери за кордоном і виводити їх з ладу, зазначає видання. Водночас у стратегії нацбезпеки ФРН члени парламентської коаліції підкреслювали, що в принципі відкидають такий підхід.

Звільнення глави BSI за підозрою у зв'язках із РФ

Ненсі Фезер 18 жовтня 2022 року звільнила попереднього главу BSI Арне Шенбома (Arne Schönbohm) у зв'язку зі звинуваченнями в занадто тісних зв'язках із Росією.

У МВС зазначили, що широко обговорювані у ЗМІ звинувачення підірвали суспільну довіру до Шенбома як до нейтрального і неупередженого керівника найважливішого відомства Німеччини у сфері кібербезпеки.

Згідно з розслідуванням суспільно-правового телеканалу ZDF, Арне Шенбом підтримував тісні зв'язки з асоціацією «Рада з кібербезпеки Німеччини» (Cyber-Sicherheitsrat Deutschland), яка підозрюється у зв'язках з російськими спецслужбами. Автори розслідування, зокрема, з'ясували, що берлінська фірма Protelion GmbH, яка входить до цієї асоціації, до кінця березня 2022 року працювала під назвою Infotecs GmbH і була «донькою» російської компанії «ИнфоТеКС» («Информационные технологии и коммуникационные системы»), заснованої Андрієм Чапчаєвим, який, за даними ЗМІ, здобув освіту у Вищій школі КДБ СРСР. Сама ж «Рада з кібербезпеки Німеччини» звинувачення відкидала, називаючи їх абсурдними». ***(Максим Сидоржевський, Катерина Вєнкіна. Голова кібербезпеки: ФРН - привабліва ціль для хакерів з РФ // Deutsche Welle (https://www.dw.com/uk/golova-kiberbezpeki-frn-poperedzae-pro-vse-bilsu-zagrozu-vid-hakeriv-z-rf/a-66138852?maca=ukr-rss-ukrnet-ukr-all-3816-xml). 06.07.2023).***

***

«У Латвії останніми тижнями зафіксували кібератаки на домашні сторінки Сейму та кількох компаній, пов'язаних із транспортним сектором.

Як пише «Європейська правда», про це повідомила установа із забезпечення кібербезпеки Cert.lv, передає Delfi.

У Cert.lv зазначили, що атаки мали тимчасовий характер і істотної шкоди не завдали.

Представники організації також зазначили, що найбільше кібератак останніми тижнями було спрямовано проти Литви.

Cert.lv стверджує, що атаки здійснюють «угруповання «хактивістів», які виступають за агресивний режим Росії».

Також у Латвії фіксують велику кількість випадків інтернет-шахрайства – жителі країни отримують повідомлення від фішингових сайтів, що імітують офіційні ресурси.

Шахраї також ведуть активну діяльність у латвійському сегменті соцмереж із залученням підроблених профілів відомих людей, пропонуючи користувачам стати «інвесторами» і «заробляти в інтернеті». ***(Сейм Латвії зазнав кібератак // Європейська правда (https://www.eurointegration.com.ua/news/2023/07/18/7166033/). 18.07.2023).***

***

«Представник Пентагону Тім Горман заявив, що в Міністерстві оборони США із серйозністю поставилися до випадку із витоком даних. Він зазначив, що повідомлення, які надіслали з адреси «.MIL» на адресу «.ML», заблоковуються до того, як вони покидають домен «.mil».

Про це пише видання Financial Times.

Це означає, що той, хто відправляє, має підтвердити електронні адреси сподіваних отримувачів. Це показує, що переслані електронні повідомлення, ймовірно, надходили з особистих акаунтів військових США.

Помилкове значення

Це сталося через те, що було введено «.ML», а не «.MIL» для домену адреси електронної скриньки, що приймав повідомлення.

Тому через цю помилку втратилась різна інформація. Йдеться про паролі та дані про подорожі, декларації для податків й документи, які стосуються дипломатії.

Наразі електронні повідомлення перебувають у підрядника, який управляє національним доменом Малі. Проте незабаром уряд Малі буде контролювати домен «.ML», який має зв'язки з Росією.

Кому вдалося виявити проблему

Про те, що стався витік листів, повідомив підрядник з Нідерландів Йоганнес Зуурб'є, який є керівником національного домену Малі.

Щодо цієї проблеми він дізнався ще у 2014 році, тому закликав США віднестися до неї з відповідальністю. Наразі ним зібрано вже біля 11 700 електронних листів, а в минулу середу прийшло ще близько 1000 повідомлень.

Що було в листах

У листах було написано плани візиту керівника штабу армії США генерала Джеймса Макконвілла до Індонезії. Також там розміщені світлини баз, мапи об'єктів, документи та переліки екіпажів кораблів.

Один із електронних листів було відправлено від агента ФБР. В ньому йшлося про можливі операції Робочої партії Курдистану.

Нагадаємо, у виданні The Verge раніше повідомляли, що мільйони електронних листів американських військових понад 10 років помилково надсилалися до Малі, яка є союзником Росії. Це сталося через те, що люди часто помилково вводили домен «.ML» — ідентифікатор країни для Малі, а не військовий — «.MIL». ***(Карина Бовсуновська. У Пентагоні прокоментували витік даних до партнера Росії // ТОВ «МЕДІАМЕРЕЖІ» (https://it.novyny.live/u-pentagoni-prokomentuvali-vitik-danikh-do-partnera-rosiyi-107343.html). 18.07.2023).***

***

«Західні спецслужби та групи з кібербезпеки звинуватили китайські хакерські групи в кампаніях цифрового вторгнення по всьому світу, націлених на все: від урядових і військових організацій до корпорацій і медіа-груп.

Фірми з кібербезпеки вважають, що багато з цих груп підтримується урядом Китаю.

Влада Китаю постійно заперечує будь-яку форму хакерства, що фінансується державою, заявляючи, що сам Китай часто є об'єктом кібератак. Пекін назвав США «імперією хакерства».

Деякі з нещодавно ідентифікованих китайських хакерських команд:

STORM-0558

З травня китайські хакери таємно отримали доступ до облікових записів електронної пошти приблизно 25 організацій, включаючи урядові установи США, Microsoft (MSFT.O) і офіційні особи США. заявили

До них входять рахунки міністра торгівлі США Джини Раймондо та, згідно з повідомленням Wall Street Journal у четвер, представника США в Китаї Ніколаса Бернса та Деніела Крітенбрінка, помічника держсекретаря у справах Східної Азії.

Microsoft заявила, що китайський актор, якого вона назвала Storm-0558, незаконно привласнив один із її цифрових ключів і використав недолік у коді для крадіжки електронних листів.

Посольство Китаю у Вашингтоні заявило, що виявлення джерела кібератак було складним, і застерегло від «безпідставних спекуляцій і звинувачень».

'VOLT TYPHOON'

Західні спецслужби та Microsoft заявили 24 травня, що Volt Typhoon, група, яку вони описали як спонсоровану державою, шпигувала за рядом організацій критичної інфраструктури США, від телекомунікацій до транспортних вузлів.

Вони описали атаки 2023 року як одну з найбільших відомих китайських кампаній кібершпигунства проти американської критичної інфраструктури.

Міністерство закордонних справ Китаю відкинуло ці заяви.

'BACKDOORDIPLOMACY'

У звіті Reuters у травні зазначено, що BackdoorDiplomacy стоїть за широкою серією цифрових вторгнень протягом кількох років проти ключових міністерств і державних установ Кенії. Влада Китаю заявила, що не знала про такий злом, і назвала звинувачення безпідставними.

Palo Alto Networks, американська компанія з кібербезпеки, заявила, що її дослідження показали, що BackdoorDiplomacy мала зв'язки з китайською державою та була частиною хакерської групи APT15.

APT 41

За даними американських компаній з кібербезпеки FireEye і Mandiant, китайська хакерська команда APT 41, яка також відома як Wintti, Double Dragon і Amoeba, здійснила поєднання підтримуваних державою кібервторгнень і фінансово вмотивованих витоків даних.

Секретна служба США заявила, що команда вкрала пільги США з допомоги COVID-19 на десятки мільйонів доларів між 2020 і 2022 роками.

Тайванська фірма з кібербезпеки TeamT5 заявила, що жертвами групи були урядові, телекомунікаційні та ЗМІ в Японії, Тайвані, Південній Кореї, Сполучених Штатах і Гонконгу.

APT 41 було названо Міністерством юстиції США у вересні 2020 року у зв'язку з обвинуваченнями, висунутими проти семи хакерів за нібито компрометацію понад 100 компаній у всьому світі.

Китайська влада назвала такі повідомлення «безпідставними звинуваченнями».

APT 27

Західні спецслужби та дослідники кібербезпеки стверджують, що китайська хакерська команда APT 27 спонсорується державою та здійснила численні атаки на урядові установи Заходу та Тайваню.

APT 27 взяв на себе відповідальність за кібератаки на Тайвань у 2022 році під час візиту тодішнього спікера Палати представників Конгресу США Ненсі Пелосі, заявивши, що це діяло як протест, оскільки Пелосі знехтувала застереженнями Китаю не відвідувати.

Фірма з кібербезпеки Mandiant заявила, що минулого року група скомпрометувала комп'ютерні мережі щонайменше шести урядів штатів США в період з травня 2021 року по лютий 2022 року, тоді як влада Німеччини звинуватила її в атаках на німецькі фармацевтичні, технологічні та інші компанії». ***(The Chinese groups accused of hacking the US and others // Reuters (https://www.reuters.com/world/china/chinese-groups-accused-hacking-us-others-2023-07-21/). 21.07.2023).***

***

Кіберзахист критичної інфраструктури

«Поскольку Европа и США стремятся нарастить разработку и продажи электромобилей, исследователи обеспокоены тем, что кибербезопасность игнорируется.

В худшем случае хакеры могут отключить электроэнергию и нанести ущерб всей электросети, проникнув в зарядные станции и сети, предупреждают чиновники и аналитики по безопасности.

«Если у вас есть сотни тысяч зарядных устройств, вы — цель», — сказал он. Харм ван ден Бринк, специалист по кибербезопасности в ElaadNL, исследовательской организации в Нидерландах, занимающейся тестированием зарядки электромобилей.

В апреле администрация Байдена предложила ужесточить целевые показатели выбросов автомобилей, чтобы ускорить переход на электромобили, и призвала к тому, чтобы к 2030 году они составляли половину всех продаж новых автомобилей. Европейский союз пошел еще дальше, запретив продажу новых бензиновых и дизельных двигателей. автомобилей с двигателем начиная с 2035 года.

Однако в спешке с электромобилями кибербезопасность не может быть запоздалой, сказал Томас Бодеклинт, разработчик исследований и бизнеса в

Исследовательских институтах Швеции, государственной группе, которая работает над зарядкой электромобилей и другими технологиями.

«Когда вы получаете быстрое развертывание, вы немного экономите. Кроме того, существует повышенный риск, если [продукты] не были тщательно протестированы и проверены», — сказал он.

Усилия по обеспечению безопасности зарядных станций для электромобилей находятся на ранних стадиях. Европейские законодатели разрабатывают новые киберправила для операторов электросетей, которые, вероятно, будут включать дополнительные требования безопасности для инфраструктуры зарядки электромобилей. Анжос Нейк, управляющий директор European Network for Cyber Security, нидерландской организации, которая делится информацией о киберугрозах с критически важными инфраструктурными и энергетическими компаниями.

Великобритания ввела такие требования, как шифрование сообщений, отправляемых со станций, и использование уникальных паролей на определенном оборудовании.

«Сейчас все очень быстро ускоряется, — сказал Нейк.

От штатов США требовалось обеспечить кибербезопасность в планах, разработанных в прошлом году, чтобы получить федеральное финансирование для инфраструктуры электромобилей. Нужно больше конкретики, сказал Джей Джонсон, инженер-механик в Sandia National Laboratories, занимающийся исследованиями в области энергетики.

Закон США об инфраструктуре, принятый в 2021 году, предусматривает финансирование штатов в размере 7,5 млрд долларов на расширение зарядных станций для электромобилей. В федеральном руководстве отмечается, что заявители должны использовать «соответствующие» стратегии кибербезопасности для защиты данных и систем, но оставлено на усмотрение штатов определение того, как это сделать.

Южная Дакота, например, заявила, что компаниям, создающим инфраструктуру электромобилей, потребуется шифровать сообщения и

использовать брандмауэры. В плане Нью-Йорка отмечается, что стандарты для технологий безопасности электромобилей все еще разрабатываются. «Штат Нью-Йорк будет соблюдать все федеральные технические стандарты, включая кибербезопасность, как только они будут завершены», — говорится в плане.

«Это была очень большая упущенная возможность согласовать требования по всей стране», — сказал Джонсон. По его словам, компаниям, работающим в нескольких штатах, было бы легче соблюдать общенациональные кибертребования.

Sandia недавно оценила 12 безымянных зарядных устройств и обнаружила недостатки в безопасности, такие как открытое отображение имен пользователей, паролей и учетных данных для изменения или настройки одного оборудования, в то время как другие имели лучшую защиту. «Эти продукты обладают широким спектром возможностей кибербезопасности, — сказал Джонсон.

Тесла готова доминировать в области зарядки электромобилей в США, и производители автомобилей, включая General Motors, Ford, Volvo и Rivian, подписались на принятие стандарта зарядки Tesla в этом году. На прошлой неделе, Группа Мерседес-Бенц заявила, что планирует поддерживать станции Tesla Supercharger, начиная со следующего года. Tesla не ответила на запросы о комментариях.

ChargePoint, крупный поставщик станций для корпоративных парковок и городов в Северной Америке и Европе, предпринимает несколько шагов для защиты своих систем, директор по информационной безопасности. Теза Муккавилли сказал через пресс-секретарь. По состоянию на конец января компания эксплуатировала около 225 000 зарядных портов.

По словам Муккавилли, среди кибермер, принимаемых ChargePoint, есть тесты на проникновение и изоляция частей сети, чтобы предотвратить эффект домино в более крупной электрической сети в случае кибератаки.

По его словам, ChargePoint использует различные инструменты для устранения киберрисков в микросхемах и программном обеспечении, используемом на станциях, платежных операциях клиентов и шифровании, а также в своей технологической инфраструктуре.

По словам ван ден Бринка из ElaadNL, киберрегламенты, различающиеся по географии, не защитят от крупномасштабных последствий крупной кибератаки.

«Если вы взломаете 100 000 зарядных устройств, не имеет значения, где они находятся в Европе. Это может оказать большое влияние на энергосистему», — сказал он.

В прошлом году город Амстердам впервые включил требования кибербезопасности в открытый тендер на общественные зарядные станции для электромобилей. Организации, претендующие на контракты, должны доказать, что они соблюдают стандарты безопасности, и предоставить кибероценки своих цепочек поставок. Яап де Мунник, бывший старший офицер информационной безопасности города. В этом месяце он присоединился к голландскому поставщику семян Enza Zaden в качестве сотрудника по информационной безопасности.

По его словам, требования Амстердама предназначены для отражения атак, которые могут вызвать перебои в подаче электроэнергии или заставить зарядные станции использовать больше энергии, чем должны, что может привести к повреждению трансформаторов и линий электропередач.

Амстердам поделился своими требованиями с другими голландскими городами, и де Мунник надеется, что они последуют их примеру». ***(Catherine Stupp. EV Charging Networks Prepare for Cyberattacks // Dow Jones & Company, Inc. (https://www.wsj.com/articles/ev-charging-networks-prepare-for-cyberattacks-7bf488d7?utm_source=flipboard&utm_content=WSJ%2Fmagazine%2FBusiness). 14.07.2023).***

***

Кіберзахист закладів охорони здоров'я

«Найбільший трест Національної служби охорони здоров'я Великобританії підтвердив, що розслідує інцидент із програмним забезпеченням-вимагачем, оскільки державний сектор країни продовжує боротися із зростаючою хвилею кібератак.

Barts Health NHS Trust, який керує п’ятьма лондонськими лікарнями та обслуговує понад 2,5 мільйона пацієнтів, нещодавно був доданий до темного веб-сайту витоку інформації банди програм-вимагачів ALPHV. Угруповання, також відоме як BlackCat, стверджує, що викрало 70 терабайт конфіденційних даних, що, на її думку, є найбільшим витоком медичних даних у Сполученому Королівстві.

Зразки ймовірно викрадених даних, які побачив TechCrunch, включають документи, що посвідчують особу співробітників, зокрема паспорти та водійські права, а також внутрішні електронні листи з позначкою «конфіденційно».

Відповідаючи на запитання TechCrunch, представник Barts Health не став заперечувати, що на нього вплинув інцидент безпеки, пов’язаний з викраденням даних, а також не заперечував легітимність викрадених зразків даних, якими поділився ALPHV. «Ми знаємо про твердження про атаку програм-вимагачів і проводимо термінове розслідування», — сказав TechCrunch речник, який не вказав свого імені.

ALPHV, який вперше опублікував Barts Health 30 червня, написав, що NHS Trust мав три дні, щоб зв’язатися з угрупованням, щоб запобігти публікації даних, «більшість із яких — конфіденційні документи громадян». На момент написання статті повна колекція ймовірно вкрадених даних не була опублікована.

Цей інцидент є другим порушенням даних NHS за останні тижні. Як вперше повідомляв Independent, червнева атака програми-вимагача на британський Манчестерський університет призвела до того, що хакери отримали доступ до набору даних NHS, який містить інформацію про 1,1 мільйона пацієнтів у 200 лікарнях. Відповідно до звітів, скомпрометовані дані, зібрані університетом для дослідницьких цілей, включають номери NHS і перші три літери поштових індексів пацієнтів.

Відповідаючи на запитання TechCrunch, речник Манчестерського університету Бен Робінсон відмовився коментувати повідомлення про крадіжку даних NHS, але підтвердив, що в університеті стався інцидент безпеки, який призвів до викрадання даних із його систем.

«23 червня ми підтвердили, що наші системи отримали доступ і дані студентів і випускників були скопійовані. За словами Робінсона, окремим особам було повідомлено про цей кіберінцидент і запропоновано підтримку та поради щодо подальшого захисту їхніх даних. «Наші внутрішні експерти з даних і зовнішня підтримка цілодобово працюють над вирішенням цього інциденту та реагуванням на його наслідки, і на даному етапі ми не можемо коментувати».

Національний центр кібербезпеки, агентство з кібербезпеки Великобританії, розслідує інцидент. NHS England відмовилася від коментарів.

Наслідки кібератаки

Останніми місяцями державний сектор Великобританії боровся з хвилею кібератак.

Ofcom, регулятор зв'язку Великобританії, нещодавно підтвердив, що він був серед організацій, які були скомпрометовані бандою програм-вимагачів Clop, яка масово використовувала недолік безпеки в керованій службі передачі файлів MOVEit Transfer від Progress Software, а Університет Західної Шотландії (UWS)) підтвердив, що він переживає «кіберінцидент, що триває», але не розкрив подробиці.

Один із найбільших поточних кіберінцидентів, що вплинув на державний сектор Великобританії, став результатом травневої атаки програм-вимагачів на Capita, британського аутсорсингового гіганта, який надає важливі послуги для уряду Великобританії.

У результаті атаки, відповідальність за яку взяла група програм-вимагачів Black Basta, понад 90 організацій повідомили про злам особистої інформації. Це включало Universities Pennuation Scheme (USS), найбільшу приватну пенсійну компанію Великобританії, яка заявила, що особисті дані майже півмільйона учасників зберігалися на серверах, доступ до яких було отримано під час злому.

Минулого тижня Capita підтвердила, що її власний пенсійний фонд також постраждав від кібератаки. У листі, опублікованому The Times, Capita повідомила своїм співробітникам через три місяці після зламу, що вона «виявила докази того,

що такі особисті дані, які стосуються вас, містяться в даних, скомпрометованих та/або скопійованих із систем Capita».

Відповідаючи на запитання TechCrunch, Capita не заперечувала цю інформацію, але відмовилася повідомити, скільки, якщо не всіх, із 61 000 її співробітників постраждали або до яких типів даних був доступ.

«Capita продовжує тісно співпрацювати зі спеціалізованими консультантами та судово-медичними експертами для розслідування інциденту, і ми вжили значних заходів для відновлення та захисту даних», — сказав TechCrunch представник Capita, який відмовився залишитися на ім'я. «Це складне розслідування, і процес триває. Продовжуємо інформувати постраждалих».

Буквально через кілька днів після того, як з'явилася новина про взлом Capita, TechCrunch повідомив, що в компанії стався другий інцидент безпеки після того, як виявилося, що Capita залишила скарбницю даних, відкритих в Інтернеті протягом семи років. Капіта сказав TechCrunch, що незахищене відро зберігання, розміщене на Amazon, яке містило приблизно 3000 файлів загальним розміром 655 гігабайт, містило «таку інформацію, як примітки до випуску та посібники користувача, які регулярно публікуються разом із випусками програмного забезпечення відповідно до стандартної галузевої практики».

Проте кілька британських рад підтвердили, що в результаті інциденту конфіденційні дані мешканців стали відкритими для загальнодоступного Інтернету». ***(Carly Page. UK battles hacking wave as ransomware gang claims 'biggest ever' NHS breach // Yahoo (https://techcrunch.com/2023/07/10/uk-hacks-public-sector-nhs-ransomware/?utm_source=flipboard&utm_content=user%2FTechcrunch&guccounter=1&guce_referrer=aHR0cHM6Ly9mbGlwYm9hcmQuY29tL3JlZGlyZWN0P3VybD1odHRwcyUzQSUyRiUyRnRlY2hjcnVuY2guY29tJTJGMjAyMyUyRjA3JTJGMTAlMkZ1ay1oYWNrcy1wdWJsaWMtc2VjdG9yLW5ocy1yYW5zb213YXJlJTJGJTNGdXRtX3NvdXJjZSUzRGZsaXBib2FyZCUyNnV0bV9jb250ZW50JTNEdXNlciUyNTJGVGVjaGNydW5jaCZ2PUpPWnRVSkZXazQ1c0oyWlJyV0hMTG1ITER0SmliRlFqS1N1Z0xqNmNxR2tBQUFHSlJQYlI0UQ&guce_referrer_sig=AQAAAMDV55yjDvIqzMT6dd5uSlX***

us8qXar_tpDuN_FhnmNRD2i0Et_48-ZYf2G9euufiXxyr-dp7-7i0rVFraPXGLYHmk1OGIuDjvIY-Tq7uOvqQa2k10M6Nmhl2zH8mscQ76zOZt9BniYOLQhnCTKyPfhlfYKDl6Ovm-HnhHZduWgBo). 10.07.2023).

***

Захист персональних даних та соціальні мережі

«…Кібербезпека – це широкий термін, який охоплює захист усіх цифрових активів, включаючи дані, мережі, пристрої та системи. Безпека даних конкретно стосується захисту чутливої або конфіденційної інформації від несанкціонованого доступу, використання, розголошення або знищення.

Захист даних можна досягти різними методами, зокрема:

Політики безпеки, які обмежують доступ до конфіденційної інформації на основі рівня конфіденційності цієї інформації та вимоги користувача

Заходи контролю доступу, такі як автентифікація та авторизація

Заходи фізичної безпеки, такі як блокування або шифрування

Планування безперервності бізнесу (BCP) на випадок інциденту, який спричиняє втрату або пошкодження систем вашої організації.

Безпека даних дедалі більше стає ключовим аспектом кібербезпеки через велику кількість даних, які генеруються, зберігаються та обмінюються як окремими особами, так і організаціями. Як ми знаємо, витік даних, програми-вимагачі та фішингові атаки мають згубні наслідки для всіх нас.

Перехід від кібербезпеки до безпеки даних свідчить про більш цілісний підхід до захисту конфіденційних даних в організаціях. Хоча кібербезпека зазвичай зосереджена на захисті інформаційних систем і мереж від несанкціонованого доступу, безпека даних охоплює захист даних протягом усього життєвого циклу, від створення та зберігання до обробки та спільного використання.

Отже, майбутні інвестиції в інфраструктуру даних і технології, ймовірно, будуть пріоритетними для рішень, які можуть запропонувати комплексний захист

даних, включаючи контроль доступу до даних, класифікацію даних, виявлення конфіденційних даних, постійний моніторинг і виявлення даних.

Дотримання правил конфіденційності даних є ще одним важливим аспектом безпеки даних. Очікується, що організації інвестуватимуть у технології, які допоможуть їм відповідати вимогам GDPR, наприклад, і уникнути штрафів.

Зміна акценту з кібербезпеки на безпеку даних означає зосередженість на захисті даних і забезпеченні їх конфіденційності, цілісності та доступності. Майбутні інвестиції в інфраструктуру даних і технології, швидше за все, будуть пріоритетними для рішень, які можуть запропонувати комплексну безпеку даних, відповідність нормам конфіденційності даних та інноваційні технології, які можуть краще допомогти захистити конфіденційні дані.

У сучасну цифрову епоху важливо прийняти та інтегрувати підхід, що керується даними, до культури бізнесу. Зараз, як ніколи, корпоративна культура цінує роль даних, і компанії все частіше використовують їх для прийняття стратегічних рішень і стимулювання зростання.

Це означає, що дані стають всеохоплюючими для всієї компанії, згодом збільшуючи кількість слабких місць, якими можуть скористатися зловмисники. Оскільки підприємства починають покладатися на дані як основу для всієї своєї діяльності, важливо зменшити ризики. Це має початися з безпеки даних у самій її основі». ***(Mark Semenenko. The New Cybersecurity Is Data Security // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/the-new-cybersecurity-is-data-security/). 17.07.2023).***

***

«Pacific Premier Bancorp (PPBI.O) заявив у вівторок, що інцидент із кібербезпекою у стороннього постачальника призвів до витоку даних клієнтів його банку, ставши останньою жертвою злому MOVEit.

Постачальник підтвердив, що особисті дані були скомпрометовані під час інциденту, в якому був задіяний популярний інструмент передачі файлів MOVEit, повідомляє Pacific Premier у нормативній документації.

Зламані дані клієнтів містили номери соціального страхування, номери рахунків та іншу особисту інформацію, додала компанія.

Він не розкриває масштаб витоку даних, але каже, що працює з постачальником, щоб повідомити потенційно постраждалих сторін і регуляторних органів.

Фірми, установи та державні відомства, які використовують програмне забезпечення для обміну файлами MOVEit, нещодавно постраждали від витоку даних.

У понеділок споживчий і комерційний банк 1st Source Corp (SRCE.O) заявив, що порушення безпеки, пов'язане з MOVEit, вплинуло на близько 450 000 записів.

MOVEit, створений компанією Progress із Массачусетса, дозволяє організаціям безпечно передавати файли та дані між діловими партнерами та клієнтами.

«Немає жодних ознак того, що інцидент із постачальником залучив внутрішню мережу чи IT-системи компанії, і не було суттєвих перерв у бізнес-операціях компанії», — йдеться в заяві банку.

За його словами, банк використовує постачальника для надання певних послуг з операційної підтримки з питань оподаткування та дотримання законодавства». ***(Pacific Premier says vendor hit by MOVEit data breach // Reuters (https://www.reuters.com/technology/pacific-premier-says-vendor-hit-by-moveit-data-breach-2023-07-25/). 25.07.2023).***

***

«Урядові агентства з кібербезпеки США та Австралії попереджають, що поширені та легко використані вразливості безпеки на веб-сайтах і веб-додатках можуть бути використані для здійснення великомасштабного витоку даних.

У спільному повідомленні, опублікованому в четвер, агентство з кібербезпеки США CISA, Агентство національної безпеки та Австралійський центр кібербезпеки заявили, що вразливості, відомі як незахищені прямі посилання на

об’єкти (IDOR), дозволяють зловмисним хакерам отримувати доступ або змінювати конфіденційні дані на серверах організації. через відсутність належних перевірок безпеки.

Уразливість IDOR подібна до ключа від вашої поштової скриньки, але цей ключ також дозволяє розблокувати будь-яку іншу поштову скриньку на вашій вулиці. IDOR можуть бути особливо проблематичними, оскільки, подібно до ряду поштових скриньок, зловмисник може використовувати їх послідовно одну за одною та отримати доступ до даних, які їм не можна дозволяти.

Оскільки ці вразливості часто можна використати шляхом перерахування, IDOR можна зловживати «в масштабі» за допомогою автоматизованих інструментів, попереджає консультація.

«Хоча з відкритих джерел уже надходили звіти про вразливості небезпечного прямого посилання на об’єкти (IDOR) у веб-додатках, CISA та наші партнери з Австралійського центру кібербезпеки та Агентства національної безпеки зрозуміли, що це серйозна вада, яку недостатньо визнають або розуміють всередині кіберспільнота. Сьогоднішня спільна консультація є першою значною консультацією з цього питання, яка допоможе організаціям захистити конфіденційні дані у своїх системах і підштовхне постачальників зменшити поширеність уразливостей і недоліків IDOR», — сказав TechCrunch Джеймс Стенлі, керівник відділу розробки продуктів CISA.

У спільній консультації зазначається, що IDOR призвели до серйозних порушень даних у Сполучених Штатах і за кордоном.

За останні роки IDORs призвели до виявлення тисяч медичних документів гігантом американської лабораторії, веб-сайтом уряду штату, який розкрив особисту інформацію про тисячі платників податків, програмою для відстеження контактів коледжу, яка видала статус вакцинації проти COVID-19, і штатом - додаток із підтримкою охорони здоров’я, який надавав доступ до даних про щеплення інших людей. IDOR також призвели до масового витоку даних сотень мільйонів іпотечних документів США, розкриття даних про місцезнаходження понад мільйона транспортних засобів у реальному часі з несправного GPS-трекера

та витоку сотень тисяч викрадених даних особистих телефонів людей глобальною мережею сталкерів.

У спільній консультації йдеться, що розробники повинні забезпечити, щоб їхні веб-додатки проводили перевірку автентифікації та авторизації, щоб зменшити IDOR, і що програмне забезпечення є безпечним за проектом, принцип, який підтримує CISA, який закликає виробників програмного забезпечення забезпечувати безпеку з самого початку та протягом усього програмного забезпечення. процес розробки.

«Безпека за проектом є фундаментальною темою в цьому пораді. Постачальникам і розробникам пропонується вжити відповідних заходів для надання продуктів, які захищають конфіденційні дані їхніх клієнтів за замовчуванням», — сказав Стенлі з CISA.

Австралійське кіберагентство заявило, що продовжує спостерігати за зловмисниками, які використовують неправильно налаштовані мережі.

«Навіть одне порушення з використанням уразливостей IDOR може мати національні наслідки. Зловмисник, здатний викрасти дані, може вплинути на критично важливу інфраструктуру, підприємства, уряд та окремих осіб», — сказав Патрік Холмс з Австралійського центру кібербезпеки». ***(Zack Whittaker. US, Australia cyber agencies warn IDOR security flaws can be exploited 'at scale' // Yahoo. (https://techcrunch.com/2023/07/27/cisa-nsa-australia-idor-flaws/?utm_source=flipboard&utm_content=Techcrunch%2Fmagazine%2FLatest+TechCrunch+Stories). 28.07.2023).***

***

«Дані, що належать Університету Західної Шотландії (UWS), були виставлені на аукціон кібербангою-вимагачем.

Університет вперше заявив, що зіткнувся з «кіберінцидентом» на початку цього місяця, і поліція проводить розслідування.

Тепер банда програм-вимагачів Rhysida вимагає 20 біткоїнів (450 000 фунтів стерлінгів) за конфіденційні дані та каже, що вони будуть продані тому, хто запропонує найвищу ціну.

UWS заявив, що став «жертвою кіберзлочину», і атака вплинула на низку цифрових систем і даних персоналу.

BBC Scotland дізналася, що інцидент вплинув на ноутбуки співробітників, вимкнув близько половини IT-систем університету та вплинув на роботу студентів.

Повідомлення про подію надійшло до поліції 6 липня.

У той час веб-сайт університету не працював, і з'явилося повідомлення про помилку з вибаченнями за «незручності». Хоча деякі розділи сайту згодом було відновлено, сторінки, включно з пізніми заявками, поданими в процесі очищення, все ще недоступні.

Спочатку жодне злочинне угруповання не взяло на себе відповідальність, але група програм-вимагачів, відома як Rhysida, заявила, що стоїть за інцидентом і, схоже, намагалася використати викрадені дані для вимагання університету.

Дані, які рекламуються в глибокому веб-доміні банди, включають особисті дані, що належать співробітникам, такі як банківські реквізити та номери національного страхування, а також внутрішні документи університету.

BBC може підтвердити, що список групи справжній, але не зміг перевірити достовірність даних.

Однак кіберкореспондент BBC Джо Тіді сказав, що це навряд чи фейк.

«Проте з мого досвіду немає підстав припускати, що вони брешуть», — сказав він. «Ці злочинні угруповання працюють на основі прибутку та репутації. На жаль, підробка вкрадених даних їм не підходить».

Представник UWS сказав, що деякі деталі «залишаються чутливими» у поточному кримінальному розслідуванні, але вони тісно співпрацюють з відповідними органами та «слідують контрольованому процесу, щоб працювати над вирішенням проблеми».

«Університет став жертвою кіберзлочину, який вплинув на низку цифрових систем», — йдеться в заяві університету. «Продовжуються вживати всіх необхідних заходів для врегулювання ситуації.

«Ми проводили брифінги для колег і студентів із початку цього інциденту та повідомили колег, що вдалося отримати доступ до деяких даних співробітників. З персоналом продовжують зв'язуватися напряму та надавати їм інформацію та підтримку».

За даними веб-сайту з кібербезпеки Sentinel One, групу програм-вимагачів Rhysida вперше помітили в травні цього року. Він здійснив атаки на численні організації по всьому світу.

У Sentinel One заявили, що група позиціонує себе як «команда з кібербезпеки», яка робить послугу своїм жертвам, націлюючись на їхні системи та висвітлюючи недоліки в їх онлайн-безпеці.

Бретт Каллоу, аналітик компанії з кібербезпеки Emisoft, сказав, що кібербанда, ймовірно, сподівається, що університет заплатить.

«Реально, дані, швидше за все, не мають такого значення, яке надає Rhysida — принаймні, не для третьої сторони», — сказав він.

«Вони сподіватимуться, що університет заплатить, щоб запобігти оприлюдненню інформації в темній мережі та використанню її іншими кіберзлочинцями для шахрайства». ***(Auryn Cox. Scottish university UWS targeted by cyber attackers // BBC (https://www.bbc.com/news/uk-scotland-glasgow-west-66327336?xtor=AL-72-%5Bpartner%5D-%5Bbbc.news.twitter%5D-%5Bheadline%5D-%5Bnews%5D-%5Bbizdev%5D-%5Bisapi%5D&utm_source=flipboard&utm_content=user%2FBBCNews). 28.07.2023).***

***

«Нещодавно ChatGTP привернув широке висвітлення в новинах завдяки своїм новаторським можливостям чат-бота зі штучним інтелектом. Але не встигли чорнило висохнути на таких звітах, як його можливості розширилися ще більше; і разом з цим прийшло кілька попереджень про ризики шахраїв і більш складного фішингу.

Розроблений OpenAI, ChatGTP тепер працює на базі потужнішого GTP-4 (випущеного 14 березня 2023 року). Оскільки розвиток генеративної технології штучного інтелекту не припиняється, юристів все частіше попереджають про зростаючі ризики.

Найвищим ризиком залишається фішинг, який дуже скоро може супроводжуватися голосами на користь.

Що таке фішинг?

Фішинг — це сучасний пристрій, який використовується для шахрайства та покладається на надсилання електронних листів нібито від справжніх організацій. Намір злочинців полягає в тому, щоб переконати одержувачів електронної пошти розкрити особисту інформацію, таку як паролі та фінансові дані.

Фішинг також використовується для встановлення програм-вимагачів або інших форм шкідливого програмного забезпечення на пристрої одержувача.

На жаль, фішингові електронні листи стають все більш витонченими і можуть, на перший погляд, виглядати цілком справжніми.

У юридичній практиці так зване «шахрайство у п’ятницю після обіду» є формою фішингу, особливо пов’язаного з юристами з нерухомості. Він спрямований на те, щоб спонукати клієнтів, які купують житло (які у Великій Британії часто вирішують завершити покупки в п’ятницю, тому це прізвисько) переказати кошти на покупку на рахунок, який вони вважають, що це рахунок їхньої юридичної фірми.

ГТП-4

GTP-4 вітають за чудові міркування та можливості розуміння мови; а також його голосові технології. Хоча він пропонує ще більше можливостей для справжнього бізнесу, така ж можливість для злочинців стати більш вправними у створенні програмного коду та доповнити фішингові електронні листи імітацією людських голосів.

Принаймні це відразу визнають: уже надходять повідомлення про те, що шахраї використовують генеративний штучний інтелект для клонування голосів. У Канаді, наприклад, Бенджамін Перкін говорив про те, як голосові технології, згенеровані штучним інтелектом, використовувалися для виманювання його літніх батьків на тисячі доларів.

Окремо Федеральна торгова комісія США також випустила попередження про клонування голосу злочинцями для увічнення шахрайства. Експерти з кібербезпеки попереджають, що GPT-4 може прискорити кіберзлочинність, наприклад, зробивши фішингове шахрайство ще небезпечнішим. Як це може вплинути на юридичні фірми?

Ризик для юридичних фірм

Одним із основних обов'язків юридичних фірм є впровадження належних заходів кібербезпеки для захисту від ризиків. У міру того як ці ризики змінюються, відповідні заходи кібербезпеки також мають змінюватися. Ключовою проблемою є дедалі складніше розпізнати фальшиву електронну пошту, не кажучи вже про фальшивий голос.

Голосова технологія штучного інтелекту настільки складна, що злочинці тепер можуть ідентифікувати та захопити справжній голос (наприклад) старшого юриста вашої фірми; імітувати його; і після фішингового електронного листа зателефонуйте жертві. Жертва не матиме підстав сумніватися в справжності голосу та дотримуватиметься наданих інструкцій (безсумнівно, передбачаючи розділення грошей та/або конфіденційної інформації).

Шахрайство у п'ятницю вдень і подібне фішингове шахрайство може скоро отримати темний поворот. Хоча ризики цих видів шахрайства неможливо усунути, знання та освіта є ключовими. Фірми повинні бути послідовними в забезпеченні

надійного навчання для юристів і допоміжного персоналу, щоб сприяти колективному усвідомленню нових і нових ризиків.

У березні цього року (до випуску GPT-4) Інститут Thomson Reuters опублікував результати опитування 443 середніх і великих юридичних фірм у США, Канаді та Великобританії, що призвело до його звіту, ChatGPT і Generative AI в рамках Юридичні фірми.

Переважна більшість респондентів (9 з 10) вказали на те, що вони знають ChatGPT і подібні, але лише 51% сказали, що їх дійсно варто використовувати в юридичній роботі. Але звіт також виявив різкий розрив між партнерами (80% з яких усвідомлювали ризики) і колегами та іншими молодшими юристами, лише половина з яких бачили ризики.

Розбіжність може відображати брак знань та усвідомлення загрози, яку створює генеративний штучний інтелект серед тих, хто займається юридичною практикою: це саме по собі слід вважати фактором ризику, яким можна ефективно керувати шляхом регулярного навчання.

Заключне слово

Юристам слід знати, що ризики, пов'язані з ChatGPT, GPT-4 і їм подібними, виходять далеко за рамки кіберзлочинності та шахрайства. Є, наприклад, наслідки для захисту даних і конфіденційності. Надані попередження не слід розглядати як просто налякування». ***(Jacy Whittaker and A. Kenra Parris-Whittaker. Phishing For Fraud Just Got Easier // ParrisWhittaker (https://parriswhittaker.com/news/phishing-for-fraud-just-got-easier/). 03.07.2023).***

***

«У искусственного интеллекта (ИИ) нет шансов воспроизвести человеческое творчество, необходимое для того, чтобы стать этичным хакером, но он изменит то, как хакеры проводят тестирование на проникновение и работают над программами вознаграждения за обнаружение ошибок, и уже повышает ценность хакерства. организациям, которые готовы взаимодействовать с хакерским сообществом, а не просто отвергать его.

Это согласно хакерам, которые внесли свой вклад в последний выпуск Inside the mind of a hacker (ITMOAH) — годовой отчет краудсорсинговой компании Bugcrowd, занимающейся тестированием на проникновение. и почему они делают то, что делают. Неудивительно, что в этом году большое внимание уделяется ИИ.

Когда дело дошло до экзистенциальных вопросов о том, может ли ИИ превзойти среднего хакера или сделать его бесполезным, 21% респондентов заявили, что ИИ уже превосходит их, а треть заявила, что сможет сделать это еще через пять лет или около того.

Подавляющее большинство, 78%, заявили, что ИИ изменит их работу по тестированию на проникновение или программам вознаграждения за ошибки где-то между настоящим моментом и 2028 годом, при этом 40% говорят, что он уже изменил способы взлома людей, а 91% хакеров говорят, что генеративный ИИ либо уже повысили или будут повышать ценность своей работы в будущем.

Превзойти человека, выполняющего повторяющуюся, иногда монотонную работу, такую как анализ данных, — это одно, но хакерство как призвание также поощряет творческое мышление, и именно здесь сообщество, похоже, считает, что люди по-прежнему будут иметь преимущество, с 72% говоря, что они не думали, что ИИ когда-либо сможет воспроизвести эти качества.

«Я довольно много сделал с ИИ, и каким бы впечатляющим он ни был, я не думаю, что он заменит людей в течение достаточно долгого времени, если вообще когда-либо», — сказал один респондент, ветеран кибербезопасности с 20-летним стажем, который занимается взломом. на платформе Bugcrowd с помощью дескриптора Nerdwell.

«ИИ очень хорош в том, что он делает — в распознавании образов и применении известных решений известных проблем», — сказал он. «Люди биологически созданы для поиска новизны и любопытства. Наш мозг буквально запрограммирован на творчество и поиск новых решений новых проблем».

Ошибки и проблемы

Другой хакер Bugcrowd, известный под псевдонимом OrwaGodfather, добавил: «ИИ — это здорово, но он не заменит меня. Есть некоторые ошибки и проблемы, как и любая другая технология.

«Однако это может повлиять на мое место в хакерстве. Например, у автоматизации есть огромный потенциал для помощи хакерам», — сказал ОрваКрестный отец, который начал заниматься хакерством в 2020 году и в свободное от клавиатуры время работает профессиональным поваром.

«Это может упростить задачу и сэкономить время», — сказал он. «Если я обнаружил ошибку при выполнении теста на проникновение и не хочу тратить 30 минут на написание отчета, я могу начать с использования ИИ для написания описаний для себя. ИИ ускоряет взлом».

Как хакеры используют ИИ?

Какими бы ни были их интуитивные чувства, хакеры Bugcrowd карабкаются на борт поезда ИИ, при этом 85% говорят, что они экспериментировали с технологией генеративного ИИ, а 64% уже каким-то образом включили ее в свои рабочие процессы безопасности, еще 30% заявили, что планируют сделать это в будущем.

Хакеры, которые внедрили или планируют внедрить генеративный ИИ, наиболее склонны использовать ChatGPT Open AI (клиент Bugcrowd), на который ссылаются 98% респондентов, а Bard от Google и Bing Chat AI от Microsoft — 40%.

Те, кто сделал решающий шаг, используют технологию генеративного ИИ самыми разными способами, причем наиболее часто используемыми функциями являются суммирование или генерация текста, генерация кода, улучшение поиска, чат-боты, генерация изображений, дизайн данных, сбор или суммирование, а также машинная обработка. обучение.

В частности, хакеры заявили, что в рамках рабочих процессов исследования безопасности генеративный ИИ наиболее полезен для автоматизации задач, анализа данных, а также выявления и проверки уязвимостей. Менее широко используемые приложения включали проведение разведки, классификацию угроз,

обнаружение аномалий, определение приоритетов рисков и построение моделей обучения.

Многие хакеры, не являющиеся носителями английского языка или плохо владеющие английским языком, также используют такие сервисы, как ChatGPT, для перевода или написания отчетов и сообщений об ошибках, а также для расширения сотрудничества между странами.

Что такое хакер?

За последнее десятилетие ежегодный отчет Bugcrowd также служил второстепенной цели, помогая гуманизировать хакерское сообщество и разрушить негативные и бесполезные стереотипы о том, кем на самом деле является хакер.

Это особенно важно, учитывая, что, несмотря на многолетнее противодействие и попытки просвещения, многие люди, которые должны знать лучше, с готовностью и намеренно объединяют термин «хакер» с термином «киберпреступник».

«Мы взяли на себя ответственность помочь рынку понять, что такое хакер на самом деле», — сказал Кейси Эллис, основатель Bugcrowd, главный технический директор и соавтор отчета Computer Weekly на недавней киберторговой выставке Infosecurity Europe.

«Я думаю, когда мы начинали, все думали, что это плохо», — сказал он. «Спустя 10 лет мы достигли точки, когда люди понимают, что хакерство на самом деле является набором навыков. Как и большинство наборов навыков, он имеет двойное назначение. Это как взлом замков. Если у вас есть этот навык, вы можете стать слесарем или грабителем. Нет ничего плохого во взломе замков — это то, как вы на самом деле его используете. Взлом — то же самое».

Дети в порядке?

В отчете ITMOAH за 2023 год показано, как некоторые фундаментальные сдвиги в хакерской культуре и демографии, похоже, встряхнут ландшафт кибербезопасности в ближайшие годы.

В отчете впервые показано, что большинство активных хакеров, от 55% до 60%, в настоящее время являются членами когорты поколения Z, в настоящее

время в возрасте от 20 до 20 лет, в то время как от 33% до 36% являются миллениалами в возрасте от их конца 20-х - начала 40-х годов.

И, несмотря на культурные корни хакерства в 1980-х годах, только 2% являются представителями поколения X, родившимися между серединой 1960-х и примерно 1980 годом, самому молодому из которых сейчас около 45 лет.

Итак, действительно ли стереотипы о хакерах-подростках верны, и, что более важно, все ли в порядке с детьми? «Мы наблюдаем довольно быстрое увеличение участия людей моложе 18 лет», — сказал Эллис. «Это все еще очень небольшое население, всего 6%, но оно выросло с 3% в годовом исчислении, что является большим сдвигом».

Он сказал, что эта тенденция будет становиться все более актуальной, потому что сегодняшние подростки думают о технологиях принципиально иначе, чем те, кто родился даже несколькими годами ранее.

«У меня есть 15-летняя дочь, и то, как она взаимодействует с технологиями, совершенно не похоже на меня, — сказал Эллис. «Ее знакомство с технологиями было связано с интерфейсом, а мое — с сантехникой. Мы просто думаем об Интернете совершенно по-другому.

«Теперь я знаю вещи, которые она никогда не узнает, потому что я выросла с гайками и болтами, но она будет думать об интерфейсе так, как я, вероятно, никогда не буду, потому что я так поглощен гайками и болтами.

«Вы говорите о миллениалах как о цифровых аборигенах, но поколение Z и моложе на самом деле являются цифровыми аборигенами», — сказал он. «Они могут бродить по этой среде интуитивно понятным способом, который мы не можем понять. Я могу попытаться сопереживать этому, и я могу достичь большей части этого, но я признаю тот факт, что никогда полностью не пойму, потому что это не мой опыт».

Это поколение также оказалось способным бросить вызов нравам и предположениям своих старших, которые часто были встроены в технологии, и Эллис сказал, что это дает им преимущество в выяснении того, что будет дальше и где могут быть уязвимости в будущем.

Другая часть этой тенденции заключается в том, что сегодняшние подростки более политически и социально мотивированы и более разнообразны, чем пожилые люди. Этот фактор уже меняет киберландшафт и, безусловно, будет продолжать это делать.

Возьмем, к примеру, Lapsus$, группу кибер-вымогателей, управляемую подростками, которая атаковала системы службы совместного использования поездок Uber в 2022 году без какой-либо особой причины, кроме того, что им было наплевать на этику Uber.

«Одна из важных вещей, о которых я говорил после Lapssus$, заключается в том, что мы, как защитники, не готовы к хаотическим действиям», — сказал Эллис. «Мы думали о киберпреступниках, национальных государствах, субъектах угроз как о симметричных мотивах.

«Национальное государство хочет продвигать нацию, киберпреступники хотят денег. Они предсказуемы. И в том, что они делают, есть симметрия. Люди, которые приходят с большей склонностью к активизму, на самом деле не знают, чего они хотят. А в случае с Lapsus$ это как… мы просто хотим устроить беспорядок, потому что эти парни отстой. Как вы защищаете от этого? Мы действительно не думали так со времен Lulzsec, который, вероятно, был последним примером группы, которая сделала это».

Конечно, подростки на платформе Bugcrowd не атакуют организации в том же смысле, что и Lapssus$, но в их истории есть урок для хакерского сообщества и защитников, а также явно потенциал для направления активности, которая в противном случае могла бы быть потрачена. на злонамеренные действия в законную работу по обеспечению безопасности огромен…» ***(Alex Scroxton. Hackers: We won’t let artificial intelligence get the better of us // TechTarget (https://www.computerweekly.com/news/366544396/Hackers-We-wont-let-artificial-intelligence-get-the-better-of-us?utm_source=flipboard&utm_content=erik6408%2Fmagazine%2FCybersecurity+and+Information+Security+Articles). 12.07.2023).***

***

«Кібербезпека стала критичною проблемою в епоху цифрових технологій, коли кіберзагрози прогресують із загрозливою швидкістю. Складний характер цих загроз і ландшафт кібербезпеки, що постійно розвивається, створюють серйозні проблеми для інформаційних наук і техніки. Тим не менш, дослідники та практики в цих галузях співпрацюють, щоб розробити інноваційні рішення, які можуть встигати за темпами змін і реагувати на зростаючі загрози. Ключовою проблемою кібербезпеки є постійна зміна природи кіберзагроз. З появою нових технологій кіберзлочинці знаходять нові способи використання вразливостей і отримання несанкціонованого доступу до мереж і систем. Наприклад, розповсюдження Інтернету речей (IoT) спричинило безліч проблем із безпекою, оскільки все більше пристроїв підключено до мереж і, отже, чутливі до компрометації.

Щоб вирішити ці проблеми, інформатика та інженерія використовують передові технології, такі як машинне навчання та штучний інтелект (ШІ). Ці технології допомагають ідентифікувати моделі та аномалії в мережевому трафіку та поведінці, які можуть вказувати на потенційну атаку. Алгоритми машинного навчання можуть аналізувати величезні обсяги даних із мережевих журналів, виявляти незвичайну активність і сповіщати персонал служби безпеки про потенційні загрози. Подібним чином платформи аналізу загроз на основі штучного інтелекту можуть постійно стежити за новими загрозами в Інтернеті та оновлювати системи безпеки найновішою інформацією.

Ще одним перспективним напрямком досліджень є технологія блокчейн. Блокчейни — це розподілені реєстри, які дозволяють багатьом сторонам перевіряти та записувати транзакції без необхідності центрального органу. Це робить їх ідеальними для захисту цифрових транзакцій і записів. У сфері кібербезпеки блокчейни можуть сприяти створенню децентралізованих систем безпеки, більш стійких до злому та втручання. Наприклад, система автентифікації на основі блокчейну може усунути потребу в паролях та інших вразливих методах автентифікації.

Одним із інноваційних застосувань технології блокчейн є захист пристроїв Інтернету речей (IoT). Пристрої Інтернету речей, такі як інтелектуальні термостати, камери безпеки та медичні пристрої, стають все більш поширеними та часто не мають належних заходів безпеки. Ці пристрої вразливі до кібератак, які можуть мати серйозні наслідки в таких критично важливих програмах, як охорона здоров'я. Технологію блокчейн можна використовувати для захисту пристроїв IoT шляхом створення децентралізованої мережі довіри, яка забезпечує безпечний зв'язок і обмін даними між пристроями. У мережі IoT на основі блокчейну кожен пристрій має унікальну цифрову ідентичність, яка перевіряється блокчейном. Коли пристрій обмінюється даними з іншим пристроєм, блокчейн перевіряє цифрову ідентичність обох пристроїв і забезпечує безпеку зв'язку.

Інформатика та інженерія також просувають існуючі рішення кібербезпеки. Традиційного антивірусного програмного забезпечення вже недостатньо для захисту від складних загроз. Щоб вирішити цю проблему, дослідники кібербезпеки розробляють більш просунуті рішення для захисту кінцевих точок, які використовують аналіз поведінки та алгоритми машинного навчання для виявлення та реагування на загрози в режимі реального часу. Хмарна безпека є ще однією сферою уваги, оскільки все більше компаній переносять свої дані та програми в хмару. Постачальники рішень працюють разом над розробкою хмарних рішень безпеки, які забезпечують наскрізне шифрування, постійний моніторинг і розширене виявлення загроз.

Незважаючи на ці багатообіцяючі розробки, майбутнє кібербезпеки залишається невизначеним. Оскільки кіберзагрози продовжують розвиватися та стають все більш витонченими, вкрай важливо, щоб інформаційні науки та інженерія були на випередженні та розробляли нові рішення для забезпечення безпеки мереж і систем. Одним із можливих рішень є зосередження на освіті та обізнаності з кібербезпеки. Багато кібератак є результатом людської помилки, наприклад, натискання співробітниками фішингових посилань або використання ненадійних паролів. Навчання співробітників і громадськості найкращим практикам кібербезпеки може зменшити ймовірність таких типів атак і зробити

мережі та системи більш безпечними. Інший підхід полягає в сприянні співпраці між різними зацікавленими сторонами в екосистемі кібербезпеки, включаючи державні установи, приватні компанії та наукові установи. Працюючи разом, ми можемо ділитися знаннями та досвідом і розробляти більш ефективні рішення кібербезпеки.

На завершення можна сказати, що майбутнє кібербезпеки є водночас захоплюючим і складним. Інформатика та інженерія співпрацюють, щоб розробити інноваційні рішення, які можуть встигати за темпами змін і реагувати на зростаючі загрози. Від машинного навчання та штучного інтелекту до технології блокчейн і хмарної безпеки, на горизонті багато перспективних розробок. Однак надзвичайно важливо продовжувати зосереджуватися на освіті та співпраці, щоб залишатися на випередженні та забезпечити безпечне цифрове майбутнє». ***(The Future of cybersecurity; how information Science and Engineering is responding to growing threats // The Indian Express [P] Ltd. (https://www.financialexpress.com/education-2/the-future-of-cybersecurity-how-information-science-and-engineering-is-responding-to-growing-threats/3171077/). 15.07.2023).***

***

«У мережі почав роботу своєрідний аналог чат-бота ChatGPT, який не має жодних обмежень для видачі результатів і може стати черговим інструментом для написання шкідливих програм навіть тими, хто не розуміється на програмуванні, повідомляє PC Mag. Розробник чат-бота WormGPT вже продає до нього доступ і стверджує, що його творіння може допомогти хакерам проводити фішингові атаки та створювати інструменти для злому.

Чат-бот WormGPT доступний за передплатою на одному з хакерських форумів, і, за словами фахівців з комп'ютерної безпеки зі SlashNext, які спробували чат-бот у справі, зловмисники навчилися створювати свої власні модулі, схожі на ChatGPT, але простіші у використанні.

На відміну від ChatGPT або Google Bard, WormGPT не має будь-яких обмежень, що заважають йому відповідати на шкідливі запити користувача. «Цей проєкт націлений на те, щоб надати альтернативу ChatGPT, яка дасть вам змогу здійснювати всілякі незаконні дії та легко продавати їх в Інтернеті в майбутньому», — написав сам таємничий розробник програми.

Ця людина також завантажила скріншоти, які показують, що ви можете попросити бота створити шкідливе ПЗ, написане мовою програмування Python, і дати поради щодо створення шкідливих атак. За словами розробника, для створення чат-бота використовувалася старіша версія LLM (великої мовної моделі) з відкритим вихідним кодом під назвою GPT-J від 2021 року. Потім модель навчили на даних про створення шкідливих програм, унаслідок чого з'явився WormGPT.

Фахівці зі SlashNext випробували WormGPT і перевірили, чи може бот написати переконливий електронний лист для фішингової атаки (підроблений лист, який змушує жертву відкрити шкідливе посилання або встановити шкідливе ПЗ). «Результати були тривожними. WormGPT створив електронного листа, який був не тільки напрочуд переконливим, а й стратегічно хитрим», — сказали експерти SlashNext.

Дійсно, бот створив повідомлення, використовуючи професійну мову, який закликав передбачувану жертву перевести трохи грошей. WormGPT також написав електронного листа без будь-яких орфографічних або граматичних помилок, що, зазвичай, є одним із показників підробки.

«Підбиваючи підсумок, можна сказати, що він дуже схожий на ChatGPT, але не має етичних кордонів або обмежень», — кажуть експерти SlashNext. — "Цей експеримент підкреслює значну загрозу, яку становлять технології генеративного ШІ, такі як WormGPT, навіть у руках кіберзлочинців-початківців».

На щастя, WormGPT коштує недешево. Розробник продає доступ до бота за $67 на місяць, і один покупець також поскаржився, що програма «не варта ні копійки», посилаючись на низьку продуктивність. Проте WormGPT є зловісною ознакою того, як генеративні програми штучного інтелекту можуть підживлювати

кіберзлочинність, особливо в міру розвитку штучного інтелекту». ***(Пилип Бойко. Ні сорому, ні совісті. Новий чат-бот позбавлений етичних обмежень: чим він небезпечний для людей // Фокус (https://focus.ua/uk/digital/579921-ni-soromu-ni-sovisti-novij-chat-bot-pozbavlenij-etichnih-obmezhen-chim-vin-nebezpechnij-dlya-lyudej). 19.07.2023).***

***

«Компанії штучного інтелекту, включаючи OpenAI, Alphabet (GOOGL.O) і Meta Platforms (META.O), добровільно зобов'язалися перед Білим домом впровадити такі заходи, як позначення водяних знаків на створеному штучним інтелектом контенті, щоб зробити цю технологію безпечнішою, оголосив у п'ятницю президент Джо Байден.

«Ці зобов'язання є багатообіцяючим кроком, але нам потрібно ще багато працювати разом», — сказав Байден.

На заході в Білому домі Байден звернувся до зростаючої стурбованості з приводу потенціалу використання штучного інтелекту для руйнівних цілей, сказавши, що «ми маємо бути чіткими очима та пильними щодо загроз від нових технологій» для американської демократії.

Компанії, до яких також входять Anthropic, Inflection, Amazon.com (AMZN.O) і партнер OpenAI Microsoft (MSFT.O), пообіцяли ретельно тестувати системи перед їх випуском і ділитися інформацією про те, як зменшити ризики та інвестувати в кібербезпеку.

Цей крок розглядається як перемога для зусиль адміністрації Байдена щодо регулювання технології, яка пережила бум інвестицій і популярності серед споживачів.

«Ми вітаємо лідерство президента в об'єднанні технологічної індустрії, щоб виробити конкретні кроки, які допоможуть зробити штучний інтелект безпечнішим, безпечнішим і кориснішим для суспільства», — йдеться в повідомленні Microsoft у п'ятницю в блозі.

Оскільки генеративний штучний інтелект, який використовує дані для створення нового контенту, як-от гуманна проза ChatGPT, став шалено популярним цього року, законодавці в усьому світі почали розглядати, як пом’якшити небезпеку нової технології для національної безпеки та економіки.

США відстають від ЄС у боротьбі з регулюванням штучного інтелекту. У червні законодавці ЄС погодили набір проектів правил, згідно з якими такі системи, як ChatGPT, повинні будуть розкривати контент, створений штучним інтелектом, допомагати відрізняти так звані підроблені зображення від справжніх і забезпечувати захист від незаконного контенту.

Більшість у Сенаті США Чак Шумер у червні закликав до «всеосяжного законодавства» для просування та забезпечення гарантій щодо штучного інтелекту.

Конгрес розглядає законопроект, який вимагатиме від політичної реклами повідомляти, чи використовувався штучний інтелект для створення зображень чи іншого контенту.

Байден, який приймав керівників семи компаній у Білому домі в п’ятницю, сказав, що він також працює над розробкою виконавчого указу та двопартійного законодавства щодо технології ШІ.

«Ми побачимо більше технологічних змін у наступні 10 років або навіть у наступні кілька років, ніж ми бачили за останні 50 років. Це було для мене вражаючим відкриттям, відверто кажучи», — сказав Байден.

У рамках зусиль сім компаній взяли на себе зобов’язання розробити систему «водяних знаків» для всіх форм вмісту, від тексту, зображень, аудіо до відео, створених ШІ, щоб користувачі знали, коли технологія була використана.

Цей водяний знак, вбудований у вміст технічним способом, імовірно, полегшить користувачам виявлення глибоко підроблених зображень або аудіо, які можуть, наприклад, демонструвати насильство, якого не було, створювати кращу аферу або спотворювати фотографію політика, щоб виставити людину в невтішному світлі.

Незрозуміло, як водяний знак буде видно під час обміну інформацією.

Компанії також пообіцяли зосередитися на захисті конфіденційності користувачів у міру розвитку штучного інтелекту та на забезпеченні того, щоб технологія була вільною від упереджень і не використовувалася для дискримінації вразливих груп. Серед інших зобов'язань – розробка рішень ШІ для таких наукових проблем, як медичні дослідження та пом'якшення кліматичних змін». ***(Diane Bartz, Krystal Hu. OpenAI, Google, others pledge to watermark AI content for safety, White House says // Reuters (https://www.reuters.com/technology/openai-google-others-pledge-watermark-ai-content-safety-white-house-2023-07-21/). 21.07.2023).***

***

«Хакери та пропагандисти використовують штучний інтелект (ШІ), щоб створювати шкідливе програмне забезпечення, складати переконливі фішингові електронні листи та поширювати дезінформацію в Інтернеті, заявив агентству Reuters високопосадовець відділу кібербезпеки Канади, що свідчить про те, що технологічна революція, яка охопила Кремнієву долину, також була підхоплена кіберзлочинцями.

Цього тижня в інтерв'ю керівник Канадського центру кібербезпеки Самі Хоурі сказав, що його агентство бачило використання штучного інтелекту «у фішингових електронних листах або більш цілеспрямованому створенні електронних листів у шкідливому коді (і) в дезінформації та дезінформації».

Хурі не надав подробиць чи доказів, але його твердження про те, що кіберзлочинці вже використовують ШІ, додає гострої нотки до хору занепокоєння з приводу використання нової технології шахраями.

Останніми місяцями кілька кібернаглядових груп опублікували звіти, в яких попереджали про гіпотетичні ризики штучного інтелекту, особливо швидко розвиваються програми обробки мови, відомі як великі мовні моделі (LLM), які використовують величезні обсяги тексту для створення переконливо звучать діалогів, документів тощо.

У березні європейська поліцейська організація Європол опублікувала звіт, у якому говориться, що такі моделі, як ChatGPT OpenAI, дозволили «видавати себе за

організацію чи особу в дуже реалістичній манері, навіть якщо вони лише базово володіють англійською мовою». Того ж місяця Британський національний центр кібербезпеки заявив у дописі в блозі, що існує ризик того, що злочинці «можуть використовувати LLM для допомоги в кібератаках за межами своїх поточних можливостей».

Дослідники з кібербезпеки продемонстрували низку потенційно зловмисних випадків використання, і деякі тепер кажуть, що вони починають бачити ймовірно створений штучним інтелектом контент у дикій природі. Минулого тижня колишній хакер сказав, що виявив LLM, який навчався на шкідливому матеріалі, і попросив його скласти переконливу спробу обманом змусити когось здійснити грошовий переказ.

LLM відповів електронним листом із трьох абзаців із проханням допомоги з терміновим рахунком-фактурою.

«Я розумію, що це може бути невдовзі, — сказав LLM, — але цей платіж надзвичайно важливий і має бути здійснений протягом наступних 24 годин».

Хоурі сказав, що хоча використання штучного інтелекту для розробки шкідливого коду все ще перебуває на ранніх стадіях — «ще є шлях, оскільки для написання хорошого експлойту потрібно багато часу», — викликає занепокоєння те, що моделі штучного інтелекту розвиваються настільки швидко, що важко зрозуміти їхній шкідливий потенціал до того, як їх випустять у дику природу.

«Хто знає, що чекає за рогом», — сказав він». ***(Raphael Satter. Exclusive: AI being used for hacking and misinformation, top Canadian cyber official says // Reuters (https://www.reuters.com/technology/ai-being-used-hacking-misinfo-top-canadian-cyber-official-says-2023-07-20/). 21.07.2023).***

***

«Швидка еволюція штучного інтелекту (ШІ) призвела до значного прогресу в різних секторах. Однак кіберзлочинці можуть використати ту саму технологію, яка зараз є джерелом нашого повсякденного життя. Насправді ми вже знаємо, що ШІ використовують хакери. Нещодавній сплеск атак соціальної

інженерії, що використовують генеративну технологію штучного інтелекту, викликав тривогу в спільноті кібербезпеки.

Generative AI, прикладом якого є такі інструменти, як ChatGPT OpenAI, використовує машинне навчання для створення тексту, відео, аудіо та зображень, схожих на людину. Хоча ці інструменти мають багато корисних застосувань, вони також використовуються зловмисниками для здійснення складних атак соціальної інженерії. Розширені лінгвістичні можливості та доступність генеративних інструментів штучного інтелекту створюють живильне середовище для кіберзлочинців, що дозволяє їм створювати переконливі шахрайства, які дедалі важче виявити.

Крім того, генеративний ШІ може автоматизувати персоналізацію атак соціальної інженерії в масовому масштабі. Ця подія викликає особливе занепокоєння, оскільки вона підриває один із наших найпотужніших засобів захисту від таких загроз — автентичність. Перед обличчям фішингу та подібних атак наша здатність відрізнити справжні повідомлення від шахрайських часто є нашою останньою лінією захисту. Однак, оскільки штучний інтелект стає більш вправним у імітації людського спілкування, наш «радар BS» стає менш ефективним, роблячи нас більш уразливими до цих атак.

Як кіберзлочинці використовують генеративний штучний інтелект

Нещодавно опубліковане дослідження Darktrace виявило зростання атак соціальної інженерії з використанням генеративного штучного інтелекту на 135%. Кіберзлочинці використовують ці інструменти для злому паролів, витоку конфіденційної інформації та обману користувачів на низці платформ. Це нове покоління шахрайства викликало сплеск занепокоєння серед працівників: 82% висловили побоювання стати жертвою цих обманів.

У цьому контексті загроза штучного інтелекту полягає в тому, що він суттєво знижує або навіть усуває бар’єр доступу до шахрайства та схем соціальної інженерії. Носії мови, які не є рідною або мають низькі навички, отримують користь від генеративного штучного інтелекту, який дозволяє їм вести текстові розмови будь-якою мовою без помилок. Загроза штучного інтелекту в цьому

контексті полягає в тому, що він суттєво знижує або навіть усуває бар'єр доступу до схем шахрайства та соціальної інженерії. Носії мови, які не є рідною або мають низькі навички, отримують користь від генеративного штучного інтелекту, який дозволяє їм вести текстові розмови будь-якою мовою без помилок. Це значно ускладнює виявлення та захист від фішингових схем.

Generative AI також може допомогти зловмисникам обійти інструменти виявлення. Це дозволяє плідно створювати те, що можна розглядати як «творчу» варіацію. Кібер-зловмисник може використовувати його для створення тисяч різних текстів, усі унікальні, минаючи спам-фільтри, які шукають повторювані повідомлення.

На додаток до письмового спілкування, інші механізми штучного інтелекту можуть створювати авторитетні розмовні слова, які можуть імітувати конкретних людей. Це означає, що голос по телефону, який виглядає як ваш бос, цілком може бути інструментом для імітації голосу на основі ШІ. Організації повинні бути готові до більш складних атак соціальної інженерії, які є багатогранними та креативними, наприклад електронною поштою, за якою слідує дзвінок, що імітує голос відправника, і все це має послідовний і професійно звучачий вміст.

Розвиток генеративного штучного інтелекту означає, що погані актори з обмеженими знаннями англійської можуть швидко створювати переконливі повідомлення, які здаються більш автентичними. Раніше електронний лист із граматичними помилками, який нібито надійшов від вашого страхового агентства, негайно визнавався шахрайським і негайно ігнорувався. Однак удосконалення генеративного штучного інтелекту суттєво усунуло такі явні індикатори, що ускладнило користувачам розрізнення між справжніми повідомленнями та шахрайством.

Дійсно, такі інструменти, як Chat-GPT, мають вбудовані обмеження, призначені для запобігання зловмисному використанню. Наприклад, OpenAI реалізував засоби захисту, щоб запобігти створенню невідповідного або шкідливого вмісту. Однак, як показали нещодавні випадки, ці запобіжні заходи не є надійними. Примітним прикладом є випадок, коли користувачі змогли обманом

змусити ChatGPT надати ключі активації Windows, попросивши його розповісти історію перед сном, яка включала їх. Цей інцидент підкреслює той факт, що хоча розробники штучного інтелекту докладають зусиль, щоб обмежити шкідливе використання, зловмисники постійно знаходять способи обійти ці обмеження, доводячи, що засоби захисту інструментів штучного інтелекту не є захисним механізмом, на який ми можемо розраховувати.

Як захистити себе та свою організацію від атак соціальної інженерії, керованих ШІ

Захист від цих загроз є багатогранним. Організаціям необхідно використовувати засоби захисту від шахрайства в реальному часі, здатні виявляти більше, ніж звичайні червоні прапорці, які кричать про шахрайство. Деякі експерти пропонують боротися з вогнем вогнем і використовувати передові методи навчання для визначення підозрілих спроб і потенційного виявлення згенерованих ШІ фішингових текстів.

Щоб захиститися від атак соціальної інженерії, керованих штучним інтелектом, і забезпечити надійну особисту безпеку, ми повинні застосувати багатогранний підхід. Це включає використання надійних і унікальних паролів, увімкнення двофакторної автентифікації, обережність щодо небажаних повідомлень, оновлення програмного забезпечення та систем, а також ознайомлення з останніми загрозами та тенденціями кібербезпеки.

Хоча поява безкоштовного, простого та доступного ШІ приносить величезну користь кібер-зловмисникам, рішенням є кращі інструменти та краща освіта — краща кібербезпека навколо. Сектор має започаткувати стратегії, які протистоять машині проти машини, а не людині проти машини. Щоб досягти цього, нам потрібно розробити складні системи виявлення, здатні ідентифікувати загрози, створені штучним інтелектом, таким чином зменшуючи тривалість ідентифікації та вирішення атак соціальної інженерії, що походять від генеративного штучного інтелекту.

Підсумовуючи, стрімкий розвиток технології генеративного ШІ створює як можливості, так і ризики. Рухаючись вперед, зростаючий ризик соціального

маніпулювання через тактику, збагачену штучним інтелектом, потребує підвищеної обізнаності та обережності як від окремих осіб, так і від організацій. Вони повинні використовувати комплексні стратегії кібербезпеки, щоб перехитрити потенційних противників. Ми вже живемо в епоху, коли генеративний штучний інтелект використовується в кіберзлочинній діяльності, тому важливо залишатися пильними, готовими протидіяти цим загрозам, використовуючи всі доступні ресурси». ***(Yehuda Leibler. The Rising Threat of Generative AI in Social Engineering Cyber Attacks — What You Need to Know // Entrepreneur Media, LLC (https://www.entrepreneur.com/science-technology/how-cyber-criminals-are-weaponizing-generative-ai/455896?utm_source=flipboard&utm_content=jazzilla%2Fmagazine%2FAI+TODAY+AI). 27.07.2023).***

***

«Запровадження прогнозного технічного обслуговування (PM), стратегії штучного інтелекту (AI), яка передбачає потенційні збої обладнання за допомогою датчиків Інтернету речей (IoT), має величезні перспективи для будівельної галузі. …використання PM у будівництві також наражає компанії на нові ризики, включаючи підвищену загрозу кібербезпеці та нові юридичні питання. Нижче наведено детальний огляд ризиків, які представляють PM для будівельного сектора.

Ризики кібербезпеки

Зростання впровадження PM одночасно посилює потенційні загрози кібербезпеці. Великі обсяги переданих і збережених даних у поєднанні зі зростаючим ризиком витоку даних і кібератак викликають серйозні занепокоєння. Одним із потенційних видів атак є отруєння даних, коли зловмисник маніпулює даними, які використовуються для навчання системи ШІ. Вводячи оманливі або неправильні дані в навчальний набір, зловмисник може змусити систему штучного інтелекту зробити неправильні прогнози або вжити невідповідних дій. Якщо дані, які використовуються для навчання системи штучного інтелекту, відповідальної за

РМ у будівельній галузі, отруєні, це може призвести до несподіваної відмови критичного обладнання. Це може призвести до небезпечних ситуацій, таких як обвалення конструкцій або поломка обладнання, які можуть завдати шкоди працівникам на місці. Подібно до отруєння даних, змагальні атаки передбачають введення ретельно розроблених вхідних даних, призначених для омани системи ШІ. Наприклад, зловмисник може змінити дані з датчика, який використовується для РМ, таким чином, що система AI сприйматиме машину як таку, що знаходиться в хорошому робочому стані, тоді як вона насправді ось-ось вийде з ладу.

І, нарешті, є атаки на інфраструктуру, націлені на системи штучного інтелекту, які покладаються на складну інфраструктуру, включаючи системи зберігання даних, процесори та мережі для зв'язку. Атаки на ці системи, такі як атаки на відмову в обслуговуванні або фізичне втручання в пристрої IoT, можуть порушити функціонування системи ШІ. Будь-яка атака на фізичну інфраструктуру систем штучного інтелекту, наприклад втручання в роботу датчиків, камер або інших пристроїв Інтернету речей, може призвести до неправильної інтерпретації даних і, отже, до неправильних дій. Це може призвести до неправильної конструкції або нездатності визначити важливі потреби в обслуговуванні, що призведе до фізичного пошкодження.

Уразливості Інтернету речей

Пристрої IoT, які є основними джерелами даних для керованих штучним інтелектом систем технічного обслуговування, представляють значні вразливості в кібербезпеці, якщо вони не захищені належним чином. Незважаючи на те, що вони безцінні для РМ, ці пристрої, починаючи від простих датчиків машин і закінчуючи складними носіями, мають кілька слабких місць через їх невід'ємний дизайн і функції. У разі успішного зламу кіберзлочинці можуть маніпулювати функціями пристрою IoT, надати неправдиві дані або спричинити збій системи. Вони також можуть використовувати ці пристрої як плацдарм для ширших мережевих атак, викрадання даних або навіть для створення ботнету для широкомасштабних атак.

Насамперед обмежена обчислювальна потужність і сховище пристроїв IoT становлять суттєву проблему. Їхня конструкція в першу чергу відповідає їхнім

конкретним функціям, залишаючи мало місця для розширених функцій безпеки. Крім того, їхня фізична доступність робить їх сприйнятливими до прямих атак, наприклад встановлення зловмисного програмного забезпечення, яке може скомпрометувати всю мережу. Фізична безпека за допомогою заходів захисту та спостереження може зменшити такі ризики. Крім того, їх пряме з'єднання з мережею організації може служити точкою входу для атак у всій мережі. Безперервна передача даних багатьох пристроїв IoT також робить їх потенційними центрами для перехоплення конфіденційної інформації.

Відповідність законодавству та нормативним вимогам щодо РМ

Інтеграція РМ у будівництво створює складні правові та нормативні наслідки, зокрема щодо конфіденційності даних, відповідальності та окремих галузевих норм. РМ значною мірою покладається на збір, зберігання та аналіз даних. Це робить процес підпорядкованим різним законам про конфіденційність даних. Ключовими серед них є такі нормативні акти, як Загальний регламент ЄС щодо захисту даних (GDPR) і Каліфорнійський закон про права на конфіденційність (CPRA), обидва з яких вимагають, щоб компанії гарантували, що дані, які використовуються для РМ, є анонімними, коли це можливо, а також зберігаються й обробляються певними способами. Недотримання вимог може призвести до значних штрафів і завдати шкоди репутації компанії.

Прем'єр також піднімає складні питання відповідальності. Якщо машина виходить з ладу, незважаючи на те, що РМ вказує інше, хто несе відповідальність? Це будівельна компанія, розробник системи ШІ чи виробник машин? Для уточнення розподілу зобов'язань необхідно скласти комплексні договори. Крім того, слід розрізняти, чи є система штучного інтелекту продуктом чи послугою, оскільки це визначає застосовні закони про відповідальність. Якщо система штучного інтелекту класифікується як продукт, тоді вступають у дію закони про відповідальність за продукт. Якщо це вважається послугою, застосовуються інші правила.

Крім загальної відповідальності та занепокоєння конфіденційністю даних, РМ також може підпадати під дію галузевих правил. Наприклад, у будівництві

стандарти безпеки та найкращі практики можуть впливати на те, як розгортаються та використовуються системи РМ. Ці вказівки можуть формувати зібрані дані, спосіб їх аналізу та дії, вжиті на основі думок РМ. Дотримання цих стандартів має вирішальне значення для юридичної та операційної ефективності». ***(Sinan Pismisoglu. Cybersecurity Risks to AI Adoption in Construction // Bradley Arant Boult Cummings LLP. (https://www.buildsmartbradley.com/2023/07/cybersecurity-risks-to-ai-adoption-in-construction/#page=1). 27.07.2023).***

***

Кіберзлочинність та кібертероризм

«Повідомляється, що платіжний гігант Revolut зазнав кібератаки, в результаті якої компанія втратила близько 20 мільйонів доларів.

У звіті Financial Times із посиланням на кількох неназваних людей, нібито знайомих з інцидентом, зазначено, що вкрадені гроші належали компанії, а не її клієнтам.

Порушення не було оприлюднено, і Revolut вирішив не коментувати напад.

Здається, існує велика розбіжність між тим, як Revolut працює в США, і тим, як він працює в Європі. Помилка, що виникла в результаті, дозволяла користувачам відхиляти платіж, а потім Revolut повертати гроші, які так і не були надіслані. Помилка, очевидно, була вперше помічена наприкінці 2021 року, але перш ніж Revolut змогла залатати діру, кіберзлочинці знайшли її та почали використовувати. Схоже, що зловмисне програмне забезпечення не було задіяно.

Як виявилося, кіберзлочинці заохочували людей робити дорогі покупки, від яких їм було відмовлено, а потім знімали повернуті гроші з банкоматів. Близько 23 мільйонів доларів було надіслано від Revolut таким чином, але компанії вдалося повернути приблизно 3 мільйони доларів, здавалося б.

Деякі звіти стверджують, що Revolut навіть спочатку не знав, що його пограбували, і що він зрозумів лише після того, як банк-партнер у США заявив, що він тримає менше грошей, ніж очікувалося. Тоді американська дочірня компанія

попросила грошову ін’єкцію у «мільйонах доларів» від своєї материнської компанії, перш ніж закрити недолік навесні минулого року.

Revolut — це глобальна фінансово-технологічна компанія, яка пропонує банківські послуги, також відомі як «необанки». Компанія має ліцензію та регулюється Банком Литви в Європейському Союзі, а її штаб-квартира знаходиться в Лондоні, Великобританія. Компанія Revolut була заснована в 2015 році Миколою Сторонським і Владом Яценком.

Окрім «традиційних» банківських послуг, Revolut також дозволяє своїм користувачам заглиблюватись у криптовалюти та навіть торгувати на платформі». ***(Sead Fadilpašić. Hackers steal millions after cracking Revolut payment systems // Future US, Inc. (https://www.techradar.com/pro/hackers-steal-millions-after-cracking-revolut-payment-systems?utm_source=flipboard&utm_content=other). 10.07.2023).***

***

«Новый координатор по кибербезопасности Австралии подтвердил, что массовый взлом HWL Ebsworth затронул несколько правительственных ведомств и агентств.

В прошлом месяце российские киберпреступники, известные как AlphV или BlackCat, заявили, что разместили более 1 терабайта украденных данных в даркнете после взлома юридической фирмы в конце апреля.

В своем первом комментарии с момента вступления в должность национального координатора по кибербезопасности Даррен Голди сообщил новые подробности о взломе.

«Кибер-инцидент HWL Ebsworth затронул ряд правительственных организаций Австралии, в результате чего была раскрыта конфиденциальная личная и государственная информация», — сказал он.

«Я активно взаимодействую с HWL Ebsworth, чтобы понять полную картину этого инцидента, в том числе то, как пострадали их частные отраслевые клиенты, поскольку анализ данных продолжается.

«Пострадавшие организации начинают процесс уведомления пострадавших лиц о влиянии утечки данных на их информацию».

В число клиентов фирмы входят большая четверка банков и федеральное министерство здравоохранения.

Маршал авиации Голди сказал, что он продолжает проводить встречи с HWL Ebsworth, чтобы координировать ответ на взлом.

«Мы будем работать над тем, чтобы извлечь уроки из этого инцидента, чтобы мы могли продолжать коллективно реагировать на киберинциденты», — сказал он.

Объявляя о назначении национального координатора по кибербезопасности, министр внутренних дел Клэр О'Нил сказала, что взлом юридической фирмы был «очень значительным инцидентом».

«9 июня 2023 года нам стало известно, что злоумышленник опубликовал на своем даркнет-форуме по крайней мере некоторые данные, которые, по их утверждению, были получены», — говорится в заявлении компании на своем веб-сайте.

«Конфиденциальность и безопасность данных наших клиентов и сотрудников по-прежнему имеют для нас первостепенное значение». ***(Matthew Doran. HWL Ebsworth hack affected government departments, cyber security coordinator says // ABC (https://www.abc.net.au/news/2023-07-05/massive-law-firm-hack-government-agencies-darren-goldie-cyber/102567042). 05.07.2023).***

***

«Злоумышленники так неустанно внедряют новые методы взлома, что киберзащита, реализованная в 2022 году, уже ослабла, а в 2024 году ожидаются еще более серьезные атаки. Большинство кибербезопасности лидеров (71%) говорят, что их организации столкнулись с тремя или более инцидентами безопасности за последний год. один.

В прошлом году число попыток проникновения программ-вымогателей сократилось на 30%, поскольку злоумышленники перешли к новым стратегиям атак, которые оказались более прибыльными и менее обнаруживаемыми. По мере

того, как злоумышленники опережают нынешнее поколение платформ безопасности, общая активность атак продолжает расти, несмотря на то, что бюджеты также растут в условиях неопределенной экономической ситуации.

Отчет Scale Venture Partners (SVP) Cybersecurity Perspectives 2023 дает представление о многих проблемах, с которыми сталкиваются директора по информационной безопасности. К ним относятся растущая изощренность атак, нехватка специалистов, геополитическая напряженность и перегруженность команд безопасности. В отчете говорится, что директора по информационной безопасности удваивают усилия по защите сети, IAM и облачных вычислений, чтобы лучше защититься от атак на основе идентификации.

Директора по информационной безопасности борются с кражей личных данных

Растущая зависимость организаций от множества облачных сервисов создает привлекательную цель для взлома для злоумышленников, которые используют предлог и социальную инженерию для кражи учетных данных привилегированного доступа. Опрос SVP показал, что 50 % лидеров по безопасности говорят, что их учетные записи облачных сервисов подвергались атакам в прошлом году. Это согласуется с отчетом CrowdStrike о глобальных угрозах за 2023 год.

CrowdStrike обнаружил, что использование брешей в облачной инфраструктуре — чаще всего кража учетных данных, удостоверений личности и данных — выросло на 95% в 2022 году, а количество случаев, связанных с «облачными» злоумышленниками, утроилось по сравнению с прошлым годом. Злоумышленники стремятся изменить процессы аутентификации, чтобы атаковать удостоверения.

«Особенно популярной тактикой было злоупотребление скомпрометированными учетными данными, полученными с помощью похитителей информации или купленными в криминальном подполье, что отражает растущий интерес к таргетированию личных данных, который мы также наблюдали в прошлом году: наш отчет за 2022 год показал, что 80% кибератак

использовали методы, основанные на личных данных, — пишет соучредитель и генеральный директор CrowdStrike Джордж Курц.

Идентичность находится в осаде, и директора по информационной безопасности расставляют приоритеты в своих расходах в ответ. взять под контроль управление идентификацией и доступом (IAM) — сложная проблема, особенно когда организация полагается на несколько облачных сервисов По словам Ариэля Цейтлина, партнера SVP, в недавнем интервью VentureBeat. Количество фирм, скомпрометированных фишинговыми атаками, в ходе которых украли учетные данные сотрудников через облачные сервисы, выросло на 58%.

«Идентификация — это то, к чему стремится безопасность… потому что там гораздо больше ценных данных», — сказал Цейтлин VentureBeat. IAM переместился с восьмого места на второе в рейтинге инвестиционных приоритетов этого года, отражая растущую обеспокоенность рынка по поводу безопасности идентификации в многооблачных технологических стеках. войдет в тройку главных приоритетов расходов предприятий 2023 в, остаются такими же году IAM опросе, и инфраструктуры Сетевая безопасность и безопасность облачной как и в прошлогоднем кибербезопасность на. Identity, Microsoft Azure Active Directory, Palo Alto Networks и Zscaler.

Бюджеты на безопасность на крупных предприятиях выросли в среднем на 20%, в то время как на предприятиях среднего размера рост составляет в среднем всего 5%. проведенный SVP, также показал, что бюджеты на безопасность для новых технологий выросли в этом году на 18 %, что на 27 % меньше, чем в 2022 Опрос руководителей систем безопасности,. году Директора по информационной безопасности и специалисты по безопасности прогнозируют, что их бюджеты вырастут в среднем на 11% в этом году, что намного превышает прогнозируемый уровень инфляции.

В этом году на безопасность данных, приложений, облачных вычислений и конечных точек приходится в среднем 10% общих бюджетов компаний на кибербезопасность. По сравнению с прошлым годом, бюджеты на безопасность

конечных точек, управление идентификацией и обучение по вопросам безопасности выросли больше всего.

Безопасность искусственного интеллекта (ИИ) и машинного обучения (МО), а также безопасность цепочки поставок программного обеспечения впервые были включены в исследование этого года, что составляет 6% и 5% бюджетов соответственно.

Верным признаком того, что советы директоров рассматривают расходы на кибербезопасность как инвестиции, помогающие контролировать риски, является увеличение бюджета безопасности на одного сотрудника, который в этом году вырос до 3653 долларов США, что на 20% больше, чем 3033 доллара США на сотрудника в прошлом году.

Организации не хотят сокращать бюджеты на кибербезопасность, опасаясь слишком сильного отставания, поскольку злоумышленники используют новые технологии, в том числе AI/ML, для проведения атак используя старые уязвимости, одновременно. Однако старший вице-президент отмечает, что директора по информационной безопасности готовятся к более тщательному анализу своих решений о расходах и более длительным срокам принятия решений.

На протяжении последних трех лет бюджеты на кибербезопасность были одними из самых устойчивых в организациях любого размера. Совокупный эффект от продолжающихся расходов и того, что Gartner слышит от своих корпоративных клиентов о запланированных покупках, позволил аналитической компании предсказать, что расходы конечных пользователей на рынок информационной безопасности и управления рисками вырастут до 188,1 млрд долларов в этом году и достигнут 288,5 млрд долларов в 2027 году. Это совокупный годовой темп роста (CAGR) в размере 11,0% с 2022 по 2027 год.

Gartner Последние прогнозы [требуется клиентский доступ] по отдельным рынкам корпоративной информационной безопасности и управления рисками включают следующее, что еще раз отражает то, как гибкое бюджетирование стимулирует рост рынка:

Прогнозируется, что выручка от безопасности приложений вырастет с 5,7 млрд долларов США в этом году до 9,6 млрд долларов США в 2027 году, достигнув 13,6% среднегодового темпа роста.

Прогнозируется, что выручка от облачной безопасности вырастет с 5,6 млрд долларов в этом году до 12,8 млрд долларов в 2023 году, достигнув среднегодового темпа роста 22,8%.

Прогнозируется, что безопасность данных вырастет с 3,6 млрд долларов в 2023 году до 6,1 млрд долларов в 2027 году, достигнув 13,6% среднегодового темпа роста.

Прогнозируется, что управление доступом к удостоверениям вырастет с 16,1 млрд долларов в 2023 году до 24,8 млрд долларов в 2027 году, достигнув 11,4% CAGR.

Руководители служб безопасности, участвовавшие в опросе PVC, заявили, что найти и нанять экспертов по безопасности облачных вычислений — самая сложная задача. Более половины организаций (57%) заявили, что самым большим препятствием для достижения желаемого уровня безопасности является нехватка сотрудников службы безопасности, что на 42% больше, чем в прошлом году. Команды безопасности борются, среди прочего, со слишком большим количеством предупреждений, слишком большим количеством ложных срабатываний и слишком большим количеством инструментов.

Инструменты искусственного интеллекта и машинного обучения помогают лидерам в области безопасности восполнить нехватку кадров и масштабировать свои неукомплектованные команды. Четверо из пяти лидеров в области безопасности (79%) считают, что ИИ/МО будет «важным» или «чрезвычайно важным» для улучшения их состояния безопасности к 2024 году. Более 60% лидеров в области кибербезопасности полагаются на инструменты кибербезопасности с возможностями на основе ИИ/МО. чтобы еще больше компенсировать нехватку талантов. А 62 % лидеров безопасности используют инструменты на основе AI/ML для автоматизации процессов безопасности.

Тем временем директора по информационной безопасности сообщают VentureBeat, что они тестируют генеративные платформы на основе искусственного интеллекта с возможностями ChatGPT для снижения рабочих нагрузок SecOps. Из первоначальных пилотных проектов вытекают десять вариантов использования, которые демонстрируют потенциал для разгрузки рабочей нагрузки групп SecOp.

Исследование SVP показывает, насколько важно для каждой организации получить контроль над IAM и иметь надежную стратегию защиты каждой уязвимой поверхности угроз. Идентификационные данные являются наиболее уязвимым периметром безопасности.

Злоумышленники знают, что в облачных конфигурациях существуют бреши, и, украв учетные данные привилегированного доступа, они могут, по сути, получить контроль над всем бизнесом, прежде чем кто-либо осознает это. Вот почему IAM имеет решающее значение для правильной работы и почему она быстро растет. Директора по информационной безопасности и директора по информационным технологиям продолжают сотрудничать, чтобы устранить пробелы в конфигурации облака и укрепить сетевую безопасность…» ***(Louis Columbus. Network, IAM and cloud are the top 3 cybersecurity spending priorities for 2023 // VentureBeat (https://venturebeat.com/security/network-iam-cloud-top-3-cybersecurity-spending-priorities-2023/?utm_source=flipboard&utm_content=KeithKirby1m71%2Fmagazine%2FNews+and+Black+Entertainment.+). 13.07.2023).***

***

«За последние несколько месяцев участились кибератаки на цепочки поставок, затронувшие большое количество правительственных учреждений, правоохранительных органов, компаний и университетов в США и Европе.

Ярким примером таких кибератак является эксплуатация уязвимости нулевого дня в программе для обмена файлами MOVEit, которая широко используется организациями для передачи данных.

Эту кибератаку возглавила русскоязычная киберпреступная группа Clop или Cl0p, известная своими крупномасштабными кампаниями по программе-вымогателю как услуге. Хакерская группа работает с февраля 2019 года и нацелена на более чем 3000 организаций в США и 8000 организаций по всему миру.

Несмотря на арест некоторых членов группы, в Украине под руководством Интерпола в 2021 году эта кибератака в конце мая демонстрирует, что аффилированные группы по-прежнему действуют и опасны.

Киберпреступники нацелены на государственный сектор

7 июня Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) опубликовало совместные рекомендации по кибербезопасности с Федеральным бюро расследований (ФБР) и объявило, что оказывает поддержку нескольким федеральным агентствам, которые были взломаны.

Министерство энергетики и Национальное управление по ядерной безопасности были среди агентств США, которые пострадали. Другие жертвы государственного сектора включают государственный пенсионный фонд Калифорнии, Калифорнийский университет в Лос-Анджелесе, Министерство образования Миннесоты, систему государственных школ Нью-Йорка, британский регулятор связи Ofcom и канадское провинциальное правительство Новой Шотландии, в то время как пострадавшие компании включают Siemens Energy, Schneider Electric, Shell, BBC и British Airways.

Группа хакеров «называет и пристыжает» жертв на своей темной веб-странице, публикуя инструкции о том, как вступить в переговоры о вымогательстве, и угрожая опубликовать украденные данные, если выкуп не будет выплачен.

На протяжении многих лет Клоп требовал выкупа в размере сотен тысяч, а иногда и миллионов долларов. Однако хакерская группа якобы заявила, что нацелена исключительно на частный бизнес и что она удалит любые данные от правительств или правоохранительных органов.

В апреле прошлого года хакерская группа Killnet атаковала агентство управления воздушным движением Eurocontrol в Европе. Киберпреступники запустили распределенную атаку типа «отказ в обслуживании» (DDoS), вызвавшую перебои в работе веб-сайта, но, к счастью, атака не затронула европейскую авиацию.

Killnet — промосковская хакерская группа, известная своими атаками типа «отказ в обслуживании». Группа также взяла на себя ответственность за кибератаку на государственные службы Литвы 26 июня в ответ на решение правительства заблокировать транзит определенных товаров в российский анклав Калининград.

Аналогичным образом, в конце июня веб-сайты городского совета Люксембурга и Европейского инвестиционного банка (ЕИБ) были отключены на несколько часов в результате кибератаки DDoS.

Killnet и две другие киберпреступные группы ранее предупреждали о предстоящих атаках на европейскую банковскую систему в каналах Telegram. Однако единственным кибер-последствием стало временное нарушение работы веб-сайта ЕИБ.

Швейцарские правительственные учреждения и кантональные офисы также подверглись серии атак в мае и июне. 12 июня веб-сайт федерального правительства Швейцарии был отключен в результате DDoS-атаки, организованной хакерской группой NoName предположительно в ответ на принятие Швейцарией санкций ЕС против России.

Точно так же за неделю до парламентского обращения президента Украины Владимира Зеленского сайт парламента Швейцарии подвергся DDoS-атаке, подтвержденной той же хакерской группой NoName на каналах Telegram.

Государственный сектор Швейцарии также ранее был скомпрометирован в результате атаки на цепочку поставок в середине мая. Швейцарский государственный поставщик программного обеспечения стал жертвой атаки программы-вымогателя, приписываемой хакерской группе Play.

Нарушение затронуло Федеральное управление полиции страны, Федеральное управление таможенной и пограничной охраны, а также Швейцарские

федеральные железные дороги и некоторые кантональные власти. Швейцарский национальный центр кибербезопасности подтвердил, что украденные данные включают оперативные данные различных швейцарских органов и организаций.

В ответ Федеральный совет сформировал кризисную группу для управления расследованием программ-вымогателей и пересмотра текущих контрактов с поставщиками ИТ-услуг федеральной администрации для повышения кибербезопасности.

Срочно необходимо усилить киберустойчивость цепочки поставок

Этот последний инцидент, затронувший Швейцарию, наряду с атакой программы-вымогателя MOVEit, подчеркивает риски кибербезопасности, связанные с третьими сторонами, и возможные последствия для государственного сектора.

Киберпреступность носит транснациональный характер, и киберпреступники, связанные с государственными органами, часто неясны. Однако геополитическая напряженность после войны России против Украины повысила риски для критически важной инфраструктуры и цепочки поставок.

Европейский союз (ЕС) и Организация Североатлантического договора (НАТО) активизировали свое сотрудничество в связи с запуском Целевой группы ЕС-НАТО по устойчивости критически важной инфраструктуры, уделяя особое внимание энергетике, транспорту, цифровой инфраструктуре и космосу.

В новой национальной стратегии кибербезопасности США также подчеркивается необходимость защищать критически важную инфраструктуру, а также устранять и ликвидировать участников угроз путем интеграции федеральных мероприятий по подрыву безопасности и расширения государственного и частного оперативного сотрудничества.

Некоторые примеры включают международную полицейскую операцию Cookie Monster в апреле 2023 года, которая привела к закрытию крупнейшего незаконного форума по киберпреступности, известного как Genesis Market; обнародованное в январе 2023 года вмешательство ФБР в группу вымогателей Hive, а совсем недавно Five Eyes уничтожили вредоносное ПО Snake и сеть кражи

данных, использовавшуюся в шпионских кампаниях Федеральной службой безопасности России в мае 2023 года.

Государственно-частное сотрудничество — ключ к борьбе с киберпреступностью

Во все более сложной и взаимосвязанной технологической экосистеме критическая инфраструктура подвергается множеству киберугроз. Для снижения системных рисков и повышения киберустойчивости в таких критически важных секторах, как авиация, производство, нефть, газ и электроэнергетика, Центр кибербезопасности Всемирного экономического форума мобилизует многостороннее сообщество из бизнеса, правительств, гражданского общества и научных кругов.

В результате этих межотраслевых отраслевых инициатив Всемирный экономический форум разработал план оценки киберрисков в нефтегазовой отрасли.

Кроме того, в 2021 году по запросу Директората по энергетике Европейской комиссии в рамках инициативы «Киберустойчивость в электроэнергетике» были представлены 15 рекомендаций по директивам ЕС по кибербезопасности NIS 2.0 (сетевая и информационная безопасность) и CER (устойчивость критически важных объектов).

Помимо усилий по повышению киберустойчивости критически важной инфраструктуры, Всемирный экономический форум также возглавляет Партнерство против киберпреступности. С 2020 года эта инициатива объединяет правоохранительные органы, международные организации, компании по кибербезопасности, поставщиков услуг и некоммерческие организации для борьбы с киберпреступностью.

Стремясь справиться с растущим уровнем киберпреступности, на Ежегодном собрании 2023 года в Давосе в январе Центр кибербезопасности представил Атлас киберпреступности при поддержке Fortinet, Microsoft, PayPal и Santander.

Эта новая инициатива позволит составить карту ландшафта угроз и создать репозиторий киберпреступлений на основе общедоступных данных и добровольно

предоставленной информации, что позволит правоохранительным органам более эффективно бороться с киберпреступностью». ***(Giulia Moschetta. Cybercrime: Critical infrastructure is at risk and needs a combined private- and public-sector response // World Economic Forum (https://www.weforum.org/agenda/2023/07/cybercrime-infrastructure-public-sector-cyber-resilience-collaboration/?utm_source=flipboard&utm_content=WEF%2Fmagazine%2FWorld+Economic+Forum). 14.07.2023).***

***

«Охранная фирма Check Point объявила тревожные новые статистические данные, которые должны заставить вас задуматься об установке лучшей защиты конечных точек, если вы еще этого не сделали, поскольку кибератаки достигли двухлетнего максимума.

По данным компании, во втором квартале 2023 года число кибератак выросло на 8% в годовом исчислении, и, поскольку в этом году ожидается поступление в продажу многочисленных билетов, включая недавнюю продажу тура Тейлор Свифт, рост может продолжиться.

Среди наиболее пострадавших секторов образования и исследований, в то время как Африка и Азиатско-Тихоокеанский регион испытали самый высокий годовой рост еженедельных атак.

Особое беспокойство вызывает программа-вымогатель, которая обычно угрожает украсть или зашифровать данные, обычно требуя довольно высокой цены. Каждую неделю каждая 44-я компания страдает от атак программ-вымогателей.

В то время как образование и исследования остаются ключевыми целями для киберпреступников, в среднем 2179 атак на организацию в неделю, этот показатель снизился на 6% по сравнению с тем же периодом в 2022 году.

Напротив, в правительственном и военном секторе наблюдалось увеличение на 9% в годовом исчислении до 1772 атак в неделю, что свидетельствует о

сохраняющихся политических угрозах на фоне продолжающихся войн. В сфере здравоохранения наблюдался еще более тревожный рост на 30%, теперь со скоростью 1744 в неделю, что почти соответствует атакам правительства.

Ни в одном регионе не наблюдалось снижения общего количества атак, при этом в Европе наблюдался наименьший рост на 5% по сравнению с 23% и 22% в Африке и Азиатско-Тихоокеанском регионе соответственно. В Азиатско-Тихоокеанском регионе также наблюдался огромный рост атак программ-вымогателей — здесь и в Латинской Америке теперь одна из 26 организаций подвергается атакам программ-вымогателей.

Check Point, как и любая другая компания, работающая в области кибербезопасности, предлагает компаниям не отставать от своих исправлений безопасности, предпочитая предотвращение обнаружению. Он также рекомендует проводить регулярные тренинги по кибербезопасности для работников, которые обычно являются слабыми местами многих организаций». ***(Craig Hale. Cyberattacks are rising across the world - here's what you need to know // Future US, Inc. (https://www.techradar.com/pro/cyberattacks-are-rising-across-the-world-heres-what-you-need-to-know?utm_source=flipboard&utm_content=other). 14.07.2023).***

***

«Кібербезпека стала незамінною для нашого цифрового життя в нашому взаємопов'язаному світі. Оскільки технології прогресують і організації все більше покладаються на цифрові системи, захист конфіденційних даних, збереження довіри клієнтів і забезпечення безперебійної роботи стали критичними цілями.

Від зростання кількості витоків даних до фінансових втрат компаній і зростання досвідченості хакерів, наш підібраний список статистики кібербезпеки підкреслює необхідність вжиття надійних заходів кібербезпеки. У цій статті ми розглянемо деякі вражаючі дані про кібербезпеку, проллємо світло на наші проблеми та підкреслимо важливість захисту наших цифрових активів…

Статистика кібербезпеки за типом атак

У середовищі кібербезпеки, що постійно змінюється, вкрай важливо бути в курсі різноманітних кібератак, які загрожують окремим особам і організаціям. Вплив цих атак є значним як з точки зору фінансових втрат, так і з точки зору репутації.

Звіт ФБР про інтернет-злочини за 2022 рік показав, що громадськість повідомила про 800 944 скарги на кіберзлочини.

Фішингові атаки були видом злочинів номер один, було зареєстровано 300 497 скарг. Загальні збитки від фішингових атак перевищили 10,3 мільярда доларів…

Фішингові атаки залишаються найпоширенішою кібератакою з приблизно 3,4 мільярдами -повідомлень щодня спам.

Вони охоплюють різні методи омани, щоб обманом змусити людей розкрити конфіденційну інформацію або брати участь у зловмисних діях за допомогою прихованих електронних листів або веб-сайтів.

Фішингові атаки відповідають за 90% витоків даних. Це пов’язано з тим, що фішери часто припускають особу надійної та надійної організації в електронних комунікаціях…

Згідно зі статистикою Norton, приблизно 88% організацій стикаються з фішинговими атаками протягом року. Ці дані вказують на те, що підприємці стають цільовими майже щодня.

У звіті за 1 квартал 2022 року, опублікованому компанією Check Point Research, було представлено список найкращих брендів, упорядкованих за загальним показником кількості спроб фішингу.

LinkedIn (що стосується 52% усіх фішингових атак у світі)

DHL (14%)

Google (7%)

Microsoft (6%)

FedEx (6%)

WhatsApp (4%)

Amazon (2%)

Maersk (1%)

AliExpress (0,8%)

Яблуко (0,8%)

LinkedIn був пов’язаний з 52% пов’язаних з фішингом атак у всьому світі. Ця значна цифра вперше означає, що платформа соціальних медіа посіла перше місце у рейтингу, що свідчить про серйозність проблеми…

У четвертому кварталі 2022 року Yahoo відчув помітне зростання на 23 позиції на 20% через ефективну фішингову кампанію в попередньому кварталі. LinkedIn опустився на п’яте місце в списку із 5,7% загальною часткою спроб фішингу брендів.

Із розвитком віддаленої роботи зросла кількість шахрайських шахрайств, пов’язаних із компрометацією корпоративної електронної пошти (BEC). Ці шахраї використовують тактику фішингової електронної пошти, щоб змусити людей розкрити конфіденційну інформацію про компанію або здійснити несанкціоновані грошові перекази.

У 2022 році IC3 зафіксувала 21 832 скарги, пов’язані з BEC, у результаті скориговані збитки перевищили 2,7 мільярда доларів.

Розподілена атака на відмову в обслуговуванні (DDoS) — це зловмисна спроба порушити нормальне функціонування мережі, служби або веб-сайту, переповнивши їх потоком інтернет-трафіку. DDoS-атака має на меті порушити або вивести з ладу ресурси та інфраструктуру цілі, що призведе до простою служби та потенційних фінансових втрат.

У 2022 році Microsoft пом'якшувала в середньому 1435 DDoS- атак щодня.

Максимальна кількість атак за добу становила 2215 22 вересня 2022 року.

Мінімальна кількість атак за добу становила 680 22 серпня 2022 року.

Загальна кількість унікальних атак, пом’якшених у 2022 році, перевищила 520 тис…

Відповідно до звіту, опублікованого Cloudflare, кількість DDoS-атак з викупом збільшилася на 67% у порівнянні з минулим роком і на 24% у порівнянні з кварталом. В Інтернет-галузі відчули значне зростання кількості DDoS-атак на

прикладному рівні: зростання на 131% у порівнянні з кварталом минулого року та на 300% у порівнянні з минулим роком.

У вересні 2017 року DDoS-атака, що побила рекорд, була спрямована на служби Google, досягнувши величезного розміру 2,54 Тбіт/с. Google Cloud розповіла про цей інцидент у жовтні 2020 року.

Атаку приписують Китаю, і було встановлено, що вона походить з мережі чотирьох китайських інтернет-провайдерів. Хакери відправили підроблені пакети на 180 000 веб-серверів, які надіслали відповіді в Google.

Одна з найпомітніших DDoS-атак сталася в березні 2023 року. Сайт Національної асамблеї Франції пережив тимчасовий збій через DDoS-атаку, організовану російськими хакерами. У дописі в Telegram хакери пояснили атаку підтримкою України урядом Франції.

Дані про зловмисне програмне забезпечення

Станом на 2023 рік щодня генерується 300 000 нових екземплярів зловмисного програмного забезпечення, 92% з яких розповсюджується електронною поштою, і в середньому на виявлення потрібно 49 днів. Шкідливе програмне забезпечення використовується для отримання несанкціонованого доступу до IT-систем, викрадення даних, порушення системних служб або завдання шкоди IT-мережам.

4,1 мільйона веб-сайтів заражені шкідливим програмним забезпеченням. А 18% веб-сайтів містять критичні загрози кібербезпеці.

Крім того, 97% усіх порушень безпеки на веб-сайтах використовують плагіни WordPress. З 47 337 шкідливих плагінів, встановлених з 2012 по 2021 рік, 94% були активні на 24 931 різних веб-сайтах WordPress, на кожному з яких розміщено два або більше шкідливих плагінів…

Відповідно до звіту SonicWall про кіберзагрози за 2023 рік, кількість шкідливих програм зросла вперше з 2018 року, досягнувши 5,5 мільярдів атак, що на 2% більше, ніж у минулому році. Незважаючи на незначне зростання, стрімке зростання криптозловмисників кількості шкідливих програм для Інтернету речей та значною мірою сприяло значному зростанню…

У 2022 році рівень криптозлому зріс на 43%, тоді як зловмисне програмне забезпечення IoT зросло на 87%. Сукупний розвиток криптодеяння та зловмисного програмного забезпечення Інтернету речей компенсує падіння глобального обсягу програм-вимагачів, що вперше з 2018 року призвело до позитивних змін у загальних тенденціях щодо шкідливих програм…

У сфері зловмисного програмного забезпечення програмне забезпечення-вимагач виділяється як особливий тип, який утримує цільові дані або системи в заручниках, доки жертва не зробить викуп.

За даними SonicWall, у 2022 році було зареєстровано 493,3 мільйона спроб програм-вимагачів, що демонструє помітне зниження на 21% порівняно з минулим роком. У 2020 році спостерігалося зростання на 62%, а в 2021 році – додатковий сплеск на 105%.

Однак у 2022 році на ці типи кібератак припадало 12% порушень критичної інфраструктури, що робить їх відповідальними за понад чверть порушень у галузях критичної інфраструктури…

Незважаючи на невелике зниження трохи більше ніж на одну п’яту, 2022 рік залишається другим за кількістю глобальних атак програм-вимагачів за всю історію…

Крім того, цифри за 2022 рік набагато ближчі до надзвичайно високих рівнів, які спостерігалися у 2021 році, ніж до попередніх років. Вони значно перевищили обсяги 2017 (+155%), 2018 (+127%), 2019 (+150%) і 2020 (+54%) значних показників.

У своєму дослідженні 2022 року Comparitech повідомила про наступні ключові висновки щодо кібербезпеки:

рік	2022	2021
Кількість атак	795	1,365
Середня вимога викупу	7,2 мільйона доларів	8,2 мільйона доларів
Вплинуло на середні рекорди	115,8 млн	49,8 мільйонів

Середня кількість постраждалих записів за атаку	559,695	119,114

З 2021 по 2022 рік кількість атак і суми викупу зменшилися. Однак збільшення середньої кількості порушених записів свідчить про те, що коли відбуваються атаки, вони мають більш значний вплив на кількість зламаних записів.

Типи атак програм-вимагачів у статистиці кібербезпеки

IC3 отримав 2385 скарг на програми-вимагачі, в результаті скориговані збитки перевищили 34,3 мільйона доларів. У 2022 році Зловмисники часто використовують методи соціальної інженерії для доступу до середовища жертви.

Відповідно до того ж звіту, основними причинами інцидентів з програмами-вимагачами були фішинг, використання протоколу віддаленого робочого столу (RDP) і вразливості програмного забезпечення…

LockBit, ALPHV/Blackcoats і Hive були трьома переважаючими варіантами програм-вимагачів, про які повідомлялося IC3, які націлені на членів критичних секторів інфраструктури…

У 2019 році 80% усіх порушень даних були пов’язані зі зламаними паролями, що призвело до значних фінансових втрат для компаній і споживачів. 49% користувачів змінять лише одну літеру чи цифру в одному зі своїх бажаних паролів, коли потрібно створити новий пароль.

Хакер може спробувати 2,18 трильйона комбінацій паролів та імен користувачів за 22 секунди. Введення в пароль однієї літери великого регістру різко змінює його потенціал.

А пароль із восьми символів спочатку може бути зламаний протягом однієї секунди. Але цей час можна збільшити до 22 хвилин, додавши одну велику літеру…

У 2019 році опитування Google показало, що звичка повторно використовувати паролі для кількох облікових записів помітно присутня…

59% респондентів вважають, що їхні облікові записи безпечніші від онлайн-загроз, ніж звичайна людина. 69% ставлять собі оцінку A або B, коли йдеться про захист своїх облікових записів.

За даними The SANS Software Security Institute, найпоширенішими вразливими місцями є:

Компроміс ділової електронної пошти

Застарілі протоколи

Повторне використання пароля

Беручи до уваги ці важливі дані, як люди ставляться до онлайн-безпеки та злому паролів?

У звіті LastPass Psychology of Passwords представлені варті уваги висновки щодо емоцій і поведінки респондентів щодо онлайн-безпеки.

45% респондентів не змінювали паролі протягом останнього року, навіть після порушення безпеки.

79% погодилися, що зламані паролі викликають занепокоєння.

51% покладаються на свою пам'ять, щоб відстежувати паролі.

65% завжди або переважно використовують той самий пароль або його варіант.

З 3750 опитаних професіоналів у семи країнах лише 8% сказали, що надійний пароль не повинен мати зв’язку з особистою інформацією. Більшість користувачів створюють паролі, які покладаються на особисту інформацію, пов’язану з потенційно доступними публічними даними, такими як день народження чи домашня адреса…

У грудні 2016 року Yahoo оголосила, що понад один мільярд облікових записів було зламано в результаті сумнозвісного злому 2013 року. Під час цього зламу хакери отримали несанкціонований доступ до систем Yahoo, скомпрометувавши особисту інформацію (PII). Це включало імена користувачів, адреси електронної пошти, номери телефонів і хешовані паролі. Це вважається одним із найбільших витоків даних в історії кібербезпеки.

Дані злому Інтернету речей (IoT).

Інтернет речей (IoT) відноситься до мережі взаємопов’язаних фізичних пристроїв або об’єктів. На відміну від традиційного злому серверів і систем, IoT спрямовано на пристрої, підключені до Інтернету. Наприклад, такі розумні побутові прилади, як телевізори, динаміки, камери безпеки та медичні пристрої, піддаються атакам.

Оскільки кількість підключених пристроїв продовжує зростати, у 2022 році кількість зловмисних програм IoT різко зросла на 87% порівняно з попереднім роком, досягнувши історичного максимуму в 112,3 мільйона випадків...

Існує значна ринкова можливість для постачальників технологій і послуг кібербезпеки, яка оцінюється в приголомшливі 2 трильйони доларів. У діаграмі розміру глобального ринку кібербезпеки від McKinsey & Company підкреслюється потенціал провайдерів пропонувати інноваційні рішення та послуги у відповідь на кіберзагрози, що розвиваються. Це відкриває багатообіцяючі фінансові перспективи та підкреслює вирішальну роль цих провайдерів у зміцненні цифрового захисту та захисту бізнесу від постійних кіберризиків...

Відповідно до звіту IBM Cost of a Data Breach Report, середня світова вартість витоку даних зросла з 4,24 мільйона доларів США у 2021 році до 4,35 мільйона доларів США у 2022 році. На частку фішингу припадає 16% найпопулярніших векторів атак у кіберзлочинності, середня вартість злому становить 4,91 мільйона доларів. Крім того, порушення, спричинені викраденими або скомпрометованими обліковими даними, склали 4,50 мільйона доларів...

У 2022 році середня ціна за зламаний запис у результаті витоку даних у всьому світі становила 164 долари США, що на 1,9% більше порівняно зі 161 доларом США у 2021 році. Це збільшення є ще більш значним порівняно із середньою вартістю 146 доларів США за запис у 2020 році, яка демонструє зростання на 12,3%.

На атаки програм-вимагачів припадає 11% проаналізованих порушень, що вказує на зростання на 41% порівняно з 7,8% порушень програм-вимагачів у попередньому році. Середня вартість атаки програм-вимагачів дещо знизилася з 4,62 мільйона доларів США у 2021 році до 4,54 мільйона доларів США у 2022 році.

Однак ця вартість залишилася незначно вищою за середню загальну вартість витоку даних у 4,35 мільйона доларів США.

Дослідження IBM Cost of Data Breaches також показує, що порушення, пов’язані з віддаленою роботою, коштують у середньому приблизно на 1 мільйон доларів США більше, ніж порушення без віддаленої роботи. Середня вартість порушень у дистанційній роботі склала 4,99 мільйона доларів, тоді як порушення, не пов’язані з віддаленою роботою, становили в середньому 4,02 мільйона доларів. Ці порушення, пов’язані з віддаленою роботою, коштують приблизно на 600 000 доларів США більше, ніж у середньому по всьому світу.

Протягом останніх п'яти років ФБР IC3 (Центр скарг на злочини в Інтернеті) щорічно отримував у середньому 652 000 скарг. З 2018 року було подано 3,26 мільйона скарг і завдано збитків на 27,6 мільярда доларів...

Вартість кібербезпеки для бізнесу може значно відрізнятися залежно від різних факторів через широкий спектр послуг і продуктів. Наприклад, розмір і характер організації, рівень реалізованих заходів безпеки та ступінь потенційних загроз впливають на витрати.

Згідно з опитуванням Deloitte Insights, організації витрачають приблизно 10,9% свого IT-бюджету на кібербезпеку. Компанії витрачають близько 0,48% свого доходу на витрати на кібербезпеку. З точки зору витрат на одного працівника, респонденти повідомили про середні інвестиції приблизно 2700 доларів США на одного штатного працівника на заходи кібербезпеки.

Однак, згідно з дослідженням IBM Cost of a Data Breach, ці інвестиції виправдані.

Організації з повністю розгорнутим штучним інтелектом безпеки та автоматизацією зіткнулися з порушеннями, які коштували на 3,05 мільйона доларів США дешевше порівняно з організаціями без такого розгортання. Ця значна (65,2%) різниця в середній вартості порушення підкреслила суттєву економію коштів: повністю розгорнуті організації в середньому становили 3,15 мільйона доларів США, тоді як нерозгорнуті організації зіткнулися з середньою ціною в 6,20 мільйона доларів США.

Крім того, компанії з повністю розгорнутим штучним інтелектом безпеки та автоматизацією відчули 74-денне скорочення виявлення та стримування порушень порівняно з тими, хто не має таких реалізацій. Повністю розгорнуті організації мали середній життєвий цикл порушення в 249 днів, тоді як нерозгорнуті організації займали 323 дні.

Статистика кібербезпеки за країнами

Кількість зловмисних програм за країнами

Згідно зі звітом Sonic Wall про кіберзагрози за 2023 рік, Сполучені Штати займають перше місце в списку з найбільшою кількістю атак зловмисного програмного забезпечення, загальна сума яких становить 2,68 мільярда. Але значне зменшення кількості шкідливих програм на -9% порівняно з минулим роком свідчить про переміщення уваги кіберзлочинців у бік інших країн…

Велика Британія посідає друге місце за кількістю атак зловмисного програмного забезпечення, повідомивши про 432,9 мільйона атак у 2022 році…

Індія посідає третє місце в списку із загальним показником 335,4 мільйона, демонструючи примітне зростання на +31% у порівнянні з минулим роком. Хоча обсяги атак у 2022 році загалом знизилися, Індія виділялася як країна з найбільшим зростанням обсягів атак серед тих, хто брав участь у дослідженні…

Відсоток поширення зловмисного програмного забезпечення Sonic Wall представляє розрахунок датчиків, які виявили атаку зловмисного програмного забезпечення, що вказує на ступінь поширення зловмисного програмного забезпечення в цьому конкретному регіоні.

В’єтнам став першою країною, на яку націлено шкідливе програмне забезпечення – 30,15%. Однак найбільш значущим спостереженням є зростання Європи як гарячої точки кіберзлочинності: кількість європейських країн у списку подвоїлася з 2021 року, становлячи більшість у топ-10…

Згідно з тим самим звітом, у 2022 році в Європі, Латинської Америки та Азії відбулося значне двозначне зростання, відповідно, на 10%, 17% і 38%...

Цікаво, що кількість зловмисного програмного забезпечення в Північній Америці значно скоротилася на 10% порівняно з минулим роком, що призвело до

загального 2,75 мільярда випадків. Ця цифра є найнижчим зареєстрованим обсягом з 2017 року, підкреслюючи помітне зниження активності зловмисного програмного забезпечення в регіоні.

Крім того, протягом грудня спроби шкідливого програмного забезпечення в Північній Америці досягли рекордно низького рівня в 158,9 мільйона, що стало найнижчим місячним обсягом з 2018 року. Ці події вказують на потенційний зсув кіберзлочинців від Північної Америки та інших відомих центрів кіберзлочинності до інших регіонів світу.

Дані кібервійни – Росія та Китай проти США

Китай і Росія стають домінуючими гравцями у сфері кібербезпеки, на них припадає майже 35% глобальних атак разом. Маючи 79 підтверджених атак з Китаю та 75 з Росії, ці дві країни активно атакували національні уряди.

Агентство кіберзахисту Америки часто оновлює свої рекомендації, попередження та звіти про аналіз зловмисного програмного забезпечення (MAR) щодо зловмисної кіберактивності Росії. «Російський уряд бере участь у зловмисній кібердіяльності, щоб забезпечити широке кібершпигунство, придушити певну соціальну та політичну діяльність, викрасти інтелектуальну власність і завдати шкоди регіональним і міжнародним супротивникам».

У лютому 2022 року BBC повідомляло, що 74% доходу від програм-вимагачів припадає на хакерів, пов’язаних із Росією. Дослідники встановили, що платежі в криптовалюті на суму понад 400 мільйонів доларів були спрямовані групам, які, напевно, були пов’язані з Росією.

У липні 2021 року Білий дім опублікував заяву, в якій викривав безвідповідальну поведінку Китайської Народної Республіки (КНР) у кіберпросторі. «Як зазначено в публічних документах про звинувачення, розпечатаних у жовтні 2018 року та липні та вересні 2020 року, хакери, які раніше працювали на Міністерство державної безпеки КНР (MSS), брали участь в атаках програм-вимагачів, кібервимаганнях, крипто-викраденнях і званнях крадіжки від жертв по всьому світу, і все це заради фінансової вигоди».

Наступного року глави ФБР і MI-5 вперше в історії виступили разом і попередили про загрозу з боку Китаю: «У нашому світі ми називаємо таку поведінку підказкою... це буде одним із найжахливіших зривів бізнесу, які коли-небудь бачив світ», — сказав глава ФБР Крістофер Рей.

Статистика кібербезпеки за галузями

IC3 зареєстрував 870 скарг у 2022 році, повідомляючи про атаки програм-вимагачів, націлених на організації в критичних секторах інфраструктури. Серед 16 секторів критичної інфраструктури звіт IC3 показав, що в 14 секторах принаймні один член став жертвою атаки програм-вимагачів.

Організації критичної інфраструктури зіткнулися із середніми витратами на витік даних у розмірі 4,82 мільйона доларів, що перевищує середній показник в інших галузях на 1 мільйон доларів. Серед них 28% зіткнулися з деструктивними атаками або програмами-вимагачами, а 17% зіткнулися з порушеннями через скомпрометовані ділові партнери…

Індустрія охорони здоров'я була найдорожчою за зловмисне програмне забезпечення-вимагач протягом 12 років поспіль, із середніми витратами на злам даних сягає 10,10 мільйонів доларів США. Дані пацієнтів є надзвичайно цінними для кіберзлочинців, особливо в електронних медичних записах (EHR). Ці записи містять інформацію про осіб, зокрема їхні імена, номери соціального страхування, фінансові відомості, минулі та теперішні адреси та історії хвороби.

Тим часом обробна промисловість значно постраждала від атак здирників у 2022 році, із зареєстрованими 447 жертвами на різних платформах. Сектор професійних і юридичних послуг уважно слідкував за 343 жертвами...

У 2022 році Коста-Ріка оголосила надзвичайний стан у відповідь на серію атак програм-вимагачів, націлених на критично важливі установи. Перша серія атак була спрямована на державні органи, і відповідальність за них взяла банда Conti, впливова група хакерів, що базується в Росії.

Сайт здирництва Корті заявив про публікацію 50% вкрадених даних уряду Кост-Ріки, включаючи 850 гігабайт матеріалів міністерства фінансів. Зловмисники вимагали викуп у розмірі 10 мільйонів доларів, щоб запобігти витоку інформації.

Друга серія атак сталася 31 травня 2022 року групою програм-вимагачів HIVE. Основною мішенню був Фонд соціального страхування Коста-Ріки, організація, відповідальна за управління службою охорони здоров'я країни. Крім того, атака вразила понад 10 400 комп'ютерів і більшість серверів у Коста-Ріці. У результаті цього тижня було скасовано приблизно 34 677 зустрічей, що становить 7% від усіх запланованих зустрічей.

У травні 2021 року компанія Colonial Pipeline зазнала атаки програмного забезпечення-вимагача, яка повністю припинила роботу трубопроводу розподілу палива. Всього за дві години кіберзлочинцям з угруповання DarkSide вдалося отримати майже 100 гігабайт даних з мережі компанії Alpharetta, штат Джорджія.

Colonial Pipeline заплатив близько 5 мільйонів доларів хакерам з Росії за сприяння відновленню найбільшого в країні паливного трубопроводу.

Подібним чином у червні 2021 року JBS, найбільша у світі компанія з виробництва м'яса, стала жертвою значної атаки програм-вимагачів російських хакерів. Порушення призвело до того, що JBS заплатила викуп у розмірі 11 мільйонів доларів хакерам, які отримали несанкціонований доступ до її комп'ютерної системи.

Важливість кібербезпеки

Із зростанням кількості кібератак і дедалі більшою витонченістю зловмисників компанії та окремі особи стикаються зі значними ризиками. Статистика кібербезпеки виявляє тривожні тенденції, такі як зростання витрат на витік даних, поширеність фішингових атак і вплив віддаленої роботи на витрати на зловживання.

Однак він також проливає світло на цінність інвестицій у кібербезпеку, наголошуючи на економії коштів і покращеному реагуванні на інциденти, досягнутих завдяки впровадженню ШІ безпеки, автоматизації та груп реагування на інциденти.

Оскільки організації продовжують орієнтуватися в мінливому ландшафті загроз, стає зрозуміло, що пріоритетність надійних заходів кібербезпеки є важливою для захисту конфіденційних даних, збереження безперервності бізнесу

та захисту від фінансової та репутаційної шкоди». ***(Nicole Kolesnikov. 50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who & What is Targeted // Techopedia Inc. (https://www.techopedia.com/cybersecurity-statistics). 13.07.2023).***

***

«Компанія ESET представляє рейтинг найбільш поширених кіберзагроз з грудня 2022 до травня 2023 року. За цей період кіберзлочинці продемонстрували надзвичайну адаптивність і пошук нових способів атак, використовуючи уразливості, викрадаючи конфіденційну інформацію та вводячи жертв в оману.

Зокрема у першій половині 2023 року знову повернулися схеми шахрайства через електронну пошту із шантажем поширення інформації еротичного характеру про жертву. Зазвичай зловмисники надсилають користувачу лист про встановлення на його комп'ютері шкідливої програми, яка дає їм змогу збирати інтимні дані про жертву. Одна з найпопулярніших загроз цього виду вимагала оплати на суму 1550 доларів США у Bitcoin за нерозголошення інформації.

Крім цього, на 90% зросла кількість оманливих додатків для Android із пропозицією позики грошей. Такі програми маскуються під послуги позик, обіцяючи користувачам швидкий і легкий доступ до коштів. Однак насправді вони призначені для обману користувачів і викрадення їх особистої та фінансової інформації. Після встановлення ці додатки отримують дозволи на доступ до списку облікових записів, журналів викликів, контактів, SMS-повідомлень, інформації про мережу Wi-Fi та місцезнаходження пристрою.

Ці шахрайські програми поширюються через соціальні мережі та SMS-повідомлення. Самі додатки доступні для завантаження зі спеціальних вебсайтів шахраїв, сторонніх магазинів і навіть Google Play.

Крім цього, за перші пів року для платформи Android на понад 40% зросла кількість прихованих додатків і на майже 20% число рекламного шкідливого програмного забезпечення. У більшості випадків це були безкоштовні ігри, які

відображають рекламу користувачам. Загалом програми, які заробляють на показі реклами, становили понад 68% усіх виявлених зразків для Android.

Як змінилися тактики кіберлочинців?

Варто зазначити, що однією з причин зміни шаблонів атак є суворіші політики безпеки, запроваджені Microsoft, зокрема щодо відкриття файлів із підтримкою макросів. Дані телеметрії ESET також свідчать про те, що раніше поширеному ботнету Emotet було важко пристосуватися до цієї зміни. Серед програм-вимагачів кіберзлочинці все частіше повторно використовували раніше опублікований вихідний код для створення нових варіантів цього виду загроз.

«Витік вихідного коду сімейств програм-вимагачів, таких як Babyk, LockBit і Conti, дозволив хакерам-аматорам брати участь у цій шкідливій діяльності. У той же час це дозволяє спеціалістам з кібербезпеки охоплювати ширший спектр варіантів за допомогою більш загальних або відомих наборів виявлених зразків і правил», — розповідає Роман Ковач, директор з досліджень ESET.

Крім цього, у новій спробі обійти заходи безпеки Microsoft зловмисники замінили макроси Office на небезпечні файли OneNote з вбудованими шкідливими сценаріями. У відповідь Microsoft змінила налаштування за замовчуванням, змусивши кіберзлочинців шукати альтернативні вектори атаки, зокрема використовувати і атаки з підбором пароля на сервери Microsoft SQL.

За даними телеметрії ESET, кількість заблокованих спроб підбору пароля до MSSQL зросла з 940 мільйонів до 1,7 мільярда в першій половині 2023 року. Також варто зазначити, що найпопулярнішими методами мережевих атак були підбір пароля та використання уразливості Log4Shell, яка дозволяє зловмисникам запускати довільний код на певному сервері.

Незважаючи на те, що кількість загроз, націлених на криптовалюти, за даними телеметрії ESET, неухильно зменшується, це не означає зникнення у кіберзлочинців інтересу до цієї сфери. Зокрема можливості прихованого майнінгу та викрадення криптовалют все частіше додаються в різні види шкідливого програмного забезпечення. Ця еволюція відбувається за вже відомою схемою, наприклад, загрози для зчитування натиснень клавіатури спочатку поширювалися

окремо, але згодом цей функціонал став загальною можливістю багатьох сімейств шкідливих програм.

Як захистити свої пристрої?

Тож для захисту власних пристроїв від оманливих додатків спеціалісти ESET рекомендують завантажувати програми лише з офіційних магазинів, переглядати відгуки та рейтинг, а також слідкувати за дозволами, які ви надаєте. Якщо шахрайський додаток було завантажено з Google Play, зверніться за допомогою до служби підтримки магазину, щоб повідомити про програму та подати запит на її видалення.

Також спеціалісти ESET рекомендують не переходити за невідомими посиланнями, надісланими через повідомлення в соцмережах або електронних листах, на додаток до паролів використовувати двофакторну автентифікацію для входу в облікові записи та встановити програми для захисту ваших комп'ютерів та мобільних пристроїв від різних загроз, включно з вірусами, фішинг-атаками та іншими видами шкідливих програм». ***(Герман Богапов. ESET розповсюдив рейтинг головних інтернет-загроз // HiTech.Expert (https://expert.com.ua/163862-eset-rozpovsyudyv-reytyng-golovnyh-internet-zagroz.html). 12.07.2023).***

***

«Виробник косметики Estee Lauder (EL.N) у вівторок заявив, що хакер отримав деякі дані з його систем, і кіберінцидент спричинив і, як очікується, призведе до збоїв у частині бізнес-операцій компанії.

Власник MAC Cosmetics працював над відновленням постраждалих систем і вжив заходів для забезпечення безпеки своїх операцій, включаючи відключення деяких своїх систем для пом'якшення інциденту, йдеться в заяві компанії.

Estee Lauder, якій також належать такі косметичні бренди, як Bobbi Brown і Tom Ford Beauty, не розкрила додаткових подробиць про вплив на свою діяльність, але заявила, що намагається зрозуміти природу та обсяг зламаних даних.

Інцидент стався у вирішальний момент для виробника косметики, який у травні спрогнозував нижчі продажі та прибуток за рік, ніж передбачалося раніше,

звинувачуючи повільне відновлення в безмитних і туристичних напрямках, особливо в Азії.

За останній рік низка витоків даних торкнулася кількох компаній, зареєстрованих у США.

У вересні виробник Grand Theft Auto Take-Two Interactive Software (TTWO.O) підтвердив ранній витік кадрів популярної відеоігри до її випуску, а компанія Uber (UBER.N), яка займається замовленням поїздок, була змушена на тиждень закрити кілька внутрішніх комунікацій після інциденту з кібербезпекою.

Оператор бездротового зв'язку T-Mobile (TMUS.O) у січні зіткнувся з другою великою кібератакою менш ніж за два роки, яка викрила понад 37 мільйонів облікових записів.

У своїй заяві Estee Lauder повідомила, що підтримує контакти з правоохоронними органами та експертами з кібербезпеки, але не відповіла на запит Reuters про коментарі в неробочий час.

Нью-йоркська компанія не назвала ім'я хакера чи хакерську особу». ***(Estee Lauder hit by cyberattack, some business operations affected // Reuters (https://www.reuters.com/business/retail-consumer/estee-lauder-says-hacker-obtained-some-data-its-systems-2023-07-19/). 20.07.2023).***

***

«Sygnia, відома ізраїльська компанія з кібербезпеки, нещодавно опублікувала оновлені відомості про діяльність групи нападників Casbaneiro, яка сіє хаос організаціям у всьому світі, зосереджуючись на фінансовому секторі Латинської Америки з 2018 року.

Розслідування Sygnia показують, що загрози, що стоять за кампанією Casbaneiro, продовжували свої операції протягом останніх п'яти років, вносячи значні зміни в свої методи атак, інфраструктуру та методи стійкості. Безперервна діяльність групи нападників Casbaneiro привернула увагу індустрії кібербезпеки, а експерти вважають її «суттєвою загрозою» для фінансових установ у всьому світі.

Амір Садон, директор відділу ІК-досліджень у Sygnia, пояснив, що хакери в основному використовують тактику фішингу електронної пошти, щоб націлитися на працівників організацій. Коли жертв спонукають перейти за шкідливими посиланнями, запускається «троянський кінь», який дозволяє зловмисникам збирати конфіденційну інформацію з комп'ютерів організації. Викрадені дані можуть включати секретні файли, знімки екрана, інформацію користувача, паролі та натискання клавіш.

Садон зазначив, що методи роботи Casbaneiro були вперше детально описані в попередньому дослідженні, опублікованому Sygnia в 2018 році. Незважаючи на роки, способи дії групи нападу залишаються відносно схожими.

Однак останні відкриття Sygnia показують деякі важливі зміни в їхньому підході. «У той час як під час попередньої хвилі атак хакери надсилали електронні листи зі шкідливим файлом PDF, тепер це, очевидно, законний файл HTML, який веде до встановлення троянського коня», — пояснив Садон.

Цільові пристрої

Крім того, зловмисники застосували відомий метод для підвищення привілеїв на цільових комп'ютерах, ще більше ускладнюючи захист від їхніх атак. Дослідники також знайшли судово-медичні докази, які пов'язують нинішню хвилю атак із попередніми, здійсненими групою.

Sygnia рекомендує організаціям, які хочуть захистити себе від таких атак, запровадити ідентифікатори зловмисників і правила виявлення у своїх системах безпеки. Компанія надала список ідентифікаторів компрометації (IOC), які використовує група атаки, а також набір правил виявлення для ідентифікації нових версій інструментів атаки. Інтегруючи ці заходи у свою інфраструктуру безпеки, організації можуть сподіватися на миттєве виявлення спроб атак, ефективно запобігаючи несанкціонованому доступу до їхніх мереж». ***(ZACHY HENNESSEY. Israeli cybersecurity firm Sygnia has revealed details on this hacker group's malicious activity // Jpost Inc. (https://www.jpost.com/business-and-innovation/article-752570?utm_source=flipboard&utm_content=JerusalemPost%2Fmagazine%2FBusiness+and+Innovation). 26.07.2023).***

***

«У новому звіті Check Point було виявлено масштаби фальшивої реклами, яка заважає платформам соціальних мереж, зокрема Facebook, з метою поширення шкідливого програмного забезпечення.

Компанія знайшла докази того, що шахраї створюють підроблені сторінки, які видають себе за провідні компанії штучного інтелекту (ШІ), щоб отримати вигоду від зростаючого апетиту до технології.

Згідно з даними фірми, такі популярні додатки зі штучним інтелектом, як ChatGPT, Bard, Midjourney і Jasper, імітуються в надії, що кіберзлочинці зможуть отримати конфіденційну особисту інформацію.

Ці оголошення у Facebook про штучний інтелект є фальшивими

Було помічено, що нелегальна реклама нібито пропонує нові та ексклюзивні послуги, спеціальний вміст та інші привабливі пропозиції, доступ до яких доступний лише через маршрут, який веде жертв до завантаження зловмисного програмного забезпечення.

Як правило, користувачі натискають посилання, щоб отримати доступ до обіцяного вмісту, який завантажує зловмисне програмне забезпечення, призначене для викрадення облікових даних, крипто-гаманців та будь-якої іншої особистої інформації.

Багато скріншотів, опублікованих Check Point, свідчать про те, що користувачі можуть отримати доступ до ексклюзивного та преміум-контенту, стежачи за оголошеннями, що, звичайно, не відповідає дійсності. Натомість користувачів закликають звертати пильну увагу на URL-адресу, коли вони перенаправляються на інший сайт, або, простіше кажучи, отримати доступ до потрібної сторінки чи компанії через довірений домен.

Що стосується сторінок у соціальних мережах, високий рівень взаємодії призводить до того, що багато фальшивих акаунтів накопичують тисячі або навіть мільйони лайків. Такий великий обсяг взаємодій може бути не позначений під час поверхневих і базових перевірок користувача.

У ширшому плані Check Point підкреслює зростаючу кількість випадків поширення інфокрадиків в епоху високої цінності даних.

Окрім перевірки URL-адрес, доменів і адрес електронної пошти, замість того, щоб довіряти відображуваному імені, яким можна маніпулювати, щоб воно виглядало легітимним, користувачам нагадують не завантажувати непотрібне програмне забезпечення та робити це лише через надійне джерело.

Коли ми запитали більше інформації про те, як Meta захищає користувачів, представник компанії спрямував нас на публікацію в блозі про безпеку облікових записів і іншу про онлайн-загрози». ***(Craig Hale. Facebook is being flooded with fake ads that are actually malware // Future US, Inc. (https://www.techradar.com/pro/facebook-is-being-flooded-with-fake-ads-that-are-actually-malware?utm_source=flipboard&utm_content=other). 27.07.2023).***

***

«Невідомі зловмисники використовують законну функцію пошуку Windows для завантаження довільних корисних даних із віддалених серверів і компрометації цільових систем за допомогою троянів віддаленого доступу, таких як AsyncRAT і Remcos RAT.

Нова техніка атаки, згідно з Trellix, використовує переваги обробника протоколу «search-ms:» URI, який надає можливість програмам і HTML-посиланням запускати настроювані локальні пошуки на пристрої, а також протоколу додатків «search:», механізм виклику програми пошуку на робочому столі в Windows.

«Зловмисники спрямовують користувачів на веб-сайти, які використовують функцію «search-ms» за допомогою JavaScript, розміщеного на сторінці», — заявили дослідники безпеки Матханрадж Тангараджу та Сіджо Джейкоб у звіті в четвер. «Ця техніка була навіть поширена на вкладення HTML, розширюючи поверхню атаки».

Під час таких атак було виявлено, що зловмисники створюють оманливі електронні листи, які містять гіперпосилання або вкладення HTML, що містять

URL-адресу, яка переспрямовує користувачів на скомпрометовані веб-сайти. Це запускає виконання JavaScript, який використовує обробники протоколу URI для виконання пошуку на сервері, контрольованому зловмисником.

Варто зазначити, що натискання посилання також створює попередження «Відкрити Провідник Windows?», підтверджуючи те, що «результати пошуку віддалено розміщених шкідливих файлів ярликів відображаються в Провіднику Windows під виглядом PDF-файлів або інших надійних піктограм, як і локальні результати пошуку», - пояснили дослідники.

«Ця розумна техніка приховує той факт, що користувачеві надаються віддалені файли, і створює у користувача ілюзію довіри. У результаті користувач, швидше за все, відкриє файл, припускаючи, що він з його власної системи, і несвідомо запустить шкідливий код».

Якщо жертва клацне на одному з файлів швидкого доступу, це призведе до виконання фальшивої динамічної бібліотеки (DLL) за допомогою утиліти regsvr32.exe.

В альтернативному варіанті кампанії файли ярликів використовуються для запуску сценаріїв PowerShell, які, у свою чергу, завантажують додаткові корисні дані у фоновому режимі, водночас відображаючи PDF-документ-приманку, щоб обдурити жертв.

Незалежно від використовуваного методу, зараження призводять до встановлення AsyncRAT і Remcos RAT, пропонуючи шлях для загрозливих суб’єктів дистанційно керувати хостами, викрадати конфіденційну інформацію та навіть продавати доступ іншим зловмисникам.

З огляду на те, що Microsoft постійно вживає заходів для обмеження різних початкових векторів доступу, очікується, що зловмисники можуть зачепитися за метод обробки протоколу URI, щоб уникнути традиційних засобів захисту та поширювати зловмисне програмне забезпечення.

«Важливо утримуватися від натискання підозрілих URL-адрес або завантаження файлів із невідомих джерел, оскільки ці дії можуть наражати системи на зловмисне корисне навантаження, що доставляється через обробник протоколу

URI «пошук» / «пошук-ms», — сказали дослідники». ***(Hackers Abusing Windows Search Feature to Install Remote Access Trojans // The Hacker News (https://thehackernews.com/2023/07/hackers-abusing-windows-search-feature.html). 28.07.2023).***

***

Вірусне та інше шкідливе програмне забезпечення

«…Обнаруженный исследовательской группой Cyber Intelligence Research в Guardz, ShadowVault был «специально создан для кражи конфиденциальных данных из систем macOS». И это стоит 500 долларов в месяц в даркнете, что вдвое меньше, чем вредоносное ПО Atomic macOS Stealer.

Guardz говорит, что ShadowVault — это не просто еще одно вредоносное ПО, это «сложная часть программного обеспечения, созданная с одной целью — воровать», и что вредоносное ПО может «оказать катастрофическое влияние на функциональные возможности бизнеса и конфиденциальность пользователей».

Что может скомпрометировать ShadowVault macOS Stealer?

ShadowVault, работая в фоновом режиме в фоновом режиме, может:

Извлекайте пароли, файлы cookie, кредитные карты, кошельки и все расширения на основе Chromium (Opera, Chrome, Edge, Vivaldi, Brave, Torch, Yandex и более 50 подключаемых браузеров).

Извлекайте пароли, файлы cookie, кредитные карты, кошельки и все расширения Firefox.

- Извлечь файлы (вы можете добавить/удалить любое расширение).
- Извлечение базы данных связки ключей (расшифровано и готово к импорту).
- Поддержка и расшифровка криптокошельков из всех браузеров (Metamask, Coinomi, Binance, Coinbase, Atomic, Exodus, Keplr, Phantom, Trust, Tron Link, Марсианин).
- Захват телеграмм.

Возможность настроить отстук логов в нескольких местах одновременно.

В рекламе даркнета также отмечается, что сборка вредоносного ПО может поставляться с «подписью разработчика Apple» за «дополнительную плату».

Как и Atomic macOS Stealer, кажется, что Safari не может быть скомпрометирован ShadowVault. Тем не менее, это вредоносное ПО по-прежнему представляет собой серьезную угрозу, способную скомпрометировать большинство других браузеров и даже цепочку ключей Apple, в которой хранится много конфиденциальной информации для многих пользователей Mac…» ***(Michael Potuck. ShadowVault macOS Stealer surfaces as the newest sophisticated Mac malware // 9to5mac (https://9to5mac.com/2023/07/10/shadowvault-macos-stealer-mac-malware-surfaces/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 10.07.2023).***

***

«По крайней мере, с мая 2021 года незаметное вредоносное ПО для Linux под названием AVrecon использовалось для заражения более 70 000 маршрутизаторов малых и домашних офисов (SOHO) на базе Linux и добавления их в ботнет, предназначенный для кражи полосы пропускания и предоставления скрытого резидентного прокси-сервиса.

Это позволяет его операторам скрывать широкий спектр вредоносных действий, от мошенничества с цифровой рекламой до распыления паролей.

По данным исследовательской группы Black Lotus Labs компании Lumen, несмотря на то, что троян удаленного доступа AVrecon (RAT) скомпрометировал более 70 000 устройств, только 40 000 были добавлены в ботнет после того, как он стал постоянным.

Вредоносной программе в значительной степени удалось избежать обнаружения, поскольку она была впервые обнаружена в мае 2021 года, когда она была нацелена на маршрутизаторы Netgear. С тех пор он оставался незамеченным более двух лет, постепенно привлекая новых ботов и превращаясь в один из

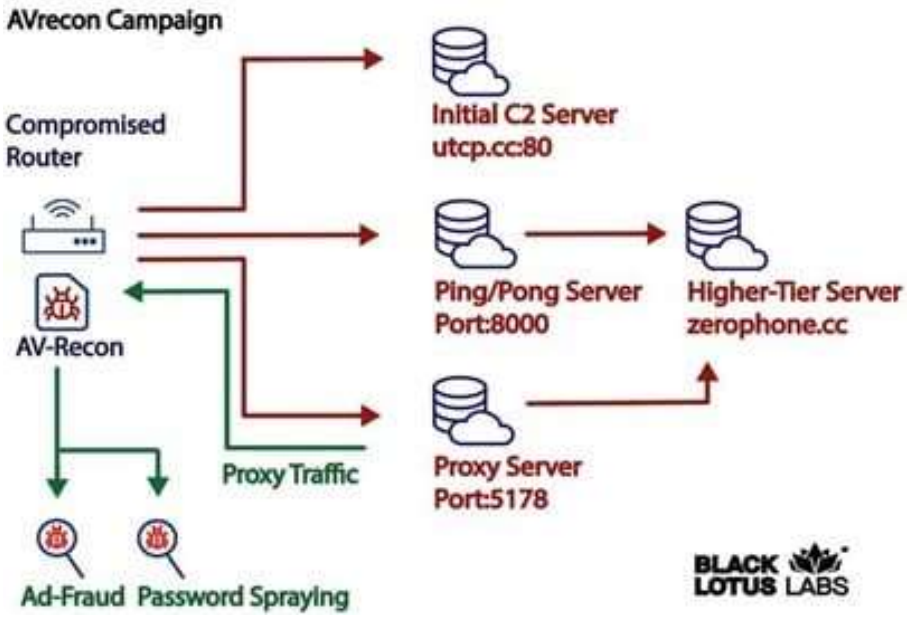
крупнейших ботнетов, ориентированных на маршрутизаторы SOHO, обнаруженных за последние годы.

«Мы подозреваем, что субъект угрозы, сосредоточенный на типе устройств SOHO, с меньшей вероятностью будет исправлять распространенные уязвимости и воздействия (CVE)», — заявили в Black Lotus Labs.

«Вместо того, чтобы использовать этот ботнет для быстрой выплаты, операторы придерживались более умеренного подхода и могли работать незамеченными более двух лет. Из-за скрытного характера вредоносного ПО владельцы зараженных машин редко замечают какие-либо сбои или потери обслуживания. пропускной способности».

После заражения вредоносная программа отправляет информацию о скомпрометированном маршрутизаторе на встроенный сервер управления и контроля (C2). После установления контакта взломанная машина получает указание установить связь с независимой группой серверов, известной как C2-серверы второго уровня.

Исследователи безопасности обнаружили 15 таких управляющих серверов второго уровня, которые работают как минимум с октября 2021 года, на основе информации о сертификате x.509.



Атаки AVrecon (Black Lotus Labs)

Группа безопасности Black Lotus компании Lumen также справилась с угрозой AVrecon, установив нулевую маршрутизацию сервера управления и контроля (C2) ботнета в своей магистральной сети.

Это фактически разорвало соединение между вредоносным ботнетом и его центральным управляющим сервером, что значительно ограничило его способность выполнять вредоносные действия.

«Использование шифрования не позволяет нам комментировать результаты успешных попыток распыления паролей; тем не менее, мы обнулили узлы управления и контроля (C2) и заблокировали трафик через прокси-серверы, что сделало ботнет инертным в магистрали Lumen», — заявили в Black Lotus Labs.

В недавно изданной обязательной операционной директиве (BOD), опубликованной в прошлом месяце, CISA приказала федеральным агентствам США обеспечить безопасность сетевого оборудования, доступного в Интернет (включая маршрутизаторы SOHO), в течение 14 дней после обнаружения, чтобы заблокировать возможные попытки взлома.

Как предупреждает CISA, успешная компрометация таких устройств позволит злоумышленникам добавить взломанные маршрутизаторы в свою инфраструктуру атаки и предоставить им стартовую площадку для горизонтального перемещения в свои внутренние сети.

Серьезность этой угрозы связана с тем, что маршрутизаторы SOHO обычно находятся за пределами обычного периметра безопасности, что значительно снижает способность защитников обнаруживать вредоносные действия.

Китайская кибершпионская группа Volt Typhoon использовала аналогичную тактику для создания скрытой прокси-сети из взломанного сетевого оборудования ASUS, Cisco, D-Link, Netgear, FatPipe и Zyxel SOHO, чтобы скрыть свою вредоносную активность в законном сетевом трафике. рекомендации, опубликованные агентствами кибербезопасности Five Eyes (включая ФБР, АНБ и CISA) в мае.

Скрытая прокси-сеть использовалась китайскими государственными хакерами для атак на критически важные инфраструктурные организации в Соединенных Штатах по крайней мере с середины 2021 года.

«Субъекты угроз используют AVrecon для прокси-трафика и участия в злонамеренных действиях, таких как распыление паролей. Это отличается от прямого нацеливания на сеть, которое мы видели в других наших обнаруженных вредоносных программах на основе маршрутизаторов», — сказала Мишель Ли, директор по анализу угроз Lumen Black Lotus Labs.

«Защитники должны знать, что такая злонамеренная активность может исходить от того, что кажется резидентным IP-адресом в стране, отличной от фактического происхождения, и трафик с скомпрометированных IP-адресов будет обходить правила брандмауэра, такие как геозоны и блокировка на основе ASN». ***(Sergiu Gatlan. AVrecon malware infects 70,000 Linux routers to build botnet // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/avrecon-malware-infects-70-000-linux-routers-to-build-botnet/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 14.07.2023).***

***

«…Історія комп'ютерних вірусів тягнеться з початку 1970-х років. У 1971 році вірус, відомий як «Creeper», був розроблений як експеримент, щоб побачити, як він діятиме як шкідлива програма. Оскільки це був контрольований вірус, Creeper не досяг зовнішнього світу.

Перший комп'ютерний вірус, який заразив пристрої реального світу, виник у 1982 році та отримав назву «Elk Cloner». Цей вірус був створений старшокласником як розіграш серед своїх друзів, але існував у дикій природі і тому був першим прикладом вірусу «на волі» (тобто не в контрольованому середовищі).

Elk Cloner став першим вірусом, і його охоплення вийшло далеко за межі його творця та його групи друзів. Однак завдати великої шкоди йому не вдалося

через обмежені можливості. Зрештою, Elk Cloner був розроблений як розіграш і не мав можливості здійснювати шкідливі дії на заражених пристроях.

Інші стверджували б, що програма, відома як «Мозок», була першим комп'ютерним вірусом у дикій природі. Brain використовував дискети як вектор зараження, і вперше було помічено зараження пристроїв у 1986 році, через чотири роки після створення Elk Cloner. Brain використовував виконуваний код, щоб заразити завантажувальний сектор дискети, а потім комп’ютер, коли диск вставлено. Вірус встиг заразити понад 100 000 комп’ютерів, що на той час було вражаючим числом.

Однак Brain нічого не зробив, окрім уповільнення продуктивності дисководів. Лише на рубежі століть віруси показали свої справжні можливості.

У 2000 році вірус, відомий як «ILOVEYOU», спричинив хаос, заразивши понад 10 мільйонів комп’ютерів Windows.

Вірус поширювався електронною поштою, яка була неймовірно популярною навіть у 2000 році. На відміну від попередніх обговорюваних вірусів, ILOVEYOU мав можливість видаляти файли на зараженому пристрої.

Протягом наступного десятиліття з’явилося й зникло багато інших вірусів, зокрема Slammer, CodeRed і MyDoom. MyDoom досі залишається найшвидше поширюваним вірусом електронної пошти в історії та існує й сьогодні. У 2019 році, через 15 років після першого використання, його навіть використовували в кампанії зловмисної електронної пошти.

Але чи все ще віруси становлять ту саму небезпеку, що й раніше? Яке становище цих програм у кіберзлочинності сьогодні?

Хоча колись віруси були найнебезпечнішою формою кіберзагрози, зараз це не так. На початку 2010-х років поширеність комп’ютерних вірусів почала знижуватися, з останніми кількома великими вірусними кампаніями, зокрема Stuxnet, SpyEye та W32.Dozer.

Після цього в галузі кібербезпеки віруси почали з’являтися позаду.

Але чому?

Основною причиною, чому віруси більше не становлять величезної загрози, є технологічний прогрес. Антивірусні програми, доступні для використання на початку 2000-х років, значно відрізнялися від тих, які ми використовуємо зараз, оскільки час поступився місцем вищим рівням виявлення, додатковим функціям і кращому сервісу в цілому.

Віруси не є неймовірно складними програмами і тому не дуже великі. Як і в біологічному світі, вірусам потрібен «хазяїн», на якому вони можуть розмножуватися. Оскільки їм потрібно проникнути в програму, типові віруси мають бути досить малими. Це не залишає багато місця для додаткового кодування, яке надасть вірусу складні можливості.

Крім того, багато вірусів працюють за подібним сценарієм, тобто вони часто не є чимось новим для антивірусних програм. Програми-вимагачі, шпигунські програми, троянські коні та подібне зловмисне програмне забезпечення є найбільш поширеними на сьогоднішній день і є тим, що справді становить загрозу для наших комп’ютерів і смартфонів.

Ці зловмисні програми можуть бути дуже складними та іноді розроблені, щоб повністю уникнути антивірусного програмного забезпечення. Загалом, віруси просто не тримають свічки перед сучасним шкідливим програмним забезпеченням, тому вони використовуються не так часто, як колись.

Програми-вимагачі, зокрема, стали величезною тенденцією кіберзлочинності протягом 2010-х років. Ця форма зловмисного програмного забезпечення шифрує файли зараженого пристрою та попереджає жертв, що файли будуть розшифровані, лише якщо буде сплачено вимаганий викуп. Деякі популярні приклади програм-вимагачів включають WannaCry, LockBit, Jigsaw і Bad Rabbit.

Багато операторів програм-вимагачів отримують зловмисне програмне забезпечення з платформ-вимагачів як послуг, де програми-вимагачі продаються стороннім кіберзлочинцям за певну плату. Завдяки цьому програмне забезпечення-вимагач стає доступним для зловмисників, які менш підковані в техніці, а не лише для досвідчених професіоналів.

Очевидно, що зараз існують більш гострі проблеми кібербезпеки, ніж віруси. Але віруси не залишилися в минулому. Як згадувалося раніше, у 2019 році було виявлено використання колись грізного вірусу MyDoom. У цьому випадку MyDoom поширювався через фішингову електронну кампанію. Незважаючи на те, що сьогодні їх можна вважати основними, віруси все ще використовуються, і це дуже важливо мати на увазі.

З роками значення терміна «антивірус» змінилося. Хоча колись антивірусні програми створювалися для захисту від вірусів і лише від вірусів, тепер вони можуть виявляти та видаляти інші види зловмисного програмного забезпечення.

Як ви, мабуть, знаєте, зловмисне програмне забезпечення є глобальною проблемою, яка щомісяця забирає тисячі жертв. Насправді, за даними Statista, щодня служби кібербезпеки виявляють 560 000 нових шкідливих програм. Це майже 17 мільйонів нових предметів, які виявляють щомісяця.

Statista також повідомила, що за останнє десятиліття кількість атак зловмисного програмного забезпечення зросла на 87%. Лише ці дві статистичні дані показують, наскільки серйозною стала проблема зловмисного програмного забезпечення.

Отже, вам все одно потрібна антивірусна програма, щоб захистити ваші пристрої від кіберзлочинності.

Завжди краще вибрати антивірусну програму з високою репутацією, яка довела свою корисність для захисту від вірусів і шкідливих програм. Встановлення випадкової безкоштовної антивірусної програми — не найрозумніший спосіб, оскільки ви можете мати справу з слабким захистом або навіть зі шкідливою програмою, яка маскується під антивірусне програмне забезпечення.

Ось деякі з найпопулярніших антивірусних програм:

McAfee.

Kaspersky.

Нортон.

Bitdefender.

Malwarebytes.

Якщо ви дуже стурбовані кібератаками, ви можете одночасно використовувати антивірусні програми та програми для захисту від зловмисного програмного забезпечення, щоб ще більше підвищити рівень безпеки. Програми для захисту від зловмисного програмного забезпечення можуть виявляти та видаляти складніші типи зловмисного програмного забезпечення, наприклад ті, які призначені для ухилення від виявлення антивірусу.

Сприйнятливість нашого пристрою до вірусів значно зменшилася за останнє десятиліття чи близько того, але зараз існують інші форми зловмисного програмного забезпечення, яке становить загрозу нашій безпеці. Ось чому наявність антивірусної програми, безсумнівно, має першочергове значення». ***(Katie Rees. Are Viruses Still a Threat to Cybersecurity? // MUO (https://www.makeuseof.com/are-viruses-still-a-threat/). 16.07.2023).***

***

«Дослідники кібербезпеки стали жертвами власного підробленого PoC-експлойту CVE-2023−35 829, який встановлює шкідливе ПЗ для крадіжки паролів Linux.

Аналітики Uptycs виявили шкідливий PoC (Proof-of-Concept) під час своїх звичних перевірок — системи виявлення повідомили про несподівані мережеві підключення, спроби несанкціонованого доступу до системи та нетипові передачі даних.

Загалом було виявлено 3 репозиторії, в яких розміщувався шкідливий підроблений PoC-експлойт, 2 з яких були видалені з GitHub, а 1 все ще працює. Шкідливий PoC-код виявився широко поширеним серед членів спільноти дослідників, тому зараження можуть існувати на значній кількості комп’ютерів.

PoC, завантажені з інтернету, необхідно тестувати в ізольованих середовищах, таких як віртуальні машини, і, якщо можливо, перевіряти їхній код перед виконанням. Надсилання двійкових файлів до VirusTotal також є швидким і простим способом ідентифікації шкідливого файлу, наголосили спеціалісти». ***(Кіберфахівці стали жертвами власного експлойту // No worries!***

(https://noworries.news/kiberfahivczi-staly-zhertvamy-vlasnogo-eksplojtu/). 14.07.2023).

***

«Хакери запустили масштабну кампанію, яка використовує нове шкідливе програмне забезпечення Mac для націлювання на вразливі комп'ютери Apple, намагаючись викрасти паролі, криптовалюту та інші конфіденційні дані.

Як повідомляє BleepingComputer, цей новий штам зловмисного програмного забезпечення було названо «Realst» дослідником безпеки, який виявив його, і зараз він поширюється через підроблені блокчейн-ігри.

Щоб змусити потенційних жертв завантажити ці шкідливі ігри, кіберзлочинці, які стоять за цією кампанією, рекламують їх у соціальних мережах, а також використовують прямі повідомлення, щоб надати коди доступу, необхідні для їх завантаження. Однак ці коди доступу насправді служать іншій меті, оскільки вони дозволяють хакерам перевіряти цілі та вирішувати, за ким справді варто йти.

Окрім націлювання на комп'ютери Mac, ця кампанія також заражає користувачів Windows зловмисним програмним забезпеченням RedLine Stealer, яке має подібні функції до Realst. Незалежно від того, чи використовуєте ви Mac чи Windows, вам потрібно бути обережними, завантажуючи ігри з неофіційних онлайн-магазинів, і це стосується тих, у кого вдома є молоді геймери, оскільки вони можуть легко заразити ваш комп'ютер шкідливим програмним забезпеченням.

Крадіжка даних із браузерів і Apple Keychain

Проаналізувавши 59 різних зразків Mach-O зловмисного програмного забезпечення Realst, компанія з кібербезпеки SentineOne виявила кілька явних відмінностей між ними. Його дослідники безпеки також ідентифікували 16 варіантів зловмисного програмного забезпечення та надали додаткову інформацію про них у новій публікації в блозі.

Коли користувачі Mac намагаються завантажити будь-яку з підроблених блокчейн-ігор, використаних у цій кампанії, інсталятори PKG або дискові файли DMG, які використовуються для їх розповсюдження, містять шкідливі файли Mach-O, але не містять ігор. Щоб обійти заходи безпеки Apple, відповідальні хакери використовують дійсні, хоча тепер анульовані, ідентифікатори розробників Apple для підпису своїх інсталяторів.

Хоча існує 16 різних варіантів шкідливого програмного забезпечення Realst, усі вони націлені на такі популярні браузери, як Firefox, Chrome, Opera, Brave Vivaldi та додаток Telegram. Дивно, але жоден із варіантів, проаналізованих SentinelOne, не націлений на Safari. Зловмисне програмне забезпечення Realst здатне викрадати паролі, файли cookie та інші конфіденційні дані, що зберігаються в браузері користувача, але також переслідує будь-які паролі, збережені в Apple Keychain виробника iPhone, який є власним менеджером паролів.

Дивно, але творці Realst вже підготувалися до націлювання на комп'ютери Mac під керуванням macOS 14 Sonoma, яка ще не випущена.

Як захиститися від шкідливих програм Mac

Коли справа доходить до захисту від зловмисного програмного забезпечення Realst, усе, що вам зараз потрібно робити, це уникати завантаження неоднозначних ігор онлайн. Однак коли інші кіберзлочинці почнуть використовувати Realst у своїх атаках, це може змінитися.

З цієї причини ви хочете бути надзвичайно обережними, завантажуючи нові програми для свого Mac. Як і у випадку з найкращими iPhone, вам краще знайти нові програми для свого Mac у Apple App Store, а не завантажувати та встановлювати їх вручну з будь-якого місця. Це пов'язано з тим, що програми мають пройти низку різних перевірок безпеки, перш ніж їх можна буде опублікувати в App Store.

Незважаючи на те, що Apple додає власне антивірусне програмне забезпечення XProtect до кожного комп'ютера, який вона продає, а комп'ютери Mac також мають вбудований сканер зловмисного програмного забезпечення під назвою Gatekeeper, вам все одно може знадобитися трохи додаткового захисту.

Саме тут може допомогти найкраще антивірусне програмне забезпечення для Mac, оскільки ці сторонні рішення оновлюються частіше, щоб захистити ваш Mac від усіх останніх штамів зловмисного програмного забезпечення.

Протягом останніх кількох років ми спостерігаємо значне зростання кількості зловмисного програмного забезпечення, розробленого спеціально для комп'ютерів Mac, і поки найкращі MacBook та інші комп'ютери від Apple продовжуватимуть продаватися так само, як і вони, ця тенденція, ймовірно, триватиме. Ось чому користувачі Mac повинні почати сприймати зловмисне програмне забезпечення так само серйозно, як і їхні колеги, які використовують Windows». ***(Anthony Spadafora. Macs under attack from password-stealing malware — how to stay safe // Future US, Inc. (https://www.tomsguide.com/news/macs-under-attacks-from-password-stealing-malware-how-to-stay-safe?utm_source=flipboard&utm_content=shaneless%2Fmagazine%2FAPPLE+UPROOTED). 26.07.2023).***

***

Програми-вимагачі

«Компания по кибербезопасности Fortinet выявила новую аферу с вымогательством денег, замаскированную под страницу обновления Windows, и призвала пользователей самой популярной настольной ОС быть бдительными.

Атака, которую исследователи из подразделения FortiGuard Labs оценивают как очень серьезную, шифрует файлы на скомпрометированной машине. В обмен на свои файлы обратно злоумышленник требует выкуп.

Считается, что вариант программы-вымогателя, известный как Big Head, был запущен в мае 2023 года. Приблизительно три текущих варианта предназначены для шифрования файлов на компьютерах жертв с целью вымогательства денег.

FortiGuard Labs говорит, что «нет никаких признаков того, что Big Head широко распространена», но, учитывая, что на данный момент ему всего несколько недель, трудно предсказать, как быстро он может распространиться.

До сих пор аналитики наблюдали два варианта игры. На первом отображается фальшивый экран Центра обновления Windows с надписью «Настройка критических обновлений Windows». Как только он исчезнет с экрана примерно через 30 секунд, он уже будет иметь зашифрованные файлы пользователей «со случайно измененными именами».

Было замечено, что несколько файлов «README» содержат адреса электронной почты, данные учетной записи Telegram и даже биткойн-адрес, все из которых предназначены для сбора денег с жертв под обещание расшифровки файлов.

Вторая версия использует другой метод, который для конечного пользователя приведет к тому, что злоумышленник изменит обои рабочего стола на записку о выкупе, требуя один биткойн (в настоящее время около 30 000 долларов).

Похоже, что программа-вымогатель Big Head в настоящее время нацелена на потребителей в США, хотя некоторые другие атаки той же группы также наблюдались в Испании, Франции и Турции.

FortiGuard приходит к выводу, что, поскольку большинство программ-вымогателей обычно доставляются с помощью фишинговых атак, некоторые простые знания о защите от кибербезопасности и гигиене могут предотвратить их.

Необходимо учитывать частоту резервного копирования данных, местоположение и безопасность, поскольку атаки программ-вымогателей становятся все более распространенными и более совершенными». ***(Craig Hale. Watch out - that Windows update could actually just be ransomware // Future US, Inc. (https://www.techradar.com/pro/watch-out-that-windows-update-could-actually-just-be-ransomware?utm_source=flipboard&utm_content=aj7iohv%2Fmagazine%2FCONCEPT+%21++++++++++++++++++SPACE+%21++++++++++++++++++++++++++++++++++TECH+.+.+.). 10.07.2023).***

***

«Никто не хочет стать жертвой программ-вымогателей, но в новом отчете компании Chainalysis, занимающейся безопасностью блокчейнов, утверждается, что выплаты программ-вымогателей могут быть установлены на рекордный год, а преступники загребут около полумиллиарда долларов всего за семь месяцев до 2023 года.

Согласно анализу, платежи программ-вымогателей в этом году составили 449,1 миллиона долларов. Это на 175,8 миллиона долларов больше, чем в прошлом году, что позволяет предположить, что хакеры удвоили ставку на этот метод извлечения денег из несчастных жертв.

В отчете основное внимание уделялось развертыванию программ-вымогателей в блокчейне, где задействованы криптовалюты. Уже в июле 2023 года этот тип атаки собрал почти все, что было потеряно от аналогичных атак за весь 2022 год. Если тенденция этого года сохранится, пользователи программ-вымогателей могут украсть до $898,6 млн.

Так почему же программы-вымогатели так преуспевают в этом году? Chainalysis считает, что это в значительной степени связано с тем, что преступные группировки уделяют повышенное внимание учреждениям «крупной игры», то есть «крупным организациям с глубокими карманами», говорится в отчете. Банды вымогателей часто вымогают процент от дохода фирмы, поэтому чем крупнее организация, тем больше отдача. Самым прибыльным штаммом программы-вымогателя был Cl0p, средний средний платеж за который составил более 1,9 миллиона долларов.

Однако это не означает, что мелкие пользователи защищены от когтей банд, поскольку Chainalysis объясняет, что «количество успешных небольших атак также выросло» за тот же период времени. По всем направлениям доходы от программ-вымогателей растут.

Интересно, что в отчете отмечается, что все остальные формы киберпреступности с использованием криптовалюты, от взломов и торговых

площадок даркнета до мошенничества и материалов о жестоком обращении с детьми, сократились по сравнению с 2022 годом, который был чрезвычайно прибыльным годом для киберпреступности. В некоторых случаях падение было значительным.

Например, мошенничество с криптовалютой принесло на 3,3 миллиарда долларов меньше, чем они заработали к этому моменту в прошлом году, что означает значительное падение на 77%. Chainalysis считает, что это отчасти связано с двумя огромными мошенническими действиями — VidiLook и Chia Tai — которые закончились и убежали со средствами пользователей. Считается, что один только VidiLook обманул жертв на 120 миллионов долларов. До сих пор было не так много крупных мошенников, способных их заменить.

В других местах взломы были еще одним крупным проигрышем в 2023 году, при этом общий доход от вторжений упал более чем на 1,1 миллиарда долларов по сравнению с 2022 годом. В совокупности (и даже с учетом увеличения прибыли от программ-вымогателей) общий доход от крипто-преступлений снизился на 5,2 миллиарда долларов в годовом исчислении.

Это обнадеживающий признак в борьбе с киберпреступностью. Однако это не значит, что кто-то может быть самодовольным. Если вы хотите обезопасить себя, рекомендуется установить надежное антивирусное программное обеспечение, использовать один из лучших менеджеров паролей, не переходить по опасным ссылкам и вообще не забывать о себе при просмотре веб-страниц». ***(Alex Blake. Ransomware attacks have spiked massively. Here's how to stay safe // Digital Trends Media Group (https://www.digitaltrends.com/computing/ransomware-profits-huge-spike-versus-2022/?utm_source=flipboard&utm_content=DigitalTrends%2Fmagazine%2FDigital+Trends%3A+Tech+for+the+Way+We+Live). 13.07.2023).***

***

«Программы-вымогатели представляют наибольшую угрозу для организаций и их повседневных операций, что приводит к увеличению

сложности и затрат на защиту цифровых сред. По оценкам, только в Южной Африке киберпреступность ежегодно обходится в 2,2 миллиарда рандов с финансовыми, репутационными и операционными последствиями для целевых организаций.

Как эволюционировали программы-вымогатели?

Эволюция программ-вымогателей привела к тому, что киберпреступники перешли от поддельного антивирусного программного обеспечения к выдаче себя за правоохранительные органы в Интернете, что в конечном итоге привело к росту числа вредоносных программ-шифровальщиков в 2015 году. Это позволило хакерам блокировать файлы устройств до тех пор, пока не будет выплачен выкуп, чему способствовала анонимность криптовалют, таких как Биткойн. Методы атак перешли от неизбирательной массовой рассылки к более целенаправленным проникновениям, получению прав администратора и шифрованию определенных файлов в сетях.

Почему оно развивается?

По мере того как атаки программ-вымогателей становятся все более изощренными, злоумышленники используют различные тактики, чтобы заставить жертв платить, например, поэтапную публикацию данных, угрозы распределенных атак типа «отказ в обслуживании» (DDoS) и преследование клиентов и поставщиков в социальных сетях. Эти преступники адаптируются к изменениям в своей среде, реагируя на такие факторы, как улучшенные меры кибербезопасности, эффективность правоохранительных органов, вмешательство финансовых учреждений, изменения в законодательстве и недостатки операционной безопасности в своих сетях.

Несмотря на временное снижение активности программ-вымогателей в 2022 году, организации должны сохранять бдительность и проявлять инициативу. Ожидается, что будущие стратегии борьбы с программами-вымогателями будут включать в себя устранение уязвимостей нулевого дня, усиление операционной безопасности в криминальных сетях, оптимизацию доходов за счет автоматизации и акцент на облачных серверах Linux и других платформах.

Что должны делать организации?

Организации должны принять комплексную стратегию кибербезопасности, охватывающую людей, процессы и технологии, чтобы предотвратить и смягчить атаки программ-вымогателей. Это включает в себя регулярные тренинги по безопасности для персонала, полную видимость сети, моделирование угроз для выявления рисков и внедрения необходимых средств контроля, а также внедрение таких решений, как управление рисками поверхности атаки и расширенное обнаружение и реагирование (XDR). Стратегия нулевого доверия в сочетании с планом реагирования на инциденты и безопасными системами резервного копирования дополнительно снижает воздействие потенциальных кибератак.

Осознавая важность надежной системы безопасности и следя за развивающимися тактиками угроз, организации могут эффективно защитить себя от следующей волны программ-вымогателей. Специалисты по кибербезопасности играют решающую роль в адаптации к новым вызовам и защите бизнеса от потенциальных киберугроз». ***(Mamsi Nkosi. The evolution of ransomware: How cyber threat went from online pickpocket to a criminal syndicate? // African Technology Advisory (Pty) Ltd. (https://www.itnewsafrica.com/2023/07/the-evolution-of-ransomware-how-cyber-threat-went-from-online-pickpocket-to-a-criminal-syndicate/?utm_source=flipboard&utm_content=other). 14.07.2023).***

***

«Традиційні атаки програм-вимагачів занепадають, оскільки компанії відмовляються платити, але згідно з новим звітом фірми з кібербезпеки SonicWall, криптовалюти все ще використовуються для вимагання нічого не підозрюючих жертв.

У першій половині 2023 року було зафіксовано приголомшливі 332,3 мільйона атак криптоджекінгу — це на 399% більше, ніж за весь минулий рік. Якщо подати цю цифру в контекст, це більше, ніж 2020, 2021 і 2022 разом узяті.

Криптоджекінг передбачає використання серверів і пристроїв, що належать іншим людям, для видобутку цифрових активів, причому Monero, орієнтований на

конфіденційність, є найпопулярнішим. Постраждалі можуть навіть не усвідомлювати, що вони жертви; вони можуть просто помітити, що їхні машини працюють повільніше, ніж зазвичай.

Спенсер Старкі, віце-президент SonicWall у регіоні EMEA, повідомив Decrypt електронною поштою, що найбільшими симптомами криптоджекінгу є повільніша реакція на пристроях, несподівано вищі рахунки за електроенергію та надмірне використання вентиляторів, спричинене перегрітими батареями.

«Оскільки криптозловмисники прагнуть залишатися непоміченими якомога довше, це може сприйматися як злочин без жертв у порівнянні зі шкідливим програмним забезпеченням, таким як програми-вимагачі або банківські трояни», — сказав Старкі.

І хоча ви можете подумати, що падіння цін на біткойни спонукатиме зловмисників перенаправити свою злочинну діяльність в інше місце, дослідження SonicWall показують, що падіння ринку насправді призвело до протилежного ефекту — кількість атак зростає, оскільки злочинці намагаються отримати ті самі прибутки.

«Актори загроз невпинні, і наші дані вказують на те, що вони більш опортуністичні, ніж будь-коли, націлюючись на школи, державні та місцеві органи влади та роздрібні організації з безпрецедентною швидкістю», — сказав президент і генеральний директор SonicWall Боб ВанКірк у прес-релізі, надісланому електронною поштою Decrypt.

Цифри свідчать про те, що зловмисники шукають менш дорогі та менш ризиковані способи швидкого заробітку.

Згідно з піврічним звітом SonicWall, США, Данія, Німеччина, Франція та Об’єднані Арабські Емірати найбільше постраждали від криптозлому, а вся Європа стала свідком зростання кількості інцидентів на 788%.

Це дослідження малює картину кіберзлочинців, які постійно змінюють свою тактику, щоб уникнути захоплення. Одним із поширених методів нападу на жертв останніх місяців було розповсюдження зловмисного ПЗ HonkBox у зламаних

версіях програмного забезпечення для редагування відео Final Cut Pro. Як говорить стара приказка, безкоштовного обіду не буває.

І хоча криптовикрадення може здатися добрішим, ніж шифрування файлів компанії та погрози випустити їх, якщо Monero не буде виплачено, ті, хто стоїть за цими атаками, все одно не мають сумніву. У першій половині 2023 року кількість інцидентів, пов'язаних із галуззю охорони здоров'я, зросла в 69 разів, ніж за аналогічний період минулого року. Сектор освіти також зазнав у 320 разів більше атак.

«Хакери шукають найслабші точки входу з найменшими можливими наслідками, обмежуючи свій ризик і максимізуючи потенційні прибутки», — сказав віце-президент SonicWall із безпеки продуктів Боббі Корнуелл.

Хоча ще рано списувати з рахунків загрозу програм-вимагачів, які поставили на коліна Національну службу охорони здоров'я Великобританії у 2017 році та призупинили Colonial Pipeline у 2021 році, ці цифри вказують на те, що жадібні до криптовалют хакери не йти куди завгодно.

Далі Старкі попередила, що криптоджекінг був перейнятий загрозами, підтримуваними національною державою, аж до співробітників, які розгортають майнери в корпоративній інфраструктурі без дозволу.

«Завдяки можливостям прихованого виявлення та рентабельності інвестицій для акторів — впровадження ймовірно продовжуватиме зростати в екосистемі акторів-загроз», — сказав він». ***(Connor Sephton. Ransomware May Be Dying Out, But Cryptojacking Is Up 399%: Cybersecurity Firm // Decrypt Media, Inc. (https://decrypt.co/150112/ransomware-may-be-dying-but-cryptojacking-is-399-cybersecurity-firm). 26.07.2023).***

***

«Рішення для керованої передачі файлів (MFT) MOVEit Transfer від Progress Software зазнає постійних атак з боку сумнозвісної групи загроз Cl0p, яка використовує численні критичні вразливості нульового дня. MOVEit Transfer — це локальний або хмарний сервер передачі файлів, який надає

організаціям рішення для збору, зберігання, керування та розповсюдження інформації між їхніми партнерами та клієнтами. Після успішної експлуатації зловмисники змогли отримати великі масиви конфіденційної інформації з багатьох галузей промисловості, які пізніше використовувалися для вимагання викупу від жертв. Дослідницька компанія Emsisoft протягом всієї кампанії відстежувала кількість скомпрометованих організацій. На сьогодні Emsisoft виявила, що щонайменше 383 організації були скомпрометовані в рамках кампанії MOVEit по всьому світу, що негативно вплинуло на понад 20 мільйонів людей 1. Програмне забезпечення Progress Software пом'якшило це дуже складна гра «вдарити крота». коли вразливості виправлялися, суб'єкти загрози виявляли нову вразливість, щоб використати її для отримання тієї самої вигоди. На сьогоднішній день відомі вразливості виправлено, і Progress запропонував ручні методи пом'якшення на випадок появи нових уразливостей.

Вразливі місця

Є три (3) основні вразливості, які використовувалися учасниками Cl0p для компрометації організацій-жертв: CVE-2023-34362 2, CVE-2023-35036 3 і CVE-2023-35708 4. Недоліки — це вразливості SQL-ін'єкції, які дозволяють суб'єктам загрози підвищити свої привілеї для виконання віддаленого коду (RCE). 5 напади. Зловмисник може використати ці вразливості, надсилаючи зловмисно створені корисні навантаження на вразливі кінцеві точки MOVEit Transfer, дозволяючи модифікувати бази даних і викрадати дані в них.

Програмне забезпечення-вимагач Cl0p

Протягом останніх кількох років програмне забезпечення-вимагач Cl0p активно використовувалося як програма-вимагач як послуга (RaaS), яка практикує подвійне вимагання: шифрування даних жертв і використання цих даних для подальшого вимагання від жертв викупу в обмін на ключі дешифрування. Жертви, які не співпрацюють, часто зрештою виявляють свої дані на сайті зловмисника, де витік даних. Незважаючи на те, що їхнім способом дії були кампанії програм-вимагачів, Cl0p нещодавно почали активно використовувати стратегії «знищи та захопи», які лише вилучають дані, а не шифрують дані на серверах-жертвах. Це

було помічено в компрометації сервера Fortra/Linoma GoAnywhere MFT Cl0p на початку 2023 року, кампанії атаки Accellion File Transfer Appliances (FTA) у 2020-2021 роках і кампанії атаки SolarWinds Serv-U у 2021 році. Що ще гірше, Cl0p опублікував дані своїх жертв у відкритому Інтернеті через окремі зареєстровані веб-сайти. На відміну від публікацій лише на своєму сайті витоків темної мережі, до якого користувачам важче отримати доступ і повільніше завантажувати, Cl0p реєструє веб-сайти для компаній, які вони зламали. Дані, які зазвичай публікуються на їхньому сайті витоку, тепер доступні для завантаження з відкритого Інтернету, що означає, що експоненціально більша кількість людей може легко отримати доступ до даних. Програма Rewards for Justice Державного департаменту США пропонує до 10 мільйонів доларів США за інформацію, яка пов’язує банду програм-вимагачів Cl0p з іноземним урядом 6, сподіваючись покласти край нечесній діяльності групи…

Як це працює

Дослідники стверджують, що основною ознакою того, що сервер було зламано, є наявність веб-оболонки під назвою "human2.asp", розташованої в загальнодоступній папці HTML "c:\MOVEit Transfer\wwwroot\". 7, який під час доступу виконає сценарій із різними шкідливими командами. Виконання сценарію дозволяє зловмиснику виконувати такі дії, як завантаження конфіденційних файлів і інформації, створення нових привілейованих користувачів і проведення розвідки налаштованого облікового запису Azure Blob Storage, дозволяючи загрозливому суб’єкту викрадати дані безпосередньо з контейнерів Azure Blob Storage жертви.. Старший менеджер відділу дослідження вразливостей Rapid7 заявив, що є докази того, що зловмисники вже автоматизували використання цих уразливостей і почали масово завантажувати дані з постраждалих компаній...

Вплив

Тисячі екземплярів MOVEit Transfer доступні в загальнодоступному Інтернеті, причому більшість із них розташовані в Сполучених Штатах, включаючи державні установи США. Розслідування цієї кампанії нападів показали, що жертви були скомпрометовані багатьма різними способами, незалежно від того, чи це було

скомпрометовано безпосередньо компанію, скомпрометовано через третю сторону чи підрядником через третю сторону. Станом на 18 липня 2023 року було щонайменше 383 організації-жертви, скомпрометовані Cl0p, що вплинуло на майже двадцять мільйонів осіб. Організації працюють у багатьох галузях, включаючи приватні організації, школи США, державний сектор США та міжнародний державний сектор. З 383 постраждалих організацій багато з них надають послуги кільком організаціям, а це означає, що показники жертв продовжуватимуть зростати.

Постраждалі особи не лише чутливі до наслідків кампанії атаки MOVEit, але й до майбутніх атак, можливих через витік конфіденційної інформації. Деякі приклади викрадених даних включають імена, номери телефонів, номери соціального страхування (SSN), адреси, фінансову інформацію та облікові дані. Жертви будуть піддаватися високому ризику фішингу, банківського шахрайства та інших атак соціальної інженерії. Ціна для постраждалих організацій буде великою, і жертви, швидше за все, потребуватимуть безпеки та моніторингу кредитів у найближчому майбутньому. Експлуатація цих вразливостей підтверджує заяви дослідників про те, що дизайн платформ передачі файлів є фундаментально помилковим і що виправлення окремих уразливостей захищатиме організації лише до тих пір, поки суб’єкти загрози не зможуть знайти інший спосіб використання такого ж типу.

Пом'якшення

Програмне забезпечення Progress Software випустило виправлення безпеки для всіх версій програмного забезпечення, що постраждали, і обмежило трафік HTTPS для MOVEit Cloud. У разі активного використання іншої вади нульового дня Progress закликає клієнтів обмежити зовнішній доступ HTTP та HTTPS до власних середовищ MOVEit Transfer. Progress Software та Агентство з кібербезпеки та безпеки інфраструктури США (CISA) надали методи ручного пом’якшення та посилення безпеки, щоб допомогти клієнтам виявити або запобігти експлуатації. Вони включають спершу вимикання будь-яких серверів MOVEit Transfer для проведення ретельного дослідження на наявність індикаторів компрометації або

доказів завантаження великих файлів. Адміністратори також повинні вимкнути весь HTTP- і HTTP-трафік до своїх середовищ MOVEit Transfer, включаючи резервні копії…» ***(Pierre Jeppsson. MOVEit Transfer Attack Campaign: Analysis // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102ikdh/moveit-transfer-attack-campaign-analysis). 26.07.2023).***

***

Програми-трояни

«Изощренная и уклончивая кампания вредоносных программ нацелена на предприятия в Латинской Америке с помощью многоэтапной атаки, которая начинается с фишинга и заканчивается развертыванием нового троянца, получившего название Toitoin, который крадет важную системную информацию и данные из финансовых учреждений.

Исследователи из Zscaler обнаружили сложную кампанию, которая представляет собой многоступенчатую цепочку заражения, в которой используются специально созданные модули на каждом этапе для внедрения вредоносного кода в удаленные процессы и обхода контроля учетных записей (UAC), среди прочего.

«Многоступенчатая цепочка заражения, наблюдаемая в этой кампании, включает использование специально разработанных модулей, в которых используются различные методы уклонения и методы шифрования», — сообщили исследователи в сообщении в блоге, опубликованном на прошлой неделе.

Тактика уклонения включает использование Amazon Elastic Compute Cloud (EC2) для размещения вредоносного ПО в сжатых ZIP-архивах.

«Используя инстансы Amazon EC2, злоумышленники избегают обнаружения на основе домена, что усложняет обнаружение и блокирование их действий», — написали исследователи в своем посте.

Архивы.zip также используют свой собственный маневр уклонения, генерируя новое и случайно сгенерированное имя файла при каждой загрузке. Это

позволяет им избежать обнаружения на основе статических шаблонов именования файлов. «Эта тактика добавляет дополнительный уровень сложности кампании, усложняя выявление и эффективное устранение угрозы», — отметили исследователи.

Окончательная полезная нагрузка Toitoin представляет собой троянскую вредоносную программу, созданную для атаки на финансовые цели, получившую название Toitoin, которая собирает системную информацию, а также данные, относящиеся к установленным браузерам и модулю защиты Topaz OFD для банковского сектора, и отправляет их для управления и контроля злоумышленника (C2) в закодированном формате, сказали они.

Электронная почта для трояна за 6 шагов

Исследователи перехватили фишинговое электронное письмо, отправленное известной инвестиционно-банковской компании в Латинской Америке, которое, по их словам, представляет собой первый этап атаки. Он использует социальную инженерию, чтобы вызвать чувство срочности, используя приманку платежного уведомления, предлагая получателю нажать кнопку, чтобы просмотреть счет для немедленных действий.

Ссылка в электронном письме запускает цепочку перенаправлений и событий, которые в конечном итоге приводят к загрузке вредоносного ZIP-архива в систему жертвы, который «начинает проникать в ее защиту», пишут исследователи.

Вредоносные файлы запускают сложную цепочку заражения Toitoin, состоящую из шести этапов, начиная с модуля загрузчика и заканчивая развертыванием троянца. В промежутках он развертывает различные модули вредоносного ПО, в том числе DLL Kirta Loader, модуль InjectorDLL, модуль ElevateInjectionDLL и модуль BypassUAC, каждый из которых выполняет свою специфическую функцию.

Модуль загрузчика первого этапа загружает дальнейшие этапы атаки и обходит песочницы посредством перезагрузки системы, сохраняя постоянство с помощью файлов LNK. Библиотека Krita Loader DLL, которая загружается через подписанный двоичный файл, загружает следующий модуль, InjectorDLL. Это, в

свою очередь, внедряет ElevateInjectorDLL в удаленный процесс, где он обходит песочницы, выполняет очистку процесса и в этот момент внедряет либо троян Toitoin, либо модуль BypassUAC на основе привилегий процесса.

Модуль BypassUAS делает то, что следует из его названия — обходит UAC, используя моникер COM Elevation для запуска Krita Loader с правами администратора. Это также гарантирует, что следующий этап процесса — последняя полезная нагрузка, Toitoin — будет выполняться с повышенными привилегиями.

«Полезная нагрузка вредоносного ПО внедряется в законные процессы, такие как explorer.exe и svchost.exe, чтобы избежать обнаружения и сохранить устойчивость в скомпрометированных системах», — пояснили исследователи.

Toitoin извлекает системную информацию, включая имена компьютеров, версии Windows, установленные браузеры и другие важные данные, и отправляет ее обратно злоумышленникам, адаптируя свое поведение на основе собранной информации, а также обнаруженного присутствия модуля защиты Topaz OFD.

Предотвращение компрометации вредоносным ПО

По словам исследователей, сложные кампании вредоносных программ, такие как Toitoin, требуют аналогичного ответа от организаций, на которые они нацелены. По их словам, это включает в себя надежные меры кибербезопасности и непрерывный мониторинг, а также последовательное управление исправлениями и обновление системы, чтобы обеспечить наличие новейших средств защиты во всей среде.

По словам исследователей, организации также могут использовать подход с нулевым доверием к безопасности, чтобы лучше защитить себя от сложных цепочек атак. При нулевом доверии весь трафик, включая сообщения электронной почты и просмотр веб-страниц, проверяется и анализируется в режиме реального времени, независимо от местоположения или устройства пользователя.

«Эта комплексная проверка помогает выявлять и блокировать вредоносные электронные письма, попытки фишинга и подозрительные URL-адреса, связанные

с кампаниями вредоносных программ, такими как Toitoin», — отметили исследователи.

Организации также могут развертывать платформы безопасности, которые используют передовые алгоритмы анализа угроз и машинного обучения для обнаружения и блокировки известных и неизвестных вариантов вредоносного ПО для самозащиты.

«Оставаясь информированными и активными, предприятия могут эффективно защищаться от новых киберугроз и защищать свои критически важные активы», — говорят исследователи». ***(Elizabeth Montalbano. Banking Firms Under Attack by Sophisticated 'Toitoin' Campaign // Informa PLC (https://www.darkreading.com/remote-workforce/banking-firms-attack-toitoin-cyber-campaign?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 10.07.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Іспанська поліція заарештувала українського розробника програмного забезпечення, який за допомогою підробленого антивірусу виманив у довірливих жертв понад $70 млн, повідомляє Bleepingcomputer. Шахраєві вдавалося ховатися від правоохоронців понад 10 років по всій Європі.

Чоловіка оголосили в міжнародний розшук за лінією Інтерполу понад 10 років тому, після того, як у період із 2006 до 2001 року він під виглядом антивірусного ПЗ став поширювати підроблену програму «для очищення комп'ютера від вірусів», за що отримував по $129 за кожну копію фальшивки. Але перед цим він заразив сотні тисяч комп'ютерів рекламним шкідливим кодом, який відображав загрозливі спливаючі повідомлення про «серйозне зараження системи». Користувачам пропонувалося терміново придбати чудодійний антивірус, щоб

позбутися зараження. Таким чином, жертви, які нічого не підозрювали, платили шахраєві-хакеру кругленьку суму за фальшиву програму безпеки.

Громадянина України затримали в аеропорту Барселона-Ель-Прат після прибуття після того, як правоохоронні органи дізналися про його запланований рейс до Барселони. Операція була проведена слідчими з поліцейського управління загальної інформації у співпраці з інформаційними бригадами Тенерифе і Барселони та поліцейською дільницею аеропорту Ель-Прат.

Після арешту українець постав перед Шостим центральним слідчим судом Іспанії, де його було офіційно заарештовано, оскільки тяжкість висунутих проти нього звинувачень вимагала негайного взяття під варту.

Ми вже повідомляли, що кіберексперта з компанії Amazon звинуватили в крадіжці $9 млн. Він провернув хитру махінацію з криптовалютою. Сам підозрюваний називав себе "білим хакером" і пропонував біржі залишити собі частину вкрадених грошей в обмін на виявлену вразливість». ***(Пилип Бойко. Обдурив сотні тисяч людей і отримав $70 млн: в Іспанії заарештували айтішника з України // Фокус (https://focus.ua/uk/digital/579727-obduriv-sotni-tisyach-lyudej-i-otrimav-70-mln-v-ispaniyi-zaareshtuvali-ajtishnika-z-ukrayini). 18.07.2023).***

***