**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

№ 10 (жовтень)

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.– №10 (жовтень) . – 320 с.

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

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

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

ЗМІСТ

«В Україні триває робота над удосконаленням системи підготовки кадрів і посиленням кадрового потенціалу у сфері інформаційної та кібербезпеки. Реформа передбачає, зокрема, розроблення та впровадження нових професійних стандартів із урахуванням найкращого міжнародного досвіду. Нові профстандарти важливі як для роботодавців, так і для закладів освіти, які можуть адаптувати відповідно до них свої освітньо-професійні програми.

Як саме це відбувається? Що вже вдалося реалізувати і які плани на майбутнє? Ці та інші питання обговорили 26 жовтня під час круглого столу «Презентація оновлених освітніх програм із кібербезпеки», який організували фахівці Проєкту USAID «Кібербезпека критично важливої інфраструктури України». У заході взяли участь представники Держспецзв'язку, які працюють над розробленням профстандартів, Міністерства освіти, Мінцифри, закладів вищої освіти тощо.

Заступник голови Держспецзв'язку Олександр Потій подякував американському народові та Проєкту USAID за підтримку та співпрацю. Також він розповів про екосистему професійної стандартизації, роль Держспецзв'язку в ній і нагадав, що у 2022 році в Україні були розроблені, затверджені та внесені до Реєстру кваліфікацій перші шість нових професійних стандартів у галузі кібербезпеки. Це «Розробник систем захисту інформації», «Адміністратор мереж і систем», «Фахівець сфери захисту інформації», «Аналітик з безпеки інформаційно-телекомунікаційних систем», «Фахівець з питань безпеки (інформаційно-комунікаційні технології)», «Інструктор-методист з інформаційної безпеки та кібербезпеки». У 2023 році розроблені проєкти ще 15 нових профстандартів, які невдовзі будуть затверджені.

«Вже під час навчання важливо враховувати виклики сьогодення, які постають перед нами у кіберпросторі, а також актуальні потреби ринку. Фахівці з інформаційної та кібербезпеки повинні мати відповідні знання, уміння та навички, щоб ефективно протистояти загрозам та забезпечувати надійний кіберзахист. І нові профстандарти покликані допомогти цьому», – підкреслив Олександр Потій.

Він зауважив, що основна робота з розроблення основних профстандартів майже закінчена. Далі додаватимемо кілька стандартів у рік.

Також Олександр Потій поділився планами щодо подальших кроків з посилення кадрового потенціалу у сфері кібербезпеки. Серед них побудова професійного ринку праці, формування кадрового резерву, внесення необхідних змін до посадових інструкцій та критеріїв оцінювання фахівців у держсекторі та інші – все для того, щоб наш кіберпростір, інформаційно-комунікаційні системи захищали професіонали.

Зауважимо, що навчальні заклади вже почали оновлювати освітньо-професійні програми відповідно до сучасних вимог, а також – згідно з новими професійними стандартами. Зокрема, такий досвід вже має Києво-Могилянська академія, Маріупольський державний університет, Харківський національний університет електроніки тощо. Про свій досвід представники цих закладів розповіли під час круглого столу.

Ця робота триватиме і наступного року. Впровадження нових профстандартів сприятиме покращенню якості підготовки професійних кадрів у галузі кібербезпеки та захисту інформації.

Нагадаємо, також в межах реформування до державного класифікатора професій вперше за багато років були додані зміни та нові професії у галузі кібербезпеки та інформаційної безпеки (зараз їх 27). Окрім того, в планах – створити в Україні мережу незалежних кваліфікаційних центрів, де фахівці зможуть підтверджувати рівень своїх знань, навичок та компетенцій». ***(Герман Богапов. В Україні оновлюються освітні програми у сфері кібербезпеки // HiTech.Expert. (https://expert.com.ua/170288-v-ukraini-onovlyuyutsya-osvitni-programy-u-sferi-kiberbezpeky.html). 27.10.2023).***

***

Кібервійна проти України

«У четвер стало відомо, що українська «ІТ-армія» відповідальна за злом російської системи бронювання авіакомпаній Leonardo, що спричинило збої в найбільших аеропортах країни.

«Якщо українські аеропорти не можуть працювати через війну, навіщо російським?» – запитав міністр цифрової трансформації України в Telegram.

Незважаючи на те, що військові аналітики, багато з яких очікували, що Україна впаде протягом декількох днів після повномасштабного вторгнення Росії, були шоковані тим, наскільки добре Україні вдалося захищатися та навіть атакувати на суші та на морі, існує ще одна сфера, де українці утримали свої сили. власний – кібервійна.

Заступник голови Державної служби спеціального зв'язку та захисту інформації України Віктор Жора заявив, що хоча Росія продовжує використовувати свої кіберпотужності для підтримки свого повномасштабного вторгнення в Україну, вона не досягла великих перемог.

«Вони (українці) створили вражаючий захист від російської агресії в кіберпросторі, як і на фізичному полі бою», — сказала Лінді Кемерон, головний виконавчий директор Національного центру кібербезпеки (NCSC) у Великобританії.

Але, попередив Кемерон, «загроза залишається реальною».

Російські військові хакери останнім часом намагаються отримати доступ до Android-телефонів українців, розповів Жора Kyiv Post. в ексклюзивному інтерв'ю

Особливу увагу хакери приділили отриманню доступу до телефонів військовослужбовців України.

Одна російська хакерська група під назвою «Sandworm», яка має зв'язки з ГРУ (спадкоємцем КДБ), використовувала шкідливе програмне забезпечення під назвою «Infamous Chisel» для злому додатків Android і отримання постійного доступу до даних телефону, включаючи інформацію про місцезнаходження, про це повідомляє Defense Intelligence.

Жора зазначив, що українці, особливо військові, повинні дотримуватися «кібергігієни». Тобто вони повинні вжити заходів безпеки, наприклад, вимкнути служби геолокації та уникати російських мереж.

Також не варто зберігати на своїх пристроях документи чи фотографії обладнання та обговорювати на них робочі проблеми. І варто обмежити користування соцмережами, – сказав Жора.

Але, мабуть, найбільшою новиною стала відсутність новин про успішні масштабні російські кібератаки.

«Навіть якщо деякі втручання мають певний успіх, вони швидко локалізуються та нейтралізуються», – сказав Жора.

26 лютого 2022 року, через два дні після того, як Москва почала ракетний обстріл українських міст, величезна українська спільнота IT-фахівців створила добровольчу IT-армію.

Добровольців розділили на наступальні та оборонні кіберзагони. Наступальний волонтерський загін допомагав українським військовим проводити операції цифрового шпигунства проти російських військ.

Оборонний підрозділ використовувався для захисту інфраструктури, як-от електростанції та системи водопостачання.

І багато провідних фахівців у сфері кіберзахисту прийшли служити в SSSCIP, що дуже позитивно вплинуло на кіберзахист країни, сказав Жора.

«Вони не лише виконували роль додаткових рук, але й привнесли нові підходи, нове бачення того, як покращувати існуючі процеси та системи, а також як створювати нові», — сказав Жора.

За перші вісім місяців 2023 року було зареєстровано та розслідувано понад 1500 кіберінцидентів.

«Найбільша кількість кібератак спрямована на центральні, місцеві органи влади та державні організації – це понад 370 кібератак», – сказав Жора.

Хоча Жора зазначив, що не варто недооцінювати можливості росіян щодо кібератак, зазвичай вони не досягають своїх цілей, принаймні не в повному обсязі.

І це тому, що українці виявилися дуже гнучкими. Це стосується не лише боротьби з кібератаками на українську інфраструктуру, а й проти фізичних атак.

У перші дні повномасштабного вторгнення Росія ракетним ударом пошкодила один із об'єктів Національного центру резервування державних інформаційних ресурсів, повідомив Жора.

Зараз у відповідь на подібні атаки створені мобільні дата-центри, які можуть пересуватися по країні і навіть залишати її межі при необхідності.

«Головне тут те, що ми не збираємося здаватися. З якими б кібератаками ми не зіткнулися, ми плануємо перемогти», — сказав він.

Подібно до того, як потужність української армії різко зросла після 2014 року, коли Росія незаконно анексувала Крим і підтримала сепаратистів на українському Донбасі, – так само зросла здатність України протистояти кібератакам і здійснювати їх.

У 2015 році Росія зламала українську електромережу, залишивши близько 230 000 людей у невіданні.

У 2017 році відбулися руйнівні кібератаки, націлені на український фінансовий і енергетичний сектори та державні служби, що призвело до збійних наслідків для інших європейських партнерів, а Київський метрополітен і Одеський аеропорт були порушені програмним забезпеченням-вимагачем, яке шифрувало жорсткі диски.

А 14 січня 2022 року близько 70 українських урядових сайтів, зокрема Міністерства закордонних справ, Кабінету міністрів і РНБО, були тимчасово зіпсовані російськими хакерами.

На ранок після кібератак Росії в січні 2022 року представники Великобританії, США та ЄС звернулися до українських служб і запропонували свою допомогу, в тому числі в розслідуванні кіберінцидентів, сказав Жора.

«Ми знали, що росіяни прийдуть», — сказав Роберт Блек, який співпрацює з Оборонною кібершколою Великої Британії над навчанням вищого керівництва Міністерства оборони війні в епоху інформації.

«Вони (українці) зробили свої мережі дуже складними для злому, тому будь-які очевидні вразливості були усунені, а будь-яка російська діяльність у цих мережах

припинялася якнайкраще до початку російського вторгнення», — сказав Блек Kyiv Post.

Уряд Блека, Великобританія, був одним із тих, хто підтримав кіберзахист України невдовзі після повномасштабного вторгнення Росії.

Велика Британія надала Україні пакет підтримки на суму 6,45 мільйона фунтів стерлінгів (близько 7,82 мільйона доларів США) для захисту її критичної національної інфраструктури та життєво важливих державних послуг від кібератак.

Це включало створення брандмауерів для запобігання атакам і захист від деструктивного шкідливого програмного забезпечення, такого як Industroyer2, яке двічі використовувалося для атаки на енергомережу України.

За словами Жори, через постійні кібератаки з початку повномасштабного вторгнення Росії в Україну більшість українських установ перенесено в інші хмари або навіть за кордон.

«Ми тісно співпрацюємо з країнами ЄС і НАТО, обмінюємося досвідом, інформацією про загрози, вчимося у них», – сказав Жора.

«Такі компанії, як Amazon, Microsoft, Google і Oracle, також надали велику допомогу Україні з хмарною інфраструктурою для тимчасової передачі даних критичних реєстрів», – сказав Жора.

Інші кібергрупи приєдналися до бійки, наприклад група хакерів «Анонім», яка розпочала «кібероперації» проти Росії у відповідь на її вторгнення.

Цільовими веб-сайтами були RT та інші російські державні телеканали. Вони грали українську музику та демонстрували проукраїнські зображення.

Повідомляється, що яхта, яка нібито належить Путіну, була зламана групою, де вони змінили її позивний на «FCKPTN» і встановили цільовий пункт призначення на «пекло». ***(Kateryna Zakharchenko, Tony Leliw. How Ukraine Has Fought Off an Onslaught of Russian Cyber Attacks // BIZNESGRUPP TOV (https://www.kyivpost.com/post/22416?utm_source=flipboard&utm_content=LindaCypert%2Fmagazine%2F%0AImportant+Trending+Stories+). 07.10.2023).***

***

«…У серпні західні служби сигналів і кіберрозвідки оприлюднили звіт, в якому детально описується, як російські військові та спецслужби використовують шкідливе програмне забезпечення для злому телефонів українських військових.

Кіберзброя, яка отримала назву «Гнезвісне долото», відстежує пересування українських сил.

«Зловмисне програмне забезпечення періодично сканує пристрій на наявність цікавої інформації та файлів, які відповідають попередньо визначеному набору розширень файлів. Він також містить функціональність для періодичного сканування локальної мережі, зіставляючи інформацію про активні хости, відкриті порти та банери», – йдеться у звіті.

Зловмисне програмне забезпечення спеціально націлено на мобільні пристрої Android.

Звіт був підписаний кількома західними агентствами, включаючи Національний центр кібербезпеки Великобританії (NCSC), Агентство національної безпеки США (NSA), Агентство з кібербезпеки та безпеки інфраструктури США (CISA), Федеральне бюро розслідувань США (FBI), Національний центр кібербезпеки Нової Зеландії (NCSC-NZ), Канадський центр кібербезпеки та Австралійське управління сигналів (ASD).

«Зловмисне програмне забезпечення, яке називається «Infamous Chisel», використовувалося російською групою кіберзагроз, відомою як Sandworm. Раніше NCSC відносив Sandworm до Головного центру спеціальних технологій (ГЦСТ) Головного розвідувального управління (ГРУ) російського Генштабу», – оцінила британська військова розвідка в оцінці війни.

Одним із способів використання зловмисного програмного забезпечення є забезпечення постійного доступу, тобто росіянам потрібно скомпрометувати пристрій один раз, а не кожного разу, коли вони звертаються до нього, якщо немає оновлення, а потім збирати та викрадати дані зі скомпрометованих пристроїв Android. Ці дані можуть включати додатки, які використовуються українськими військовими для цілей.

Компрометація даних про націлювання означає, що російські війська можуть уникати наближення вогню на великій відстані, а також атакувати такі українські системи. Це надзвичайно важливо, оскільки вогонь на великі відстані — артилерія та ракети — був єдиним джерелом смертоносних втрат на полі бою для обох сторін.

«Infamous Chisel, швидше за все, використовувався з метою викрадення конфіденційної військової інформації. Ця діяльність демонструє продовження використання Росією кіберпотенціалу для підтримки вторгнення в Україну», – додала британська військова розвідка.

Зловмисне програмне забезпечення також може контролювати мережу та збирати її трафік…» ***(Stavros Atlamazoglou. Russia Deploys Cyber Weapon in Ukraine // 19fortyfive (https://www.19fortyfive.com/2023/10/russia-deploys-cyber-weapon-in-ukraine/?utm_source=flipboard&utm_content=Matthes2020%2Fmagazine%2FRUSSIAN+WAR+%28D%2FE%29). 09.10.2023).***

***

«Кіберфахівці Служби безпеки системно протидіють загрозам інформаційно-підривної діяльності окупантів. З початку цього року нейтралізовано майже 4 тис. кібератак на електронні системи центральних органів влади та критичної інфраструктури України.

Про це було наголошено у ході практичного семінару, який проводив кібердепартамент СБУ для працівників, відповідальних за інформбезпеку урядових органів та стратегічних об’єктів України. Загалом у заході взяли участь більше ніж 70 представників різних відомств.

Під час семінару співробітники Служби безпеки провели тренінг із підвищення кібербезпеки України, а також поділилися кращими практиками з протидії кіберзагрозам. Зокрема щодо використання систем управління подіями інформаційної безпеки (SIEM), захисту кінцевих пристроїв (EDR) та поштових сервісів.

Як зазначили фахівці СБУ, більшість ворожих кібератак спрямована на пошук несанкціонованого доступу до електронного документообігу держустанов і технологічних систем інфраструктури.

Зазвичай такими «точками входу» для російських хакерів є публічно доступні сервіси, насамперед – електронна пошта.

Під час семінару його учасники відпрацювали алгоритми спільних дій щодо реагування та мінімізації негативних наслідків відповідних кібератак.

Для посилення міжвідомчої взаємодії СБУ підключила електронні системи понад 1700 представників урядових структур і стратегічно важливих об’єктів до платформи обміну інформацією про виявлені кіберінциденти MISP-UA.

Усі комплексні заходи, які були відпрацьовані у ході практичного семінару, відбувалися у рамках так званого «місяця кібербезпеки» і суттєво посилять захисний потенціал державних автоматизованих систем від російських кібератак в умовах війни». ***(З початку року СБУ нейтралізувала майже 4000 кібератак на органи влади та критичну інфраструктуру України // Голос українською (https://uagolos.com/z-pochatku-roku-sbu-nejtralizuvala-majzhe-4000-kiberatak-na-organy-vlady-ta-krytychnu-infrastrukturu-ukrayiny/). 03.10.2023).***

***

«Ворог щодня атакує Україну в Мережі, проте фахівцям вдається ліквідувати загрози з боку російських хакерів. Подробиці 6 жовтня розкрив міністр цифрової трансформації Михайло Федоров.

За його даними, окупанти намагаються отримати доступ до інформації, яку зберігають державні органи країни. Також під увагою ворога залишаються об'єкти критичної інфраструктури та сфера бізнесу.

Міністр повідомив, що росіян цікавлять докази злочинів країни-терористки проти України, дані про полонених військовослужбовців окупаційної армії та шпигунів.

Із січня по червень 2023 року було відбито 762 кібератаки. Критичної шкоди країні або її обороноздатності завдано не було, стверджує міністр.

Такого результату було досягнуто завдяки посиленню сфери кібербезпеки за останні кілька років. Були залучені кваліфіковані фахівці та партнери із зарубіжжя.

Для створення стійкості України перед хакерськими атаками використовували стандарти НАТО та європейські норми, наголосив очільник Мінцифри.

Раніше українські хакери зупинили роботу найбільших російських аеропортів». ***(Олександр Воєйков. Україна відбила 762 кібератаки за 2023 рік: статистика від глави Мінцифри // META.UA (https://meta.ua/uk/news/incidents/90061-ukrayina-vidbila-762-kiberataki-za-2023-rik-statistika-vid-glavi-mintsifri/). 06.10.2023).***

***

«Російські кібератаки стають все більш витонченим і повсякденним явищем, спрямованим на руйнування життєво важливої інфраструктури під час війни.

Про це заявив заступник міністра закордонних справ Антон Демьохін в інтерв'ю Bloomberg, передає Укрінформ.

За словами заступника міністра, який відповідає за питання цифрового розвитку, цифрових трансформацій і цифровізації, хакери продовжують атакувати державні органи, служби безпеки та комерційні підприємства, включаючи фінансові установи, намагаючись зашкодити наданню послуг та отримати особисті дані. Хоча Україна значною мірою здатна стримувати спроби, Демьохін наголосив, що вони ефективні в тому сенсі, що держава докладає багато зусиль у протистоянні хакерам.

«У цьому сенсі – так, вони забирають у нас і час, і увагу, і ресурси», – сказав дипломат, додавши, що інциденти стали більш скоординованими: кілька хакерів у різних місцях одночасно атакують різні частини однієї інфраструктури.

Інші зловмисники залишили сплячі віруси в інформаційних системах, які активуються після початку наступальної операції, пояснив Демьохін.

«Коли ви все це об'єднуєте, ви розумієте, що це новий рівень витонченості», – підсумував заступник глави МЗС.

Насамкінець він поінформував, що провів двосторонні зустрічі із заступником радника США з національної безпеки Енн Нойбергер під час своєї поїздки до Південно-Східної Азії та обговорив питання розвідки загроз і технології кібербезпеки…» ***(У МЗС заявили, що російські кібератаки стали більш скоординованими і витонченими // Укрінформ (https://www.ukrinform.ua/rubric-technology/3778368-u-mzs-zaavili-so-rosijski-kiberataki-stali-bils-skoordinovanimi-i-vitoncenimi.html). 25.10.2023).***

***

«…У 2014 році Росія незаконно анексувала Крим, а потім напала на Луганську та Донецьку області, де зіткнулася зі збройним опором української армії. Домовленості, укладені у Мінську у вересні 2014 року та лютому 2015 року, не врегулювали суперечку, і на тимчасовому кордоні між російськими сепаратистами та Україною постійно була стрілянина. Водночас Росія створила український полігон у кіберпросторі.

У 2015 і 2016 роках посеред зими росіянам вдалося відключити мільйони українців від світла. Однак, кульмінацією став 2018 рік і атака з використанням шкідливого ПЗ NotPetya, яка паралізувала роботу українського уряду, підприємств та інфраструктури. На перший погляд, NotPetya був ще одним прикладом шифруючого програмного забезпечення-вимагача [яке дозволяє повторно отримати доступ до скомпрометованих даних після сплати викупу – прим ред.], однак на практиці виявилося, що це вайпер, тобто шкідливе програмне забезпечення, яке знищує дані. Напад швидко перетнув кордони України та поширився на весь світ. Постраждали глобальні компанії, такі як фармацевтична компанія Merck, виробник продуктів харчування Mondelez і транспортні компанії FedEx, TNT Express і Maersk. Білий дім оцінив збитки у 10 мільярдів доларів.

Окрім цих вражаючих і небезпечних атак, російськими хакерами також була здійснена велика кількість набагато менших інцидентів. Проте, ці дії дозволили українцям ближче познайомитися зі своїм супротивником, його технікою та

методами дії, що виявилося надзвичайно важливим під час повномасштабного вторгнення Росії.

Прелюдія до російського вторгнення

Початок 2022 року та численні дипломатичні зусилля та посилення риторики Кремля вказували на те, що вторгнення стає дедалі ймовірнішим. Це підтвердили сигнали, що надходять із кіберпростору. На початку січня 2022 року на сайти уряду України відбулися DDoS-атаки (Distributed Denial of Service). Їх швидко відбили, і домени відновили роботу. Втім, це була прелюдія до більш серйозних дій.

У ніч з 23 на 24 лютого 2022 року російська військова розвідка провела операцію проти американської компанії Viasat, яка надає високошвидкісний широкосмуговий супутниковий доступ комерційним і військовим замовникам. Десятки тисяч терміналів компанії були пошкоджені. Українські військові використовували їх як резервний зв'язок, а головною метою російської операції було позбавити їх зв'язку – що підтвердили у спільній заяві ЄС, Великої Британії та США. Застосування засобів радіоелектронної боротьби разом із кібератакою на Viasat призвело до проблем зі зв'язком військ, які захищали Київ. В інших країнах ЄС атака порушила роботу тисяч компаній, а лише у Німеччині призвела до збою 5,8 тисяч вітрових турбін.

Проте, проблему зв'язку з українськими захисниками вдалося швидко вирішити шляхом негайної поставки телекомунікаційної супутникової системи виробництва американської компанії Ілона Маска SpaxeX. Starlink забезпечила безпечне та ефективне спілкування, виявившись стійкою до діяльності російських хакерів та інших збоїв.

На початку вторгнення росіяни також атакували головного українського інтернет-провайдера «Тріолан» і найбільшого українського телекомунікаційного оператора «Укртелеком», намагаючись порушити український зв'язок і отримати домінування в інформаційному середовищі, що відповідало російській інформаційній доктрині. Як наслідок, користувачі «Тріолана» та «Укртелекому» постраждали від тимчасових перебоїв у наданні інтернет-послуг. Внутрішні пристрої компаній перестали працювати через те, що російські хакери змусили їх

скинути заводські налаштування. Відновлення інтернет-послуг виявилося значно ускладненим через постійні російські повітряні атаки й тривало кілька днів.

Масована атака зловмисного програмного забезпечення

За перші чотири місяці війни росіяни використовували 8-10 різних типів шкідливих програм для очищення даних, призначених для знищення збережених даних. Цілями атак було майже 50 різних українських установ і підприємств. У деяких випадках спостерігалися тимчасові труднощі з роботою, але вони були швидко вирішені. Масштаби цієї атаки були величезними, оскільки Росія використовувала таку ж кількість шкідливих програм за попередні 6 років.

У міру того, як війна тривала, кількість атак та їх серйозність зменшилися, і у серпні та вересні 2022 року не було зафіксовано жодної активності зловмисного програмного забезпечення. Заступник голови Державної служби спеціального зв'язку та захисту інформації України Віктор Жора зазначив, що з розвитком війни російські атаки ставали менш прогресивними та скоординованими, що підтверджує спостереження стосовно використання програмного забезпечення для видалення. Експерти американського аналітичного центру Carnegie вважають, що зниження витонченості російських кібератак стало наслідком необхідності перебудови власних наступальних можливостей через те, що використовувані шкідливі програми стали розпізнавати антивірусні програми. На це також вплинули кібератаки українців та хакерів з усього світу, спрямовані проти Росії, що призвело до необхідності залучення сил для захисту російських систем.

Одним із найважливіших об'єктів російських атак в Україні став енергетичний сектор. До кінця 2022 року українці зафіксували 84 спроби проникнення у мережі та системи за допомогою передового шкідливого програмного забезпечення, призначеного для зриву електропостачання. Наприклад, жертвою хакерів і російських військових стала найбільша українська компанія в енергетиці «ДТЕК». Однак, на відміну від 2015 і 2016 років, цього разу операції провалилися. Українці винесли уроки з минулого і, безумовно, були краще підготовлені. Вони вклали значні кошти у покращення кібербезпеки, особливо в енергетичному секторі.

Атакам також піддавалися суб'єкти логістики, транспорту та сільського господарства, але з часом інтенсивність операцій знизилася. Традиційні кінетичні заняття виявилися набагато ефективнішими.

Кіберелемент російської військової машини

З самого початку повномасштабного вторгнення були деякі ознаки того, що діяльність у кіберпросторі координується з операціями, які проводять регулярні війська. Напередодні захоплення Запорізької АЕС у березні 2022 року російські хакери зламали її мережу у пошуках інформації. Схожий інцидент стався у Вінницькій області, де 4 березня 2022 року хакери зламали державні системи, а через чотири дні вісім ракет влучили в аеропорт у цьому районі.

Подібна ситуація могла бути 29 квітня 2022 року, коли атакували залізничну інфраструктуру поблизу Львова. Кінетичній атаці передувала операція у кіберпросторі. Не виключено, що росіяни знайшли інформацію про те, що цього дня буде транспортуватися зброя із Заходу (дати та маршрути військових транспортів секретні), і вирішили її знищити. Через високу інформаційну дисципліну України невідомо, чи досягли росіяни свого.

Операції у кіберпросторі також мали на меті полегшити відступ російських військ з Києва та затримати просування українських військ на схід країни. Тому закономірною мішенню стали системи та мережі транспортних організацій, розташовані на заході та у центрі України.

Окрім використання шкідливих програм, призначених для знищення даних, протягом перших чотирьох місяців вторгнення росіяни провели понад 240 шпигунських операцій у кіберпросторі, основною метою яких було викрадення інформації. Отримані дані могли допомогти російським військовим у стратегічному плануванні, виборі цілей, зайнятті окупованих районів, переговорах і проведенні оперативних дій. Але ефективність операцій кібершпигунства неможливо чітко перевірити через те, що немає публічної інформації про те, чи були вони успішними та яку інформацію було отримано. Однією з найактивніших організацій була російська хакерська група Turla, яка була ідентифікована лише на початку 2023 року. Її діяльність була зосереджена в основному на урядових документах, створених після

1 січня 2021 року. Останнім часом діяльність російського кібершпигунства була зосереджена в основному на поточному українському контрнаступі, але важко оцінити, чи отримали росіяни якусь інформацію, яка могла б вплинути на його хід.

Об'єктом нападів є Захід

Росія також використовувала операції у кіберпросторі проти країн Заходу, які брали участь у масштабній допомозі Україні. До них належать фішингові операції, під час яких, наприклад, російські хакери намагалися видати себе за довірених людей або установи та спонукати отримувачів їхніх повідомлень клацати вкладений файл, який містив шкідливе програмне забезпечення. Такі дії були спрямовані проти урядових і військових установ у Польщі, ядерних дослідницьких лабораторій Брукхейва, Аргонна та Лоренса у Сполучених Штатах, установ НАТО та аналітичних центрів, які займаються питаннями безпеки та міжнародної політики. Більшість цих атак були спрямовані на отримання інформації.

Також росіяни проводили операції зі шифрування даних. Наприкінці 2022 року у звіті Microsoft вказувалося на загрозу нового програмного забезпечення для шифрування Prestige, яке, окрім українських організацій, також вразило цілі у Польщі. Але Microsoft не надала жодних подробиць у своєму звіті.

Це лише деякі з атак, спрямованих на західні країни, тому так важливо надавати увагу кібербезпеці. Що може статися, якщо росіяни здійснять успішну кібератаку? Про такий сценарій свідчить, наприклад, аварія на польській залізниці, яка сталася 17 березня 2022 року. Вона призвела до паралічу, який зупинив рух сотень потягів по всій Польщі. Спочатку припускали, що причиною стала кібератака, але потім виявилося, що із 33 локальних центрів управління вийшли з ладу 19. У цьому випадку вийшло з ладу IT-обладнання, але подібного ефекту можна було досягти за допомогою кібератаки.

Чому росіяни не зламали кіберзахист України?

Повномасштабне вторгнення та пов'язані з ним масові кібератаки, ймовірно, найбільші в історії, не здолали український кіберзахист. Це здивувало, наприклад, генерал-майора та командувача Силами оборони кіберпростору Кароля Моленду, який сказав під час круглого столу на Міжнародному форумі з кібербезпеки у

французькому Ліллі у червні 2022 року, що він очікує цифрового еквівалента Перл-Харбора. Він також додав, що українці показали, що можна готуватися до конфлікту у кіберпросторі. На їхній успіх вплинуло кілька факторів.

По-перше, протягом восьми років, починаючи з 2014 року, Україні доводиться мати справу з різними операціями у кіберпросторі, які проводять російські хакери. За цей час вона познайомилася зі своїм опонентом, його методами роботи, використовуваним шкідливим програмним забезпеченням і зробила значні інвестиції в кіберзахист, покращивши захист власних мереж і систем, особливо у секторі критичної інфраструктури, і збільшивши кількість експертів з кібербезпеки. Наприклад, один із найбільших телекомунікаційних операторів України збільшив кількість людей, відповідальних за кібербезпеку, на дві третини між 2015 і 2022 роками, а українська енергорозподільча компанія «Укренерго» лише за два роки витратила 20 мільйонів доларів на інвестиції в системи кіберзахисту. Важливі зміни відбулися і у законодавстві, наприклад, у 2016 році в Україні було ухвалено Національну стратегію кібербезпеки, положення якої були ефективно імплементовані. Також відбулися інституційні зміни і у 2021 році було створено Кіберцентр UA30, який координує діяльність суб'єктів, відповідальних за кіберзахист.

Другий фактор – це безпрецедентна допомога Заходу. Україна також отримала фінансову підтримку США у розмірі 40 мільйонів доларів на розвиток кіберзахисту, а Командування кіберпростору США (USCYBERCOM) скерувало свою команду в Україну для зміцнення та обміну ноу-хау. Американці разом з українцями намагалися відстежити та виявити зловмисну діяльність в українських мережах і системах, яка може свідчити про злом. Крім того, американці провели для українців навчання з використання інноваційних технологій кіберзахисту. Останні члени USCYBERCOM покинули Київ напередодні російського вторгнення. Тож вони все ще були на місці, коли у січні 2022 року почалися російські кібератаки, допомагали їх аналізувати та обмінювалися інформацією з агентствами у Сполучених Штатах. Незважаючи на те, що в Україні немає американських солдатів, USCYBERCOM бере участь у допомозі українцям, ділячись, серед іншого, інформацією про атаки.

Допомагали також естонці, поляки та інші члени НАТО. Такі приватні компанії, як американські Microsoft, Google і Amazon, залучилися в безпрецедентному масштабі, надаючи свої хмарні сервіси для зберігання інформації від українського уряду, обміну даними про зловмисне програмне забезпечення та надання інших функцій, які підвищують кібербезпеку. Словацька компанія з кібербезпеки ESET, яка чудово знає шкідливе програмне забезпечення, що працює у Центральній та Східній Європі, також зіграла важливу роль. Ніколи раніше приватний сектор не залучався до таких масштабів.

Зрештою, відповідальність за успіхи українського кіберзахисту лежить і на росіянах, а саме за погано проведену військову операцію та переоцінку власних сил. По-перше, росіяни не мають еквівалента американських чи європейських кібервійськ, які могли б здійснювати операції у кіберпросторі у тісній взаємодії зі звичайними військами. Операції в Україні проводили групи, пов'язані з ГРУ, ФСБ і СВР, тому важко уявити, наприклад, ефективну співпрацю між армією та цивільною розвідкою та контррозвідкою, особливо у Росії, де ці середовища сильно конкурують між собою. Іншим важливим питанням був той факт, що лише невелика група людей знала про вторгнення в Україну, про що писав, серед інших, Оуен Метьюз у своїй книзі Overreach: The Inside Story of Putin and Russia's War Against Ukraine, хакери не встигли ретельно підготувати операцію.

Резюме

Незважаючи на відсутність значних успіхів російських хакерів під час повномасштабного вторгнення в Україну, їх не варто недооцінювати. Вони є гнучкими і готові адаптувати свої методи та шкідливі програми, які вони використовують, до мінливих умов. Росіяни відновлюють свої можливості і зосереджуються на інших цілях. Наразі, як повідомляє Держспецзв'язку України, більша увага приділяється кібершпигунству, в якому росіяни мають великий досвід і успіхи. На сторожі має бути не лише Україна, але й країни, які її підтримують у війні, зокрема, насамперед, Польща, яка стала ключовим хабом для України». ***(Анджей Козловський. Як Україна завдала нищівної поразки Росії у кібервійні //***

Foreign Ukraine (https://foreignukraines.com/2023/10/23/how-ukraine-inflicted-a-devastating-defeat-on-russia-in-a-cyber-war/). 23.10.2023).

***

«Дві українські хактивістські групи заявляють про злом найбільшого російського приватного банку «Альфа-Банк».

У дописі в блозі минулого тижня хакери з груп KibOrg і NLB поділилися скріншотами того, що, здається, є внутрішньою базою даних, що належить Альфа-Банку, а також особистими даними кількох росіян як «підтвердження» злому. За словами хакерів, у базі даних міститься понад 30 мільйонів записів, включаючи імена, дати народження, номери рахунків і номери телефонів російських клієнтів.

Додаючи трохи законності цим твердженням, представник української розвідки, який побажав залишитися анонімним для обговорення конфіденційної операції, підтвердив NPR, що головне контррозвідувальне агентство України, СБУ, допомогло хакерам зламати Альфа-Банк.

Чиновник не поділився додатковими подробицями щодо участі СБУ та подальших планів щодо поширення вкрадених даних. українські журналісти, в тому числі з кібербезпекового сайту The Record. Про зв'язок із СБУ раніше повідомляли

Хоча хактивісти не відразу відповіли на прохання обговорити злом, вони написали в блозі, опублікованому на власному сайті, що вони поділяться даними, отриманими від Альфа-Банку, з журналістами-розслідувачами.

Альфа-Банк публічно не відреагував на новину про злом.

Хакерство стало інструментом опору України.

Альфа-Банк відомий тим, що обслуговує російську верхівку. Уряд США ввів санкції проти банку та багатьох його членів ради після повномасштабного вторгнення Росії в Україну в лютому 2022 року.

У серпневому прес-релізі про деякі з цих санкцій заступник міністра фінансів Воллі Адейемо сказав, що «багаті російські еліти повинні відмовитися від думки, що вони можуть вести бізнес як завжди, поки Кремль веде війну проти українського народу».

Крім західних санкцій, хактивізм і волонтерські кібероперації стали важливими інструментами для України в її опорі вторгненню Росії.

Незважаючи на те, що IT-армія є однією з найвідоміших груп, офіційно схвалених Міністерством цифрової трансформації України на початку війни, існує багато інших добровольчих груп, які розпочинають операції, починаючи від помірних руйнівних атак на відмову в обслуговуванні до широкомасштабних. порушення та скидання даних.

Багато експертів очікували, що кваліфіковані російські хакери зроблять дуже руйнівні та деструктивні атаки на Київ, як це було в минулому, виводячи з ладу електромережу або знищуючи комунікації. Однак ці очікування не виправдалися. З моменту вторгнення російським хакерам вдалося неодноразово атакувати та порушувати роботу електромережі, комунальних послуг, постачальників послуг зв'язку та новинних видань, зокрема. Однак наслідки не були тривалими або остаточно збитковими, за словами ряду українських чиновників і керівників з кібербезпеки. Незалежні експерти компаній з кібербезпеки, багато з яких пожертвували свої послуги Україні, підтвердили ці заяви.

Проте з перших днів війни кваліфіковані українські хакери та експерти з кібербезпеки стали хактивістами, а також офіційними та неофіційними радниками українських державних установ.

Ці агентства офіційно визнали свою важливість. Під час ексклюзивного інтерв'ю NPR у серпні керівник кібервідділу СБУ Ілля Вітюк сказав, що в його роботу входить як стежити, так і певною мірою «спрямовувати» або «давати поради» хактивістам, які підтримують його роботу проти російських шпигунів. «Це як наша кібертериторіальна оборона», – продовжив Вітюк. Він каже, що одна з причин, чому його служба так тісно співпрацює з приватними громадянами, полягає в тому, щоб переконатися, що вони використовують свої повноваження на благо. «Дуже важливо, що після війни... ці люди працюють на благо нашої країни».

За останні тижні українські хактивісти здобули кілька перемог, крім очевидного злому Альфа-Банку…» ***(Jenna McLaughlin. Ukrainian hackers and intel officers partner up in apparent hack of a top Russian bank // npr***

(https://www.npr.org/2023/10/25/1208352887/ukraine-russia-bank-hack?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 25.10.2023).

***

«Нещодавно сформована «ІТ-армія» України відіграє вирішальну роль у війні з Росією, запускаючи руйнівні кібератаки та крадіжки даних проти російського уряду та інших відомих цілей, таких як енергетичний гігант «Газпром».

ІТ-армія налічує тисячі волонтерів по всьому світу, які використовують канали Twitter і Telegram для спілкування, координації та звітування про дії. Його члени вже брали участь у різноманітних атаках. Вони варіюються від викрадення та розголошення важливої інформації до успішного зриву російських комунікацій та інших критично важливих мереж, щоб перешкодити військовим зусиллям Росії.

Створення ІТ-армії стало відповіддю українського уряду на занепокоєння щодо ролі російських кібератак у війні. 26 лютого 2022 року віце-прем'єр-міністр України Михайло Федоров закликав до зброї всіх хакерів, які бажають приєднатися до його ІТ-армії та підтримати Україну проти російських кібератак і порушити роботу російських мереж.

Створення української ІТ-армії вважається першим у світі в операціях кібервійни. Вважається, що це був перший випадок, коли державний чиновник відкрито закликав хакерів з усього світу приєднатися до військових оборонних зусиль нації проти сил вторгнення та діяти в рамках їхніх гібридних військових операцій.

Українську ІТ-армію також підтримують групи хактивістів, які не пов’язані з Україною, але хочуть підтримати країну проти Росії.

Одна з найбільш руйнівних атак була здійснена в 2022 році та була спрямована на російську систему автентифікації «Честный знак», яка додає унікальний ідентифікатор і штрих-код до всіх товарів у країні.

Ця кібератака заповнила сервери «Честного Знака» інформацією, внаслідок чого він припинив роботу, створивши масові збої з серйозними економічними втратами та навіть змусивши російський уряд скасувати певну політику маркування.

IT -армії та іншим хактивістським групам також вдалося націлитися на російські радіо- та телестанції, щоб додавати фрагменти відео про війну в Україні до програм і транслювати фейкові сповіщення про авіанальоти. Наприклад, у червні 2023 року російське державне телебачення та інші канали були зламані та транслювали відео, нібито створене Міністерством оборони України, яке включало кадри військових дій України, а також повідомлення українською мовою «Настала година розплати».

Це згуртування хакерів для України спонукало такі групи в Росії, як Killnet, Sandworm і XaKnet, почати власні кібератаки на українські та західні цілі. Однак російські кібератаки почалися задовго до вторгнення та посилилися в лютому 2022 року. Вони включали низку менших нападів на українські державні та приватні мережі та навіть велику кібератаку на систему супутникового зв'язку Viasat з метою запобігання моніторингу Пересування російських військ під час вторгнення.

Міжнародні розгалуження

Кібератака Viasat 23 лютого мала серйозні наслідки за межами України, вплинувши на тисячі німецьких вітряних турбін через відключення їхніх систем дистанційного керування. Цей інцидент показав, що тепер усі війни мають дуже реальний вимір кіберпростору, який може мати глобальні наслідки за межами зони бойових дій.

Крім глобальної стурбованості кібербезпекою, яку породив цей конфлікт, створення IT-армії викликало важливі дискусії навколо ролі кібервійни в реальних військових операціях. Одне важливе питання полягає в тому, чи можна вважати такі групи, як IT-армія, комбатантами, а не цивільними особами, що може вплинути на те, чи можуть вони бути законними мішенями російських військових, втрачаючи частину захисту, наданого міжнародним правом.

При цьому деякі країни, зокрема Естонія, вже офіційно створили подібні резерви кіберсил. Це те, що зараз розглядається в українському уряді для своєї ІТ-армії.

Іншим фактором є непередбачуваність хакерських груп, які діють як децентралізовані «кіберпартизани». Це може мати серйозні побічні ефекти за межі зони бойових дій, потенційно призводячи до ескалації в інших країнах.

Міжнародне співтовариство та наукові експерти докладали зусиль, щоб подати заявку права війни та міжнародного гуманітарного права до кібероперацій, кульмінацією яких стала публікація Таллінських посібників. Ці посібники намагаються висвітлити питання міжнародного права щодо кіберінцидентів. Але багато проблем, які ІТ-армія висунула на перший план, залишаються оскарженими, особливо тому, що ці документи не є обов'язковими.

Конфлікти можуть стати ще складнішими, оскільки інструменти штучного інтелекту все частіше використовуються в кібератаках і поступово стануть частиною сучасної інформаційної війни в найближчі кілька років.

Ось чому нам потрібні більш узгоджені зусилля для вирішення практичних і юридичних проблем, перш ніж настане нова ера кібервійни». ***(Vasileios Karagiannopoulos. Ukraine's IT army is a world first: here's why it is an important part of the war // The Conversation Media Group Ltd (https://theconversation.com/ukraines-it-army-is-a-world-first-heres-why-it-is-an-important-part-of-the-war-212745?utm_source=flipboard&utm_content=Farawayman%2Fmagazine%2FMilitary+Technology). 25.10.2023).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Сполучені Штати та Данія допоможуть Україні зменшити вразливість і зміцнити стійкість критичної інфраструктури до кіберзагроз.

Про це повідомляє РБК-Україна з посиланням на посольство США в Україні.

Зазначається, що країни реалізовуватимуть це через проєкт USAID «Кібербезпека критично важливої інфраструктури України». Данія інвестує в проєкт 2,8 мільйона доларів.

«Починаючи з 2014 року та особливо перед початком брутального повномасштабного вторгнення в Україну в лютому 2022 року, Російська Федерація спрямовувала та спрямовує численні кібератаки проти урядових установ та критичної інфраструктури України, зокрема: телекомунікаційних систем, електромереж та систем зберігання даних», — йдеться у повідомленні.

Сполучені Штати з цією новою підтримкою з боку Данії, продовжать свою діяльність зі зміцнення кібербезпекового середовища України, зокрема законодавчої, нормативної та інституційної бази; підготовки фахівців у сфері кібербезпеки, зокрема через підвищення кваліфікації чинних спеціалістів.

Також мова йде про розбудову пулу спеціалістів у сфері кібербезпеки, підвищення взаємодовіри та посилення співробітництва між приватним та державним сектором з метою формування в Україні більш стійкої галузі кібербезпеки.

Посол США в Україні Бріджит Брінк заявила, що розширення можливостей України у сфері кібербезпеки є критично необхідним для забезпечення захисту органів влади та об’єктів критичної інфраструктури від численних кібератак, які Росія спрямовує проти України.

Також Сполучені Штати заявили, що пишаються партнерством із Данією та Новою Зеландією в рамках проєкту USAID «Кібербезпека критично важливої інфраструктури України» і сподіваються на продовження тісної співпраці.

Приєднавшись до цього проєкту, Данія висловлює свою підтримку українському народу, допомагаючи захищати Україну від кібератак. На початку 2023 року свій внесок у кібербезпекові програми зробила Нова Зеландія, інвестувавши в 0,49 мільйона доларів…» ***(Юлія Ткач. США і Данія виділять допомогу для посилення кібербезпеки України // Онлайн-медіа «НикВести» (https://nikvesti.com/ua/news/politics/277249). 03.10.2023).***

***

«Агентство національної безпеки (NSA) і Агентство з кібербезпеки та безпеки інфраструктури (CISA) оприлюднили сьогодні десятку найпоширеніших неправильних конфігурацій кібербезпеки, які виявили їхні червоні та сині команди в мережах великих організацій.

У сьогоднішньому повідомленні також детально описано, які тактики, прийоми та процедури (TTP) використовують суб'єкти загроз, щоб успішно використовувати ці неправильні конфігурації з різними цілями, включаючи отримання доступу до конфіденційної інформації чи систем, переміщення в бік і націлювання.

Інформація, включена до звіту, була зібрана Червоною та Синьою командами двох агенцій під час оцінки та заходів з реагування на інциденти.

«Ці групи оцінили безпеку багатьох мереж у Міністерстві оборони (DoD), Федеральному цивільному виконавчому відділі (FCEB), урядах штатів, місцевих, племінних і територіальних (SLTT) і приватному секторі», — заявили в АНБ.

«Ці оцінки показали, як поширені неправильні конфігурації, такі як облікові дані за замовчуванням, дозволи на обслуговування та конфігурації програмного забезпечення та програм; неправильне розділення привілеїв користувача та адміністратора; недостатній моніторинг внутрішньої мережі; погане керування виправленнями, піддають ризику кожного американця», — сказав Ерік. Голдштейн, виконавчий помічник директора з кібербезпеки CISA.

До 10 найпоширеніших мережевих конфігурацій, виявлених під час оцінювання червоною та синьою командами, а також командами пошуку та реагування на інциденти NSA та CISA належать:

Стандартні конфігурації програмного забезпечення та програм

Неправильне розділення прав користувача/адміністратора

Недостатній моніторинг внутрішньої мережі

Відсутність сегментації мережі

Погане керування виправленнями

Обхід системи контролю доступу

Слабкі або неправильно налаштовані методи багатофакторної автентифікації (MFA).

Недостатньо списків керування доступом (ACL) до мережевих ресурсів і служб

Погана гігієна облікових даних

Необмежене виконання коду

Як зазначено в спільній консультації, ці поширені неправильні конфігурації зображують системні вразливості в мережах численних великих організацій.

Це підкреслює критичну необхідність для виробників програмного забезпечення прийняти принципи безпеки за проектом, тим самим зменшуючи ризик компромісу.

Гольдштейн закликав виробників програмного забезпечення застосувати набір проактивних практик, спрямованих на ефективне вирішення цих неправильних конфігурацій і полегшення проблем, з якими стикаються захисники мережі.

Вони включають інтеграцію засобів контролю безпеки в архітектуру продукту з початкових етапів розробки та протягом життєвого циклу розробки програмного забезпечення.

Крім того, виробники повинні припинити використовувати паролі за замовчуванням і переконатися, що компрометація єдиного елемента безпеки не загрожує цілісності всієї системи. Важливо також вживати профілактичних заходів для усунення цілих категорій вразливостей, наприклад, використовувати безпечні для пам’яті мови кодування або реалізувати параметризовані запити.

Нарешті, Голдштейн сказав, що обов’язково ввести багатофакторну автентифікацію (MFA) для привілейованих користувачів і встановити MFA як функцію за замовчуванням, що робить її стандартною практикою, а не необов’язковим вибором.

NSA та CISA також заохочують захисників мережі впроваджувати рекомендовані заходи пом’якшення, щоб знизити ризик використання зловмисниками цих поширених неправильних конфігурацій.

Пом’якшення, які мали б такий ефект, включають:

- усунення облікових даних за замовчуванням і конфігурацій посилення,
- дезактивація невикористаних послуг і впровадження суворого контролю доступу,
- забезпечення регулярних оновлень і автоматизація процесу виправлення, надаючи пріоритет виправленню відомих уразливостей, які були використані,
- а також скорочення, обмеження, перевірка та ретельний моніторинг адміністративних облікових записів і привілеїв.

У сьогоднішньому пораді NSA та CISA рекомендують, окрім застосування наведених заходів пом’якшення, «відпрацьовувати, тестувати та перевіряти програму безпеки вашої організації щодо поведінки загроз, пов’язаних зі структурою MITER ATT&CK for Enterprise».

Обидва федеральні агентства також радять протестувати існуючий інвентар засобів контролю безпеки, щоб оцінити їх ефективність у порівнянні з методами ATT&CK, описаними в пораді». ***(Sergiu Gatlan. NSA and CISA reveal top 10 cybersecurity misconfigurations // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/nsa-and-cisa-reveal-top-10-cybersecurity-misconfigurations/?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 05.10.2023).***

***

«Цього тижня корпорація Майкрософт попередила відправників електронної пошти Microsoft 365 про необхідність автентифікації вихідних повідомлень. Цей крок був викликаний нещодавнім оголошенням Google про суворіші правила боротьби зі спамом для масових відправників.

«Налаштувавши автентифікацію електронної пошти для свого домену, ви можете гарантувати, що ваші повідомлення з меншою ймовірністю будуть відхилені або позначені як спам постачальниками послуг електронної пошти, такими як Gmail, Yahoo, AOL, Outlook.com», — заявила команда Microsoft Defender для Office 365.

«Це особливо важливо під час масового надсилання електронної пошти (великого обсягу електронної пошти), оскільки це допомагає підтримувати доступність і репутацію ваших електронних кампаній».

Недотримання нещодавно оголошених стандартів автентифікації електронної пошти може призвести до відхилення електронних листів або позначення їх як спаму.

Корпорація Майкрософт також попередила, що службу Microsoft 365 не слід використовувати для масової розсилки електронною поштою, оскільки електронні листи, які не відповідають обмеженням надсилання, блокуватимуться або надсилатимуться до спеціальних пулів доставки з високим ризиком засобами контролю вихідного спаму, вбудованими в Exchange Online Protection (EOP).

Ті, хто хоче масово надсилати електронні листи, повинні використовувати власні локальні сервери електронної пошти або сторонніх постачальників масової розсилки, що допоможе забезпечити належну практику надсилання електронних листів.

Організації, які хочуть масово доставляти електронні листи через EOP, повинні дотримуватися цих вказівок із захисту вихідного спаму:

Будьте обережні, щоб не перевищувати ліміти надсилання в службі, надсилаючи електронні листи з високою швидкістю або обсягом. Це включає утримання від надсилання електронних листів великому списку одержувачів BCC.

Утримайтеся від використання адрес у вашому основному електронному домені як відправників для масових електронних листів, оскільки це може вплинути на доставку звичайних електронних листів від відправників у межах домену. Натомість подумайте про використання спеціального субдомену виключно для масової електронної пошти.

Переконайтеся, що для будь-яких спеціальних субдоменів налаштовано записи автентифікації електронної пошти в DNS, зокрема SPF, DKIM і DMARC.

Однак Microsoft попередила, що навіть «виконання цих рекомендацій не гарантує доставку. Якщо вашу електронну пошту відхилено масово, надішліть її через локальний або сторонній постачальник».

Попередження Редмонда було викликане оголошенням Google щодо введення нових інструкцій щодо боротьби зі спамом, націлених на відправників понад 5000 електронних листів щодня користувачам Gmail.

Починаючи з 1 лютого 2024 року, Google зобов'яже відправників, які перевищують цей поріг, застосовувати автентифікацію електронної пошти SPF/DKIM і DMARC для своїх доменів. Цей захід спрямований на посилення захисту від спроб спуфінгу та фішингу електронної пошти.

Крім того, масові відправники повинні надати одержувачам Gmail можливість одним клацанням миші скасувати підписку на комерційні електронні листи та негайно розглядати запити на скасування підписки протягом двох днів.

У рамках цих зусиль по боротьбі зі спамом Google заявив, що також буде ретельно стежити за пороговими значеннями спаму, а у випадках, коли буде виявлено масових відправників, позначатиме їхні електронні листи як спам, щоб захистити користувачів від небажаних і потенційно шкідливих повідомлень.

«Якщо ви не відповідаєте вимогам [..], ваша електронна пошта може бути доставлена не так, як очікувалося, або може бути позначена як спам», — попереджає Google». ***(Sergiu Gatlan. Microsoft 365 admins warned of new Google anti-spam rules // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/microsoft-365-admins-warned-of-new-google-anti-spam-rules/?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology) . 08.10.2023).***

***

«Існують певні ринкові теми, які незаперечні з точки зору довгострокового зростання та потреб. Одним із них є кібербезпека. Світ стає все більш оцифрованим, що призводить до зростання потреби в передових рішеннях кібербезпеки. Одним із інструментів інвестування, який скористався цією тенденцією, є First Trust NASDAQ Cybersecurity ETF (NASDAQ: CIBR). Цей ETF надає інвесторам доступ до диверсифікованого портфеля компаній, які є піонерами в секторі кібербезпеки. CIBR прагне відтворити показники індексу кібербезпеки Nasdaq CTA (NQCYBR). Цей індекс відстежує ефективність компаній, залучених у сектор кібербезпеки, включно з тими, які пропонують послуги та продукти, пов'язані зі створенням, впровадженням і керуванням протоколами безпеки, що застосовуються до приватних і публічних мереж, комп'ютерів і мобільних пристроїв.

На перший погляд, можна було б подумати, що це проста інвестиція, і багато в чому я вважаю, що це правда. Проблема полягає в тому, що коли ви дивитесь на співвідношення CIBR до S&P 500 ETF (SPY), то воно дійсно не перевершує на стійкій основі. Показники фонду з моменту заснування приблизно відповідають показникам S&P.

Чому фонд не переміг індекс S&P 500 як тематична гра на кібербезпеку, незважаючи на очевидні майбутні перспективи простору? Найпростіша відповідь, мабуть, правильна – тому що це не фонд із великою капіталізацією.

Середня ринкова капіталізація становить 9,5 мільярда доларів, що робить цю стратегію більше середньої капіталізації. Коли ми дивимося на S&P MIDCAP 400 ETF (MDY) відносно S&P 500 ETF (SPY), стає зрозуміло, що компанії із середньою капіталізацією боролися з концентрованими середніми значеннями для компаній із великою капіталізацією. CIBR серед середніх компаній із середньою капіталізацією загалом показав кращі результати, ніж порівняно з компаніями з великою капіталізацією.

Холдинги CIBR

CIBR мав загалом 33 холдинги з максимальною ринковою капіталізацією 342 мільярди доларів США та середньою ринковою капіталізацією 9 мільярдів доларів.

Мінімальна ринкова капіталізація зараз становить 430 мільйонів доларів. ETF зосереджується на індустрії програмного забезпечення, яка становить 53% його портфеля. IT-послуги та комунікаційне обладнання є двома іншими визначними секторами в портфоліо.

П’ять найбільших холдингів CIBR, які складають приблизно 30% портфеля ETF, включають:

Infosys, Ltd.

Palo Alto Networks, Inc.

Fortinet, Inc.

Cisco Systems, Inc.

Broadcom

Оцінки холдингів мають широкий діапазон. Infosys виглядає розумно на 25, а Пало-Альто — на 195 (звичайно дорого, але акції значно зросли). Fortinet займає 45, а стійка Cisco є найпривабливішою з 17,41, а Broadcom – 26. Дехто стверджуватиме, що співвідношення ціни та прибутку не має значення, але показник усе ще дає відчуття потенційної переоцінки акцій, які мають значний прибуток. відсоток форвардних доходів.

Порівняння однолітків

Порівняння CIBR з аналогами виявляє його конкурентну перевагу. ETF WisdomTree Cybersecurity Fund (WCBR), Global X Cybersecurity ETF (BUG), ETFMG Prime Cyber Security ETF (HACK) і iShares Cybersecurity and Tech ETF (IHAK) є одними з подібних ETF на ринку. Однак CIBR перевершує більшість цих ETF з точки зору прибутковості та активів під управлінням.

Справа для CIBR

Кібербезпека – це галузь, яка швидко розвивається, і прогнозується, що до 2025 року глобальні витрати від кіберзлочинності досягнуть 10,5 трильйонів доларів США. Таким чином, існує значний попит на ефективні рішення з кібербезпеки, і компанії, які працюють у цьому просторі, мають хороші можливості для отримання вигоди. З цієї точки зору можна стверджувати, що цей фонд має бути в більшості портфелів, просто майте на увазі, що більшість середніх ринкових показників у будь-

якому випадку матиме вплив на ці компанії. Це більше питання про те, наскільки ви хочете переважити тему відносно основного розподілу.

Завдяки різноманітному портфоліо компаній з кібербезпеки CIBR пропонує інвесторам унікальну можливість отримати доступ до цієї процвітаючої галузі. CIBR продемонстрував високу ефективність і потенціал зростання з поправкою на його середню ринкову капіталізацію в циклі, який в основному надавав перевагу великим капіталізаціям. Це свідчить про те, що він може бути цінним доповненням до інвестиційного портфеля за умови відповідного розміру відносно основного фонду акцій.

Я думаю, що це хороший фонд і чудова довгострокова тема. First Trust NASDAQ Cybersecurity ETF представляє привабливу інвестиційну можливість для тих, хто хоче отримати вигоду від зростаючого попиту на рішення з кібербезпеки.

Ринки не такі ефективні, як вам здається. Між ринковими сигналами та реакцією інвесторів часто виникають розриви, які допомагають визначити, чи ми перебуваємо в середовищі «ризику» чи «ризику».

Звіт Lead -Lag може дати вам перевагу в читанні ринку, щоб ви могли приймати рішення про розподіл активів на основі досліджень, які отримали нагороди. Я дам вам сигнали – вам вирішувати, чи піти в атаку (тобто збільшити ризикові активи, такі як акції, коли ризик «увімкнено»), чи захиститися (тобто схилятися до більш консервативних активів, таких як як облігації/готівка, коли ризик «вимкнено»)». ***(Michael A. Gayed. CIBR: Volatile Alpha That's Hard To Hack // Seeking Alpha (https://seekingalpha.com/article/4639700-cibr-volatile-alpha-hard-to-hack?feed_item_type=article&utm_source=flipboard&utm_content=user%2Fseekingalpha). 09.10.2023).***

***

«Університети Великої Британії (UUK), Jisc, орган цифрової та даних для вищої освіти та досліджень, і Національний центр кібербезпеки (NCSC) випустили нові рекомендації з кібербезпеки для керівників вищої ланки та технічних команд у секторах вищої освіти та досліджень.

Рекомендації замінюють попередні версії та окреслюють основні загрози кібербезпеці, з якими стикається сектор вищої освіти (ВО), вплив нещодавніх атак на окремі організації, а також визначають обов’язки щодо розуміння та пом’якшення цих ризиків.

Три підкреслюють, що університети залишаються привабливою мішенню для кіберзлочинців через особисті дані, які вони зберігають, потенційно чутливі дослідження та розмір їхньої цифрової інфраструктури. У зв’язку з цим ІТ-лідерів університетів заохочують завантажити цей ресурс, щоб краще зрозуміти потенційну кіберзагрозу та допомогти не лише запобігти, але, сподіваємося, навіть пом’якшити вплив потенційно руйнівних кіберінцидентів.

Охоплені питання:

обов'язки керівника

поточні загрози кібербезпеці

вплив кібератак

нормативні вимоги

мінімізація ризику атак

пом'якшення впливу атак.

«Університети досягли значного прогресу в розробці процесів, які керують ризиками, пов’язаними з безпекою», — сказав професор Пол Бойл, віце-канцлер Університету Суонсі та голова Jisc.

«Однак ще багато чого потрібно зробити, і кібербезпека ніколи не була такою важливою [оскільки] зв’язок і цифрові технології тепер лежать в основі майже всіх аспектів роботи університету чи дослідницького центру. Це робить безпеку наших мереж, даних і людей надзвичайно важливою, і як лідери, ми несемо основну відповідальність.

«Це керівництво демонструє критичність кібербезпеки [і] нагадує нам, що через роботу, яку ми виконуємо, і дані, які ми маємо, наш сектор залишається привабливою мішенню для всіх видів кіберзлочинців — від оппортуністів до державних -спонсоровані високоорганізовані групи».

«Середовище вищої освіти, яке дедалі більше глобалізується, щодня надає можливості людям і установам у всьому світі», – додав Джеймі Ерроусміт, директор Міжнародних університетів Великобританії.

«Підтримка надійної та комплексної системи кібербезпеки є ключем до того, щоб ми могли максимізувати ці переваги та продовжувати спостерігати за їхнім зростанням у безпечний і надійний спосіб. Це керівництво містить чіткі поради для керівників вищої ланки, які хочуть переконатися, що кібербезпека їх установи відповідає цим зростаючим викликам. У ньому описано нові ризики та дієві способи їх усунення, а також інформацію про розвиток відкритої та спільної інституційної культури у боротьбі з кіберзагрозами».

«Ми наполегливо заохочуємо всіх керівників вищої ланки та технічні команди з університетів дотримуватися порад в оновлених інструкціях і скористатися інструментами та ресурсами NCSC для підвищення своєї кіберстійкості», — додала Сара Лайонс, заступник директора NCSC з економіки та стійкості суспільства.

Нові рекомендації, які підтримує Асоціація інформаційної безпеки університетів і коледжів (UCISA), замінюють попередню версію, видану в 2021 році…» ***(Gary Flood. HE sector issued with new cyber security guidance // Informed Communications Ltd. (https://www.ukauthority.com/articles/he-sector-issued-with-new-cyber-security-guidance/). 05.10.2023).***

***

«Загроза, яку несуть порушення кібербезпеки для організацій, лише зростає з кожним роком. Фактично, наші останні дані в Resilinc показують, що кібератаки були восьмим за кількістю повідомлень про збої в першому півріччі 2023 року, що залишається проблемою для керівників проектів. Зовсім нещодавно ми стали свідками нападів на аеропорт Лондон-Сіті, аеропорт Бірмінгема та навіть на виборчі реєстри Великобританії, намагаючись викрасти особисті дані та вивести з ладу послуги, об’єкти чи інфраструктуру.

Ці атаки мають далекосяжні наслідки, починаючи від фінансових втрат і закінчуючи репутаційною шкодою. Щоб пом’якшити ці ризики, організації повинні

інвестувати в ресурси кібербезпеки, прийняти проактивні заходи безпеки та сприяти співпраці в рамках ланцюжка поставок.

У цій статті буде висвітлено, як компанії можуть вжити запобіжних заходів, щоб запобігти збитку, спричиненому кібератаками, і як пом'якшити порушення, якщо вони стаються.

Передаварійне планування: висвітлення вразливості постачальника

Відстеження того, хто з ваших постачальників послуг і партнерів піддається особливому ризику кіберзломів, допоможе забезпечити безпеку вашої організації. Переважна більшість організацій використовує технологію IoT у своїй повсякденній діяльності, чи то для пошуку товарів, що зберігаються, відстеження матеріалів і послуг, чи для більш загальних телекомунікацій. Це означає, що тепер є багато способів, за допомогою яких порушення можуть вивести з ладу ваш ланцюжок поставок на будь-якому рівні в IoT, чи то через рівень сприйняття, мережевий рівень, рівень обробки чи рівень додатків.

Опитування Уряду Великої Британії щодо порушень кібербезпеки за 2023 рік показало, що невеликі організації виявляють кібератаки рідше, ніж минулого року, і, можливо, вони не здійснюють достатній рівень моніторингу чи реєстрації порушень.

Прозоре спілкування між вами та вашими партнерами є першим кроком до мінімізації вашого кіберризику. Цього можна досягти, спершу визначивши та відобразивши, хто є у вашому ланцюжку постачання, на кількох рівнях. Дізнавшись, хто є у вашому ланцюжку постачання, ви зможете проводити оцінку ризиків кібербезпеки постачальника та відстежувати відповідні сертифікати серед компаній, з якими ви працюєте, на підрівнях ланцюга постачання. Вирішальною є кількісна оцінка того, які з ваших постачальників послуг і партнерів мають надійні можливості керування, а які – ні.

Тоді у вас є можливість відстежувати (цілодобово та без вихідних) усіх своїх постачальників на предмет потенційних порушень або ризиків кібербезпеки. Завдяки відображенню та моніторингу ланцюга постачання ваша організація зможе працювати над усуненням недоліків, знаходити постачальників із більш надійними

процесами та зменшувати ризики за допомогою спільних планів з іншими партнерами. Відстеження прогресу має основне значення для забезпечення найкращих можливостей безпеки: пам’ятайте, комунікація є ключовою для усунення вразливості постачальника!

Активна підготовка до інциденту: вирішальне значення для обмеження збитків

Хоча планування перед інцидентом є невід’ємною частиною зниження ризику, кіберзломи залишаються невід’ємною загрозою при використанні IoT та інших цифрових технологій. Насправді витрати на рішення для кібербезпеки IoT досягнуть понад 6 мільярдів доларів США до 2023 року, тому сьогодні це сфера, яка викликає дедалі більше занепокоєння для компаній.

Але опитування уряду Великої Британії щодо порушень кібербезпеки також показало, що 32% компаній пам’ятають про кіберзлам або атаку за останні 12 місяців, і цей показник зростає для середнього бізнесу (59%) і великого бізнесу (69%).

Це підкреслює, що підприємства ще не розширили свої можливості кібермоніторингу настільки, щоб зменшити кіберризик до достатнього рівня. Відповідно, у 2022 році майже 90% професіоналів у сфері технологій виявили значні ризики для свого ланцюга постачання програмного забезпечення.

У разі кіберзлому ви повинні вжити негайних заходів, щоб стримати та зменшити шкоду. Такі заходи можуть включати зміну системних кодів доступу, скасування доступу до послуг IoT для сторін, які також можуть постраждати, і сповіщення персоналу та партнерів, щоб вони могли бути напоготові. Половину битви для керівників проектів можна виграти просто завдяки тісній співпраці із зацікавленими сторонами.

Далі компанії повинні оцінити вплив кіберзлому шляхом кількісної оцінки впливу на набори даних, системи та фінанси. Це не тільки полегшить вирішення проблем, але це важлива інформація, яку можна задокументувати, щоб запобігти подібним порушенням у майбутньому. Починаючи з кількісного визначення впливу, керівники проектів повинні потім переконатися, що порушення будь-якого впливу

керується. Це означає спілкування з партнерами та тими, хто пропонує послуги, щоб забезпечити відновлення безпечного доступу та надійності в наборах даних і системах.

Посилення процесів, щоб протистояти майбутнім атакам

Удосконалення ваших процесів має бути головним пріоритетом для менеджерів проектів у всіх секторах, які прагнуть зміцнити свої ланцюжки поставок. У той час як дані з нашого EventWatch із визначенням збоїв ШІ рішення показує, що в першому кварталі 2023 року було менше кібератак, ніж у першому кварталі 2022 року. Наші останні дані про зареєстровані кібератаки підкреслюють, що збої фактично зросли на 24% у всьому світі в першому півріччі 2023 року порівняно з першим півріччям 2022 року. Не кажучи вже про постійну нестачу робочої сили в кібер галузі безпеки та IT, які лише погіршили цю проблему.

Ви також можете мінімізувати ймовірність порушення за допомогою кращого навчання персоналу, яке передбачає чіткі цілі та процедури, яких слід дотримуватися. Значна частина порушень, які трапляються, відбувається через людську помилку, тому в майбутньому керівники проектів повинні забезпечити належне навчання, яке є важливим для будь-якого робочого середовища у 2023 році.

Застосовуючи як стратегію підготовки до інциденту, так і активну підготовку до інциденту, менеджери проектів матимуть найкраще місце для захисту ланцюжків поставок свого бізнесу. Ефективна комунікація між персоналом, постачальниками послуг і партнерами є одним із найкращих способів мінімізації кіберризику та підготовки до будь-яких порушень, які стаються. Тому керівники проектів повинні прагнути запровадити рішення для відображення та моніторингу ланцюга поставок, яке виявляє слабкі місця в кіберготовності, а також процес пом’якшення у разі порушення». ***(Bindiya Vakil. Planning, Prep And Mitigation: Minimise Cyber Security Risk In Your Supply Chain // PM Today (https://www.pmtoday.co.uk/planning-prep-and-mitigation-minimise-cyber-security-risk-in-your-supply-chain/). 02.10.2023).***

***

«Згідно з новим дослідженням, половина фахівців із кібербезпеки стверджують, що стрес, пов'язаний з роботою, не дає їм спати вночі.

Занепокоєння щодо зростаючого професійного навантаження було визначено як одне з головних джерел стресу для співробітників служби безпеки разом із загрозою кібератаки на їхню організацію.

Висновки, що містяться у звіті про стан професій за 2022/2023 роки Дипломованого інституту інформаційної безпеки (CIISec), підкреслюють інтенсивний тиск, який чиниться на співробітників служби безпеки в період ескалації загроз.

CIISec зазначив, що галузь безпеки «все ще страждає від проблем, включаючи стрес і перевтому», причому майже чверть (22%) респондентів працюють більше 48 годин на тиждень.

За даними Всесвітньої організації охорони здоров'я, 8% працюють більше 55 годин на тиждень, що позначає критичну межу між безпечною та небезпечною практикою праці.

Виконавчий директор CIISec Аманда Фінч сказала, що ці результати викликають серйозне занепокоєння, і закликала організації приділяти більше уваги допоміжному персоналу служби безпеки.

А ті, хто не визнають тиску, з яким стикаються практики, можуть втратити життєво важливий талант у період, сповнений широкого розголосу дефіциту навичок.

«Індустрія не може спочивати на лаврах», – сказала вона. «Він повинен зробити більше, щоб забезпечити належну підтримку талантів і не згоріти. Ключем до цього буде надання їм відповідних навичок і залучення свіжої крові в галузь, щоб команди не зазнавали надмірного тиску».

Культура «завжди ввімкненої» кібербезпеки

Існують тривалі занепокоєння щодо стресу, пов'язаного з роботою, і тиску робочих місць у сфері безпеки. У дослідженні Gartner, проведеному в лютому 2023 року, майже половина з половини CISO і старших спеціалістів InfoSec можуть залишити галузь у найближчі п'ять років через стрес.

Тессіан окремо виявив, що вимоги до старших практиків призвели до того, що деякі працюють надто багато годин і навіть пропускають життєві події або скасовують відпустку.

Тессіан виявив, що в середньому CISO працюють 11 додаткових годин на тиждень через вимоги до них.

за 2022 рік, близько 91% спеціалістів із безпеки також заявили, що відчувають дедалі більше стресу у своїй ролі Відповідно до звіту Voice of SecOps.

У червні керівники вищого рівня безпеки повідомили ITPro, що індустрія має звернути увагу на культуру «завжди ввімкнено», яка заважає професії. Лідери попереджають, що дискусії про психічне здоров'я та благополуччя є незначними й незначними в галузях, які увічнюють негативну культуру на робочому місці.

Економічні ризики та тиск

Макроекономічні умови також викликали занепокоєння серед практиків безпеки. Респонденти сказали CIISec, що поточний економічний клімат призведе або вже створив додаткові ризики для організацій.

Понад три чверті сказали, що вони стурбовані ризиками, пов'язаними з шахрайством, у той час як 58% респондентів виділили загрози від інсайдерів як ключову проблему.

Практики менш стурбовані економічними наслідками для робочих місць, виявив CIISec. Фахівці з безпеки фактично показали позитивний погляд на галузь і можливості в космосі, незважаючи на поточні виклики.

Майже 80% сказали, що вони мають «добрі» або «чудові» кар'єрні перспективи, а понад 80% сказали, що галузь «зростає» або «процвітає».

Фінч припустив, що поточний ландшафт загроз означає, що професія безпеки більш-менш «стійка до кризи» через зростаючу потребу в навичках, пов'язаних з безпекою, в організаціях будь-якого розміру.

«Приємно бачити, що професіонали з кібербезпеки позитивно оцінюють свої кар'єрні перспективи», – сказала вона.

«Індустрія кібербезпеки процвітає. Він має багато можливостей для людей майже будь-якого походження, і потреба в кібербезпеці є більшою, ніж будь-коли,

оскільки загрози постійно зростають, що робить критично важливу функцію, по суті, стійкою до рецесії». ***(Ross Kelly. Work-related stress "keeps cyber security professionals awake at night" // Future US, Inc. (https://www.itpro.com/security/work-related-stress-keeps-cyber-security-professionals-awake-at-night). 12.10.2023).***

***

«Оскільки кіберзагрози стають все більш різноманітними та витонченими, базових знань про кібербезпеку вже недостатньо. Дуже важливо розуміти, як працюють різні загрози, як їх виявляють і протидіють. У цьому світлі кібербезпека — це не лише технічна навичка, але й важлива життєва навичка, яка допомагає захистити нас і наше довкілля.

Ця стаття присвячена галузям із високим ризиком, таким як iGaming, де особливо підкреслюється роль кібербезпеки. Ці галузі потребують ще більшої уваги до стандартів кібербезпеки через обробку конфіденційних персональних даних і значні фінансові операції. Постійна пильність і оновлення інформації про кібербезпеку важливі як для окремих осіб, так і для компаній, які працюють у цих сферах.

Простіше кажучи, розуміння кібербезпеки перетворилося з необов'язкового на обов'язкове. Незалежно від галузі, знання кібербезпеки дає нам інструменти, необхідні для захисту від цифрових загроз.

Симбіоз кібербезпеки та iGaming

Кібербезпека – це не просто технічна майстерність – це основа сучасного життя, що дозволяє людям виявляти потенційні кіберзагрози, боротися з ними та запобігати їм. Це особливо важливо в індустрії iGaming, де ризики експоненціально вищі, ніж в інших онлайн-діяльності. Щодня платформи iGaming обробляють тисячі, якщо не мільйони, операцій із значними сумами грошей і конфіденційною особистою інформацією.

Обговорюючи iGaming і кібербезпеку, ми розуміємо, що ігрові платформи є головною ціллю для кіберзлочинців. Хакери намагаються використати вразливі місця системи, щоб отримати доступ не лише до коштів, але й до конфіденційної

інформації, що може призвести до крадіжки особистих даних та інших шахрайств. Незважаючи на те, що ігрові компанії повинні інвестувати в системи кібербезпеки, обізнаність і освіта користувачів не менш важливі.

Завдяки інформації користувачі можуть не лише виявляти підозрілі дії та повідомлення, а й приймати зважені рішення в режимі онлайн. Наприклад, безпечні способи оплати та методи захисту даних на платформах iGaming можуть значно підвищити безпеку користувачів. Зрозуміло, що розуміння кібербезпеки — це не просто додаткова функція чи перевага, а абсолютна необхідність у світі iGaming.

Уразливості iGaming: критична роль кібербезпеки

iGaming є однією з найбільш швидкозростаючих цифрових галузей, популярність якої різко зросла за останні роки. Хоча це відкриває нові можливості для гравців, це також приносить численні виклики кібербезпеці. Платформа iGaming, яка щодня обробляє величезні суми грошових переказів і особистих даних, природно, стає прибутковою мішенню для злочинців і хакерів.

Уразливості в системах iGaming є проблемою не лише бізнесу; вони також впливають на користувачів широко. Навіть одна слабка ланка – будь то погано захищений платіжний портал або необізнаність користувача – може вивести з ладу всю систему. Тому вкрай важливо, щоб і компанії, і окремі користувачі вкладали час, гроші та ресурси в розуміння та посилення кібербезпеки.

Хоча зараз багато платформ iGaming серйозно ставляться до кібербезпеки, користувачі повинні бути проактивними. Розуміння таких основ, як важливість двофакторної автентифікації та використання надійних паролів, може зменшити багато ризиків. Також важливо бути в курсі заходів безпеки платформи та потенційних загроз.

Загалом, уразливість iGaming вимагає постійної пильності як від компаній, так і від користувачів. Важливість кібербезпеки неможливо переоцінити – це важлива частина довіри між платформою та її користувачем.

Короткі поради щодо кібербезпеки: ефективні заходи для окремих осіб і компаній

Кібербезпека — це не лише відповідальність компаній; Люди беруть участь у забезпеченні власної безпеки та безпеки громади. Тут ми пропонуємо набір простих, але ефективних порад щодо покращення вашої кібербезпеки незалежно від того, чи є ви користувачем iGaming чи ні. Ось кілька порад:

Двофакторна автентифікація: один із найефективніших способів захисту облікових записів і особистої інформації. Це особливо корисно для платформ iGaming, які часто мають справу зі значними фінансовими операціями та особистими даними. Використовуйте його, коли це можливо.

Надійні паролі: складні та унікальні паролі є основою надійної кібербезпеки. Уникайте використання одного пароля для кількох служб і регулярно змінюйте паролі.

VPN-з'єднання: використання VPN не лише захищає вашу конфіденційність, але й підвищує рівень безпеки, особливо в загальнодоступних мережах Wi-Fi. Він шифрує вашу інформацію та робить її невидимою для сторонніх.

Оновлення програмного забезпечення: Оновлення не просто приносять нові функції; вони часто містять важливі покращення безпеки. Оновлюйте все програмне забезпечення та системи на своєму комп'ютері чи мобільному пристрої.

Програмне забезпечення безпеки: інвестуйте в програмне забезпечення безпеки преміум-класу з антивірусом, брандмауером та іншими засобами захисту. Це особливо важливо для активних користувачів iGaming.

За допомогою цих порад ви можете значно посилити власну кібербезпеку та кібербезпеку своєї спільноти. Пам'ятайте, що кібербезпека – це постійна робота, яка потребує активної участі всіх нас.

Висновок

Дійсно, знання – це сила, особливо у сфері кібербезпеки. Весь цифровий ландшафт став складнішим, і iGaming виділяється як галузь, де кібербезпека має першорядне значення. Залишаючись поінформованими та старанними, люди можуть забезпечити безпечне цифрове майбутнє для себе та всієї спільноти. Зробіть кібербезпеку важливою частиною сучасного життя та прокладіть шлях до безпечнішого цифрового світу». ***(The imperative of cyber security: Why knowledge is***

power // Nord News (https://nord.news/2023/10/06/the-imperative-of-cyber-security-why-knowledge-is-power/). 06.10.2023).

***

«Очікується, що до кінця наступного року вартість кібератак на світову економіку перевищить 10,5 трильйона доларів.

Ця приголомшлива сума відображає зростаючу потребу в тому, щоб кібербезпека розглядалася як стратегічний пріоритет на індивідуальному, організаційному та урядовому рівнях.

Як і в будь-якій іншій сфері бізнесу та технологій, штучний інтелект (ШІ) матиме трансформаційний вплив як на атаку, так і на захист. Його вплив буде відчутно в кожній із розглянутих тут тенденцій.

Останні роки прискорили темпи технологічного прогресу в багатьох сферах, і кіберзагрози не відрізняються. Як то кажуть, попереджений – значить озброєний, тож читайте далі, щоб дізнатися, які мої прогнози щодо тенденцій кібербезпеки, до яких усі мають бути напоготові, коли ми прямуємо до 2024 року.

Критика навичок кібербезпеки

Дефіцит фахівців із навичками, необхідними для захисту організацій від кібератак, продовжує бути актуальною темою протягом 2024 року. Насправді, здається, ситуація погіршується – дослідження показують, що більшість (54 відсотки) фахівців з кібербезпеки вважають, що вплив нестачі навичок на їхню організацію погіршився за останні два роки. Ми можемо очікувати, що зусилля, спрямовані на виправлення цієї ситуації, включатимуть постійне підвищення заробітної плати тим, хто володіє необхідними навичками, а також більші інвестиції в програми навчання, розвитку та підвищення кваліфікації.

Генеративний ШІ, прийнятий з обох сторін битви

У міру того, як штучний інтелект стає складнішим із відверто тривожною швидкістю, ми продовжуватимемо бачити все більш складні та розумні атаки на основі ШІ. Це варіюється від спроб глибокої фейкової соціальної інженерії до автоматизованого шкідливого програмного забезпечення, яке розумно адаптується,

щоб уникнути виявлення. У той же час це допоможе нам виявляти, уникати або нейтралізувати загрози завдяки виявленню аномалій у реальному часі, інтелектуальній автентифікації та автоматичному реагуванню на інциденти. Якщо кібератака та захист у 2024 році — це гра в шахи, то штучний інтелект є королевою — зі здатністю створювати потужні стратегічні переваги для тих, хто грає в неї найкраще.

Фішингові атаки нового рівня

Атаки соціальної інженерії, що включають обманом користувачів, щоб надати зловмисникам доступ до систем, також стануть складнішими. Інструменти генеративного штучного інтелекту (такі як ChatGPT) дозволяють більшій кількості зловмисників використовувати розумніші, більш персоналізовані підходи, а атаки deepfake ставатимуть все більш поширеними. Реакція на це в основному буде зосереджена на обізнаності та освіті всієї організації, хоча ШІ та нульова довіра також відіграватимуть зростаючу роль.

Кібербезпека в залі засідань

У 2024 році кібербезпека стане стратегічним пріоритетом, який ІТ-відділ більше не може ігнорувати. За прогнозами Gartner, до 2026 року 70 відсотків рад директорів включатимуть принаймні одного члена з досвідом у цій галузі. Це дає змогу організаціям вийти за межі реактивного захисту, тобто вони можуть діяти, використовуючи нові бізнес-можливості, які постають під час підготовки.

Кібератаки IoT

Більше пристроїв, які спілкуються між собою та мають доступ до Інтернету, означають більше потенційних «входів», якими можуть скористатися кібер-зловмисники. З продовженням революції роботи вдома ризики, пов’язані з підключенням або обміном даними через неправильно захищені пристрої, залишатимуться загрозою. Часто ці пристрої призначені для простоти використання та зручності, а не для безпечних операцій, і домашні споживчі пристрої IoT можуть бути під загрозою через слабкі протоколи безпеки та паролі. Той факт, що галузь загалом зволікає з впровадженням стандартів безпеки IoT, незважаючи на те, що вразливості були очевидними протягом багатьох років, означає, що вона й надалі

залишатиметься слабким місцем кібербезпеки, хоча це змінюється (докладніше про це нижче).

Кіберстійкість – за межами кібербезпеки

Два терміни, які часто використовуються як синоніми, це кібербезпека та кіберстійкість. Однак ця різниця ставатиме все більш важливою протягом 2024 року та далі. Хоча кібербезпека зосереджена на запобіганні атакам, зростаюче значення стійкості багатьма організаціями відображає сувору правду про те, що навіть найкращий захист не може гарантувати 100-відсотковий захист. Заходи стійкості призначені для забезпечення безперервності операцій навіть після успішного порушення. Стратегічним пріоритетом у 2024 році стане розвиток здатності швидкого відновлення з мінімізованою втратою даних і простоєм.

Довіра менше нуля

Фундаментальна концепція нульової довіри – завжди перевіряти – розвивається в міру того, як системи стають все більш складними, а безпека інтегрується в бізнес-стратегію. Нульова довіра стверджує, що немає периметра, у межах якого мережева діяльність може вважатися безпечною. У міру розвитку ландшафту загроз цей принцип поширюється за межі корпоративної мережі до екосистеми віддалених працівників, партнерських організацій та пристроїв Інтернету речей. У 2024 році нульова довіра переходить від технічної моделі безпеки мережі до чогось адаптивного та цілісного, що забезпечується безперервною автентифікацією в реальному часі та моніторингом активності на основі ШІ.

Кібервійна та фінансовані державою кібератаки

Війна в Україні, яка, схоже, вступає в третій рік, виявила, наскільки держави бажають і здатні розгортати кібератаки проти військової та цивільної інфраструктури в 2024 році. Можна впевнено посперечатися, що в майбутньому, де б не відбувалися військові операції по всьому світу вони будуть йти пліч-о-пліч з операціями кібервійни. Найпоширеніші тактики включають фішингові атаки, спрямовані на отримання доступу до систем з метою збою та шпигунства, а також розподілені атаки на відмову в обслуговуванні для вимкнення комунікацій, комунальних послуг, транспорту та інфраструктури безпеки. Крім бойових дій, у

2024 році відбудуться великі вибори в таких країнах, як США, Великобританія та Індія, і ми можемо очікувати зростання кібератак, спрямованих на зрив демократичного процесу.

Навички програмного забезпечення стають усе більш важливими для фахівців з кібербезпеки

Протягом 2024 року спеціалісти з кібербезпеки все частіше будуть виконувати складніші робочі навантаження, оскільки ландшафт загроз стає дедалі складнішим. Це означає не просто в технічному сенсі – тим, хто відповідає за протидію кіберзагрозам, також доведеться виконувати складніші соціальні та культурні аспекти пом'якшення загроз. Це призведе до зростання залежності від навичок спілкування, таких як міжособистісне спілкування, побудова стосунків і вирішення проблем.

Регламент кібербезпеки

Уряди та організації все більше усвідомлюють ризики національній безпеці та економічному зростанню, які становлять кіберзагрози. Потенційні соціальні та політичні наслідки великомасштабних витоків даних також є головним чинником появи нових правил щодо питань кібербезпеки. Наприклад, компанії у Великій Британії мають до квітня 2024 року переконатися, що вони відповідають вимогам Закону про безпеку продуктів і телекомунікацій, який визначає мінімальні вимоги безпеки, яких мають відповідати мережеві продукти (наприклад, вони не повинні постачатися з паролем за замовчуванням). Імплементація подібної Директиви ЄС щодо радіообладнання була відкладена до 2025 року, але ця тема все ще, ймовірно, буде головною в порядку денному законодавців протягом 2024 року…» ***(Bernard Marr. The 10 Biggest Cyber Security Trends In 2024 Everyone Must Be Ready For Now // Forbes (https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/?sh=6c3dd5665f13). 11.10.2023).***

***

«Створення безпечних продуктів потребує перетасування та коригування бізнес-пріоритетів, роботи над організаційною зрілістю та відповідних процесів для встановлення чітких показників.

Кібербезпека залишається критично важливою основою цифрового програмного та апаратного забезпечення, що швидко розширюється у всьому цифровому світі, яке забезпечує роботу всього, від персональних пристроїв до глобальної інфраструктури. За останнє десятиліття було досягнуто значного прогресу в кількох сферах безпеки, особливо у вдосконаленні процесів розробки безпечного програмного забезпечення.

Протягом багатьох років апаратній безпеці приділялося лише обмежена увага. Однак нещодавно було виявлено основні вразливості чіпів, такі як Spectre і Meltdown, які служать суворим нагадуванням про те, що системи можуть бути настільки ж безпечними, наскільки їхня найслабша ланка.

Згідно з даними Національного інституту стандартів і технологій, протягом останніх кількох років галузі спостерігали експоненціальне зростання вразливостей апаратного забезпечення, швидко наздоганяючи зростання програмного забезпечення, зафіксоване протягом останніх десятиліть.

Хоча програмне забезпечення можна виправити, апаратне забезпечення ніколи не може бути легко оновлено; таким чином потенційний негативний вплив таких недоліків безпеки на бізнес різко зростає.

Створення безпечних продуктів, будь то апаратне чи програмне забезпечення, — це шлях, який включає не лише технічні рішення, але й постійне коригування бізнес-пріоритетів, вдосконалення продуктів і процесів, а також встановлення чітких показників для аналізу бізнес-ризиків і прогресу в напрямку їх зменшення. Підприємства повинні комплексно вирішувати всі питання безпеки, приділяючи однакову увагу безпеці обладнання.

Сьогодні, коли ризики зростають не по днях, а по годинах, кібербезпека розглядається здебільшого у відключених силосах. Однак важливо пам’ятати, що безпека – це властивість системи, яка, щоб бути швидкою та всебічною, має розглядатися в різних доменах (програмне забезпечення, апаратне забезпечення,

вбудоване програмне забезпечення, ОС, програма, хмара, мережа тощо) та в усій системі. життєвий цикл (проектування, виробництво, розробка, ланцюг постачання, підтримка та технічне обслуговування тощо).

Апаратна безпека, без сумніву, залишається однією з найважливіших основ загальної безпеки системи. Інтеграція апаратної безпеки з «нижчими» рішеннями забезпечить більш швидкий і більш непроникний підхід до кібербезпеки.

Оскільки безпека стає ще однією вимогою до продукту, виникає природне занепокоєння, чи не уповільнить процес розробки затримка виходу на ринок і, отже, вплине на продуктивність і прибутковість бізнесу.

Щоб стратегії безпеки були успішними, вкрай важливо, щоб вони мінімально впливали на швидкість розробки, щоб уникнути створення суперечливих виборів між своєчасною доставкою продукту та безпекою продукту.

Успішну програму безпеки відзначають:

Чітко визначені бізнес-цілі та пріоритети, визначені заздалегідь і узгоджені між усіма зацікавленими сторонами.

Групи безпеки та розробки повинні тісно співпрацювати протягом усього життєвого циклу продукту від відображення проекту до доставки продукту та підтримки.

Функціональне тестування, розробка продукту та тестування безпеки мають бути тісно інтегровані, щоб працювати узгоджено, щоб забезпечити своєчасне вирішення проблем.

Інструменти тестування безпеки повинні підтримувати процес розробки щодня, а не заважати йому. Серед іншого, тут багато в чому стосується автоматизованого застосування тестів у поточному процесі, низького рівня хибнопозитивних результатів разом із чіткими порадами щодо виправлення, які підтримуються швидким розумінням і вирішенням проблем.

Управління безпекою та контроль має здійснюватися в режимі реального часу за допомогою значущих показників, щоб забезпечити швидке втручання та уникнути пізніх сюрпризів безпеки.

Забезпечення дотримання всього вищезазначеного та усвідомлення ролі, яку апаратне забезпечення має відігравати в цих збоях, надає належного значення безпеці апаратного забезпечення, щоб компанії могли масштабувати свій бізнес до нових висот успіху». ***(Debjani Chaudhury. Hardware Security – An Easily Missed but Crucial Piece of the Cyber Security Puzzle // Media © (https://itsecuritywire.com/featured/importance-of-hardware-security/). 12.10.2023).***

***

«Сучасна екосистема безпеки різноманітна та постійно змінюється, це місце, де кіберризик є головним для керівників усіх рівнів, а загрози безпеці інформації/даних і конфіденційності розвиваються зі швидкістю технічних інновацій, що рушійно рухають прогрес. У цій динамічній екосистемі ми все більше зв’язані по всьому світу, де організації (і окремі особи) однаково стикаються з постійною загрозою кібератак. Ніхто не застрахований, і потенційний вплив успішної цифрової атаки на ваші активи може вплинути на операції, репутацію, доброзичливість клієнтів і багато іншого.

Наші дані все більше піддаються атакам. Інформація є джерелом життя нашої глобальної спільноти, яка постійно розвивається та стає все більш зв’язаною. Силу даних можна побачити в усіх аспектах сучасної епохи, де цінність інформації ніколи не була високою, що дало початок передовим розробкам і прогресу. На жаль, як це часто буває, ризик для цінного об’єкта зростає з такою ж або більшою швидкістю, як і ризик розширення об’єкта. Інформація стала одним із найцінніших нематеріальних активів у світі, водночас займаючи позицію одного з найбільш вразливих активів у світі. Внутрішній ризик є очікуваним результатом цього трансформаційного процесу, який передбачає велику відповідальність за захист інформації, яка є рушієм нашого прогресу.

Ця стаття зосереджена на професійних знаннях, процесах і технологіях, необхідних для пом’якшення постійно зростаючого ризику кібератак і потенційних перерв у роботі компаній, організацій і окремих осіб.

Загрозу інформації можна виміряти багатьма способами – від необережного поводження з даними до постійних зусиль зловмисників використати, змінити або викрасти дані. Часто саме усвідомлений вплив цього ризику сприяє розвитку кібербезпеки. Цей товар, який ми називаємо інформацією, змінив спосіб мислення світу, і його місце у функції безпеки стало завжди присутнім і важливим.

Зважаючи на цей динамічний клімат, вирішення проблеми кібербезпеки та впливу перерв у бізнесі ніколи не було настільки важливим для управління ризиками та успіху організації. Незалежно від розміру вашої організації кібератака може бути надзвичайно дорогою та завдати шкоди виживанню вашого бізнесу. Середовище підвищеної загрози змусило організації підтримувати кіберстрахування через зростаючу складність учасників загроз. У той же час страхування кібервідповідальності стало дорожчим і його важче отримати. Премії за цими планами зросли через збільшення втрат, пов’язаних із претензіями, зростання попиту на покриття та великі виплати від атак програм-вимагачів. Премії кіберстрахування зросли в середньому на 28% у першому кварталі 2022 року порівняно з четвертим кварталом 2021 року. Еволюція ринку кіберстрахування стала причиною переходу від загальних полісів із широкими включеннями та високими лімітами до полісів із детальним покриттям, чіткі технічні вимоги та вимоги безпеки, а також керовані обмеження на основі тенденцій вимог.

Складний ландшафт страхування можна розглядати як один із кількох факторів, що об’єднуються для створення середовища, яке може бути зручним для турбулентної погоди. Можливі елементи, які можуть бути включені в майбутній шторм, це:

Все більш успішні атаки на підприємства будь-якого розміру, що потребують викупу,

Рекордна кількість заяв про кіберстрахування,

Зростаючі збитки від кіберінцидентів, включаючи вимоги щодо кіберстрахування та зростання виплат за цивільними судовими процесами,

Посилення уваги регуляторних і законодавчих органів не лише до методів запобігання та реагування, але й до готовності організацій належним чином

інвестувати в кібербезпеку напередодні атаки, як видно з останніх рекомендацій щодо кібербезпеки від Комісії з цінних паперів і бірж США (SEC).

Розуміння того, як боротися з актором кіберзагрози

Хоча нинішня ситуація здається жахливою, ніколи раніше не було доступних інструментів і ресурсів у обсязі, розумінні та різноманітності, щоб подолати виклик і зменшити ризик.

У міру розвитку загрози від кібератак розвивалися й ті, хто хотів би оскаржити очевидну непереможність суб'єктів загрози. Часто здається, що вони на крок попереду та краще підготовлені. Однак, якщо ми використовуємо наявні в нашому розпорядженні ресурси напередодні потенційної атаки, ми можемо ефективно підготуватися та відреагувати, щоб мінімізувати вплив цього, здавалося б, непереможного ворога – «актора кіберзагроз».

Щоб впоратися зі зростаючими викликами, фахівці з кібербезпеки повинні використовувати людей, процеси та технології, які є в їхньому розпорядженні, щоб захистити конфіденційність, цілісність і доступність даних/інформації, за які вони відповідають; таким чином, забезпечуючи безпеку та конфіденційність.

Є кілька фундаментальних концепцій, які мають вирішальне значення для успіху.

Культура важлива. Низхідний підхід до вирішення проблем безпеки в організації є життєво важливим для досягнення цілісної участі. Кібербезпека — це командна подія, у якій для досягнення найефективніших результатів бере участь кожен, від адміністратора до генерального директора. Якщо відповідна культура безпеки та залучення вищого рівня не досягнута, надихаюче впровадження практик, які створюють хорошу кіберкультуру, може бути складним завданням. Залучення найвищого рівня має вирішальне значення, і нещодавні вказівки SEC щодо кращої прозорості на рівні ради директорів підкріплюють цю основоположну концепцію.

Планування та підготовка до інциденту також є важливими компонентами ефективної програми кібербезпеки. Враховуючи зростання перерв у бізнесі та збитків, пов'язаних із порушеннями, потрібна стратегія для зменшення ризику значного впливу. Ця концепція стає все більш важливою у спробах отримати

кіберстрахування, яке ефективно покриває ідентифікований ризик із відповідними лімітами. Унікальні для кожної організації міркування включають стратегію безпеки та реагування, реагування на інциденти (IRP), безперервність бізнесу (BCP), стратегії аварійного відновлення (DRP), політику/процедури, управління, план фінансового відновлення до події та навчання. Ефективне реагування на кіберінцидент включає підготовку до впровадження технічних заходів, а також фінансову підготовку та планування. Пом'якшення потенційних фінансових наслідків порушення включає розуміння фінансових наслідків порушення, страхового покриття та часових рамок, а також внутрішніх проблем, включаючи нарахування заробітної плати та періоди очікування, і це лише деякі з них.

Ідентифікація технологічного всесвіту вашої організації часто не помічається спеціалістами з безпеки. Сфери розгляду повинні включати інвентаризацію та відображення активів (апаратне забезпечення, програмне забезпечення та дані для конфіденційності, включаючи нематеріальні активи, такі як бізнес-секрети та інтелектуальна власність), аналіз прогалин, ризики та управління вразливістю для включення ризиків третіх сторін. Ідентифікація не обмежується технологією. Під час оцінки критично важливих даних організації слід звернути увагу на комерційні таємниці, які підлягають юридичному захисту, якщо вони захищені за допомогою «розумних заходів». Відповідно до окружного суду США Північного округу Нью-Йорка «[о]цінюючи розумні заходи секретності, суди дивляться на те, чи... інформація захищена фізичною чи кібербезпекою». Елементи персоналу та процесу, які слід враховувати, можуть включати резервне копіювання критично важливих документів для кадрових питань, нарахування заробітної плати, а також фінансовий аналіз для виявлення втраченого доходу та, зрештою, витрати на пом'якшення наслідків інциденту.

Захист і захист мережі включає такі елементи, як обізнаність і навчання, керування виправленнями, керування доступом, захисні технології та операції безпеки. Саме в рамках цієї тематичної області ми обговорюємо важливість шарів захисту та те, що гігієна стосується не лише людей. Гарна кібергігієна означає використання програмного забезпечення, яке сканує комп'ютерні віруси та

зловмисне програмне забезпечення, встановлення мережевих брандмауерів, регулярну зміну паролів, регулярне оновлення програм і операційних систем на всіх пристроях тощо.

Виявлення як концепція диктує, що потужного захисту недостатньо. Добре підготовлені організації постійно шукають аномалії за допомогою журналів, сканування мережі, моніторингу подій і періодичного тестування експлойтів. Важливо пам’ятати, що моніторинг проблем кібербезпеки повинен забезпечувати огляд як ззовні (захисний периметр), так і зсередини.

Реагування на інциденти вимагає скоординованих, добре спланованих, навчених і відпрацьованих зусиль. Попереднє планування має вирішальне значення для реагування. Практика виконання планів на всіх рівнях зміцнює здатність організації ефективно реагувати за допомогою проактивного стратегічного фокусування. IRP часто включають заходи щодо стримування, дослідження та викорінення загроз, а також виявлення та усунення першопричин вразливості під час документування доказів для різних цілей. Ця інформація також допоможе відповісти на питання, важливі для страховиків, яким потрібно буде отримати чітке розуміння того, що сталося, і який вплив мав на операції фізично та фінансово.

Відновлювальні операції зазвичай проводяться пізніше в ході реагування, але, тим не менш, є критичними. Резервне копіювання часто є основною темою обговорення відновлення, але відновлення операцій часто є набагато складнішим і може включати постійне полювання на загрозливих учасників, додаткові програми безпеки та належну обачність у всьому підприємстві. Попередня підготовка в цій категорії надає організації можливість чітко сформулювати витрати на відновлення операцій на відміну від впровадження вдосконалень, які стануть тригером для перевірки страховиком і можуть вплинути на відновлення прибутку вашого бізнесу.

Нарешті, застосування отриманих уроків для вдосконалення дає організації можливість використовувати навіть найменші події для посилення реагування на майбутні інциденти.

Висновок

Щоб об’єднати ці компоненти в ефективну програму кібербезпеки, потрібен проактивний лідер із баченням, який підтримує співпрацю. Як зазначалося, кібербезпека — це командний вид спорту, який вимагає знання найкращих галузевих практик, здатності створити найкращий набір послуг і можливостей для організації, щоб забезпечити очікувану позицію управління ризиками, а також рішучості дотримуватись зусиль, щоб повноцінно впровадження.

Очікується, що правильний лідер з інформаційної безпеки/конфіденційності розширить можливості, захистить і забезпечить підприємство, операції та конкурентоспроможність шляхом надання найкращої доступної програми забезпечення безпеки. Якщо це буде потрібно як частина підприємства, цей лідер керуватиме дотриманням нормативних вимог, включаючи нормативні, правові та управлінські програми, надихаючи при цьому культуру безпеки та ініціативи.

Ресурси, необхідні для виконання цієї місії, не завжди доступні в організації. Партнерство з постачальником послуг, який може відповісти, коли це необхідно, щоб розширити можливості, є життєво важливим для найкращих лідерів кібербезпеки. Деякі з найкращих постачальників послуг надають індивідуальні послуги, щоб заповнити прогалини, де це необхідно. Організаціям слід шукати постачальників, які пропонують послуги, індивідуально налаштовані для кожного клієнта, намагаючись створити або вдосконалити свою програму кібербезпеки. Зрештою, найкращі постачальники повинні надати команду експертів, які привносять десятиліття досвіду в кожну роботу, спеціалізуються на реагуванні на інциденти та відновленні, проактивному формуванні стійкості, фінансовому плануванні до події та аналізі фінансових втрат». ***(Jessica Eldridge, Ron Yearwood Jr., Robert McSorley. Cyber Security & Business Interruption: Foundations for Prevention and Mitigation // Ocean Tomo, J.S. (https://oceantomo.com/insights/cyber-security-business-interruption-foundations-for-prevention-and-mitigation/). 04.10.2023).***

***

«Враховуючи зростання загрози кібератак, зростають і операційні ризики у фінансовому секторі. Відповідь на це має дати DORA. DORA не покладається на розподіл капіталу для управління цими ризиками. DORA вимагає, щоб фінансові компанії дотримувалися конкретних правил щодо захисту, виявлення, стримування та відновлення інцидентів інформаційно-комунікаційних технологій (ІКТ) у майбутньому. Регламент припускає, що відсутність операційної стійкості може поставити під загрозу надійність усієї фінансової системи, навіть якщо підтримується достатній капітал.

Це перший випадок, коли існує нормативний акт ЄС, який, за деякими винятками, поширюється на всі європейські фінансові компанії. Це також підвищує важливість ІТ у дотриманні нормативних вимог.

Зосередьтеся на постачальниках послуг ІКТ

Фінансовий сектор значною мірою залежить від інформаційно-комунікаційних технологій (ІКТ), зокрема інфраструктури та хмарних сервісів. Тому DORA особливо націлена на цю групу сторонніх постачальників ІКТ-послуг. Вперше постачальники послуг будуть регулюватися однаково, якщо вони класифікуються як критичні. Особливо це стосується великих хмарних провайдерів.

DORA уточнює та посилює існуючі вимоги. Він встановлює детальні правила для фінансових компаній, приділяючи особливу увагу управлінню ризиками ІКТ, звітності про інциденти ІКТ і моніторингу ризиків сторонніми постачальниками послуг ІКТ. Метою є сприяння цифровізації фінансового ринку, сприяння конкуренції та інноваціям і забезпечення фінансової стабільності.

DORA можна розглядати як lex specialis до настанови NIS 2, опублікованої одночасно. Система моніторингу DORA для критично важливих сторонніх постачальників послуг ІКТ доповнює правила постачальників хмарних обчислень відповідно до Директиви NIS 2.

Значна потреба в реалізації до кінця 2024 року

DORA базується на існуючих нормах і стандартах ІТ. Однак він уточнює та розширює їх до такого ступеня, що може викликати значну потребу у впровадженні.

Наскільки значними будуть ці зусилля, залежить від типу фінансової компанії та статусу впровадження поточних нормативних вимог до ІТ.

Оскільки всі вимоги мають бути запроваджені з 17 січня 2025 року, фінансові компанії вже повинні бути ознайомлені з вимогами DORA, проаналізувати необхідність дій і планувати впровадження. Перш за все, DORA чітко дає зрозуміти, що цифрова відмовостійкість вимагає співпраці, яка перетинає межі організацій. Загальну відповідальність керівництва за такі теми, як управління безперервністю бізнесу, не можна делегувати окремим організаційним підрозділам. Тепер керівництво має визначити, які послуги ІКТ підтримують критичні чи важливі функції.

Комплексне управління контрактами

Це також вимагає визначення нових ролей і обов'язків, адаптації політик і стратегій, а також створення процесу для управління збоями в ІКТ.

Це також робить управління контрактами більш комплексним. Він повинен охоплювати всі контракти з ІКТ і приділяти особливу увагу підключенню критично важливих сторонніх постачальників послуг ІКТ. Важливу роль відіграють переговори з великими провайдерами США». ***(Michaela Witzel. DORA: Neuer Maßstab für Cybersicherheit in der Finanzwirtschaft // Witzel Erb Backu & Partner (https://www.web-partner.de/en/journal/dora-neuer-massstab-fuer-cybersicherheit-in-der-finanzwirtschaft). 09.10.2023).***

***

«Нещодавній звіт Accenture під назвою «Стійкий до кібернетики генеральний директор» (NYSE: ACN) розкриває парадокс у мисленні глобальних керівників щодо кібербезпеки. Незважаючи на те, що 96% генеральних директорів визнають вирішальну роль кібербезпеки в організаційному зростанні та стабільності, 74% не впевнені у своїй здатності запобігти або мінімізувати шкоду від кібератак. Цей парадокс пояснюється насамперед реактивним підходом до кібербезпеки, а не проактивними заходами, як повідомлялося в понеділок.

Дослідження показує, що 60% генеральних директорів не впроваджують кібербезпеку в початкові бізнес-стратегії, послуги чи продукти. Натомість вони віддають перевагу спорадичному втручанню, а не постійній увазі до кіберзагроз. Цей підхід було визначено як значний фактор підвищення вразливості до порушень безпеки.

У звіті Accenture також підкреслюється хибне уявлення керівників компаній про вартість впровадження заходів кібербезпеки. Більше половини (54%) помилково вважають, що впровадження кібербезпеки коштує дорожче, ніж витримати кібератаку. Цьому сприйняттю суперечить зростаюча вартість кіберзлочинності, яка, за прогнозами Cybersecurity Ventures, до 2025 року досягне 10,5 трильйонів доларів США з 8 трильйонів доларів цього року.

Незважаючи на те, що 90% генеральних директорів вважають кібербезпеку відмінним фактором зміцнення довіри, лише 15% присвячують їй засідання правління. Це ймовірно тому, що 91% відносять це до технічної функції, а не до невід'ємної частини бізнес-стратегії.

Дослідження Accenture також визначає потенційні загрози від генеративного штучного інтелекту, що турбує 64% керівників компаній, які побоюються його використання в складних кібератаках. Паоло Даль Сін, глобальний керівник Accenture Security, підкреслює необхідність захисту даних і цифрових активів завдяки еволюції генеративного штучного інтелекту.

Дослідження розрізняє «кіберстійких генеральних директорів» і «кібервідстаючих». Перші відмінно справляються з ефективним керуванням кіберзагрозами, мають менші витрати на порушення та покращують фінансові показники. Останні, що становлять 46% опитаних генеральних директорів, не завжди вживають проактивних дій і, як правило, реакційні.

Accenture рекомендує п'ять проактивних дій для досягнення кібервідмовостійкості: вбудовування кібербезпеки в бізнес-стратегію з самого початку, встановлення спільної підзвітності в кібербезпеці в усій організації, захист цифрового ядра, розширення кібервідмовостійкості за межі організаційних меж і силосів, а також впровадження постійної кібервідмовостійкості». ***(CEOs' lack of***

confidence in cybersecurity resilience may hinder growth // Fusion Media Limited (https://za.investing.com/news/ceos-lack-of-confidence-in-cybersecurity-resilience-may-hinder-growth-93CH-2895534?utm_source=flipboard&utm_content=InvestingZA%2Fmagazine%2FSouth+Africa+Financial+Markets). 16.10.2023).

***

«Підтримання міцної позиції в галузі кібербезпеки — це постійна робота, а не те, що ви дійсно можете коли-небудь викреслити зі свого списку справ. Це більше, ніж просто дотримання певної структури чи придбання та розгортання рішень безпеки кінцевих точок: суб'єкти загроз постійно розвиваються та знаходять способи обійти ці існуючі елементи керування та рішення безпеки кінцевих точок.

Важливо дотримуватися активного та постійного підходу до пошуку та усунення нових загроз. Хоча це не нова концепція, нещодавно ми спостерігали, як популярні стандарти кібербезпеки та найкращі практики розвиваються, щоб визнати та врахувати постійну розвідку про загрози.

Стандарти та найкращі практики зміщують фокус, щоб спонукати організації:

Збирайте інформацію про поточні загрози

Розробіть план внутрішнього аналізу та використання інформації

Регулярно оцінюйте нові інструменти та процеси для усунення прогалин у безпеці як відповідь на тенденції загроз і спостережувані тактики

Щоб залишатися попереду, зверніть увагу на зміни та створіть процеси для керування поточними загрозами.

H2. ISO 27001

ISO 27001 є провідним у світі стандартом інформаційної безпеки та чудовим прикладом стандарту, який розвивається, щоб зосередитися на зростаючих загрозах безпеці. Найновіша версія ISO 27001, представлена в 2022 році, включає абсолютно новий контроль навколо «розвідки загроз» (ISO27001 Додаток A 5.7 / ISO27002: 2022 пункт 5.7 Розвідка загроз).

Цей контроль вимагає від організацій постійного збору та аналізу інформації про загрози безпеці для проактивного зменшення ризику.

Це актуальна зміна, яка демонструє, як ISO та інші провідні голоси в галузі кібербезпеки вирішують питання ризику. Це говорить про те, що загрози постійно розвиваються. Зменшення ризику є безперервним процесом, а не одноразовим завданням.

H2. Топ-10 OWASP

OWASP (Фонд безпеки програм з відкритим кодом) Top Ten – це інформаційний документ для розробників програм, присвячений загрозам безпеці програм. Його використовують не лише розробники, але й багато посилань на документ для розробки моделей тестування на проникнення, які імітують тактику злому для виявлення вразливостей у системах і процесах організації. Багато інструментів безпеки, наприклад інструменти статичного аналізу коду, використовують набори правил, які посилаються на десятку найкращих OWASP.

Оновлення представило нову категорію: незахищений дизайн. Ця категорія зосереджена безпосередньо на архітектурних недоліках у програмах і закликає до більшого використання моделювання загроз, безпечних шаблонів проектування та безпечної еталонної архітектури.

OWASP описує безпечний дизайн як «культуру та методологію, які постійно оцінюють загрози та гарантують, що код надійно розроблений і перевірений для запобігання відомим методам атак. Моделювання загроз має бути інтегровано в сеанси вдосконалення (або подібні дії); шукайте зміни в потоках даних і контролі доступу чи інших засобах безпеки».

Опис торкається ідеї постійної оцінки загроз. Подібно до оновлення, яке ми бачили в ISO 27001:2022, мета цієї нової категорії в OWASP Top Ten — підвищити обізнаність про важливість проактивного керування загрозами.

Як захистити свою організацію

Незалежно від того, чи налаштовуєте ви систему управління інформаційною безпекою за стандартами ISO 27001:2022, тестуєте свої програми на відповідність OWASP Top Ten або щось зовсім інше, інтеграція функції для оцінки поточних

загроз для вашої організації має вирішальне значення. Хакери постійно розвиваються та змінюють свою тактику, і одного аудиту (або щорічного тесту на проникнення) просто недостатньо, щоб виявити всі слабкі місця, оскільки вони не враховують час після аудиту чи тесту.

Ці стандарти та перевірки слід вважати основою, на якій можна будувати. Найкраще інтегрувати надійну стратегію, яка поєднує в собі дотримання провідних стандартів кібербезпеки, постійне тестування на проникнення (принаймні раз на квартал) і культуру проактивного аналізу загроз і управління ними». ***(Joe Cortese. How Cybersecurity Best Practices are Evolving to Manage Ongoing Threats // ISACA (https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/how-cybersecurity-best-practices-are-evolving-to-manage-ongoing-threats). 16.10.2023).***

***

«…Незважаючи на зростання кількості атак, дані CNBC і SurveyMonkey показують, що дивовижна кількість власників малого бізнесу не турбується; лише 4% назвали кібербезпеку найбільшим ризиком, з яким стикається їхній бізнес, у той час як дві третини компаній (64%) вважають, що вони можуть швидко усунути кібератаку.

Коли компанії стикаються з кібератакою, вже занадто пізно знати, чи зможуть вони швидко її вирішити. Боротьба із загрозою вимагає від компаній спочатку розуміння своїх уразливих місць.

Дані Агентства з кібербезпеки та безпеки інфраструктури (CISA) показують, що більшість (понад 90%) кібератак починаються з фішингових атак». Verizon У «Звіті про розслідування витоку даних за 2022 рік показали, що 74% витоків даних були спричинені людським фактором, підкреслюючи критичну потребу в підвищенні обізнаності та освіти з кібербезпеки.

Маркетологи мають найкращі позиції в організації, щоб підтримувати кібербезпеку, оскільки ми вже працюємо з кожним відділом і знаємо, як передавати повідомлення, які повинні почути наші команди.

Як і маркетинг, безпека потребує плану.

Оскільки кібератаки стають все більш поширеними, організації повинні готуватися до найгіршого.

Звичайно, найкращі галузеві практики, такі як протоколи багатофакторної автентифікації, відіграють важливу роль у підтримці безпеки організації. Однак компаніям важливо спочатку визначити свої слабкі місця та сліпі плями.

Оцінка прогалин у кібербезпеці може допомогти компаніям оцінити свій підхід до безпеки, порівнюючи його з найкращими практиками та галузевими стандартами.

Ця оцінка зосереджена на стратегіях безпеки та операційній безпеці, визначенні областей, дуже вразливих до інцидентів і порушень — підхід, який працює для організацій будь-якого розміру. Оцінка містить рекомендації, які допоможуть організаціям зменшити ризики безпеки, одночасно оптимізуючи вплив свого бюджету безпеки.

Забезпечення базового навчання кібербезпеки для працівників є життєво важливим, щоб запобігти тому, щоб вони стали жертвами тактики зловмисників і зупинити шкідливі кіберзагрози від поширення в мережі. Навчання з питань безпеки — це потужний інструмент, який дозволяє співробітникам брати активну участь у розробці рішення.

Однак навчання з питань безпеки не буде успішним, якщо розглядати його як формальність, яку потрібно встановити. Ефективна безпека має включати постійні курси підвищення кваліфікації та симуляції реального життя, наприклад симуляції фішингу.

Зробіть співробітників частиною процесу.

Хоча людський фактор є одним із найважливіших факторів у спричиненні кіберінцидентів, він також є одним із основних інструментів організації в її боротьбі. Компанії повинні надавати співробітникам повноваження, щоб підтримувати безпеку організації.

Такий інструмент, як виявлення вхідних повідомлень і реагування на них, дозволяє користувачам повідомляти про підозрілі електронні листи для автентифікації служби. Безпечні електронні листи повертаються користувачеві, тоді

як шкідливі електронні листи видаляються із сервера, гарантуючи безпеку користувача та всієї команди від електронної пошти.

Жодна організація не застрахована від зловмисників, які хочуть завдати шкоди, будь то малий бізнес, транснаціональна корпорація чи державна установа. Розмірковуючи над тим, як усвідомлення загроз — і доступна освіта з питань безпеки — розвивалися протягом десятиліть, ми повинні оцінити заходи, необхідні для забезпечення безпеки та безпеки взаємопов'язаного світу.

Саме там маркетологи допоможуть компаніям перетнути фінішну пряму. Кожен — чи майже кожен — знає, що загроза існує; вони повинні розуміти, що на них лежить обов'язок боротися з цим і ціною бездіяльності.

Незважаючи на те, що нові процеси та процедури безпеки можуть здатися обтяжливими, подумайте про вартість (і простої, спричинені) інцидентом безпеки. Крім того, враховуйте репутаційні витрати такої події, крім грошових витрат.

Це показник, який кожен у компанії може зрозуміти та підтримувати 12 місяців на рік, а не лише раз на рік. Чи є ваша маркетингова організація лідером у передачі важливих повідомлень для забезпечення безпеки вашого бізнесу?» ***(Lauren Wickstead. Marketers Must Make Cybersecurity A Priority Every Day // Forbes (https://www.forbes.com/sites/forbescommunicationscouncil/2023/10/17/marketers-must-make-cybersecurity-a-priority-every-day/?sh=5e6f751f6fe3). 17.10.2023).***

***

«Нове дослідження Juniper Research, провідного експерта з технологічних ринків, виявило, що протягом наступних п'яти років кількість промислових кінцевих точок із захистом кібербезпеки зросте на 107%.

Дослідження виявило зростання взаємопов'язаних процесів у рамках революції «Індустрія 4.0» як дедалі більше наражаючи критичну промислову інфраструктуру на зовнішні загрози; вимагаючи повноцінних змін у тому, як промислові зацікавлені сторони захищають свою діяльність.

Juniper Research визначає промислову кінцеву точку як будь-який фізичний або віртуальний пристрій, підключений до мережі для надсилання та отримання інформації в промислових умовах…

Зростаючі загрози прискорюють витрати на безпеку промислових кінцевих точок

Дослідження показало, що витрати на кібербезпеку промислових кінцевих точок досягнуть 7,8 мільярдів доларів США до 2028 року; зросла з 3,8 мільярда доларів США у 2023 році. Це швидке зростання на 105% демонструє, наскільки швидко розвивається ринок і як кібербезпека промислових кінцевих точок швидко стає пріоритетом для постачальників засобів кібербезпеки.

Співавтор дослідження Нік Мейнард прокоментував: «Чим більше процесів стає доступним для підключення, загрозливе середовище в промислових умовах експоненціально зростає. Постачальники кібербезпеки повинні співпрацювати з ключовими промисловими постачальниками Інтернету речей, щоб краще захистити цю проблемну сферу».

Чи промислові постачальники достатньо готові до нових загроз?

Згідно з прогнозами дослідження, до 2028 року 21% промислових кінцевих точок будуть захищені службами кібербезпеки кінцевих точок, це, зрештою, дуже низька частка від загальної кількості промислових кінцевих точок. Таким чином, промислові зацікавлені сторони повинні діяти набагато швидше, щоб забезпечити свою критично важливу діяльність, інакше вони зіткнуться зі спіральними загрозами з боку нечесних акторів. Підвищення видимості в промисловому ланцюжку поставок і оптимізація хмарної безпеки для критично важливих операцій будуть життєво важливими для забезпечення вищого рівня захисту». ***(Endpoint Cybersecurity Systems to Secure 210 Million Industrial Endpoints by 2028; Driven By Critical Infrastructure Threats // BDC Magazine (https://bdcmagazine.com/2023/10/endpoint-cybersecurity-systems-to-secure-210-million-industrial-endpoints-by-2028-driven-by-critical-infrastructure-threats/). 17.10.2023).***

***

«Сумна реальність кібербезпеки полягає в тому, що зловмисники часто майже такі ж розумні, як і доброзичливі, що призводить до постійної гри в кішки-мишки. Фахівці з кібербезпеки часто знаходяться на менш вигідній стороні паркану, а також змушені реагувати на нові загрози, наприклад, коли розробляється нове шкідливе програмне забезпечення.

Крім того, групи кіберзлочинців намагатимуться заблокувати дослідникам і професіоналам розуміння зловмисного програмного забезпечення чи будь-яких інших атак. Вони можуть використовувати ту саму стратегію, що й багато інших веб-сайтів – блокувати IP-адреси, які вважають підозрілими.

З цих та багатьох інших причин проксі-сервери стали однією з основ для всіх процесів кібербезпеки. Хоча вони відіграють лише допоміжну роль, тобто дозволяють дослідникам безперешкодно виконувати свої завдання, виконання тих самих завдань без довірених осіб було б або набагато дорожчим, або зовсім неможливим.

Численні випадки використання в одному продукті

Оскільки проксі-сервери є відносно простою технологією, яка забезпечує доступ до безлічі IP-адрес із різних джерел і маршрутизує трафік, коли це необхідно, на перший погляд може здатися, що використання таких продуктів може бути досить обмеженим. Проте більшість атак пов’язані з мережею, тому все, що може змінити певний її аспект, уже є корисним.

Фішингові атаки, наприклад, здебільшого відбуваються у формі веб-сайтів-імітаторів, які маскуються під законні установи, від банківських банків до електронної комерції магазинів. Ці веб-сайти будуть доставлені через електронну пошту, SMS або інші служби обміну повідомленнями. Компанії найчастіше піддаються атакам через фішинг електронної пошти, оскільки ці повідомлення легше виглядати як законні повідомлення.

Проксі-сервери використовуються у спеціальному внутрішньому програмному забезпеченні, як правило, у формі скребків, які можуть автоматично сканувати вкладення та переходити за посиланнями, які надсилаються електронною поштою, перевіряючи легітимність. Оскільки IP-адреси, отримані від проксі-

серверів, будуть нешкідливими, будь-яке блокування чи фальсифікація вмісту не буде активовано.

Іншим поширеним застосуванням, яке зазвичай розгортається як незалежна бізнес-модель, є захист бренду або боротьба з підробкою. Багато товарів продається на місцевих ринках або веб-сайтах із геообмеженим доступом, зазвичай недоступним для тих, хто живе в цій конкретній частині світу. Завдяки достатньо широкому діапазону IP-адрес можна відвідати будь-який заборонений веб-сайт.

Потім ці компанії зазвичай шукають нелегітимних продавців фірмових продуктів, створених без отримання прав на виробництво, іншими словами, підробок. Оскільки підробки є набагато більш поширеними, ніж вважає більшість людей, і становлять до 3,3% світової торгівлі, таке використання проксі-серверів захищає як споживачів, так і підприємства від нелегітимної продукції.

Ідучи на крок далі

Хоча дослідники кібербезпеки інколи можуть залишатися на задньому плані, коли мова йде про зловмисників, час на реакцію, коли щось з'являється, значно скоротився. Основною частиною такого вдосконалення є технології веб-збирання, які, у свою чергу, покладаються на проксі-сервери.

Веб-збирання може збирати інформацію про загрози як з чистої, так і з темної мережі, дозволяючи фахівцям із кібербезпеки відстежувати будь-які нові випадки зловмисної діяльності. Одним із найпоширеніших випадків використання, який багато хто з нас помітив, є виявлення витоку даних.

Компанії, що займаються кібербезпекою, можуть сканувати Інтернет на наявність дампів даних із витоків компанії, які включають електронні листи, паролі та, можливо, численні інші інформаційні точки. Потім вони можуть створювати бази даних (або порівнювати зі своїми власними) для інформування користувачів, які постраждали від витоку.

Крім того, веб-збирання можна використовувати для пошуку новостворених веб-сайтів і перевірки того, що вони не використовуються для цілей фішингу. Порівнювати вміст нещодавно виявленого та законного веб-сайту відносно просто, тому рішення для сканування веб-сайтів можуть допомогти компаніям із

кібербезпеки та фінансовим чи державним установам відстежувати будь-які спроби фішингу.

Нарешті, інші методи моніторингу стають доступними через веб-збирання. Можна відстежувати обговорення розробки шкідливих програм, розкриття вразливостей та багато інших загальнодоступних дій, пов’язаних із кібербезпекою.

Однак слід зазначити, що веб-збирання не без недоліків. У всьому світі діють різні закони про захист даних, які можуть впливати на застосовність таких рішень. Наприклад, GDPR є звичайним підводним каменем, оскільки будь-які персональні дані не можна очищати. Приватні дані, як-от щось, що знаходиться за екраном входу, також виходять за рамки веб-збирання.

Поєднання сканування зі штучним інтелектом

Ще одним надзвичайно перспективним напрямком для проксі та веб-скрейпінгу є розвиток штучного інтелекту. Здебільшого багато сучасних реалізацій штучного інтелекту базуються на машинному навчанні, технології, яка потребує надзвичайно великих даних. Веб-скопіювання вирішує проблему даних, надаючи доступ майже до всієї загальнодоступної інформації в Інтернеті.

Машинне навчання вже використовувалося різними компаніями, такими як Microsoft. Їх Microsoft Defender успішно запобігає великим атакам, автоматично виявляючи нове шкідливе програмне забезпечення.

Виявлення аномалій, на якому, ймовірно, базувався успіх Microsoft, є одним із найуспішніших застосувань для машинного навчання, оскільки воно легко піддається цій технології. Моделі відстежують мережеву активність і сповіщають експертів з кібербезпеки щоразу, коли трапляється щось незвичайне, які потім можуть вжити заходів, якщо це необхідно.

Однак машинне навчання не обмежується виявленням аномалій. Вищезгаданий варіант використання скрапінгу для веб-скрейпінгу можна покращити за допомогою машинного навчання. Веб-сайти зазвичай мають певний набір критеріїв, як-от глибина URL-адреси, вік домену, ключові слова та багато інших, які можна використовувати для перевірки легітимності. Ці фактори можна

включити в моделі машинного навчання, щоб автоматично визначати, чи був веб-сайт створений з метою фішингу.

Висновок

Кібербезпеку стає важко уявити без використання проксі-серверів і веб-збирання. Ці рішення створюють багато варіантів використання, які дозволяють дослідникам стати більш проактивними у своїй ролі, водночас скорочуючи їхній час на реакцію, коли щось трапляється. І проксі-сервери, і веб-скрейпінг служать основою для багатьох поточних досягнень у сфері кібербезпеки, і, ймовірно, вони й надалі залишатимуться фундаментальними для подальших розробок у цій галузі». ***(Vaidotas Šedys. Enabling cybersecurity businesses through proxies // Future US, Inc. (https://www.techradar.com/pro/enabling-cybersecurity-businesses-through-proxies). 06.10.2023).***

***

«Щоб захистити вашу мережу та програми від хакерів, надійна програма кібербезпеки зосереджується на управлінні доступом і авторизації. Це правда, що лише ті, кому потрібен доступ, повинні мати його, але з точки зору корпоративних платформ, це всі. Це ілюструє парадокс кібербезпеки, коли ви повинні збалансувати потребу зберігати дані в безпеці та гарантувати, що вони придатні для використання та доступні.

Це може спричинити великі суперечки в організаціях між IT та бізнесом. Отже, як кіберлідери можуть зменшити це та підтримувати комфортну рівновагу?

Безпека не повинна перешкоджати доступності та зручності використання

Багато дезінформації може ширитися про те, що безпека є перешкодою для доступності та зручності використання. Ваші користувачі можуть представити вашу технічну групу складною. Ви повинні повідомити, що внутрішньої боротьби немає.

Безпека є відповідальністю кожного працівника, і коли вони розуміють і приймають це, вони можуть змінити своє сприйняття IT як поганого хлопця. Надання їм певної власності на ситуацію може розвіяти передбачуваний конфлікт.

Доступність насправді є принципом кібербезпеки. Мета полягає в тому, щоб розробити програму, яка враховує найкращі практики та міцну позицію захисту, а також задовольняє потреби ваших користувачів.

В останні роки доступність стала охоплювати місце роботи людей. Тенденція віддаленої роботи не згасає, і багато компаній прийняли її, щоб запропонувати гнучкість і розширити свій резерв талантів. Поспіх переходити на дистанційне керування не завжди враховував кібербезпеку, тому відтоді відбулося певне «очищення».

У цьому парадоксі кібербезпеки ви повинні забезпечити безпеку та розвиток бізнесу.

Поєднання безпеки з доступністю та зручністю використання

Можливо, ви вже маєте багато елементів керування, щоб збалансувати безпеку та доступність. До них належать освітні програми з кібербезпеки, політики надійних паролів, використання двофакторної автентифікації, забезпечення постійного оновлення програмного забезпечення та резервне копіювання даних.

Це мінімальні вимоги для вирішення парадоксу. Є більш просунуті технічні засоби контролю, які можна встановити, які підпадають під керування доступом до ідентифікаційної інформації (IAM). IAM має підтримувати безпеку та продуктивність співробітників. Він передбачає як автентифікацію, так і авторизацію для доступу до програм і даних.

Одним із нових аспектів цього є перехід до політики нульової довіри. Це стратегія, яка усуває неявну довіру та замінює її постійною перевіркою. Він дотримується принципу «ніколи не довіряй, завжди перевіряй». Його використання включатиме видимість і контроль над усім трафіком і користувачами вашого середовища, зокрема:

• Що зашифровано.

• Моніторинг і перевірка трафіку.

• Використання багатофакторної автентифікації крім паролів.

Це може покращити ваш захист безпеки, але не повинно перешкоджати доступу та зручності використання. Це допомагає зменшити ризик, усуваючи поверхню атаки для кіберзлочинців.

Однак у розв’язанні парадоксу кібербезпеки беруть участь не лише технічні стратегії.

Прозорість щодо заходів кібербезпеки зменшує напругу між безпекою та доступністю

Ваші користувачі повинні мати можливість виконувати свою роботу, а це означає, що їм потрібні технології та їм не потрібно стрибати через обручі. Дотримання протоколів безпеки завжди буде важливим, і люди дотримуватимуться їх і цінуватимуть, якщо ви будете прозорі та будете спілкуватися послідовно.

Більшість співробітників можуть сприймати кібербезпеку як щось, що їх не стосується, але ми знаємо, що більшість порушень та інцидентів безпеки є результатом людської помилки. Отже, зв’язок вірний і точний.

Щоб донести це повідомлення, уся ваша кібер-команда разом з вами на чолі має зосередитися на чіткій та привабливій комунікації з усіма користувачами. Хоча технічні фахівці часто стикаються з цим, не неможливо зробити це основою вашої стратегії кібербезпеки.

Це починається з вас як прикладу та того, як ви обговорюєте та ділитеся інформацією про кібербезпеку з керівництвом. Це просочується до всіх відділів і співробітників. Усі ці люди регулярно спілкуються з технічним персоналом. Замість того, щоб інші боялися цього та називали вашу команду складною, вони можуть посилити повідомлення про важливість кібербезпеки.

Якщо ви зможете переконати всіх у тому, що питання безпеки та доступності є друзями, а не ворогами, це значно допоможе зробити вашу організацію кіберстійкішою. Це вимагає зосередитися на тому, щоб бути хорошими комунікаторами та співробітниками, що залежить від того, чи ваші люди мають відкрите мислення та усвідомлюють свою поведінку та дії.

Те, що ви створюєте, — це культура, орієнтована на безпеку, не лише в технічних групах, а й у всій компанії. Це найкращий спосіб прямого вирішення

проблеми кібербезпеки. Знайти цей баланс складно і може вимагати багатьох поворотів на цьому шляху, але це варте часу та інвестицій, щоб досягти цього правильного для теперішнього та майбутнього». ***(Christian Espinosa. The Cybersecurity Paradox: Keeping Data Both Secure And Accessible // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/10/10/the-cybersecurity-paradox-keeping-data-both-secure-and-accessible/?sh=2b28d4977055). 10.10.2023).***

***

«Другий рік поспіль глобальна нестача працівників кібербезпеки зменшилася, але ще не час святкувати, а тим більше розслаблятися.

Про зниження з 3,12 мільйона до 2,72 мільйона незаповнених вакансій у жовтні повідомила (ISC)², найбільша у світі некомерційна асоціація сертифікованих фахівців з кібербезпеки, у своєму щорічному дослідженні Cybersecurity Workforce Study.

Однак дослідження показує, що дефіцит кадрів у сфері кібербезпеки збільшився в усіх регіонах світу, крім Азіатсько-Тихоокеанського регіону. Навіть незважаючи на це, дефіцит робочої сили в Азіатсько-Тихоокеанському регіоні все ще становив 1,42 мільйона, що є найбільшим серед усіх регіонів світу.

Дані свідчать про те, що повільніше, ніж очікувалося, економічне відновлення після пандемії в Азіатсько-Тихоокеанському регіоні та вплив COVID-19 на малий бізнес і критично важливі сектори, такі як IT-послуги — головний роботодавець у сфері кібербезпеки в регіоні — сприяють відносній м’якості Попит на фахівців з кібербезпеки там порівняно з Північною Америкою, Європою та Латинською Америкою, йдеться у звіті.

Дослідження оцінило, що в світі налічується 4,19 мільйона працівників кібербезпеки на основі опитувань і низки вторинних джерел. З року в рік кількість працівників зросла на 700 тис.

«Будь-яке збільшення глобальної пропозиції фахівців з кібербезпеки є обнадійливим, але давайте будемо реалістами щодо того, що нам все ще потрібно, і щодо терміновості поставленого перед нами завдання», — сказав у заяві генеральний

директор (ISC)² Клар. Россо «Дослідження показує нам, де найбільше потрібні таланти, і що традиційної практики найму недостатньо», — продовжила вона. «Ми повинні ставити людей вище технологій, інвестувати в їхній розвиток і сприймати віддалену роботу як можливість.

«І, мабуть, найголовніше», — додала вона. «Організації повинні прийняти суттєві практики різноманітності, справедливості та інклюзивності, щоб відповідати очікуванням працівників і ліквідувати розрив».

Дефіцит може призвести до більших проблем

Дефіцит може бути пов'язаний із підвищеним ризиком для компаній. «В результаті неповного укомплектування персоналом системи неправильно налаштовані», — сказав Россо з (ISC)² в інтерв'ю.

«Не вистачає часу для належної оцінки та управління ризиками. Організації повільно виправляють критичні системи. Нагляд за процесами та процедурами знаходиться на нижчому рівні, ніж це повинно бути. Вони не в змозі контролювати та знаходити загрози для організації.

«Що цікаво в цих елементах, — продовжила вона, — це те, що вони безпосередньо пов'язані з повідомленими причинами, чому організації мають витоки даних або піддаються атакам програм-вимагачів».

Задоволеність від роботи все ще висока

Всупереч деяким повідомленням у засобах масової інформації та досвіду рекрутерів у окопах, (ISC)² стверджував, що працівники кібербезпеки в основному дуже зацікавлені та задоволені своєю роботою.

Кібербезпека — це все, що завгодно, але не передбачуване, і цей динамізм і виклики, які вона створює, можуть бути причиною того, чому багато успішних фахівців у сфері кібербезпеки переважно повідомляють про задоволення від своєї роботи.

Насправді, додається у звіті, ті, хто зараз займає посади в сфері кібербезпеки, постійно висловлювали дуже високий рівень задоволеності роботою протягом останніх чотирьох років, і вони повідомили про різко вищу задоволеність протягом останніх двох років.

У 2021 році це включає найвищі показники задоволеності, які будь-коли повідомляли: 77% респондентів повідомили, що вони задоволені або надзвичайно задоволені своєю роботою, що значно вище, ніж 66%, які повідомили про такий рівень задоволеності у 2019 році.

Однак ці довгострокові цифри задоволеності роботою можуть не відображати того, що відбувається найближчим часом.

Робота вдома – головний фактор

«За останні 90 днів кількість людей, які перейшли на роботу в сферу кібербезпеки, у п’ять разів вища, ніж ми коли-небудь спостерігали протягом будь-якого 90-денного періоду», — сказала Дейдре Даймонд, засновник і генеральний директор CyberSN, кадрової фірми з кібербезпеки.

«За останні 90 днів тривали масові звільнення», - сказала вона. «Компанії почали ламати голову над тим, чи збираються вони залишатися віддаленими, навіть якщо їм сказали, що ніхто не хоче повертатися в офіс. Щойно компанії почали дивуватися, люди почали йти».

Ці настрої також знайшли відображення у звіті (ISC)², який виявив, що лише 15% глобальної робочої сили з кібербезпеки мали бажання повернутися в офіс на повний робочий день.

«Можливість бути в офісі [лише] пару днів на тиждень може бути дуже привабливою для команд служби безпеки», — сказав Джеймс МакКвігган, прихильник питань безпеки в KnowBe4, організаторі навчання. «Вони цінують можливість працювати вдома або в офісі», – додав він.

З іншого боку, збільшення кількості віддалених працівників також має негативну сторону для спеціалістів із безпеки. «Півтора роки віддаленої та гібридної роботи перетворилися на розширену поверхню атаки — все більше працівників використовують слабкі методи безпеки як у робочих, так і в домашніх мережах», — пояснив Нік Колаковскі, старший редактор Dice Insights, інформаційного агентства з питань зайнятості в галузі технологій. інформаційний сайт.

Ситуацію погіршила раптовість змін, додав Джош Дрю, регіональний директор Robert Half Technology у Бостоні. «Трансформація відбулася раптово, через

що фахівцям з кібербезпеки було надзвичайно важко впоратися з пропускною здатністю», — сказав він.

Пандемія викликає вигорання

За даними CyberSN, пандемія, схоже, сприяє збільшенню кількості звільнень у сфері кібербезпеки. З початку пандемії кількість звільнень зросла на 20% на східному узбережжі США та на 18% на західному.

Ці відставки, здається, частково пов'язані з пандемією, свідчить порівняння результатів опитувань, проведених CyberSN до пандемії та зараз.

До пандемії на Східному узбережжі основною причиною, через яку фахівці з безпеки залишали роботу, була відсутність можливостей для зростання (30%), за якою йшли низькі зарплати (30%), низька культура (25%) і відсутність навчання (15%).

Зараз, після більш ніж 20 місяців пандемії, брак можливостей для зростання залишається на першому місці (40%), але з'явилися дві нові проблеми: бажання працювати лише віддалено (30%), а також виснаження та перевантаження роботою (20%). Низька культура впала до 10%.

Опитування робітників Західного узбережжя дали подібні результати. До пандемії відсутність можливостей для зростання була основним фактором для звільнення з посади (40%), за нею йшли низька культура (25%), відсутність навчання (20%) і низька зарплата (15%).

Зараз основною причиною звільнення є виснаження (30%), за нею йдуть віддалена робота повний робочий день (20%), відсутність можливостей для зростання (20%), низька культура (20%) і проблеми з придбанням (10%).

«Вигорання раніше було другорядною причиною звільнення з роботи», — сказав Даймонд із CyberSN. «Тепер це головна причина. Люди хочуть піти туди, де організація знає, як забезпечити безпеку в масштабі».

«Це було досить погано, коли одній людині доводилося виконувати дві роботи», — додала вона. «Тепер їх просять виконати чотири роботи».

Закриття розриву

Проте інтерес до вакансій у сфері кібербезпеки залишається високим. За даними онлайн-дошки вакансій Indeed, вакансії у сфері кібербезпеки та інтерес до них зросли з жовтня 2020 року по жовтень 2021 року. Протягом цього періоду кількість оголошень про вакансії, пов'язаних з кібербезпекою, на платформі зросла на 14%, зазначається в інформації, наданій TechBeacon, а пошуки за запитом кібербезпека- суміжні ролі підскочили на 16%.

Дрю Роберта Халфа додав, що з місцевої точки зору все ще бракує кваліфікованих кандидатів у сфері кібербезпеки. «Зараз у США рівень безробіття для аналітиків інформаційної безпеки становить 0,8%», — сказав він. «Якщо пояснити це, рівень безробіття в країні становить 4,8%».

Дрю визначив три методи, які компанії використовують для усунення нестачі робочої сили в сфері кібербезпеки:

Збільшення рівня навчання, що пропонується існуючим працівникам

Просування кар'єрних шляхів, щоб дати існуючим працівникам можливість підвищити рівень своїх навичок і відповідальності, включаючи навчання кандидатів початкового рівня

Використання третіх сторін для заповнення кадрових прогалин

Завдання початкового рівня

За словами Даймонда, прийом кандидатів початкового рівня продовжує залишатися проблемою для галузі. «Я бачу, що люди початкового рівня у великій кількості намагаються потрапити», — сказала вона. «Це займає шість місяців, рік, і їм доводиться влаштовуватися на іншу роботу, поки вони товчуть тротуар».

(ISC)², зі свого боку, намагається вирішити проблему початкового рівня. «Ми розробляємо сертифікацію початкового рівня, призначену для осіб, які не мають досвіду в IT або кібербезпеці», — пояснив Россо.

За її словами, це стане кроком до сертифікації CISSP і буде запущено на початку 2022 року. Сертифікація CISSP призначена для підтвердження досвіду роботи в сфері інформаційної безпеки та практичних знань принципів і практик безпеки.

«Роботодавці з великим ентузіазмом сприйняли сертифікацію початкового рівня», — зазначив Россо. «Вони кажуть, що їм це потрібно, і раді, що це відбувається».

Необхідний певний досвід

Чи працюватиме універсальна сертифікація для новачків у сфері кібербезпеки, ще невідомо.

«Кібербезпека охоплює величезну підмножину окремих ролей, які можуть вимагати абсолютно різних навичок», — пояснив Кріс Клементс, віце-президент із архітектури рішень у Cerberus Sentinel, компанії з консалтингу з кібербезпеки та тестування на проникнення.

«Хоча існують певні основи кібербезпеки, які зазвичай застосовуються в різних дисциплінах, для того, щоб бути дійсно ефективним, потрібен досвід і знання в певній галузі», – додав він.

«Ще одна сфера, яку часто ігнорують під час обговорення кібербезпеки, полягає в тому, що вона також вимагає міцної загальної бази знань у сфері IT», — додав він. «Людина, яка не вміє адмініструвати системи Windows, швидше за все, буде дуже обмежена в своїх можливостях ефективно захистити її або атакувати».

Шлях вперед

Загалом, цьогорічний звіт (ISC)² про робочу силу в галузі кібербезпеки є показовим у багатьох аспектах. Наприклад, збільшення робочої сили на 700 000 людей у розпал всесвітньої пандемії вражає.

Було також виявлено, що розрив талантів продовжує збільшуватися в усіх регіонах, крім Азіатсько-Тихоокеанського регіону.

«На щастя, цьогорічні учасники дослідження окреслили курс вперед», — йдеться у звіті. «Співробітники з кібербезпеки — ті самі люди, які на передовій захищають наші критично важливі активи по всьому світу — говорять нам, де найбільше потрібні таланти; що старі звички під час найму на роботу потрібно змінити; що витрати на технології самі по собі не вирішать наших проблем; віддалена робота — це більше можливостей, ніж загроза; і що вони очікують від своїх роботодавців значущих ініціатив щодо різноманітності, справедливості та

залучення (DEI).» ***(John P. Mello Jr. 700K more cybersecurity workers, but still a talent shortage // Open Text Corporation (https://techbeacon.com/security/700k-more-cybersecurity-workers-still-talent-shortage). 10.2023).***

***

«На динамічному перетині штучного інтелекту та цифрової безпеки відбувається захоплюючий бум у сфері акцій кібербезпеки. Зростаюча загроза резонансних кіберзломів, що підживлюється витонченістю генеративного штучного інтелекту, викликала безпрецедентний інтерес як з боку інвесторів, так і приватних інвестиційних компаній. Цей сплеск стався в той час, коли потреба в надійних заходах кібербезпеки є більш критичною, ніж будь-коли, що робить акції кібербезпеки спокусливою перспективою для тих, хто прагне осідлати хвилю цифрового майбутнього.

Акції кібербезпеки зростають на фоні хвилі розвитку загроз ШІ

У цифровій сфері, що постійно розширюється, нещодавні кібератаки проти гігантів галузі, таких як MGM Resorts і Caesars Entertainment, підкреслюють невід'ємні ризики, пов'язані з генеративним ШІ. Терміновість вирішення цих проблем відображається в прогнозі Gartner про значне зростання корпоративних витрат на кібербезпеку на 14%, яке, як очікується, досягне приголомшливих 215 мільярдів доларів США до 2024 року. Зокрема, область продуктів і послуг хмарної безпеки готова до надзвичайного зростання, з очікуване зростання на 25%, передбачаючи ринкову вартість, яка наближається до 7 мільярдів доларів.

У той час як розвиток генеративного штучного інтелекту віщує нову еру інновацій, він водночас виявляє вразливі місця, які вимагають надійних заходів кібербезпеки. Зіткнувшись із цією загрозою, що постійно змінюється, компанії інтенсифікують свої інвестиції, щоб зміцнити захист своїх цифрових активів. Цей підвищений попит підштовхнув акції кібербезпеки до сильних позицій, надаючи інвесторам багатообіцяючу можливість отримати вигоду від конвергенції ШІ та цифрової безпеки.

Найпопулярніші акції кібербезпеки та наступна хвиля стартапів

У цьому захоплюючому ландшафті деякі акції кібербезпеки стали помітними у 2023 році. Palo Alto Networks лідирує в рейтингу з вражаючим зростанням акцій PANW на 86%, за якою слідує сплеск акцій CRWD на 76% і помітне зростання акцій Zscaler на 50%. Прогнози показують, що як фірми з кібербезпеки, так і зловмисники використовуватимуть генеративні інструменти штучного інтелекту, сприяючи подальшому розширенню частки кібербезпеки.

Конкурентне середовище на ринку сприяє інноваціям серед компаній з кібербезпеки, спонукаючи їх до розробки передових технологій для більш ефективної боротьби з кіберзагрозами. Попит на передові рішення безпеки є рушієм цієї інновації, гарантуючи, що галузь залишається на передньому краї поточної боротьби з кіберзагрозами.

У той час як такі хмарні гіганти, як Microsoft, домінують, когорта стартапів створює хвилю в секторі кібербезпеки. Такі компанії, як Netskope, Wiz, Snyk, Illumio, Venafi, Recorded Future, Noname Security, Obsidian Security, Deep Instinct і Skyflow, залучають значні інвестиції від венчурних капіталістів і великих підприємств. Ця зміна сигналізує про те, що в галузі змінюється хвиля, коли організації визнають цінність передових рішень для зміцнення своєї безпеки проти нових загроз.

Зіткнувшись із цією новою хвилею конкуренції, провідні компанії індустрії збільшують свої інвестиції в дослідження та розробки. Зосередження на інноваціях стає першочерговим, оскільки вони прагнуть створювати продукти та послуги, які зберігають конкурентоспроможність у ринковому ландшафті, що розвивається. Цей стратегічний зсув є життєво важливим для виживання та відкриває можливості для зростання та розширення на арені кібербезпеки, що постійно розвивається.

Прямий капітал і уряд сприяють буму кібербезпеки

Компанії приватного капіталу досягають значних успіхів у секторі кібербезпеки, використовуючи зростаючий попит на рішення цифрового захисту. Відомі придбання, в тому числі придбання Томою Браво ForgeRock, Ping Identity Holdings, SailPoint Technology, Proofpoint, Sophos і Barracuda, демонструють підвищений інтерес та інвестиції в сферу кібербезпеки. Інші важливі кроки включають придбання Mimecast компанією Permira та придбання KnowBe4

компанією Vista Partners, що демонструє потужний апетит до інвестицій у кібербезпеку в рамках приватного капіталу.

Роль уряду в сприянні розширенню сектору кібербезпеки важко переоцінити. Очікуване зростання ініціатив федерального уряду з кібербезпеки має намір ще більше прискорити зростання компаній у сфері комп'ютерної безпеки. Потенційне збільшення проектів, що фінансуються урядом, не тільки обіцяє значне зростання доходів для сектору кібербезпеки, але й слугує каталізатором для інновацій і дослідження нових можливостей у галузі.

Оскільки сектор кібербезпеки продовжує розвиватися, зараз вдалий час для інвесторів розглянути можливість диверсифікації своїх портфелів за допомогою акцій кібербезпеки. Оскільки корпоративні витрати на кібербезпеку зростають, а нові стартапи кидають виклик відомим гравцям, галузь відкриває широкі можливості для інвестицій. Інвестори, які користуються моментом у цьому ландшафті, що швидко розвивається, стоять на передовій технологічної революції, активно формуючи майбутнє кібербезпеки». ***(Aamir Sheikh. Why Are Cybersecurity Stocks Surging, and What's Driving the Boom? // Cryptopolitan (https://www.cryptopolitan.com/cybersecurity-stocks-surging-whats-boom/?utm_source=flipboard&utm_content=thatsmystapler%2Fmagazine%2FMoney) . 20.10.2023).***

***

«Кібербезпека продовжує залишатися головним викликом для багатьох компаній і галузей промисловості, і будівельна галузь не є винятком. Крім того, деякі особливості будівельної галузі роблять бізнес більш сприйнятливим до кібератак. Наприклад, кількість повторних платежів протягом проекту, в якому бере участь багато торгових підрядників, поширене використання додатків для автоматичної обробки щомісячних платежів і широке використання планшетів на робочих майданчиках роблять галузь вразливою до інцидентів кібербезпеки.

Окрім програм-вимагачів та інших кіберзагроз, будівельна галузь найбільш вразлива до соціальної інженерії. Соціальна інженерія — це коли хакери видають

себе за когось, наприклад, за розробника або субпідрядника, щоб отримати доступ до ІТ-систем цільової організації. Оскільки розробники часто мають велику кількість рахунків-фактур, які регулярно оплачуються субпідрядникам, хакери отримують доступ через єдину точку входу. Багато людей бере участь у процесі оплати, що надає хакерам багато можливих способів проникнення в ІТ-систему.

Компанії будівельної галузі повинні серйозно ставитися до кібербезпеки. Хоча універсального підходу до найкращих практик кібербезпеки не існує, нижче ми ділимося п’ятьма ключовими міркуваннями для компаній у будівельній галузі.

5 питань кібербезпеки, на які варто звернути увагу підприємствам будівельної галузі

Потенційний вплив кібератаки на проект. Кібератаки не лише мають негайний фінансовий вплив; вони також можуть спричинити значні затримки будівельних проектів. Наприклад, якщо хакер отримує доступ до ІТ-системи одного субпідрядника, він може вимкнути всю комп’ютерну систему Проекту, викликаючи дорогі затримки в усьому Проекті, а не лише в одній торгівлі. Оцінюючи ризики кібербезпеки, не забудьте оцінити наслідки, пов’язані з проектом, разом із фінансовими ризиками.

Належне кібер- та кримінальне страхування. Залежно від типу шахрайства, претензії щодо збитків через порушення ІТ-системи або соціальну інженерію можуть підпадати під дію кількох політик. Сума страхування від кібер-шахрайства та кримінального шахрайства змінюватиметься залежно від таких факторів, як розмір вашого бізнесу, використання технологій та інших сторін, залучених до будівельного проекту. Наприклад, проекти з високими ставками, що фінансуються державою, потребуватимуть інших потреб у кіберстрахуванні, ніж субпідрядник, який виконує електромонтажні роботи під час будівництва житлових будинків. Поговоріть з досвідченими фахівцями з кібербезпеки та страхування, щоб краще оцінити відповідну суму страхування від кібербезпеки та кримінального страхування.

Договірні права на випадок кібератаки. Ситуації злому не тільки дорогі з точки зору часу та грошей, але й можуть призвести до суперечок щодо того, хто несе

відповідальність за шкоду. Наприклад, якщо хакер отримує доступ до IT-системи субпідрядника, а потім видає себе за координатора розрахунків субпідрядника, щоб відвести платежі від розробника, хто несе відповідальність: субпідрядник, оскільки його IT-система надала хакеру доступ, або розробник, оскільки він передав платежі обліковий запис хакера?

Супровідна документація в рамках ланцюжка поставок. Оскільки кібератаки можуть виглядати як стопка доміно, що падає, важливо переконатися, що інші компанії у вашому ланцюжку постачання також належним чином захищені від кіберризиків. Подумайте над тим, щоб запросити супровідну документацію від субпідрядників, постачальників та інших учасників ланцюга постачання щодо їхньої політики кібербезпеки, практики та страхування, щоб краще зменшити власні кіберризики.

Необхідне навчання з кібербезпеки. Навіть найнадійніших засобів безпеки, пов'язаних з IT, недостатньо для усунення людських помилок. Ваші співробітники мають належним чином і часто проходити навчання щодо ризиків кібербезпеки, протоколів безпеки та контролю за проектом. У міру того, як хакери стають кмітливішими, компанії повинні відповідним чином адаптувати та оновлювати свої навчальні заходи з кібербезпеки». ***(Suzanne Karbarz Rovner. Addressing Cybersecurity Risks in the Construction Industry: 5 Things Companies in the Construction Industry Should Consider // Levenfeld Pearlstein LLC (https://www.lplegal.com/content/cybersecurity-risks-construction-industry/). 25.10.2023).***

***

«У сучасному взаємопов'язаному бізнес-середовищі дані дають змогу зрозуміти бізнес, а технології є центральними для операцій і взаємодії з клієнтами. Хоча цифровізація бізнес-операцій і корпоративних даних може принести величезні переваги, вона також створює нові можливості для зловмисників. Заходи кібербезпеки допомагають захистити ваш бізнес від вразливостей, створених залежністю від електронних даних. Важливо бути

максимально активним у виявленні потенційних загроз і впровадженні заходів для мінімізації ризику кіберінциденту. Важливо, що ключові загрози для вашого бізнесу, ймовірно, знаходяться як зовні, так і всередині. Почнемо спочатку з двох ключових зовнішніх загроз.

програми-вимагачі

Програми-вимагачі включають зловмисників, які отримують доступ до ваших бізнес-даних або систем, шифрують їх і вимагають викуп. Якщо ви відмовляєтесь платити викуп, ці зловмисники зазвичай погрожують видалити чи опублікувати важливі бізнес-дані. Регулярне резервне копіювання даних на зовнішній жорсткий диск або хмарний сервер є одним із найпростіших способів захиститися від наслідків атаки програм-вимагачів. Однак, щоб запобігти атаці, ви повинні переконатися, що ваші системи мають належне програмне забезпечення для виявлення/моніторингу, щоб швидко ідентифікувати та зупинити несанкціонований доступ. Відповідно, ви також повинні регулярно оновлювати свої операційні системи, програмне забезпечення та програми за допомогою відповідного антивірусного програмного забезпечення та брандмауерів. Найкраще також сегментувати вашу мережу на менші мережі, які працюють окремо. Крім того, вам слід обмежити права доступу користувачів, щоб користувачі мали дозволи на доступ лише до тих даних, які їм потрібні для роботи. Обидва ці заходи мінімізують обсяг інформації, до якої може отримати доступ кіберзлочинець, якщо один обліковий запис або систему зламано.

Соціальна інженерія

Соціальна інженерія передбачає використання обману, щоб змусити людей надати конфіденційну особисту, фінансову чи ділову інформацію. Поширеним прикладом є поганий актор, який видає себе за людину, з якою ваш бізнес, ймовірно, має існуючі стосунки, переконуючи вашого співробітника надати вашу банківську інформацію або переказати гроші на шахрайський рахунок. Хоча брандмауери можуть мінімізувати кількість фішингових атак, регулярне навчання команди має вирішальне значення. Цей тренінг має не лише пояснити механізми шахрайства соціальної інженерії, а й забезпечити інтерактивне навчання розпізнаванню та реагування на такі спроби обману. Безперервне навчання протягом року створює

пильну команду, здатну запобігти складним шахрайствам. Ви також повинні відстежувати прогрес ваших команд, використовуючи їх ефективність для спрямування майбутнього навчання.

Незважаючи на те, що програми-вимагачі та соціальна інженерія становлять значні зовнішні загрози для вашого бізнесу, ви також повинні знати, що внутрішні загрози можуть завдати стільки, а іноді й більше, шкоди. Давайте розглянемо кілька важливих внутрішніх загроз.

Системна інтеграція підприємства

Ймовірно, ваш бізнес включає в себе кілька систем, які збирають і аналізують дані. Іноді ці системи повністю контролюються вашим бізнесом, але частіше підприємства покладаються на сторонні технології та платформи для розрахунку заробітної плати, розробки нових продуктів і дослідження ринку. Використання сторонніх постачальників іноді може призвести до того, що компанії «втратять інформацію», які постачальники мають доступ до яких даних і до яких внутрішніх систем. Якщо ваші корпоративні дані невпорядковані, це може ускладнити виявлення вразливостей і несанкціонованого доступу. У зв’язку з цим технології сторонніх розробників, покращуючи обслуговування та роботу, створюють потенційні загрози, оскільки ваша безпека залежить від заходів кібербезпеки цієї третьої сторони. Вам потрібно ретельно перевірити постачальників і співпрацювати з ними, щоб забезпечити підзвітність, але ваша команда також повинна зміцнити ваші внутрішні системи відповідно до найкращих галузевих практик.

Внутрішні загрози

Нарешті, внутрішні загрози є однією з найчастіших причин кіберінцидентів. Ці інциденти можуть виникнути з різних джерел, наприклад, незадоволений співробітник, колишній колега або навіть невинна помилка. Ви можете мінімізувати ризик внутрішніх загроз за допомогою кількох простих заходів. По-перше, розробіть і запровадьте ретельний процес реєстрації та виключення, приділяючи особливу увагу швидкому виключенню доступу та відновленню даних, якими володіє особа, яка проходить через виключення. Відповідно, ви повинні переконатися, що

користувачі мають доступ лише до даних і систем, необхідних для завершення їх роботи під час адаптації.

Це лише кілька ключових загроз, з якими може зіткнутися ваш бізнес. Проактивний і комплексний підхід до кібербезпеки — від усунення ризику соціальної інженерії до внутрішніх загроз — має вирішальне значення для захисту вашої організації. Зберігаючи пильність і стратегію, ваш бізнес може не тільки захистити себе, але й зберегти довіру клієнтів і ділових контактів». ***(Sarah M.D. Luth. Four Key Cybersecurity Threats To Your Business // McKee Voorhees & Sease PLC (https://www.filewrapper.com/four-key-cybersecurity-threats-to-your-business/). 25.10.2023).***

***

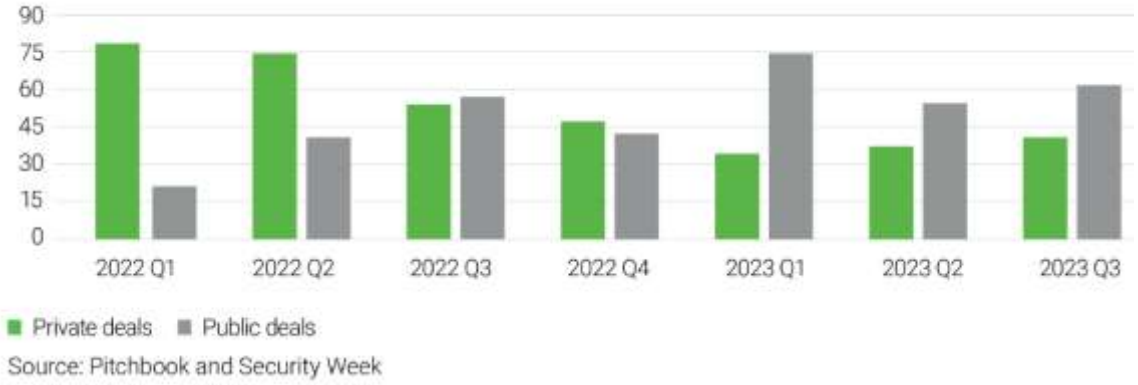
«Прогнозується, що протягом наступних 3 років CAGR (сукупний середньорічний темп зростання) у секторі кібербезпеки досягне 10% через зростання обсягу та складності кіберзагроз. Оскільки технології безпеки з’являються швидкими темпами, між провідними компаніями точиться гонка за придбання спеціалізованого досвіду, щоб справлятися із загрозами, що постійно змінюються, і залишатися конкурентоспроможними. Ця технологічна конвергенція створила високий попит на M&A (злиття та поглинання) як стратегічний шлях для інновацій у просторі кібербезпеки. Історично угоди з кібербезпеки зростали, але спостерігали тимчасове падіння під час нещодавнього спаду ринку, особливо з точки зору угод з прямим капіталом (PE). Проте злиття та поглинання в публічному просторі продемонстрували певний ступінь стабільності, причому нещодавні ознаки свідчать про відновлення активності. У цьому дописі в блозі ми досліджуємо мінливий ландшафт у сфері кібербезпеки та обговорюємо, яку вигоду можуть отримати приватні фірми, інвестуючи в компанії з кібербезпеки.

Зміна моделей угод

Ми проаналізували приватні та державні угоди з кібербезпеки у 2022 та 2023 роках. На рисунку 1 показано, що приватні інвестиції (включаючи приватний і венчурний капітал) значно скоротилися в другій половині 2022 року, але знову

почали зростати за останні шість місяців. Незважаючи на це, загальний обсяг угод залишався відносно постійним на рівні приблизно від 100 до 125 угод на квартал, головним чином завдяки більшій активності публічних M&A. Насправді ми помітили значне збільшення кількості публічних угод, починаючи з 2023 року.

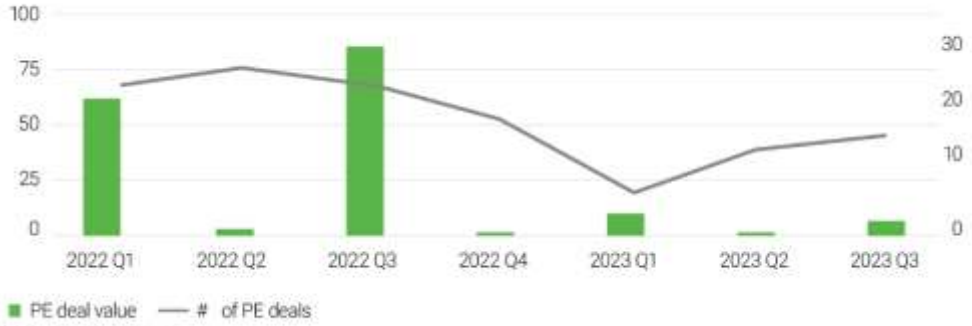
FIGURE 1: PRIVATE (INCL. VENTURE CAPITAL) AND PUBLIC DEAL VOLUME (2022-23)



Source: Pitchbook and Security Week

У категорії приватних інвестицій спостерігалося більш значне зниження обсягу угод, забезпечених PE (рис. 2). Ми також з'ясували, що фірми з приватних товарів, здається, залишаються обережними, головним чином зосереджуючись на меншій вартості угод у 2023 році. Ми вважаємо, що ця тенденція зрештою виявиться тимчасовою, оскільки сектор є привабливим для інвестицій з огляду на фактори, описані нижче.

FIGURE 2: PE BASED DEALS & VALUE ($B) EXCLUDES EARLY-STAGE VENTURE CAPITAL (2022-23)



Source: Pitchbook

Ключові фактори стимулювання угод у сфері кібербезпеки

У 2023 році галузь кібербезпеки стала свідком значної активності M&A, незважаючи на економічну невизначеність і консервативні тенденції витрат. У нашій попередній статті (Створення цінності в кібернетичному просторі: зростання, маржа та змінні цілі) ми обговорювали, як інвестори в кібербезпеку віддають перевагу зростанню доходу над прибутковістю. Цю тенденцію чітко демонструє наголос на

неорганічному зростанні через діяльність M&A. Цю тенденцію сприяють такі ключові фактори:

Зростання важливості хмарної безпеки. Із широким розповсюдженням хмари зріс попит на хмарні рішення безпеки. Оскільки організації виконують свої робочі навантаження в мультихмарі, керування безпекою та продуктивністю в хмарних середовищах стає складним завданням. Ця тенденція спричинила сплеск активності M&A, оскільки компанії з кібербезпеки прагнуть придбати або злитися з фірмами, що спеціалізуються на хмарній безпеці, ідентифікації та управлінні доступом. Помітні придбання включають придбання Google Mandiant за 5,4 мільярда доларів, придбання Bonic компанією CrowdStrike, придбання Cisco Lightspin і, останнім часом, Splunk за приголомшливі 28 мільярдів доларів.

Важливість нових технологій. Зростає попит і впровадження нових технологій, таких як виявлення загроз на основі штучного інтелекту та реагування на них, безпека даних, нульова довіра, операційна технологія (OT) / Інтернет речей (IoT) і керування доступом до ідентифікаційної інформації (IAM). Як наслідок, спостерігається сплеск активності у злиттях і поглинаннях, особливо коли провідні компанії купують стартапи, щоб залишатися інноваційними та конкурентоспроможними. Останні приклади включають придбання Cisco Armorblox і Check Point придбання Perimeter 81.

Новий вихід на ринок. Окрім злиття та поглинання, зосередженого на продуктах і технологіях, компанії прагнуть розширити свою присутність на нових ринках, щоб збільшити свою клієнтську базу, що обумовлено глобальним феноменом проблем кібербезпеки. Останні приклади включають придбання Accenture бразильської Morphus, французька компанія Thales купує австралійську компанію Tesserent, а Veridos стає мажоритарним акціонером сербської компанії NetSeT.

Урядові ініціативи. Попутний вітер з боку федерального уряду на захист інфраструктури стимулює попит у всьому наборі. Очікується, що федеральний уряд збільшить свої інвестиції в кібербезпеку, витративши понад 10 мільярдів доларів

лише у 2022 році. Такі компанії, як SailPoint, Tenable, Rapid7 і CyberArk, отримують вигоду від державних контрактів, що зміцнює стабільність сектора.

Сфери можливостей для очікуваних майбутніх угод

У зв'язку зі зростанням інтересу з боку державних компаній фірми, що спеціалізуються на приватних послугах, поступово визнають потенціал інвестицій у кібербезпеку. Такі компанії, як Thoma Bravo, TPG, KKR і Vista Equity Partners, активно брали участь у угодах у цьому секторі у 2023 році, що свідчить про зростання уваги та відданості. Ми вважаємо, що індустрія кібербезпеки спостерігатиме збільшення активності PE угод у наступних сферах.

Хмарні рішення безпеки. Консолідація хмарної безпеки триватиме, оскільки очікується, що до 2028 року ринок зросте до приблизно 63 мільярдів доларів США, що підкреслює важливість для приватних інвесторів використовувати можливості в цьому ландшафті, що швидко розвивається, перш ніж вони стануть дефіцитними. Хмарні рішення безпеки набувають додаткової популярності завдяки поширенню технологій штучного інтелекту, рішень і послуг. Хмарні гіганти мають потужність і ресурси, щоб не тільки зберігати величезні обсяги даних, але й обробляти, передавати, маніпулювати ними, і список можна продовжувати. Оскільки моделі AI/ML не лише використовують наявні дані, але й генерують значну кількість даних, які зберігаються в хмарі. Таким чином, компанії хочуть продовжувати підвищувати безпеку своїх хмарних середовищ, оскільки конфіденційні дані, які можуть надати компаніям передові переваги, знаходяться в хмарі. Інвестиції в хмарну безпеку повинні враховувати такі фактори, як суверенітет даних, безпека та захист даних, багатохмарна адаптація та сертифікати безпеки. Створення цінності після придбання передбачає економію на масштабі завдяки гібридній хмарній безпеці, підтримці керованих послуг і підтримці довгострокової конкурентоспроможності, інноваціям і персоналізації продуктів.

Рішення безпеки на основі ШІ. Поточні варіанти використання штучного інтелекту передусім включають посилення завдань безпеки, виявлення загроз і реагування на них, а також покращення загальної безпеки. Очікується, що цей ринок досягне 61 мільярда доларів із середньорічним зростанням 22%. Інвестиції в цей

сектор викликають такі проблеми, як відповідність GDPR, CCPA та HIPAA, складності інтеграції та утримання талантів. Крім того, операційні переваги використання рішень безпеки на основі штучного інтелекту включають 1) прискорений час реагування на інциденти безпеки для швидшого повернення бізнесу до нормального функціонування, 2) просте усунення вразливостей із визначенням пріоритетів і 3) покращене виявлення та прогнозування ризиків порушення безпеки. Організації шукають передові рішення з кібербезпеки, щоб зберегти цінність своїх компаній шляхом запобігання або швидкого виявлення порушень.

Рішення безпеки IoT. Прогнозується, що до 2028 року ринок безпеки IoT зросте на 23% CAGR до 59 мільярдів доларів США через кількість підключених пристроїв, уразливості мережі та проблеми із захистом даних. Безпека IoT вимагає ретельного вивчення різноманітності пристроїв, управління вразливістю та масштабованості. Економічної ефективності можна досягти за допомогою автоматизованого керування пристроями, хмарного моніторингу та прогнозованого пом’якшення загроз. Крім того, розширення верхньої лінії може бути забезпечене спеціалізацією індустрії безпеки, консультаційними послугами, апаратним забезпеченням безпеки для Інтернету речей та бездоганною інтеграцією в екосистему Інтернету речей.

Рішення для навчання та підвищення обізнаності з кібербезпеки. Співробітники часто є найслабшою ланкою в ланцюжку безпеки. Усвідомлюючи це, у 2023 році Vista Equity Partners придбала тренінги з підвищення обізнаності та імітацію фішингової платформи KnowBe4, а Accenture придбала Morphus, постачальника послуг кіберзахисту, управління ризиками та аналізу кіберзагроз. Цей ринок вимагає ретельної оцінки якості контенту, методів доставки та відповідності. Стабільності доходів можна досягти, залишаючись релевантними зі зміною вмісту, характером атак, пропонуючи індивідуальні рішення для різних галузей, а також розглядаючи потенційну гейміфікацію та партнерство, що сприятиме конкурентоспроможності.

Консалтингові послуги з кібербезпеки. Організаціям потрібна допомога, щоб оцінити стан безпеки та запровадити рішення безпеки, а консалтингові компанії з кібербезпеки можуть допомогти організаціям у вирішенні цих завдань. Придбання консалтингових фірм з кібербезпеки вимагає досвіду портфоліо та позиціонування на ринку. Досягнення операційної досконалості в цьому просторі вимагає ефективного управління знаннями, придбання й утримання талантів, можливостей дистанційного консультування, спеціалізацій із безпеки та галузевих партнерств.

Золотий момент для прямих інвестицій у кібербезпеку

Зараз настав критичний момент для фірм, що спеціалізуються на виробництві, щоб збільшити інвестиції в сектор кібербезпеки, враховуючи критичну функцію галузі в нашій технологічній епосі, що постійно розвивається. Розумні інвестиції, зроблені сьогодні, можуть принести значну віддачу в майбутньому. Нещодавній сплеск угод, ймовірно, лише початок тривалої тенденції». ***(Shagun Jain, Megha Kalsi and Satchi Mishra. Is the changing Cybersecurity landscape an opportunity for PE investors? // AlixPartners LLP (https://insights.alixpartners.com/post/102iqtb/is-the-changing-cybersecurity-landscape-an-opportunity-for-pe-investors). 23.10.2023).***

***

«Малий і середній бізнес (SMB) прагне пропонувати найкращі послуги, зберігаючи свої витрати якомога нижчими. Але їм може бути складно виділити значний бюджет на заходи кібербезпеки.

Подія кібербезпеки має численні наслідки. Наслідками витоку даних можуть бути великі штрафи, втрата довіри клієнтів і години простою. Отже, малий і середній бізнес повинен захистити себе від кіберзагроз, але в масштабі. Вони повинні впроваджувати правильні заходи для створення безпечного середовища, роблячи свої пропозиції більш надійними для клієнтів.

Малі і середні підприємства, швидше за все, матимуть менше фінансових і технічних ресурсів. На жаль, хакери знають про цей факт. Хакери, як правило, націлюються на ММСП, припускаючи, що вони мають слабші засоби безпеки, які

вони можуть легко обійти. Тому малим і середнім підприємствам необхідно розгорнути надійні заходи безпеки.

Відповідно до звіту Digital Ocean «Малі підприємства та кібербезпека», 54% малих і середніх підприємств заявили, що зараз вони більше стурбовані кібербезпекою, ніж рік тому. У звіті також висвітлюються інші проблеми безпеки, з якими стикаються SMB. Вони є наступними:

брак часу на забезпечення безпеки (25%)

втрата або крадіжка даних (23%)

атаки програм-вимагачів (12%)

DDoS-атаки (10%)

Оскільки малі фірми починають масштабувати свій бізнес, вони повинні обмежити проблеми, які можуть викликати недовіру та незадоволення клієнтів. Хоча порушення руйнує репутацію фірми та призводить до збитків, відновлення довіри потребує часу.

Ось п’ять способів, як малий бізнес може боротися з кіберризиками.

1. Використовуйте захищені мережі

Захищені технології є одним із найкращих способів запобігти доступу хакерів до даних. Встановлення надійних паролів, багатофакторна автентифікація (MFA) і регулярне оновлення програмного забезпечення – це економічно ефективні заходи, які можуть прийняти SMB.

Надійний пароль запобігає несанкціонованому доступу. Підприємства малого та середнього бізнесу повинні заохочувати своїх співробітників створювати складні паролі з цифрами, спеціальними символами, верхнім і нижнім регістрами.

Найкращий спосіб захистити паролі – зберігати їх у менеджері паролів. Це дозволяє користувачам зберігати свої паролі в одному місці. Ці менеджери паролів автоматично заповнюють інформацію, тому користувачеві не потрібно її запам’ятовувати.

Крім того, додавання MFA вимагає від користувачів надати додаткову інформацію для перевірки. Наприклад, одноразовий код надсилається на їхні телефони для підтвердження…

Вимагаючи від усіх співробітників використання MFA, малий і середній бізнес може зменшити ризики несанкціонованого доступу, навіть якщо паролі зламано.

Застаріле програмне забезпечення вразливе до кібератак. Тому оновіть програмні засоби та переконайтеся, що патчі безпеки та виправлення швидко виправляються. Заохочуйте співробітників вмикати автоматичні оновлення на своїх пристроях або системах, щоб забезпечити надійний захист даних.

2. Створіть план реагування на інциденти (IR).

Відповідно до нещодавнього звіту підрозділу 42 «Звіт про реагування на інциденти за 2022 рік», 70% випадків реагування на інциденти за останні дванадцять місяців були програмами-вимагачами та компрометацією корпоративної електронної пошти (BEC).

Створення плану IR є проактивним кроком, який допомагає малим і середнім підприємствам ефективно впоратися з кіберінцидентами та допомагає зменшити вплив. Надійний план IR демонструє відданість компанії кібербезпеці та створює довіру клієнтів і партнерів.

Для надійного IP-плану малому та середньому бізнесу необхідно:

Визначте дані та критичні активи та визначте, які дані потребують негайного захисту. Активи та дані включають дані клієнтів, фінансові записи, інтелектуальну власність та операційні системи.

Визначте потенційні загрози кібербезпеці, з якими стикалися в минулому або можуть зіштовхнутися в майбутньому.

Загрози включають витік даних, атаки програм-вимагачів та випадки фішингу. Це допомагає зрозуміти потенційні сценарії та підготуватися до будь-яких майбутніх атак.

Нарешті, для кожного потенційного сценарію складіть конкретні плани реагування. Численні плани включають ізоляцію скомпрометованих систем, сповіщення клієнтів про витоки даних і вжиття заходів для зменшення їх впливу.

3. Шифруйте конфіденційні дані

Шифрування конфіденційних даних гарантує, що дані залишаться нечитабельними та непридатними для використання без ключа дешифрування.

Підприємства малого та середнього бізнесу мають застосовувати наскрізне шифрування для конфіденційних комунікацій.

У той же час шифруйте дані, що зберігаються в базах даних, файлових серверах і зовнішніх накопичувачах, таких як USB-накопичувачі. SMB також можуть використовувати пристрої на основі шифрування як додатковий захист даних.

Керований постачальник IT-послуг може допомогти малим і середнім підприємствам переконатися, що кожен пристрій зашифровано.

4. Проведіть належне навчання співробітників

Оскільки кібератаки стають все більш витонченими, фірми повинні визнати необхідність сильної культури безпеки для всіх співробітників. Відповідно до нещодавнього звіту Fortinet, 2023 Security Awareness and Training,

Підприємства малого та середнього бізнесу мають запровадити базові практики та політику безпеки для працівників. Це включає вимогу надійних паролів і встановлення відповідних інструкцій щодо використання Інтернету.

Навчіть співробітників основним методам безпеки. Це включає використання двофакторної автентифікації та встановлення надійних паролів. Крім того, встановіть правила обробки та захисту даних клієнтів та іншої важливої бізнес-інформації.

Проводити майстер-класи по:

Основні знання про кібербезпеку

Проведіть симуляції фішингу

Безпечні онлайн-практики

Звіт про інцидент

5. Майте страхування кібербезпеки

Кібератаки можуть призвести до значних фінансових втрат, які можуть завдати шкоди малому та середньому бізнесу. Додаткові витрати на відновлення даних, юридичні збори та регуляторні штрафи можуть завдати шкоди невеликим компаніям. Кіберстрахування допоможе зменшити ці витрати. Крім того, він надає

фінансову підтримку, щоб допомогти компаніям відновитися після серйозного порушення даних.

Інцидент кібербезпеки завдає шкоди репутації компанії. Через це клієнти втрачають свої гроші та довіру до бізнесу. Кіберстрахування включає покриття витрат, пов'язаних з управлінням репутацією, щоб допомогти завоювати довіру клієнтів до компанії». ***(Apoorva Kasam. Five Ways Medium Small Businesses Can Strengthen Their Cybersecurity Landscap // ITSecurityWire (https://itsecuritywire.com/featured/five-ways-medium-small-businesses-can-strengthen-their-cybersecurity-landscape/). 27.10.2023).***

***

Багато малих підприємств, як правило, нехтують важливістю кібербезпеки, припускаючи, що їхній розмір робить їх менш вразливими до кібератак. Однак правда полягає в тому, що жодна організація не застрахована від кіберзагроз, будь то великих чи малих. Фактично, згідно зі звітом Verizon, 43% усіх кібератак спрямовані на малий бізнес.

Важливість кібербезпеки для малого бізнесу:

1. Захист конфіденційних даних. Малі підприємства часто обробляють конфіденційну інформацію, таку як дані клієнтів, фінансові записи та комерційні таємниці. Одне порушення даних може призвести до руйнівних наслідків як для бізнесу, так і для його клієнтів. Тому впровадження потужних заходів кібербезпеки має вирішальне значення для захисту цих цінних даних від потрапляння в чужі руки.

2. Збереження довіри клієнтів: на сучасному конкурентному ринку довіра відіграє життєво важливу роль у підтримці лояльної клієнтської бази. Порушення безпеки може завдати шкоди довірі між компанією та її клієнтами, оскільки вони можуть вважати, що їхня особиста інформація не в безпеці в компанії.

3. Відповідність нормативним вимогам. Малі підприємства підпадають під дію різних законів і нормативних актів щодо захисту даних і конфіденційності. Недотримання цих законів може призвести до юридичних наслідків, таких як значні штрафи або судові позови.

4. Забезпечення безперервності бізнесу: загрози кібербезпеці можуть порушити нормальні бізнес-операції, що може призвести до простою

Пояснення того, що таке інструменти кібербезпеки та їх призначення

Інструменти кібербезпеки необхідні для захисту малого бізнесу від різноманітних онлайн-загроз. Ці інструменти можуть включати апаратне забезпечення, програмне забезпечення та служби, які працюють разом для захисту цифрових активів компанії, зокрема даних, систем, мереж і пристроїв. У цьому розділі ми розглянемо специфіку інструментів кібербезпеки та їхнє загальне призначення для захисту бізнесу.

1. Апаратні засоби:

Апаратні засоби – це фізичні пристрої, які підвищують безпеку мережі підприємства. До цієї категорії підпадають брандмауери, системи виявлення/запобігання вторгненням (IDS/IPS) і маршрутизатори. Брандмауери діють як бар'єри між внутрішніми мережами та зовнішніми загрозами, контролюючи вхідний і вихідний трафік на основі заздалегідь визначених правил безпеки. Системи IDS/IPS виявляють зловмисну діяльність, наприклад спроби несанкціонованого доступу або зараження шкідливим програмним забезпеченням у системі. Маршрутизатори відіграють вирішальну роль у створенні безпечних з'єднань між різними мережами за допомогою протоколів шифрування.

2. Програмні засоби:

Програмні інструменти стосуються програм, призначених для захисту цифрових активів від онлайн-атак або вторгнень. Антивірусне програмне забезпечення є одним із найпопулярніших типів програмного забезпечення кібербезпеки, яке використовується малим бізнесом. Він постійно сканує на наявність вірусів, троянів, черв'яків та інших форм шкідливого програмного забезпечення, яке може завдати шкоди комп'ютерам або мережі компанії. Менеджери паролів — це інший тип програмного засобу, який безпечно зберігає паролі разом із можливістю генерувати складні паролі, коли це необхідно.

3. Захист кінцевої точки:

Інструменти захисту кінцевих точок — це рішення, спеціально розроблені для захисту кінцевих точок, таких як настільні комп’ютери, ноутбуки, сервери та мобільні пристрої, від кібератак. Ці інструменти використовують передові технології, такі як

7 найпопулярніших інструментів кібербезпеки для малого бізнесу:

У сучасну епоху цифрових технологій малий бізнес стає все більш уразливим до кібератак. Хакери та кіберзлочинці постійно вдосконалюють свою тактику та націлюються на малий бізнес, оскільки їм часто бракує ресурсів, щоб інвестувати в надійні заходи кібербезпеки. Тому для малого бізнесу вкрай важливо мати правильні інструменти кібербезпеки, щоб захистити свої конфіденційні дані та системи від потенційних загроз.

Ось 7 найпопулярніших інструментів кібербезпеки, у які кожен малий бізнес повинен інвестувати:

Захист брандмауером

Захист брандмауером є важливим компонентом набору інструментів кібербезпеки будь-якого малого бізнесу. Він діє як перша лінія захисту від потенційних кібератак і допомагає зберігати конфіденційні дані в безпеці. Простими словами, брандмауер — це система безпеки, яка відстежує та контролює вхідний і вихідний мережевий трафік на основі заздалегідь визначених правил безпеки.

Одним із основних способів захисту малих підприємств міжмережевими екранами є блокування несанкціонованого доступу до їхніх мереж. Це можна зробити двома способами: за допомогою списків контролю доступу (ACL) або перевірки пакетів із зазначенням стану (SPI). ACL перевіряють джерело та призначення кожного пакета даних, а потім дозволяють або забороняють його проходження на основі попередньо запрограмованих критеріїв. SPI, з іншого боку, створює поточний запис усіх мережевих з’єднань, аналізуючи кожен пакет, щоб визначити, чи був він запрошений або надісланий авторизованим користувачем.

Ще одна важлива функція захисту брандмауера — це запобігання вторгненню. Це передбачає активний моніторинг вхідних повідомлень на предмет відомих шаблонів або сигнатур, пов’язаних із кібератаками, такими як віруси, зловмисне

програмне забезпечення та спроби злому. У разі виявлення підозрілої активності система запускає сповіщення, щоб сповістити системних адміністраторів, які можуть вжити відповідних заходів.

Окрім виявлення зловмисної активності із зовнішніх джерел, брандмауери також відіграють важливу роль у захисті від внутрішніх загроз. Це може включати доступ співробітників до обмежених веб-сайтів або завантаження шкідливих файлів на пристрої компанії. Брандмауери можна запрограмувати на блокування певних веб-сайтів і обмеження завантаження файлів, щоб забезпечити доступ лише до схваленого вмісту в системах компанії.

Антивірусне програмне забезпечення

Антивірусне програмне забезпечення є життєво важливим компонентом у забезпеченні надійних заходів кібербезпеки для будь-якого малого бізнесу. Він призначений для захисту пристроїв і мереж від шкідливих загроз, таких як віруси, зловмисне програмне забезпечення, шпигунське програмне забезпечення та програми-вимагачі. Без належного антивірусного програмного забезпечення ваш бізнес може бути вразливим до кібератак, які можуть призвести до витоку даних, фінансових втрат і шкоди вашій репутації.

Сьогодні на ринку доступні різноманітні варіанти антивірусного програмного забезпечення, кожне з яких має свої унікальні функції та можливості. Вибираючи найкращий для свого малого бізнесу, важливо враховувати такі фактори, як ефективність проти різних типів загроз, сумісність із вашими пристроями та операційними системами, зручність для працівників і вартість.

Одне з найкращих імен у світі антивірусного програмного забезпечення — Norton Security. Це комплексне рішення пропонує захист від усіх типів онлайн-загроз, а також забезпечує моніторинг у реальному часі та автоматичне оновлення. Його зручний інтерфейс полегшує розуміння та ефективне використання для нетехнічних працівників. Norton Security також пропонує додаткові функції, такі як захист брандмауером і інструменти безпечного перегляду.

Іншим популярним варіантом є McAfee Total Protection, який забезпечує розширений захист від вірусів, шпигунського програмного забезпечення, програм-

вимагачів, крадіжки особистих даних та інших онлайн-загроз. Він також пропонує інструменти оптимізації продуктивності, щоб забезпечити безперебійну роботу ваших пристроїв, захищаючи їх від зловмисних атак.

Інструменти шифрування даних

Шифрування даних є важливим аспектом кібербезпеки для малого бізнесу. Він захищає конфіденційні дані від доступу неавторизованих сторін і гарантує, що інформація залишається конфіденційною та безпечною.

У сучасному цифровому середовищі компанії все більше залежать від збору, зберігання та обміну великою кількістю конфіденційних даних. Це включає фінансові записи, інформацію про клієнтів, записи про співробітників, комерційну таємницю та інші важливі бізнес-дані. Такі дані можуть бути надзвичайно цінними для кіберзлочинців, які хочуть викрасти або використати їх для власної вигоди.

Потреба в надійних інструментах шифрування даних стала більш важливою, ніж будь-коли раніше. Ці інструменти призначені для перетворення звичайного тексту в закодовану форму, яку хакери не можуть легко перехопити або розшифрувати. У цьому розділі ми обговоримо найпопулярніші інструменти шифрування даних, у які варто інвестувати кожному малому бізнесу.

1) Віртуальна приватна мережа (VPN):

Віртуальна приватна мережа (VPN) — це безпечне з’єднання між двома мережами через Інтернет. Він шифрує весь зв’язок, що проходить через нього, і гарантує, що будь-яка третя сторона, яка спостерігає за трафіком, не зможе отримати доступ до переданої інформації.

Використання VPN має важливе значення для малого бізнесу, оскільки воно дозволяє віддаленим співробітникам безпечно отримувати доступ до ресурсів компанії поза офісною мережею. Він також забезпечує додатковий рівень безпеки під час використання публічних мереж Wi-Fi.

2) Програмне забезпечення для шифрування файлів:

Програмне забезпечення для шифрування файлів використовується для захисту окремих файлів шляхом перетворення їх у нечитабельний код із паролем або ключем, відомим лише авторизованим користувачам. Цей інструмент особливо

корисний для підприємств, які мають справу з конфіденційними документами, такими як фінансові звіти чи юридичні контракти.

На ринку є кілька програм для шифрування файлів, наприклад VeraCrypt і AxCrypt, які можна використовувати для захисту конфіденційних даних від несанкціонованого доступу.

3) Шифрування електронної пошти:

Електронна пошта є одним із найпоширеніших способів спілкування для бізнесу. Однак електронні листи вразливі до перехоплення та підробки. Інструменти шифрування електронної пошти шифрують усі електронні листи, що надсилаються між сторонами, унеможливлюючи прочитання чи зміну вмісту хакерами.

Популярні інструменти шифрування електронної пошти включають ProtonMail і Virtru, які пропонують наскрізне шифрування, гарантуючи, що лише призначений одержувач зможе прочитати повідомлення.

4) Повне шифрування диска (FDE):

Повне шифрування диска (FDE) гарантує, що кожен файл на жорсткому диску буде зашифровано та захищено. Цей інструмент особливо корисний для ноутбуків або інших пристроїв, які можуть бути втрачені або викрадені, оскільки він запобігає неавторизованому доступу будь-якої інформації на пристрої.

Такі інструменти, як Microsoft BitLocker і FileVault від Apple, пропонують повні функції шифрування диска, вбудовані в їхні операційні системи.

5) Шифрування хмарного сховища:

Сервіси хмарного зберігання даних стали невід'ємною частиною сучасного бізнесу. Однак зберігання конфіденційних даних на хмарних серверах може становити значні ризики для безпеки, якщо вони не зашифровані належним чином.

Менеджери паролів

Менеджери паролів є основними інструментами для малого бізнесу, який хоче захистити свою конфіденційну інформацію в Інтернеті. Зі збільшенням кількості кібератак і витоків даних для малого бізнесу вкрай важливо вжити необхідних заходів для захисту своїх паролів і облікових даних для входу. Менеджер паролів — це програмне забезпечення, яке надійно зберігає всі ваші паролі, дані кредитної

картки та інші дані для входу в зашифроване сховище. Він діє як цифрова скринька, доступ до якої маєте лише ви за допомогою головного пароля.

Використання менеджерів паролів стало більш важливим, ніж будь-коли раніше, оскільки більшість малих підприємств працюють у цифровому середовищі, де для кількох облікових записів потрібні різні паролі. Використання слабких або поширених паролів може зробити ваш бізнес вразливим до несанкціонованого доступу та потенційних кібератак. Менеджери паролів пропонують просте вирішення цієї проблеми, генеруючи складні й унікальні паролі для кожного облікового запису, що ускладнює доступ хакерам.

Однією з найбільших переваг використання менеджера паролів є те, що він усуває необхідність запам’ятовувати декілька паролів. Натомість вам потрібно запам’ятати лише один головний пароль, який розблокує доступ до всіх збережених облікових даних. Це не тільки економить дорогоцінний час, але й зменшує ризик забути або втратити важливі дані для входу.

Більшість авторитетних менеджерів паролів використовують розширені алгоритми шифрування, такі як 256-бітне шифрування AES, що робить їх практично неможливим для хакерів. Крім того, деякі також пропонують варіанти багатофакторної автентифікації, наприклад біометричне розпізнавання або двофакторну перевірку, додаючи ще один рівень безпеки.

З огляду на те, що співробітники стають все більш мобільними та працюють віддалено з різних пристроїв, керування паролями для всієї компанії може бути складним завданням. У таких випадках підприємства можуть вибрати менеджери паролів бізнес-класу, які забезпечують централізований контроль і керування паролями на кількох пристроях і співробітниках.

Віртуальні приватні мережі (VPN)

У сучасну цифрову епоху компанії повинні вживати додаткових заходів, щоб забезпечити безпеку своїх конфіденційних даних, поки співробітники отримують віддалений доступ до баз даних компанії. Віртуальні приватні мережі, або VPN, забезпечують безпечний спосіб передачі даних через Інтернет, створюючи

зашифрований тунель між пристроєм користувача та потрібним мережевим сервером.

Коли працівник підключається до онлайнової бази даних компанії за допомогою VPN, увесь його онлайн-трафік направляється через цей зашифрований тунель, що ускладнює перехоплення з'єднання. Це робить його життєво важливим інструментом безпеки для малих підприємств, у яких віддалені співробітники працюють у громадських місцях, де можуть ховатися кіберзлочинці.

Крім того, VPN зберігають вашу онлайн-діяльність у конфіденційності від Інтернет-провайдерів (ISP), які можуть відстежувати вашу онлайн-діяльність без захисту. Він також приховує вашу IP-адресу, що ускладнює моніторинг вашої веб-активності сторонніми трекерами.

Деякі служби VPN також пропонують такі функції, як політики відмови від реєстрації та захист від зловмисного програмного забезпечення, що ще більше покращує їхні можливості безпеки.

Шифрування електронної пошти

Електронна пошта продовжує залишатися одним із найбільш часто використовуваних засобів спілкування серед компаній у всьому світі. Однак, оскільки електронна пошта є невід'ємною частиною бізнес-екосистеми, вона також стала основною мішенню для кіберзлочинців для здійснення фішингових шахрайств, розповсюдження зловмисного програмного забезпечення та інших шкідливих дій.

Шифрування електронної пошти додає додатковий рівень безпеки для компаній, захищаючи їхні повідомлення від доступу третіх сторін. Шифрування по суті шифрує вміст електронної пошти в код, який може прочитати лише призначений одержувач за допомогою ключа дешифрування. Це запобігає несанкціонованому доступу до конфіденційної інформації, що міститься в електронних листах.

Малим підприємствам слід розглянути можливість впровадження рішень для шифрування електронної пошти, які автоматично шифрують усі вихідні та вхідні повідомлення з клієнтами, партнерами чи постачальниками. Це гарантує захист усіх ділових електронних листів, навіть якщо вони містять конфіденційні дані, як-от облікові дані для входу або фінансові відомості.

Навчання співробітників

Хоча інвестиції в інструменти та програмне забезпечення кібербезпеки є важливими для будь-якого малого бізнесу, не менш важливо навчати працівників найкращим практикам кібербезпеки. Відповідно до звіту IBM Cybersecurity Intelligence Index (2020), 95% порушень кібербезпеки були спричинені помилками людини.

Співробітники відіграють важливу роль у забезпеченні безпеки даних вашого бізнесу. Таким чином, надавши їм адекватну підготовку щодо того, як розпізнавати фішингові атаки, створювати надійні паролі та безпечні онлайн-практики, дуже важливо захистити активи вашої компанії.

Крім того, регулярні тренінги з питань безпеки можуть допомогти співробітникам бути в курсі нових кіберзагроз і способів їх подолання. Також надзвичайно важливо мати чіткий набір IT-політики, якої працівники повинні дотримуватися під час ведення бізнесу в Інтернеті…» ***(The Top 7 Must-Have Cybersecurity Tools for Small Businesses // TechBullion (https://techbullion.com/the-top-7-must-have-cybersecurity-tools-for-small-businesses/). 26.10.2023).***

***

«…Trend Micro, один із провідних світових постачальників рішень для кібербезпеки, у співпраці з Бранденбурзьким інститутом суспільства та безпеки (BIGS) провели опитування керівників відділів IT та IT-безпеки щодо їх сприйняття ризиків, їх інвестиційної поведінки та ролі IT-безпеки в їхньому бізнесі. На основі цих даних BIGS визначив зв’язки в емпіричному аналізі.

Кібербезпека створює умови для цифрової трансформації

Кібератаки сьогодні є найбільшим ризиком для бізнесу. Тому захиститися від них є економічною необхідністю. Понад три чверті (76 відсотків) німецьких компаній із понад 250 співробітниками вважають IT-безпеку важливою для економіки. Але це вже не просто уникнення пошкоджень. Безпека все частіше сприймається як можливість для розвитку бізнесу. Дві третини опитаних (66 відсотків) хочуть просувати проекти цифровізації шляхом модернізації IT-безпеки.

79 відсотків компаній, які стратегічно інвестують у безпеку, вважають це актуальним для розробки нових бізнес-моделей.

«Дослідження показує, що сприйняття IT-безпеки змінилося в ключових сферах», — пояснює доктор. Тім Штухтей, керуючий директор Бранденбурзького інституту суспільства та безпеки. «У минулому це часто вважалося гальмом для інновацій. Більшість опитаних компаній визнали, що IT-безпека насправді створює передумови для цифрової трансформації. Це відкриває нові бізнес-сфери та може бути вигідно інтегровано у вашу власну бізнес-модель. Кібербезпека більше не розглядається як запобіжник, а стала стимулом».

Стратегічні інвестиції мають сенс

Зростає усвідомлення того, що інвестиції в IT-безпеку є економічно вигідними. 64 відсотки опитаних компаній вважають, що безпека приносить додаткову цінність для клієнта, а 59 відсотків уже використовують свою концепцію IT-безпеки в маркетингових цілях. Поінформованість про цю тему також зростає серед споживачів. Тому вони очікують, що компанії захищатимуть дані клієнтів якнайкраще. Отже, хороша IT-безпека може зміцнити бренд. І навпаки, неадекватні заходи безпеки негативно впливають на репутацію компанії. Шкода, заподіяна втратою репутації, часто виявляється значно вищою, ніж витрати на запобіжні заходи.

По суті, за останні 24 місяці інвестиції в кібербезпеку зросли майже в усіх галузях. Але як компанії роблять це – більш стратегічно чи більш реактивно? Дослідження показує: кожен, хто вже постраждав від кібератаки або боїться збитку від майбутніх атак, насамперед стратегічно інвестує в безпеку. Те саме стосується компаній, які бачать IT-безпеку як внесок у ланцюжок створення вартості та додаткову цінність для своїх клієнтів. З іншого боку, ті, хто не має досвіду кібератак, мають низьку обізнаність про ризики та вважають безпеку менш актуальною для економіки, швидше за все, інвестуватимуть реактивно.

Кібербезпека – це справа тих, хто приймає рішення

«Досвід останніх років показує, що стратегічні інвестиції в IT-безпеку необхідні — і окупаються», — говорить Ханнес Штайнер, віце-президент Trend

Micro у Німеччині. «Кібербезпека стала головним пріоритетом. Компанії стикаються з проблемою захисту своїх конфіденційних даних і систем від загроз кіберзлочинності. Відповідальність лежить як на IT, так і на тих, хто приймає рішення. Разом вони повинні забезпечити інтеграцію комплексних заходів кібербезпеки в екосистему для забезпечення довіри клієнтів і партнерів і забезпечення безперервності бізнесу»…» ***(Кібербезпека стимулює цифровізацію // MedPressIT GbR (https://b2b-cyber-security.de/uk/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0-%D1%81%D1%82%D0%B8%D0%BC%D1%83%D0%BB%D1%8E%D1%94-%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8E/). 13.10.2023).***

***

Сполучені Штати Америки

«Xage Security посилить кіберзахист Космічних сил США завдяки контролю доступу з нульовою довірою та захисту даних.

Нульова довіра – це стратегія кібербезпеки Міністерства оборони, яка вимагає постійної перевірки користувачів і пристроїв для захисту даних.

Безпека на основі ідентифікації

Xage розгорне свою структуру Xage Fabric на основі ідентифікації в наземній і космічній архітектурі сил, включаючи супутники та інші наземні та космічні комерційні засоби.

На відміну від підходів до кібербезпеки, які вирішують проблему, коли вона виникає, підхід до кібербезпеки на основі ідентифікації зосереджується на безпечному доступі.

«Ми використовуємо такий підхід, насамперед ідентифікацію, коли ми гарантуємо, що якщо ви торкаєтеся чогось, ми знаємо, хто ви — і ми знаємо, хто ви

насправді добре», — цитує слова Scoop Defense генерального директора Xage Security Джеффрі Меттсона.

«Ми гарантуємо, що ви є привілейованим користувачем, ми перевіряємо ваш рівень привілеїв, ми суворо контролюємо, що ви можете робити, і відстежуємо, що ви можете робити прямо зараз».

Контракт на 17 мільйонів доларів

Контракт на суму 17 мільйонів доларів укладено в той час, коли Космічні сили США розширюють співпрацю з комерційними космічними компаніями, що збільшує ризик кібератак.

«Обидві ці речі вимагають, щоб у них було рішення, за допомогою якого вони могли б захистити весь цей ланцюжок, від супутника до базової станції, мережі та самих даних», — пояснив Меттсон.

Контракт включає три пріоритетні ініціативи: кіберзміцнення наземних систем, таких як наземні станції та модеми, можливості нульової довіри в наземних і космічних системах наступного покоління та безпечний обмін даними». ***(US Space Force Taps Xage Security to Strengthen Cyber Defense // Inder Singh Bisht (https://www.thedefensepost.com/2023/10/06/us-space-force-xage-security/?expand_article=1). 06.10.2023).***

***

«3 жовтня 2023 року Рада Федерального регулювання закупівель (FAR) опублікувала два нових запропонованих правила кібербезпеки. Перший із двох під назвою «Звітування про кіберзагрози та інциденти та обмін інформацією» додає нові вимоги до зобов’язань федеральних підрядників щодо звітування про інциденти кібербезпеки. Друге правило, яке ми розглянемо в окремій публікації в блозі, називається «Стандартизація вимог до кібербезпеки для несекретних федеральних інформаційних систем» і охоплює договірні вимоги щодо кібербезпеки для несекретних федеральних інформаційних систем.

Обидва правила випливають із виконавчого наказу 14028 «Підвищення кібербезпеки нації», виданого президентом Байденом 12 травня 2021 року («Кібер

EO»). Ми висвітлювали події згідно з цим розпорядженням у рамках серії щомісячних публікацій. У першому блозі підсумовувалися ключові положення та часові рамки Cyber EO, а в наступних блогах описувалися дії, вжиті різними державними установами для впровадження Cyber EO з червня 2021 року по вересень 2023 року. У цьому блозі описано основні вимоги, які висуваються запропонованим правилом «Повідомлення про кіберзагрози та інциденти та обмін інформацією».

Нові вимоги щодо звітування про інциденти та обміну інформацією

Відповідно до вказівок Cyber EO, правило, запропоноване у справі FAR 2021-017, реалізує рекомендації OMB і CISA щодо зобов'язань федеральних підрядників повідомляти про інциденти кібербезпеки. Правило вносить зміни до положень кількох існуючих підрозділів FAR і вводить нові положення FAR для включення контрактних офіцерів до майбутніх тендерів і контрактних дій. Правило також додає нові визначення FAR і розширює інші. Наприклад, запропоноване правило широко розширює визначення «інформаційно-комунікаційних технологій (ІКТ)», вказуючи, що операційні технології, такі як промислові системи управління, системи управління будівлями та механізми контролю фізичного доступу, охоплюються правилом.

Згідно з новим правилом, офіцери-підрядники включатимуть положення про первинне звітування про інциденти, FAR 52.239-ZZ, Вимоги щодо звітування про інциденти та загрози та реагування на інциденти для продуктів або послуг, що містять інформаційно-комунікаційні технології, у всі нові пропозиції та контракти. Це правило застосовується до контрактів, нижчих спрощеного порогу придбання, а також до комерційних продуктів, у тому числі готових товарів (COTS), і комерційних послуг.

Правило накладає низку вимог, найбільш помітні з яких стосуються: (1) Звітування про інциденти безпеки; (2) доступ уряду до інформації про підрядників та інформаційних систем; (3) Заяви щодо звітування про інциденти безпеки; та (4) Специфікації програмного забезпечення (SBOM).

Зобов'язання щодо звітування про інциденти безпеки

Запропоноване правило накладає нові та суворі зобов'язання щодо звітності для підрядників, які виявляють ознаки того, що міг відбутися «інцидент із безпекою», термін, який має широке визначення та включає «фактичну або потенційну появу [] будь-якої події або серії подій…, які становлять) фактична або неминуча загроза цілісності, конфіденційності або доступності інформації або інформаційної системи» АБО, що є «порушенням або безпосередньою загрозою порушення закону, політики безпеки, процедур безпеки або політики прийнятного використання». Ці зобов'язання щодо звітування про інциденти застосовуються до всіх інцидентів безпеки, пов'язаних із продуктом або послугою, що надається уряду, включаючи інформаційно-комунікаційні технології (ІКТ) або інформаційну систему, яка використовується для розробки або надання продукту чи послуги уряду.

Правило вимагає від підрядників «негайно й ретельно досліджувати всі ознаки того, що міг статися інцидент безпеки, і подавати інформацію за допомогою порталу звітів про інциденти CISA...протягом восьми годин після виявлення... [і] оновлювати подання кожні 72 години після цього, доки Підрядник, агентство та/або будь-які розслідувальні органи не завершать усі дії з викорінення або відновлення». Цей графік звітування є набагато коротшим, ніж 72-годинний графік звітування, встановлений Міністерство оборони в DFARS 252.204-7012(c)(1)(ii). Крім того, запропоноване правило не звільняє відповідних підрядників від їхніх зобов'язань щодо звітності Міністерства оборони відповідно до DFARS, а натомість зазначає, що «продукція та системи, які підрядники пропонують федеральному уряду, можуть підлягати… іншим вимогам щодо звітності про інциденти».

На додаток до вимог щодо звітності CISA, підрядники повинні повідомити: (1) відповідного уповноваженого за контрактом; і (2) будь-які посадові особи, що підрядники, або посадові особи, які займаються замовленнями, будь-якої агенції, яка розмістила відповідне замовлення за контрактом, звіт про інцидент якого було подано до CISA. Правило не визначає часові рамки для повідомлення про потенційний інцидент постраждалим підрядникам, але згідно з Правилом, CISA зобов'язана поділитися повідомленою інформацією «з будь-яким підрядним агентством, яке потенційно постраждало від інциденту або вразливості, виявленої в

інциденті», а також правоохоронні органи. З практичної точки зору підрядники можуть мати переваги, повідомляючи своїх клієнтів перед тим, як державні регулятори звернуться до них на основі звіту до CISA.

Надання доступу до інформації про підрядника та інформаційних систем

Запропоноване правило надає CISA, ФБР і установі-підряднику «повний доступ» до відповідної інформації про підрядника, інформаційних систем і персоналу у відповідь на інцидент безпеки, про який повідомляє підрядник, або на інцидент безпеки, визначений урядом. Згідно із запропонованим пунктом FAR, «повний доступ» означає: (1) фізичний та електронний доступ до мереж, систем, облікових записів та іншої інфраструктури; і (2) «надання підрядником усіх запитаних державних даних або пов'язаних з урядом даних», включаючи зображення, файли журналів, інформацію про події та заяви співробітників підрядника.

Запропоноване правило не враховує наслідків надання уряду «повного доступу» до інформації та систем підрядника. Наприклад, у пропонованому правилі не згадуються гарантії прав третіх сторін на конфіденційність чи громадянські свободи, за винятком того, щоб запропонувати представникам галузі висловитися щодо цих тем. Запропоноване правило також не враховує, як такий доступ може вплинути на комерційну таємницю, інші конфіденційні дані підрядника або постачальників/субпідрядників і партнерів по групі підрядника, або матеріали, що підлягають законній конфіденційності. Крім того, запропоноване правило не містить вказівок щодо того, як легко чи часто може бути запущено зобов'язання підрядника щодо надання «повного доступу». Згідно із запропонованим правилом, CISA, ФБР і установа-підрядник мають право на «повний доступ» до інформації та систем підрядника «за запитом» і «у відповідь на [повідомлений або ідентифікований] інцидент безпеки». Але визначення «інциденту безпеки» в запропонованому пункті є дуже широким. Певним чином формулювання є ширшим, ніж визначення інциденту Міністерства оборони. Наприклад, навіть а потенційне політики підрядника порушення внутрішньої щодо допустимого використання є дією, яка

може стати інцидентом безпеки та спричинити зобов'язання підрядника щодо «повного доступу».

Повідомлення про інциденти безпеки

Запропоноване правило вимагає від підрядників підтверджувати, що вони «подали в актуальному, точному та повному вигляді всі звіти про інциденти безпеки, які вимагаються чинними контрактами між Заявником і Урядом», як частину кожної нової контрактної пропозиції. Згідно з новим положенням про представництво, підрядники також повинні стверджувати, що вони вимагали від кожного субпідрядника першого рівня: (1) повідомити головного спеціаліста протягом восьми годин після виявлення інциденту безпеки; і (2) передати ту саму вимогу субпідрядникам нижчого рівня.

Перелік матеріалів програмного забезпечення (SBOM)

Запропоноване правило вимагає, щоб «підрядники розробляли та підтримували специфікацію програмного забезпечення (SBOM) для будь-якого програмного забезпечення, що використовується під час виконання контракту». Запропонована норма додатково не пояснює, що означає використання під час виконання контракту. SBOM — це формальний запис різних компонентів, які використовуються для створення програмного забезпечення. Згідно з правилом і EO 14028, уряд передбачає центральне сховище для SBOM, до якого можуть запитувати інші програми та системи. Правило вимагатиме від підрядників створювати SBOM у «машиночитаному стандартному форматі та... відповідати всім мінімальним елементам», встановленим Міністерством торгівлі США, Національним управлінням телекомунікацій та інформації.

Запропоноване правило вимагає від підрядників надати офіцеру-підряднику копію або доступ до поточного SBOM для «кожної частини комп'ютерного програмного забезпечення» після першого використання цього програмного забезпечення під час виконання контракту. Крім того, згідно із запропонованим правилом, якщо будь-яке програмне забезпечення отримує значне оновлення, нову збірку або основний випуск, підрядник повинен оновити свій контракт SBOM і подати нову версію до офіцера-підрядника. Нарешті, ймовірно, що ці SBOM будуть

серед файлів, на які поширюватимуться вимоги щодо збереження та захисту даних, встановлені іншими розділами пропонованого правила.

Незрозуміло, як ці вимоги можуть бути узгоджені (якщо взагалі узгоджені) з майбутніми вимогами до самоатестації, викладеними в Меморандумі M-22-18 Управління з управління та бюджету (OMB), який вимагає SBOM лише у випадках, коли агентство визначає, що SBOM необхідний і/або що програмне забезпечення є достатньо критичним, щоб гарантувати створення та подання SBOM». ***(Robert K. Huffman, Susan B. Cassidy, Ashden Fein, Michael Wagner, Ryan Burnette and Darby Rourick. FAR Cyber Threat and Incident Reporting and Information Sharing Rule // Covington & Burling LLP. (https://www.insidegovernmentcontracts.com/2023/10/far-cyber-threat-and-incident-reporting-and-information-sharing-rule/#page=1).***
10.10.2023)

***

«Агентство з кібербезпеки та безпеки інфраструктури (CISA) і Федеральне бюро розслідувань (ФБР) оприлюднили спільну консультацію з кібербезпеки 11 жовтня 2023 року, закликаючи компанії (особливо ті, що працюють у секторі критичної інфраструктури) вжити заходів для пом'якшення кіберзагроз від програми-вимагача AvosLocker.

Консультація закликає компанії:

Інструменти безпечного віддаленого доступу

Обмежити протокол віддаленого робочого стола (RDP) та інші служби віддаленого робочого столу

Захистіть PowerShell і/або обмежте використання

Оновлюйте програмне забезпечення до останньої версії та регулярно застосовуйте оновлення

AvosLocker «працює за моделлю програми-вимагача як послуга та атакує компанії з критичною інфраструктурою в США, використовуючи законне програмне забезпечення та інструменти віддаленого адміністрування системи з відкритим кодом. Потім афілійовані особи AvosLocker використовують тактику вимагання

даних на основі ексфільтрації з погрозами витоку та/або публікації викрадених даних». ***(Linn Foster Freedman. CISA + FBI Issue Joint Advisory on AvosLocker Ransomware // Robinson & Cole LLP. (https://www.dataprivacyandsecurityinsider.com/2023/10/cisa-fbi-issue-joint-advisory-on-avoslocker-ransomware/). 12.10.2023).***

***

«Агентство з кібербезпеки та безпеки інфраструктури США (CISA) оприлюднило додаткові відомості щодо неправильних конфігурацій і вразливостей безпеки, якими користуються банди програм-вимагачів, щоб допомогти організаціям критичної інфраструктури запобігти їхнім атакам.

CISA оприлюднила цю інформацію в рамках пілотної програми Ransomware Vulnerability Warning Pilot (RVWP), запровадженої в січні цього року, коли оголосила, що буде попереджати організації критичної інфраструктури про пристрої, вразливі до програм-вимагачів, виявлені в їхній мережі.

З моменту свого заснування RVWP CISA визначив і надав інформацію про понад 800 вразливих систем із доступними через Інтернет уразливими місцями, які часто стають мішенню для різних операцій програм-вимагачів.

«Програми-вимагачі порушили роботу критично важливих служб, компаній і спільнот у всьому світі, і багато з цих інцидентів скоєно суб'єктами програм-вимагачів, які використовують відомі загальні вразливості та загрози (CVE) (тобто вразливості)», — заявили в агентстві з кібербезпеки США.

«Однак багато організацій можуть не знати, що в їхній мережі присутня вразливість, яка використовується програмами-вимагачами.

«Тепер усі організації мають доступ до цієї інформації в нашому каталозі відомих експлуатованих уразливостей (KEV), оскільки ми додали стовпець під назвою «відомо про використання в кампаніях програм-вимагачів». Крім того, CISA розробила другий новий ресурс RVWP, який служить додатковим списком неправильних конфігурацій і слабких місць, які, як відомо, використовуються в кампаніях програм-вимагачів».

Ці зусилля є частиною ширшої кампанії, розпочатої у відповідь на ескалацію загрози програм-вимагачів критичній інфраструктурі, яка з'явилася майже два роки тому з хвилею кібератак, націлених на життєво важливі об'єкти інфраструктури та урядові установи США, зокрема Colonial Pipeline, JBS Foods і Kaseya.

У червні 2021 року агентство представило Ransomware Readiness Assessment (RRA) — новий компонент інструменту оцінки кібербезпеки (CSET), призначений для того, щоб допомогти організаціям оцінити свою готовність протидіяти атакам програм-вимагачів і відновлюватися після них.

До серпня 2021 року CISA також опублікувала вказівки, щоб допомогти вразливим державним і приватним організаціям запобігти витоку даних у результаті інцидентів з програмами-вимагачами.

Підтримуючи свої зобов'язання, CISA створила альянс із приватним сектором для захисту критично важливої інфраструктури США від програм-вимагачів та інших кіберзагроз. Ця спільна ініціатива, Joint Cyber Defense Collaborative (JCDC), втілює колективну стратегію реагування всіх федеральних агентств і організацій приватного сектора, які приєдналися до партнерства.

Відтоді агентство з кібербезпеки США також запустило спеціальний онлайн-портал StopRansomware.gov, який є центральним центром для зусиль CISA щодо надання всієї інформації, необхідної захисникам для підготовки та подолання атак програм-вимагачів.

Раніше цього року CISA наказав федеральним агентствам захистити свої мережеві пристрої, які піддаються доступу до Інтернету, і в спільній консультації з ФБР і АНБ оприлюднив список із 12 найбільш часто використовуваних уразливостей у 2022 році». ***(Sergiu Gatlan. CISA shares vulnerabilities, misconfigs used by ransomware gangs // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/cisa-shares-vulnerabilities-misconfigs-used-by-ransomware-gangs/?utm_source=flipboard&utm_content=other). 13.10.2023).***

***

«Місяць поінформованості про кібербезпеку був заснований ще в 2004 році Міністерством внутрішньої безпеки США та Національним альянсом кібербезпеки (NCSA). Президент Сполучених Штатів і Конгрес щорічно оголошують цей місяць, щоб привернути увагу до кібербезпеки, а цьогорічна тема — «Легко залишатися в безпеці в Інтернеті», щоб зробити повідомлення більш позитивними та зрозумілими. Завдання для вищої освіти полягає в тому, щоб зберегти це повідомлення, розтягнувши його на інші 11 місяців року. Простіше кажучи, кібербезпека — це не «одна і готова» пропозиція. Кампуси повинні усвідомлювати ризики, розуміти витрати, збирати необхідні ресурси та розробляти креативні, стійкі плани комунікації.

ЧОМУ ВИЩА ОСВІТА БІЛЬШ ВРАЗЛИВА ДО АТАК?

Існує цілий ряд причин того, що університети стають більш уразливими до кібератак. По-перше, академічне середовище вже давно пропагує ідею свободи слова, досвіду та доступу. У цьому середовищі суворі протоколи кібербезпеки могли бути реалізовані неправильно. Зокрема, в академічних дослідженнях деякі викладачі можуть бути стійкими до кіберзахисту, стурбовані тим, що це може вплинути на їхній безперешкодний доступ до Інтернету та даних. колонці в The Chronicle of Higher Education Як зазначалося у червні, «Коледжі можуть бути особливо вразливими до кібератак. Університети побудовані на принципах відкритого дослідження та вільного обміну інформацією, які не завжди збігаються з найкращими практиками інформаційної безпеки».

Кіберзлочинці усвідомлюють ці потенційні прогалини в безпеці та будуть агресивно використовувати їх, особливо якщо кіберзахист відсутній або не є пріоритетом університетського містечка. Коледжі та університети вже давно мають доступ до Інтернету, а сама культура студентського містечка, можливо, протистояла сильному кіберконтролю. З переходом на цифрові платформи та стрімким зростанням кількості пристроїв Інтернету речей проблеми з захистом мережі стають більшими, ніж раніше, особливо якщо IT-послуги та процеси децентралізовані.

ЯКІ ВИТРАТИ?

Витрати на порушення кібербезпеки можуть бути значними, включаючи не лише фінансові втрати, але й репутацію установи, збої в роботі, втрати в дослідженнях, а також цивільні та кримінальні юридичні небезпеки.

Фінансові витрати від кібератаки вражають. У 2022 році у Звіті ФБР про злочини в Інтернеті було підраховано 10,2 мільярда доларів загальних збитків від кібератак, порівняно з 6,9 мільярда доларів у 2021 році. У звіті також зазначається, що «не всі, хто стикався з інцидентом з програмами-вимагачами, повідомили в IC3 [Центр скарг на злочини в Інтернеті].» У звіті також застерігається, що «програми-вимагачі залишаються серйозною загрозою для суспільства та нашої економіки». Це викликає занепокоєння як для бізнесу, так і для освітнього сектору, оскільки штучний інтелект має потенціал зробити атаки ще гіршими.

ПОТОЧНІ КІБЕРНЕБЕЗПЕКИ

Існує широкий спектр кіберзагроз для вищої освіти, зокрема фішинг, програми-вимагачі та ін’єкції SQL (мови структурованих запитів). Один із відомих типів фішингу називається «фішингом», який виникає, коли електронний лист, який здається дійсним, але не є таким, спрямований на конкретну особу чи відділ в організації. Кіберзлочинці досягли успіху у створенні «подібних» електронних листів, які надсилаються нічого не підозрюючим особам. У серпні новинний веб-сайт із технологій безпеки Security Today повідомив, що спільне дослідження професора Стенфордського університету та охоронної фірми Tessian показало, що 88 відсотків випадків витоку даних викликані помилками співробітників. Хоча в жовтневому кіберповідомленні сказано: «Легко залишатися в безпеці в Інтернеті», нічого не підозрюючим людям також легко натискати шкідливі посилання, не зупиняючись, щоб перевірити, чи вони справжні.

Ще однією зростаючою проблемою для вищої освіти є програми-вимагачі, які можуть шифрувати цінну інформацію та робити її марною під загрозою «сплати викупу». Подія програми-вимагача в університетському містечку може призвести до зупинки роботи, витоку важливої інформації та знищення установи та особистої репутації. Згідно зі звітом компанії Zscaler, що займається хмарною безпекою, за 2023 рік, «у 2023 році число атак програм-вимагачів зросло більш ніж на 37

відсотків... порівняно з попереднім роком, причому середній викуп підприємства перевищив 100 000 доларів США, а середній попит склав 5,3 мільйона доларів». Хоча найбільш цільовими секторами були виробництво, послуги та будівництво, опитування 2023 року, проведене британською компанією з кібербезпеки Sophos, задокументувало, що в минулому році «79 відсотків коледжів сказали, що зазнали атаки програм-вимагачів. Це зросло порівняно з 64 відсотками у 2022 році та є одним із найвищих показників серед усіх відстежуваних галузей». У травні Higher Ed Dive зазначив: «Більше половини вищих навчальних закладів, які зазнали атак програм-вимагачів, заплатили викуп за повернення своїх даних». Це може бути необхідним рішенням для деяких установ, які могли собі це дозволити або мали щастя мати кіберстрахування. На жаль, сплата викупу не гарантує, що ваші дані буде розблоковано.

Інша небезпека, ін’єкції SQL, виникає, коли зловмисник може обійти захист паролем на веб-сайті чи в програмі. Як пояснюється на платформі фрілансерів Toptal, «ін’єкції SQL працюють шляхом використання слабких місць у коді, що лежить в основі сторінок введення (таких як сторінки для входу з іменем користувача та паролем), і змушують дану базу даних повертати конфіденційну інформацію». Якщо кампус не має належного кіберзахисту та керування своїми базами даних, їхні дані піддаються серйозному ризику бути скомпрометованими або викраденими.

КІБЕРЗВ'ЯЗОК

Донести до студентів важливість кібербезпеки може бути складно. Важливо навчитися створювати повідомлення для певної аудиторії та використовувати найефективніший канал комунікації. Може бути корисно відстежувати кібер-повідомлення за допомогою графічно багатих комунікаційних платформ, таких як Mail Chimp або Constant Contact. Досягти 40-відсоткового рівня відкритих електронних листів – це досить добре, але навіть тоді 60 відсотків цільової аудиторії навіть не відкривали електронний лист. Спілкування електронною поштою – не найефективніший спосіб підключення до студентської аудиторії.

Створення публікацій у соціальних мережах, плакатів і дверних вішалок, які пропагують ефективну поведінку в галузі кібербезпеки, значно додасть загального

обміну повідомленнями на кампусі. Розгляньте можливість проведення особистих відкритих форумів і підключення до гуртожитків, а також викладачів і студентських органів управління. Також корисно використовувати інноваційні відеоповідомлення. Один із ефективних прикладів відео на YouTube, «The CyberZone The Link to Disaster», використовує теми фільмів для залучення аудиторії. Ефективне програмування кібербезпеки — це набагато більше, ніж місячне дотримання — це річна пропозиція. Плануйте це». ***(Jim A. Jorstad. Opinion: Cybersecurity Month Should Be Year-Round // e.Republic (https://www.govtech.com/education/higher-ed/opinion-cybersecurity-month-should-be-year-round). 16.10.2023).***

***

«Агентство, створене під керівництвом Дональда Трампа для захисту виборів і ключової інфраструктури США від іноземних хакерів, зараз відбивається від дедалі більш інтенсивних загроз з боку крайніх правих республіканців, які стверджують, що це зайшло занадто далеко, і шукають способи приборкати це.

Ці законодавці наполягають на тому, що робота Агентства з кібербезпеки та безпеки інфраструктури, спрямована на боротьбу з дезінформацією в Інтернеті під час виборів, виокремлює голоси консерваторів і порушує права на свободу слова — твердження, яке агентство рішуче заперечує, а адміністрація Байдена оскаржує в суді. Звинувачення почалися після виборів 2020 року та наростають перед 2024 роком, і тепер законодавці закликають до серйозних скорочень в агентстві.

«CISA відверто порушила Першу поправку та вступила в змову з Big Tech, щоб цензурувати виступи звичайних американців», — сказав Ренд Пол (R-Ky.), високопоставлений член Комітету внутрішньої безпеки Сенату, який контролює CISA, у заяві для ПОЛІТИКО.

Боротьба навколо CISA підкреслює ще один спосіб, яким твердження Трампа про фальсифікацію виборів відбиваються у 2024 році. І хоча жорсткі праві сьогодні не мають достатньо голосів, щоб скасувати фінансування CISA, зростаюча негативна

реакція на нього змушує прихильників хвилюватися, що фракція жорстких правих може перешкодити агентство в найближчі роки — підриваючи його зусилля не тільки щодо забезпечення майбутніх виборів, але й захисту ключових американських і федеральних мереж від великих хакерських атак.

CISA мала широку двопартійну підтримку в Конгресі, коли законодавці прийняли закон про створення агентства в 2018 році. На церемонії, де Трамп підписав цей закон, він назвав це «дуже, дуже важливим законодавством» для захисту США як від хакерів національних держав, так і від кіберзлочинців.

Але коли Кріс Кребс, тодішній голова CISA, розвінчав заяви Трампа про фальсифікації виборів 2020 року, президент звільнив його. І відколи Республіканська партія взяла контроль над Палатою представників у 2022 році, республіканці-однодумці посилили контроль над агентством.

У червні юридичний комітет Палати представників під керівництвом республіканців, очолюваний Джимом Джорданом з Огайо, опублікував палкий звіт, назвавши CISA «нервовим центром» цензурного апарату федерального уряду. Потім наприкінці вересня понад 100 республіканців у Палаті представників почали невдалу спробу різко скоротити бюджет CISA у 3 мільярди доларів на 25 відсотків. А на початку цього місяця генеральні прокурори Республіканської партії, які подали до суду на CISA та інші федеральні агентства через можливі порушення Першої поправки, домоглися нових обмежень проти нього.

У п’ятницю Верховний суд тимчасово заморозив ці обмеження, дозволивши уряду продовжувати працювати з платформами соціальних мереж, доки він не матиме можливості переглянути справу.

Окрім безпеки виборів, CISA захищає державні комп’ютерні мережі та важливі установи приватного сектора, як-от виробники хімікатів, школи та лікарні, від фізичного та цифрового саботажу. Відповідно до внутрішніх даних, наданих агентству POLITICO, з бюджету агентства в 3 мільярди доларів приблизно 45 мільйонів виділяються на безпеку виборів. Частина з них, менше ніж 2 мільйони доларів, йде на боротьбу з іноземним впливом і дезінформацією.

«Позбавлення фінансування CISA викликає кібератаку Китаю та/або Росії проти нашого уряду та тисячі дорогих атак програм-вимагачів проти малого та середнього бізнесу», — сказав Ерік Суолвел (штат Каліфорнія), високопоставлений член кіберпідкомітету Комітету внутрішньої безпеки. – йдеться в текстовому повідомленні.

Розчарування консерваторів щодо CISA походить від роботи, розпочатої п’ять років тому, щоб запобігти бренду операцій впливу в Інтернеті, які російські хакери розгорнули напередодні виборів 2016 року.

До виборів 2022 року CISA координувала регулярні дзвінки між платформами соціальних мереж і федеральними агентствами щодо дезінформації, пов’язаної з виборами. Під час виборів 2020 року воно також застосовувало практику, відому як «перемикання», під час якої агентство пересилало підказки про містифікації, отримані від державних і місцевих виборчих органів, таким компаніям, як Facebook і X (раніше Twitter).

Зараз консерватори стверджують, що діяльність стала димовою завісою для лівої урядової цензури. У Конгресі та в судах вони стверджують, що тиск з боку федеральних агентств, таких як CISA, спонукав компанії соціальних медіа обмежити поширення інформації, яка сприймалася як шкідлива для кампанії Джо Байдена, наприклад, історії про Хантера Байдена.

Ознакою проблем для агентства, яке колись могло похвалитися сильною двопартійною підтримкою, 108 республіканців підтримали невдалий поштовх скоротити бюджет CISA минулого місяця — майже більшість на конференції.

Прихильники скорочення бюджету включали низку дедалі більш впливових законодавців із жорстким правим настроєм, таких як Джордан і Джеймс Комер (R-Ky.), голова потужного Комітету з нагляду Палати представників. Ті, хто безпосередньо контролює CISA, також підтримали голосування, наприклад, голова Комітету внутрішньої безпеки Марк Грін (R-Техас) та інший член комісії Август Пфлугер (R-Техас).

CISA категорично заперечує звинувачення проти себе. Він стверджує, що діяв лише як посередник і ніколи не чинив тиску на платформи соціальних мереж, щоб

вони піддавали цензурі конкретні публікації. «CISA не цензурувала і ніколи не цензурувала виступи чи сприяла цензурі», — сказав у заяві речник Евері Малліган.

Прихильники CISA також стверджують, що звинувачення є надмірними та застарілими, вказуючи на те, що агентство припинило свою діяльність з комутації напередодні виборів 2022 року. Дехто стверджує, що роль CISA у спростуванні заяв Трампа в 2020 році змусила республіканців жадати відплати.

«Критикувати CISA та це керівництво за те, що сталося в попередній адміністрації, немає сенсу», — сказав колишній конгресмен Джим Ланжевін (DR.I.), давній прихильник агентства, який покинув Конгрес минулого року. Він додав, що сподівається, що той, хто стане спікером Палати представників, «зробить домашнє завдання і по-справжньому подивиться на факти».

У судовій справі проти CISA, порушеній генеральними прокурорами Республіканської Республіки, апеляційний суд, де домінують республіканці, постановив 3 жовтня, що агентство «ймовірно порушило» Першу поправку у своїй взаємодії з компаніями соціальних мереж. Він дійшов висновку, що зусилля агентства були неправомірними, оскільки воно координувало роботу з ФБР, правоохоронним органом, і висловлювало думку щодо достовірності певних публікацій, позначених на платформах соціальних мереж.

Зараз адміністрація Байдена оскаржує постанову, яка обмежує зв’язок CISA з Силіконовою долиною. Але висновки апеляційного суду, які Верховний суд має намір переглянути до червня, все ж надихнули консерваторів.

«Федеральні суди зобов’язали CISA припинити роботу, але довіра, якою CISA зловживала, не може бути відновлена, доки агентство не надасть повного звіту про те, що воно зробило, а Конгрес змінить закон, щоб запровадити суворі покарання для всіх, хто намагається зробити те саме в майбутнє», - сказав Пол у своїй заяві для POLITICO.

Кілька впливових республіканців Палати представників досі підтримують CISA, зокрема Майк Галлахер із Вісконсіна, голова кіберкомітету Комітету Палати представників із питань збройних сил, і Ненсі Мейс із Південної Кароліни, яка очолює кіберпідкомітет Комітету з нагляду Палати представників. Нещодавно

Палата представників прийняла законопроект про щорічні асигнування, згідно з яким фінансування агентства буде приблизно на рівні з тим, чого бажав Байден у бюджетному запиті цього року.

Тим не менш, прихильник CISA Ендрю Гарбаріно (RN.Y.), голова кіберпідкомітету Комітету внутрішньої безпеки, висловив стурбованість поширенням «дезінформації» всередині його партії.

«У той час, коли Америка стикається зі складнішими кіберзагрозами, ніж будь-коли раніше, спроба зруйнувати наше головне цивільне агентство з кібербезпеки є небезпечною», — сказав він у заяві для POLITICO. «Ті з нас, хто підтримує CISA, працюють над навчанням членів, які проголосували за скорочення фінансування CISA, щоб забезпечити продовження роботи з кібер- і фізичної стійкості».

Основне занепокоєння таких законодавців, як Гарбаріно, і самого агентства полягає в тому, що значні скорочення фінансування перешкоджатимуть іншим ключовим аспектам його мандату, як-от захист державних мереж, шкіл і приватних лікарень від злочинних груп програм-вимагачів.

«Оскільки наша країна продовжує стикатися зі складними та невідкладними кіберзагрозами, фінансування на рівнях, нижчих за ті, які запитувала адміністрація, поставило б під серйозний ризик безпеку критичної інфраструктури, на яку американці покладаються щодня», — сказав Малліган з CISA.

Джеррі Конноллі (D-Va.), високопоставлений член Комітету з нагляду за кібернетичними засобами Палати представників, сказав POLITICO: «Будь-які скорочення агентства, цілеспрямовані чи масштабні, завдадуть відчутної шкоди нашій здатності захищати критично важливі інфраструктури та підтримки системи безпеки в федеральному уряді». ***(John Sakellariadis. Conservatives are increasingly knives out for the nation's top cyber agency // POLITICO LLC (https://www.politico.com/news/2023/10/22/conservatives-cyber-cisa-politics-00122794?utm_source=flipboard&utm_content=politico%2Fmagazine%2FPolitics). 22.10.2023).***

***

«Відповідність Сертифікації моделі зрілості кібербезпеки (CMMC), структурі Пентагону для оцінки кібербезпеки постачальників, є настільки складним, як це звучить.

Але, згідно з дослідженням Merrill Research, проведеним на замовлення компанії з кібербезпеки CyberSheath, багато оборонних підрядників навіть не дотримуються цих стандартів, оскільки переглянута версія CMMC Міністерства оборони поспішає до впровадження.

Структура CMMC була створена Доповненням до федеральних оборонних закупівель (DFARS) 2017 року. Однак це не було остаточне правило, і поки це не станеться, компанії можуть проходити лише добровільне оцінювання. Пентагон готується випустити оновлену версію CMMC 2.0 для відгуків промисловості до кінця 2023 року з фактичною датою впровадження наступного року. CMMC зазнав кілька переглядів, але чернетки версій вказують на те, що CMMC 2.0 включатиме обов'язкову сторонню або державну сертифікацію для постачальників, які обробляють більш конфіденційну інформацію, а також завершать механізми забезпечення виконання контрактів.

DFARS визначає відповідність очікуванням CMMC як 110 балів за шкалою під назвою Система ризиків ефективності постачальника (SPRS). CyberSheath каже, що оцінка 70 вважається «досить хорошою» в оборонній спільноті. Проте дані CyberSheath показують, що середній бал, наданий основними та/або субпідрядниками Міністерства оборони, майже не змінився з липня та серпня 2022 року, коли він становив -23, до -15 у версії опитування за квітень та травень 2023 року.

З 2022 по 2023 рік відсоток федеральних постачальників оборонної продукції, які заявили, що надали результати SPRS, впав з 46% до 36%. Ті постачальники, які стверджують, що відповідають стандартам CMMC за допомогою самосертифікації, найменш суворого методу вимірювання відповідності, зросли з 71% до 81%. CyberSheath зазначив у звіті, що «значно менше повідомили про відповідність через середню або високу оцінку».

Минулого року CyberSheath виявив «надзвичайний рівень невідповідності», — сказав IT Brew генеральний директор компанії Ерік Нунан. «Отже, ми майже там, де були рік тому, а це не дуже гарне місце».

У 2022 році лише 19% підрядників повідомили, що впровадили рішення для керування вразливістю, тоді як лише 25% мали безпечні рішення для резервного копіювання IT. Обидва є показниками SPRS.

Нунан сказав IT Brew, що підрядники отримали багато попереджень щодо підвищення стандартів, включаючи ухвалення DFARS, Національної стратегії кібербезпеки та нових правил Комісії з цінних паперів і бірж, які вимагають від публічних компаній розкривати інвесторам більше інформації про кібербезпеку.

Причина того, що оцінки не вищі, полягає в тому, що «сьогодні ніхто не стежить за дотриманням вимог», — сказав Нунан, і підрядники зробили «успішну ставку протягом багатьох років», що агенції, що надають контракти, не вагатимуться порушувати звичайний бізнес.

Нунан каже, що CMMC ускладнить підрядникам, які не можуть задовольнити вимоги кібербезпеки, завершити контракти та отримати гроші.

«Поки Міністерство оборони не скаже: «Якщо ви не відповідатимете вимогам, ми не укладатимемо контракт», і це фактично завадить доходам, доки цей перемикач не буде переключено, ми не побачимо кращих результатів», — Нунан. додано.

Дослідження показує, що оборонні підрядники звертають увагу, оскільки вони почали усвідомлювати, що відповідність CMMC може бути складнішою, ніж вони собі уявляли. Сімдесят відсотків оцінили свої труднощі в розумінні того, як досягти та підтримувати вимоги CMMC, на 7 із 10 або вище.

На думку Нунана, дотримання CMMC може лякати з кількох сторін. Окрім витрат на фактичне підвищення балів SPRS, постачальники також можуть зіткнутися з витратами, пов’язаними з документацією відповідності. За його словами, менші підрядники або ті, хто не підготувався до нових правил, можуть бути «дуже перевантажені».

У 2020 році Міністерство оборони оцінило середню річну вартість відповідності вимогам CMMC для невеликих організацій у діапазоні від приблизно

1000 доларів США на найнижчому рівні до 483 000 доларів США на найвищому рівні, але Національна оборона повідомила, що у 2021 році більші підрядники оцінили витрати в мільйони.

«Великі прем'єри [підрядники], імена яких ми всі знаємо, мають цілу армію людей, які роблять це досить ефективно всередині», — попередив Нунан. «Але їхні ланцюжки постачання – ні. Якщо у них є один IT-спеціаліст, їм, мабуть, пощастило».

Нунан не очікує «драматичних» репресій, коли CMMC стане остаточним правилом, вказуючи, що деякі версії вимог уже містяться в багатьох їхніх контрактах протягом 8 років.

«Думаю, ми будемо вражені, коли якимось чином вони знайдуть спосіб виконати ці мінімальні вимоги безпеки», — підсумував Нунан. Він також додав, що Пентагон просто не натисне перемикач: «Не буде [так, що] всі понад 300 000 контрактів будуть перевірені за одну ніч».

Натомість, сказав Нунан, він вважає, що підрядники, які все ще відстають, зіткнуться з еквівалентом плану коригувальних дій.

«Отримайте оцінку, задокументуйте свої недоліки, вирушайте на шлях відповідності», — підсумував Нунан. «З мого досвіду, міністерство оборони очікує саме цього».

Речник Міністерства оборони, командувач Тімоті П. Горман сказав IT Brew, що «не може розглянути жодних істотних аспектів» майбутнього правила CMMC, «доки процес нормотворення не буде завершено». Управління з питань інформації та регулювання Він надіслав IT Brew до списку відкритих справ DFARS, у якому вказано продовжений термін для публікації звіту Радою з питань оборонних закупівель – 25 жовтня». ***(Tom McKay. Defense contractors are way behind on meeting upcoming cybersecurity standards // Morning Brew, Inc. (https://www.itbrew.com/stories/2023/10/20/defense-contractors-are-way-behind-on-meeting-upcoming-cybersecurity-standards?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 20.10.2023).***

***

«У звіті iomart і Oxford Economics показано, що британським підприємствам важко збалансувати бюджет безпеки на тлі стрімкого зростання кіберінцидентів

Новий звіт проливає світло на щоденну боротьбу британських компаній та їхніх IT-команд, які мають справу зі зростаючою кількістю «кіберінцидентів».

У новому звіті під назвою «Стан кібербезпеки у Великій Британії 2023» від постачальника безпечних хмарних та керованих IT-послуг iomart і Oxford Economics було опитано 500 керівників Великобританії (з понад 1000 співробітників).

У звіті встановлено, що за останні 12 місяців підприємства Великобританії стикалися в середньому з 30 кіберінцидентами, що на 25 відсотків більше, ніж минулого року.

Бюджетний тиск

І незважаючи на те, що організації витрачають понад 40 000 фунтів стерлінгів на рік на заходи кіберзахисту, такі як оцінка вразливості, тестування на проникнення та залучення червоних команд, звіт показує, що більше чверті (27 відсотків) вважають, що їх бюджет на кібербезпеку недостатній.

Дійсно, згідно зі звітом iomart і Oxford Economics, обмежені бюджети залишаються найбільшою перешкодою для покращення кібербезпеки.

У звіті також виявлено, що зростання вартості страхових внесків у сфері кіберстрахування є одним із найбільших фінансових витрат, причому 70 відсотків компаній відзначають зростання за останні два роки.

Це не перший раз, коли проблема кіберстрахування позначається.

Наприклад, у серпні 2022 року лондонський Lloyd's захистив свій крок щодо обмеження системного ризику від кібератак, вимагаючи, щоб у страхових полісах було звільнення від кібератак на національних державах.

Потім у грудні минулого року Маріо Греко, виконавчий директор страхової компанії Zurich, однієї з найбільших страхових компаній Європи, попередив, що

кібератаки, а не природні катаклізми, скоро стануть «неможливими для страхування».

Кіберневі сліпі зони

Але звіт iomart і Oxford Economics показав, що разом із вартістю відновлення та іншими витратами бізнесу, такими як зростання вартості енергії, розтягнутий бюджет спричиняє сліпі плями в кіберстратегіях бізнесу.

Наприклад, у звіті було виявлено, що лише 37 відсотків респондентів мають безпеку, вбудовану в усі їхні бізнес-процеси та функції, тоді як 14 відсотків визнали, що безпека вирішується лише в окремих випадках або за потреби.

Тим часом під час пандемії Covid-19 41 відсоток організацій були змушені пожертвувати кібербезпекою, щоб зберегти світло.

У звіті також виявлено, що брак ключових навичок залишається однією з головних проблем у боротьбі зі зростанням кіберзагроз. Настільки, що 30 відсотків кіберперсоналу визнають, що зараз стикаються з виснаженням.

Цей тиск також означає, що менше половини компаній впевнені у своїй здатності впоратися з найбільшими загрозами, з якими стикаються організації, включаючи фішинг (56 відсотків) і шкідливе програмне забезпечення (55 відсотків).

ШІ смакує?

Незважаючи на ці виклики, компанії оптимістично дивляться на роль нових технологій, таких як ШІ та ML.

Більше третини (38 відсотків) компаній вважають, що використання штучного інтелекту та машинного навчання стане основною тенденцією в кібербезпеці протягом наступних двох років, зокрема для підтримки перевірки електронної пошти (78 відсотків) і контекстної аналітики (69 відсотків).

«Наш останній звіт про безпеку разом з Oxford Economics — це температурна перевірка кіберпроблем, з якими стикаються підприємства», — сказала Люсі Даймс, генеральний директор iomart. «Очевидно, що загроза кіберзлочинності зростає, але існує брак впевненості в здатності організацій захистити себе від неї».

«На це впливає багато факторів, від зростання витрат на енергію та підвищення страхових премій до нестачі навичок і виснаження персоналу, що створює величезні проблеми для компаній», — сказав Даймс.

«Хоча це може бути так, є способи пом'якшити цей тиск за допомогою розробки ефективних стратегій і впровадження нових технологій, таких як штучний інтелект», – підсумував Даймс. «Співпраця з надійними партнерами також може гарантувати, що компанії мають адекватні кіберстратегії, адаптовані до їхніх бізнес-потреб і завдань».

Кіберзагроза, з якою стикаються британські організації, була чітко підкреслена урядом Великобританії цього року після того, як секретар кабінету міністрів Олівер Доуден попередив, що групи кіберзлочинців, пов'язані з Росією, є «ідеологічно вмотивованими» і хочуть «порушити або знищити» Великобританію. ***(Tom Jowitt. UK Security Budgets Under Strain As Cyber Incidents Soar // NetMedia International (https://www.silicon.co.uk/security/cyberwar/uk-security-budgets-under-strain-as-cyber-incidents-soar-532668). 04.10.2023).***

***

«Дипломований інститут інформаційної безпеки (CIISec) забезпечив державне фінансування для підтримки студентів у 2023-24 CyberEPQ – першій і єдиній у Великій Британії Extended Project Qualification (EPQ) з кібербезпеки.

Фінансування є частиною урядової Національної кіберстратегії вартістю 2,6 мільярда фунтів стерлінгів, спрямованої на захист і популяризацію Великобританії в Інтернеті, а також на розвиток кібернавичок. Він є наслідком успішного пілотного періоду з когортою 2022-2023 років, який націлений на учнів шостих класів у 10 об'єднаних мерських органах Англії. Усі залучені студенти отримали оцінки, які кваліфікували їх для членства в CIISec, причому 68% отримали оцінки від A* до B.

Цього року CIISec планує зарахувати щонайменше 400 студентів, що втричі більше, ніж у 2022-2023 роках, і продовжувати збільшувати кількість з року в рік. І CIISec, і уряд Великої Британії прагнуть залучити більш різноманітний пул талантів у галузь кібербезпеки – за допомогою таких методів, як зарахування учнів із

державних шкіл у районах соціальної депривації. Фінансування від DSIT разом із допомогою корпоративних партнерів CIISec стане вирішальним елементом у цьому, оскільки CIISec вже збільшив кількість державних шкіл, залучених до CyberEPQ, на 56% у 2022-2023 роках. Це поряд із урядовими ініціативами, такими як Cyber Explorers і програма Upskill in Cyber.

Аманда Фінч, генеральний директор CIISec, прокоментувала: «Ми раді розпочати наступний етап програми CyberEPQ, яка обіцяє зіграти ключову роль у залученні та вихованні різноманітних талантів у галузі кібербезпеки. Постійна підтримка з боку DSIT і відданість наших партнерів і членів будуть важливими для досягнення цих цілей».

Енді Пейп, керівник відділу комп'ютерних наук у школі Томаса Талліса, прокоментував: «У перший рік проведення CyberEPQ ми вже побачили, наскільки курс був корисним для наших студентів. Студенти вибирали широкий спектр тем есе, які дійсно зацікавили їх допитливість. Деякі з їхніх презентацій виглядали так, ніби ми сиділи на тренінгах з експертами з кібербезпеки. Багато хто зараз планує майбутнє в галузі кібербезпеки. Я не можу дочекатися, щоб побачити, як розвиватиметься наша наступна група протягом курсу».

Щоб підтримувати міцні стосунки зі школами, заохочувати активну участь і забезпечувати високі показники успішності, CIISec найняв спеціального координатора зі зв'язків зі школами, який буде керувати та підтримувати як вчителів, так і учнів протягом усієї програми. CIISec також провів комплексний перегляд своєї програми, плануючи оновити навчальну програму, щоб відобразити досягнення в таких сферах, як штучний інтелект, квантові обчислення та блокчейн.

Кваліфікація CyperEPQ, підкріплена власною системою навичок CIISec, пропонує навчання за темами з усього спектру кібербезпеки, від історії обчислювальної техніки та криптографії до цифрової криміналістики та людського фактора в кібербезпеці. Студенти також отримають доступ до програми розвитку CIISec, розробленої для підтримки людей на всіх етапах їхньої кар'єри, від учнівства до керівних посад. Зрештою, вони можуть стати частиною зростаючої кіберіндустрії Великобританії, яка наразі коштує 10,5 мільярдів фунтів стерлінгів і налічує 58 000

людей…» ***(Cyber security qualification gains funding following pilot // PSi Ltd (https://educationbusinessuk.net/news/04102023/cyber-security-qualification-gains-funding-following-pilot). 04.10.2023).***

***

«Рада з кібербезпеки Великої Британії оголосила про першу в країні когорту дипломованих фахівців з кібербезпеки після запуску пілотних схем управління кібербезпекою та управління ризиками та безпечної системної архітектури та дизайну минулого року. Понад 100 практиків, які завершили пілотні схеми, зараз зареєстровані в раді на рівні дипломованого, основного або асоційованого рівня.

Після успішної реалізації цих двох пілотних програм обидві спеціальності будуть відкриті для застосування в більш широкому секторі, повідомила рада. Наразі тривають пілотні програми з інших спеціалізацій, включаючи тестування безпеки та аудит і забезпечення.

Метою ради є встановлення загальновизнаного професійного стандарту для сектору кібербезпеки Великобританії, щоб надати професіоналам можливість отримати дипломований статус за 16 спеціалізаціями, привівши кібербезпеку у відповідність до інших визнаних професій, таких як бухгалтерія, інженерія та юрист.

Триває робота з приведення галузі кібербезпеки у відповідність до інших секторів

Рада з кібербезпеки Великобританії є власником Королівської хартії та єдиного органу в світі, який може присуджувати особам статус дипломованого спеціаліста з кібербезпеки.

«Рада прагне працювати із зацікавленими сторонами в усій галузі з метою створення кіберсектору світового рівня саме тут, у Великобританії», — сказав професор Саймон Хепберн, генеральний директор Ради кібербезпеки Великобританії. «Наша безперервна робота з пілотування спеціалізацій, щоб привести галузь у відповідність з іншими секторами та регулювання кваліфікацій у

космосі є життєво важливою для нашої мети допомогти уряду Великобританії зробити цю країну найбезпечнішим місцем для життя та роботи в Інтернеті».

Дипломований інститут інформаційної безпеки (CIISec) є першим ліцензованим органом ради. «Ми вже прийняли в індустрію понад 40 нових спеціалістів і з нетерпінням чекаємо на залучення ще багатьох», — прокоментувала Аманда Фінч, генеральний директор CIISec.

Підвищення професіоналізму галузі та демонстрація того, що кібербезпека — це кар'єра з реальними можливостями для будь-кого, будь-якого походження, будь-якого віку, були рушійною силою CIISec із самого початку та ключовим пріоритетом для її членів і професії в цілому, додала вона. «Ми заохочуємо професіоналів, які хочуть продемонструвати свій досвід, тих, хто хоче розпочати або побудувати свою кар'єру в галузі кібербезпеки за спеціалізаціями архітектури та дизайну безпечної системи, аудиту та гарантій, управління та управління ризиками, або будь-кого, кого цікавить галузь, зв'язатися з нами. нас і отримати всі переваги однієї з найбільш захоплюючих, повноцінних кар'єр…» ***(Michael Hill. UK Cyber Security Council announces first cohort of chartered cybersecurity practitioners // CSO (https://www.csoonline.com/article/654956/uk-cyber-security-council-announces-first-cohort-of-chartered-cybersecurity-practitioners.html). 09.10.2023).***

***

«За оцінками міжнародної професійної організації в галузі інформаційних технологій, Європі потрібно до півмільйона додаткових працівників кібербезпеки, щоб протистояти зростаючій загрозі кібератак.

Згідно з дослідженням американської компанії Isaca, дефіцит технічних працівників у ЄС наразі становить від 260 000 до 500 000.

Цей висновок підтверджує нещодавнє дослідження Cyber Ireland, яке підрахувало, що Ірландії потрібно додатково 1000 працівників кібербезпеки щорічно.

Проте уряд висловив упевненість у здатності ірландського технологічного сектора протистояти шторму.

Дефіцит виникає в той час, коли фахівці з кібербезпеки кажуть, що вони відчувають збільшення кількості кібератак, причому 52 відсотки опитаних сказали, що вони вирішували більше атак, ніж рік тому.

Нездатність проводити регулярну оцінку кіберризиків була названа Isaca фактором, що сприяє збільшенню кількості атак. Дослідження показало, що лише 8 відсотків опитаних компаній проводять щомісячну оцінку, тоді як 40 відсотків проводять щорічну оцінку.

Частково це пов'язано з нестачею персоналу: 62 відсотки респондентів заявили, що не мають достатнього персоналу з кібербезпеки.

«Наші результати показують, що компанії все ще намагаються знайти потрібних людей з потрібними навичками для управління кібербезпекою. Оскільки кібератаки зростають, якщо ми не вирішимо ці проблеми та не усунемо прогалини, підприємства, екосистеми ланцюгів постачання та органи державного сектору можуть опинитися під загрозою через відсутність життєво важливого захисту, виявлення, реагування та відновлення», – Кріс Дімітріадіс, глобальний спеціаліст. сказав головний стратегічний директор Isaca.

«Підприємства не існують ізольовано від своїх клієнтів чи інших організацій у їхній мережі, і кібератака на одну частину екосистеми може мати наслідки для всіх інших. Ось чому потрібне цілісне навчання для створення безпечнішого світу».

Ці висновки були зроблені наступного дня після того, як уряд висловив впевненість у здатності Ірландії впоратися з дефіцитом. У понеділок, Taoiseach Лео Варадкар сказав, що частка випускників Ірландії з інформаційно-комунікаційних технологій (ІКТ) вдвічі перевищує середній показник по ЄС.

Говорячи про оголошення про 100 вакансій у сфері технологій у американській аналітичній та цифровій компанії EXL, Варадкар сказав, що боротьба за глобальні таланти «загострюється» як в ірландській економіці, так і в усьому світі, оскільки багато країн наближаються до повної зайнятості.

«Багато країн відчувають нестачу робочої сили, і зростатиме попит на людей, які володіють цифровими та екологічними навичками», — повідомляє Taoiseach.

«Хороша новина полягає в тому, що частка випускників ІКТ в Ірландії зараз більш ніж удвічі перевищує середній показник по ЄС... Але нам доведеться йти в ногу з навколишнім середовищем, яке швидко змінюється. Нам знадобиться більше випускників у правильних сферах, і ми повинні ретельно це планувати». ***(Emmet Ryan. Up to 500,000 staff required to fend off growing cyber security threat to Europe // Business Post (https://www.businesspost.ie/news/up-to-500000-staff-required-to-field-off-growing-cyber-security-threat-to-europe/). 03.10.2023).***

***

«3 жовтня 2023 року Європейська комісія оголосила про публічні консультації щодо проекту імплементаційного регламенту (Проект регламенту), який запроваджує схему сертифікації кібербезпеки на основі європейських загальних критеріїв (EUCC) для продуктів інформаційних та комунікаційних технологій (ІКТ) відповідно до Закону ЄС про кібербезпеку.

Запропонована схема базується на оцінці третьої сторони, тому самооцінка не буде дозволена за цією схемою. Схема EUCC передбачає сім рівнів забезпечення оцінювання (EAL), узгоджених із встановленими міжнародними стандартами. Він базується на каталозі функціональних вимог безпеки та вимог до гарантії безпеки, що містяться в Загальних критеріях оцінки безпеки ІКТ, як викладено в стандарті ISO EN ISO/IEC 15408 (Загальні критерії), і дотримується Загальної методології оцінювання ІКТ, встановленої у стандарті ISO EN ISO/IEC 18045. EUCC використовує сімейство оцінки вразливості Common Criteria AVA_VAN, компоненти з 1 по 5, які вказують на ступінь оцінки, що виконується для визначення рівня стійкості продукту до потенційної можливості використання недоліків або слабкі сторони. Схема EUCC встановлює знак і етикетку для сертифікованого продукту ІКТ, що демонструє його надійність і дозволяє користувачам зробити усвідомлений вибір. Сертифікат EUCC видається максимум на п’ять років, якщо національний орган із сертифікації кібербезпеки не затвердить довший термін дії.

Схема EUCC дозволяє сертифікувати продукти ІКТ відповідно до цільової безпеки, яка може бути визначена заявником або може містити сертифікований

профіль захисту, що охоплює категорію продуктів ІКТ. Проект Регламенту передбачає два види органів з оцінки відповідності: засоби оцінки безпеки ІТ (ITSEF) для діяльності з калібрування та тестування продукту ІКТ та органи сертифікації для діяльності з сертифікації та перевірки. Схема EUCC встановлює спеціальні вимоги до органу сертифікації та ITSEF, які включають акредитацію, авторизацію, управління компетентністю та технічні можливості.

Схема EUCC вимагає від заявника на сертифікацію надати органу сертифікації та ITSEF всю інформацію, необхідну для сертифікаційної діяльності, включаючи докази, документацію, посилання на їхній веб-сайт, що містить додаткову інформацію про кібербезпеку, і опис їх управління вразливостями. та процедури розкриття інформації. У схемі EUCC застосовуються процедури управління вразливістю та розкриття інформації відповідно до стандартів і найсучасніших документів; він також вимагає від власника сертифіката проведення аналізу вразливості та звітування органу сертифікації та національному органу сертифікації кібербезпеки. Передбачені умови та процедури перевірки сертифіката EUCC, яку може запросити власник сертифіката, орган сертифікації або національний орган сертифікації кібербезпеки.

Схема EUCC визначає дії з моніторингу та коригувальних заходів, які повинні бути вжиті органом сертифікації, ITSEF, власником сертифіката та національним органом сертифікації кібербезпеки у разі потенційних проблем невідповідності або вразливості, що впливають на сертифікований продукт ІКТ.

Схема EUCC відводить важливу роль Європейській групі сертифікації кібербезпеки та Агентству ЄС з кібербезпеки (ENISA) у підтримці схеми, затвердженні та публікації найсучасніших документів, а також наданні вказівок і рекомендацій.

У додатках до проекту Регламенту встановлюються додаткові детальні вимоги до, зокрема:

зміст сертифіката EUCC;

підтримання безперервності впевненості;

проведення переоцінки у зв'язку зі зміною середовища загрози сертифікованого продукту;

проведення аналізу впливу внаслідок змін у сертифікованому продукті або категорії продукту;

управління латками;

зміст звіту про сертифікацію та

експертне оцінювання органу сертифікації.

Схема EUCC передбачає можливість укладення угод про взаємне визнання з третіми країнами за певних умов і гарантій.

Консультація відкрита до 30 жовтня 2023 року.

Остаточна версія регламенту очікується в 4 кварталі 2023 року та почне діяти через 12 місяців після набрання чинності. Після того, як EUCC стане застосовним, усі національні схеми сертифікації кібербезпеки та відповідні процедури для ІКТ-продуктів і ІКТ-процесів, на які поширюється EUCC, припинять свою дію, оскільки вони застосовують стандарти оцінки, охоплені Загальними критеріями. Проект Регламенту називає конкретні національні схеми в цьому відношенні, такі як сертифікація, що надається німецькою BSI Gesetz (ст. 9 (1), (2) і (4)), нідерландська Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB), Указ Франції № 2002-535 від 18 квітня 2002 року про оцінку та сертифікацію безпеки, яку пропонують продукти та системи ІКТ, а також відповідні схеми сертифікації в Іспанії, Італії, Польщі та Швеції». ***(Jane Finlayson-Brown, Thomas Declerck, Nicole Wolters Ruckert. European Commission issues consultation on the European common cybersecurity certification scheme for ICT products // Allen & Overy LLP (https://www.allenovery.com/en-gb/global/blogs/data-hub/european-commission-issues-consultation-on-the-european-common-cybersecurity-certification-scheme-for-ict-products). 11.10.2023).***

***

«Нове дослідження від Thales показує, наскільки споживачі не вживають основних заходів кібербезпеки, піддаючи ризику людей і компанії.

Дослідження понад 2000 громадян Великої Британії розглядає деякі недоліки від імені як споживачів, так і компаній, висвітлюючи деякі ключові сфери, які потребують уваги.

Заголовком звіту є те, що майже половина (47%) британців зізнаються, що підписали умови та умови, не прочитавши їх належним чином, ризикуючи своєю безпекою та конфіденційністю в Інтернеті.

Ми не можемо навіть забезпечити базову кібербезпеку, йдеться у звіті

За словами Thales, споживачі виявляють, що сторінки з положеннями та умовами надто складні для сприйняття. Більше половини (57%) висловили занепокоєння з приводу навмисного використання заплутаних формулювань, призначених для приховування ключової інформації про використання персональних даних, у той час як багато інших стикаються з простою тривалістю деяких угод.

Ця проста помилка може мати значні наслідки згодом. Наприклад, більше однієї п’ятої не мають уявлення про важливість того, де в світі зберігаються їхні дані, а ще одну п’яту не хвилює, де компанії зберігають свої особисті дані.

Інші основні помилки, які, здається, допускає багато хто з нас, включають прийняття непотрібних файлів cookie та невикористання додаткового захисту облікового запису, наприклад двофакторної автентифікації (2FA).

Технічний директор Thales EMEA Кріс Харріс сказав, що проблема полягає не у недостатній обізнаності, а радше у відчутті приголомшення. Перекладаючи провину зі споживачів, Гарріс сказав:

«Компанії повинні взяти це до уваги та враховувати те, як вони спілкуються з клієнтами щодо того, як захистити їхні дані». ***(Craig Hale. Many of us are giving up on cybersecurity best practices // Future US, Inc. (https://www.techradar.com/pro/many-of-us-are-giving-up-on-cybersecurity-best-practices). 11.10.2023).***

***

«Вибори в Європейському Союзі 2024 року знаходяться під загрозою через чат-боти зі штучним інтелектом і глибокі фейки зображень і відео, заявило в четвер агентство блоку з кібербезпеки ENISA.

У своєму щорічному звіті Threat Landscape, який містить карту загроз кібербезпеці в Європі, спостерігався сплеск чат-ботів штучного інтелекту, дипфейків і подібних технологій. Уряди та приватний сектор — і зокрема засоби масової інформації — мають бути у стані підвищеної готовності перед виборами до Європейського парламенту наступного року, щоб виявляти, розвінчувати та боротися з дезінформацією, створеною штучним інтелектом, в Інтернеті, йдеться в повідомленні.

«Довіра до виборчого процесу в ЄС критично залежатиме від нашої здатності покладатися на інфраструктуру кібербезпеки, а також від цілісності та доступності інформації», — сказав виконавчий директор агентства Юхан Лепассар.

Побоювання щодо поширення дезінформації, створеної ШІ, посилилися в Європі. Подібні дипфейки та інший контент з'являвся під час виборчих кампаній у Польщі та Словаччині протягом останніх тижнів. Цього місяця опозиційний лідер Великобританії Кейр Стармер став мішенню за допомогою аудіозапису, який нібито показує, як він лається на співробітників, який став вірусним, але виявився фальшивим.

Сполучені Штати, Європейський парламент, Великобританія, Нідерланди і, можливо, Україна є одними з демократичних країн, які мають провести вибори в наступні 16 місяців. Ті, хто працює над збереженням чесності виборів, насторожено дивляться на появу генеративного штучного інтелекту як на спосіб розпалити вже сильно поляризовані політичні дебати, загрози іноземного впливу та фейкові новини.

Європейське агентство з кібербезпеки заявило, що виявило три способи, якими хакери зловживали штучним інтелектом, щоб обдурити людей, включаючи використання технології для створення переконливих фішингових електронних листів і повідомлень, які нагадують законні джерела, створення глибоких фейків голосів і використання штучного інтелекту для видобутку даних у зловмисних цілях.

Генрі Ад’єр, запрошений дослідник Кембриджського університету, який спеціалізується на дипфейках, сказав у попередньому інтерв’ю, що «ці [AI] програми раніше були надзвичайно дорогими або важкодоступними для звичайної людини. Зараз вони є в додатках для споживачів, на веб-сайтах, часто безкоштовних або дуже дешевих».

«Безпрецедентний сплеск» програм-вимагачів

Блок спостерігав «безпрецедентний сплеск» кібератак, таких як розподілені атаки типу «відмова в обслуговуванні», щоб знищити веб-сайти, і атаки програм-вимагачів, щоб викрасти дані організацій і вимагати викуп натомість, повідомляє агентство у своєму звіті Threat Landscape.

ENISA зафіксувала понад 2500 кіберінцидентів з липня 2022 року по червень 2023 року, причому 220 з них стосувалися двох або більше країн ЄС. Державне управління та охорона здоров’я були головними цілями — 19 і 8 відсотків, тоді як 6 відсотків усіх хакерів були спрямовані на виробництво, транспорт і фінансовий сектор.

ENISA також виявила, що атаки соціальної інженерії, під час яких хакери використовують підроблені особи, щоб завоювати довіру та доступ до конфіденційних мереж і даних, значно зросли у 2023 році.

«Кіберзлочинці все частіше націлюються на хмарні інфраструктури, мають геополітичні мотиви у 2023 році та розширили свої операції здирництва не лише за допомогою програм-вимагачів, але й безпосередньо націлюючись на користувачів», — йдеться у звіті». ***(Antoaneta Roussi. European election at risk from AI, says EU’s cyber agency // POLITICO (https://www.politico.eu/article/european-union-election-risk-artificial-intelligence-interference-cybersecurity-agency-enisa/?utm_source=flipboard&utm_content=curiouscurator%2Fmagazine%2FEuropean+Spectrum). 19.10.2023).***

***

«Згідно з новим звітом у п'ятницю, з 2019 по 2022 рік кількість оголошень про роботу в сфері кібербезпеки в Індії зросла на 81 відсоток, оскільки на хвилі пандемії Covid-19 з'явилися різні загрози. Відповідно до звіту порталу вакансій Indeed, протягом багатьох років вакансії в сфері кібербезпеки демонструють послідовність у своїй траєкторії зростання.

Однак з вересня 2022 року по вересень цього року кількість оголошень про роботу впала на 25,7 відсотка, що свідчить про суворіші правила, рамки та контроль.

Однак ця зміна не вплинула на зацікавленість шукачів роботи, оскільки за той самий період кліки вакансій зросли на 6%, що свідчить про стійкий інтерес до посад у сфері кібербезпеки, йдеться у звіті.

«Поточний спад кількості оголошень про роботу є тимчасовим етапом, і він підкреслює здатність галузі адаптуватися та розвиватися. Сектор кібербезпеки залишається наріжним каменем технологічного прогресу. Наші дані також підтверджують, що майбутнє має величезний потенціал», — сказав Саші Кумар, керівник відділу продажів Indeed India.

У період з вересня 2022 року по вересень 2023 року спостерігалася невідповідність талантів на 29,9 відсотка, що вказує на зміну в наборах навичок, які шукають роботодавці в динамічному секторі кібербезпеки.

Термін «невідповідність талантів» означає розрив між навичками, які зараз потрібні роботодавцям, і набором навичок наявної робочої сили.

Бенгалуру лідирує на ринку праці в сфері кібербезпеки в Індії з часткою 23,11 відсотка, завдяки своєму статусу головного IT-центру країни.

«Це домінування також можна пояснити насиченим технологічним ландшафтом міста з численними IT-компаніями та стартапами, що підвищує потенціал для кіберзагроз і атак», — йдеться у звіті.

Згідно з провідним органом IT-індустрії Nasscom, очікується, що індійський ринок кібербезпеки зросте до 35 мільярдів доларів до 2025 року, що створить понад 1 мільйон робочих місць». ***(India saw 81% surge in cybersecurity job postings from***

2019-2022: Report // Fusion Media Limited (https://in.investing.com/news/india-saw-81-surge-in-cybersecurity-job-postings-from-20192022-report-3870833). 27.10.2023).

***

Інші країни

«На засіданні в Державній канцелярії Молдови розглянуто проект положення про організацію та діяльність відповідного відомства, яким визначено місію, напрями діяльності, функції, повноваження, в тому числі щодо керівництва Агентства з кібербезпеки. Нове Агентство підпорядковуватиметься Міністерству економічного розвитку та цифровізації, матиме статус юридичної особи публічного права, фінансуватиметься з державного бюджету, а також за рахунок коштів іноземних та місцевих донорів. Агентство відповідатиме за реалізацію державної політики кібербезпеки для забезпечення високого рівня безпеки інформаційних мереж і систем провайдерів послуг, які необхідні для функціонування держави та суспільства. Агентство кібербезпеки відповідатиме за ідентифікацію та облік постачальників послуг; державний нагляд і контроль за дотриманням постачальниками послуг законодавства; національне та міжнародне співробітництво та обмін інформацією у сфері кібербезпеки. Агентство буде єдиною точкою контакту та реагування на кіберінциденти, забезпечуватиме методологічне керівництво та регулювання, а також займатиметься дослідженнями та розробками. Його штат складатиметься з 49 осіб і очолюватиме директор, якого призначатиме міністр економічного розвитку та цифровізації. Річні витрати на заробітну плату персоналу Агентства становитимуть близько 26,3 млн леїв. При цьому персоналу групи реагування на кіберінциденти пропонується надавати конкретну надбавку в розмірі 600% посадового окладу, а решті співробітників – 200%. Персонал агентства повинен буде проходити періодичне навчання. Щоб щорічно готувати 7-8 спеціалістів, потрібно від 390 тис. до 650 тис. леїв на рік. Крім того, значні витрати - близько 10 мільйонів леїв - необхідні для придбання спеціального обладнання та програмного забезпечення. Згідно з пояснювальною

запискою до проекту, головною метою нового Агентства є забезпечення адекватного реагування на кіберінциденти, консолідація кібербезпеки та сприяння вдосконаленню нормативно-правової бази захисту кібербезпеки. Планується запровадити обов'язковий механізм повідомлення про кіберінциденти, зменшити ризики та витрати, пов'язані з кіберзлочинністю. За оцінками авторів проекту, річний збиток від кіберзлочинності в Молдові становить близько 42 мільйонів доларів (виходячи з розрахунку, що середній глобальний збиток, згідно з дослідженням McAfee, становить 0,3% ВВП)». ***(Moldova to establish a Cyber Security Agency // InfoMarket (https://infomarket.md/en/analitics/326845). 03.10.2023).***

***

«Серед глобального зростання загроз кібербезпеці Об'єднані Арабські Емірати (ОАЕ) є опорою стійкості, як зазначено в останньому звіті Acronis Cyberthreat Report 2023. У звіті, представленому на GITEX 2023, одній із найбільших технологічних подій у світі, підкреслюється надійний захист ОАЕ від атак програм-вимагачів, особливого типу кіберзагроз, які включають викрадення даних з метою отримання викупу.

Непохитний захист від кіберризиків

Незважаючи на складний рік для кібербезпеки в усьому світі, коли зростає кількість інцидентів, що спричиняють фінансові труднощі, ОАЕ встановили взірцевий стандарт у захисті свого цифрового середовища. Країна може похвалитися найнижчим рівнем кіберзараження в регіоні – лише 10%, що свідчить про суворі заходи кібербезпеки.

Одним із найважливіших висновків звіту є очікуване зниження загроз програм-вимагачів у регіоні до кінця 2023 року. Ця позитивна тенденція пояснюється проактивними стратегіями кібербезпеки, які застосовуються в ОАЕ та ширшому регіоні GCC.

Зростаючі виклики кібербезпеці

Однак арена кібербезпеки не позбавлена викликів. У звіті наголошується на сплеску різноманітних кібератак, що призвело до значних фінансових наслідків на

Близькому Сході. Зокрема, середня вартість кібератаки на організації в Саудівській Аравії та ОАЕ становить тривожні 6,53 мільйона доларів США, що значно перевищує середній світовий показник.

Крім того, хоча регіон демонструє похвальну стійкість проти програм-вимагачів, фішингові атаки — шахрайські спроби отримати конфіденційні дані — залишаються серйозним викликом, що вимагає постійної пильності та профілактичних заходів.

Інноваційні технології на передовій

Цікаво, що штучний інтелект (AI) став важливою зброєю в арсеналі кібербезпеки ОАЕ. Понад 70% підприємств ОАЕ зараз інтегрують штучний інтелект у свої процеси прийняття рішень для протидії складним кіберзагрозам, що відображає прагнення країни використовувати передові технології для національної безпеки.

Боротьба з кіберзагрозами є колективною, про що свідчить захоплююча присутність легенди Манчестер Сіті Пола Дікова на стенді Acronis під час GITEX. Під час заходу було підкреслено, що підтримка кібербезпеки є комплексною діяльністю, яка долає технологічні межі та потребує єдиних дій у всіх секторах суспільства.

Acronis: новаторський кіберзахист

Acronis, світовий лідер у галузі кіберзахисту, залишається в авангарді цього цифрового захисту. Присутність компанії на виставці GITEX 2023 — разом із живими демонстраціями та ознайомленням із тенденціями кібербезпеки — ще раз підтверджує її ключову роль у забезпеченні ОАЕ та ширшого регіону інструментами, необхідними для навігації в складній сфері кібербезпеки.

Поки світ готується до нових кіберзагроз, ОАЕ та сусідні регіони подають приклад, демонструючи, що за допомогою ефективних заходів, стратегічних інвестицій у технології та постійного навчання цифрова безпека є досяжною метою». ***(GITEX 2023 Spotlights UAE Cybersecurity Strengths // Techish (https://techish.com/2023/10/16/uae-cybersecurity-gitex-2023/). 16.10.2023).***

***

«Національне агентство з розвитку інформаційних технологій (NITDA) заявило, що Нігерія підвищує обізнаність своїх громадян про кібербезпеку, оскільки вона є основною протиотрутою проти онлайн-злочинів і крадіжки особистих даних.

NITDA заявив, що головним пріоритетом федерального уряду зараз є безпека кожного нігерійця в Інтернеті.

У заяві йдеться, що уряд присвятив жовтень місяцем підвищення обізнаності про кібербезпеку.

«Ця кампанія зосереджена на інформуванні окремих осіб і організацій про відповідні тенденції кібербезпеки, загрози та проактивні кроки для підвищення безпеки», — йдеться в повідомленні.

Він додав, що NITDA організує національний саміт з питань кібербезпеки про те, як нігерійці можуть залишатися в безпеці та бути більш захищеними в Інтернеті». ***(Cybersecurity Awareness Antidote To Online Crimes – NITDA // Microsoft (https://www.msn.com/en-xl/africa/other/cybersecurity-awareness-antidote-to-online-crimes-nitda/ar-AA1iesY1). 15.10.2023).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Кібершпигунство є потужним інструментом у сучасній війні. Його можна використовувати для шпигування за відомими особами, такими як політичні лідери, урядовці та керівники компаній, поширення дезінформації та навіть порушення інфраструктури. Країни також проводять шпигунство, щоб підготуватися до кібератак або фізичних актів війни.

Хоча багато країн ведуть певну форму кібервійни, США чітко заявляють, що Китай становить значну загрозу. За даними CISA (Агентства кібербезпеки та безпеки інфраструктури), агентства кіберзахисту Сполучених Штатів, «Китай, ймовірно, на даний момент представляє наймасштабнішу, найактивнішу та стійку загрозу

кібершпигунства уряду США та мережам приватного сектора». CISA навіть продовжує припускати, що китайські кібератаки можуть порушити роботу нафто- та газопроводів країни, а також залізничних систем.

Хоча це більш широке попередження, Китай відомий своїми складними кібероперaціями. Широко поширена думка, що китайський уряд організував сумнозвісну шпигунську систему GhostNet, яка зламала понад 1000 комп'ютерів військових, політичних, економічних і дипломатичних цілей по всьому світу. Проте з різних політичних і юридичних причин Китай ніколи не був офіційно названий винуватцем. Як наслідок, походження GhostNet досі залишається загадкою.

GhostNet була великою мережею кібершпигунства

GhostNet було виявлено, коли офіс Далай-лами в Індії попросив групу дослідників безпеки з Центру міжнародних досліджень Мунка при Університеті Торонто перевірити їхні комп'ютери на наявність ознак злому. Це призвело до розслідування, яке виявило масштабну кібератаку, яка протягом двох років інфікувала 1295 комп'ютерів у 103 країнах світу. У 2009 році Центр Мунка та аналітики Information Warfare Monitor опублікували докладний звіт, який пролив світло на масштабну шпигунську операцію, яку вони назвали «GhostNet».

GhostNet поширювався за допомогою електронних листів із вкладеннями та веб-посиланнями, які містили шкідливе програмне забезпечення. Після завантаження на комп'ютер жертви зловмисне програмне забезпечення мало здатність заражати та повністю контролювати комп'ютери, дозволяючи зловмисникам шукати та завантажувати файли та навіть дистанційно керувати зовнішніми пристроями, такими як веб-камери та мікрофони.

Близько 30% цілей GhostNet були високопоставленими, включаючи міністерства закордонних справ кількох країн Південно-Східної Азії, Південної Азії та Європи. Такі міжнародні організації, як АСЕАН, SAARC, Азіатський банк розвитку, новинні організації та навіть комп'ютер у штаб-квартирі НАТО були зламані.

Хто стоїть за атаками GhostNet?

Дослідникам GhostNet вдалося ідентифікувати командні сервери шпигунської мережі та підключитися до них. Кілька IP-адрес, які використовували зловмисники для зв'язку із зараженими комп'ютерами, були відстежені на острові Хайнань у Китаї. Загалом розслідування виявило чотири контрольні сервери, три з яких знаходилися в Китаї. Четвертий сервер був розміщений у веб-хостинг компанії в США. Крім того, із шести ідентифікованих командних серверів п'ять були розташовані в Китаї, а один – у Гонконзі.

Хоча дослідники припустили, що докази вказують на те, що Китай є найбільш очевидним організатором атак GhostNet, їхній звіт прямо не звинувачує країну. Він попередив, що це також може бути роботою злочинної організації або навіть іншої країни. Вони не змогли надати конкретних доказів причетності китайського уряду.

Сервери GhostNet вийшли з мережі через день після публікації звіту, і представник консульства Китаю в Нью-Йорку заперечив будь-яку причетність до операції, заявивши, що уряд Китаю прямо забороняє кіберзлочинність. Оскільки атаки відбулися в кількох країнах, вони спричинили правові та політичні бар'єри, які перешкоджали більш глибокому розслідуванню. Як наслідок, зловмисників, які стояли за GhostNet, так і не було офіційно ідентифіковано через понад десять років після розкриття операції». ***(Ketaki Bhojnagarwala. Why One Of The Largest Cyber-Attacks Is Still A Mystery // Static Media ® (https://www.slashgear.com/1410667/ghostnet-cyber-attack-mystery/). 08.10.2023).***

***

«Двоє відомих законодавців були одними з цілей в'єтнамських урядових агентів, які намагалися використати хакерське шпигунське програмне забезпечення, повідомляє The Washington Post.

Голову Комітету із закордонних справ Палати представників Майкла МакКола, штат Техас, і сенатора Кріса Мерфі, штат Коннектикут, члена комітету із закордонних справ і голову його підкомітету з питань Близького Сходу, намагалися переконати відвідати веб-сайти, призначені для встановити хакерське програмне забезпечення, відоме як Predator, повідомляє The Post.

Сенсори Джон Хувен, RN.D., і Гері Пітерс, D-Mich., також були мішенню.

Напад стався під час обговорення в'єтнамськими та американськими дипломатами великої угоди про співпрацю, спрямованої на протидію зростаючому китайському впливу в Азії.

Програмне забезпечення могло викрити погляди адміністрації Байдена та законодавців США щодо Китаю та регіону.

Метою було встановити шпигунське програмне забезпечення на телефони законодавців, повідомляє газета.

Немає жодних доказів того, що злом був успішним.

Американські політичні експерти та американські журналісти, включаючи експертів з Азії у вашингтонських аналітичних центрах і репортерів CNN, також були мішенню, згідно з судово-медичною експертизою посилань, розміщених на соціальній платформі X, раніше відомої як Twitter, і документів, виявлених групою новинних видань.

Amnesty International виявила масштаби спроб злому та поділилася своїми висновками з Post і 14 міжнародними ЗМІ.

Американський чиновник сказав, що 50 американських чиновників, які працюють за кордоном, раніше були мішенями комерційного шпигунського програмного забезпечення.

Програма спостереження Predator може вмикати мікрофони та камери мобільних телефонів, отримувати файли та читати приватні повідомлення, навіть якщо вони зашифровані.

«Оскільки клієнти Predator, очевидно, перебувають у важкому процесі навчання, використання Twitter є жахливою ідеєю», — сказав дослідник Джон Скотт-Рейлтон з Citizen Lab, який погодився з висновками Amnesty, повідомляє The Post. «Той факт, що це навіть станеться, доводить, що Predator все ще йде до безрозсудних операторів».

Міністерство торгівлі США вимагає від американських компаній отримати ліцензію, перш ніж вести бізнес з європейською компанією Intellexa та пов'язаною з нею фірмою Cytrox, які є частиною мережі, яка розповсюджує Predator.

«Завдяки всім доказам і документам, які ми бачили, ми вважаємо, що Predator був проданий Intellexa через кількох посередників Міністерству громадської безпеки В’єтнаму», — сказав Доннча Ó Кербхайл, керівник лабораторії безпеки Amnesty’s.

В'єтнам був причетний до інших хакерських кампаній і раніше використовував комерційні шпигунські програми, повідомляє Post». ***(Charlie McCarthy. Vietnam Tried to Hack US Lawmakers // Newsmax Media, Inc. (https://www.newsmax.com/newsfront/vietnam-hack-spyware/2023/10/09/id/1137534/?utm_source=flipboard&utm_content=Newsmax2018%2Fmagazine%2FNewsmax). 09.10.2023).***

***

«…Після недільного знищення веб-сайту Палати представників комітет з асигнувань Палати висловив підтримку збільшення фінансування DICT.

«Ми працюватимемо з нашими колегами в Сенаті, щоб шукати більше джерел фінансування для DICT», — сказав у заяві в понеділок голова комісії та член партійного списку AKO BICOL Елізалді Ко.

Реджинальд Веласко, генеральний секретар, опублікував заяву, в якій говориться: «Ми хочемо повідомити громадськості, що раніше сьогодні офіційний веб-сайт Палати представників зазнав несанкціонованого доступу. Було вжито негайних заходів для вирішення проблеми, і ми тісно співпрацюємо з Департаментом інформаційно-комунікаційних технологій (DICT), Центром з розслідування та координації кіберзлочинів (CICC) і відповідними правоохоронними органами для розслідування цього питання».

Представник наголосив на необхідності надання ресурсів DICT для боротьби з кіберзлочинністю та атаками програм-вимагачів, довівши цю потребу до Департаменту бюджету та управління.

Підвищення безпеки

Одна з пропозицій, внесена Со, полягає в тому, щоб виділити частину непрограмованих коштів із національного бюджету на 2023 рік для посилення IT-безпеки та захисту від програм-вимагачів.

Одночасно сенатор Різа Гонтіверос представила резолюцію 829, яка закликає до створення комітету для розслідування серйозної серії випадків злому та витоку даних. Гонтіверос наголосив на загрозі безпеці філіппінців через викрадання особистої та конфіденційної інформації, якою володіє держава.

Нещодавня серія порушень включала Філіппінську корпорацію медичного страхування (PhilHealth) і Філіппінське статистичне управління (PSA) наприкінці вересня та на початку жовтня.

Критичне попередження

Національна комісія з конфіденційності випустила «критичне попередження» щодо скомпрометованої особистої інформації внаслідок зламу PhilHealth.

Хоча витік даних PSA обмежувався системою моніторингу на основі спільноти, остання атака була спрямована на веб-сайт Палати представників. В інциденті анонімний користувач зіпсував веб-сайт мемом із обличчям троля та змінив розклад засідань комітету.

У понеділок близько 17:00 веб-сайт Палати представників було відновлено. Він залишався недоступним більше доби після злому користувача «3musketeerz» у неділю вранці.

9 жовтня секретар Філіппінського департаменту інформаційно-комунікаційних технологій (DICT) Іван Джон Уі висловив глибоку стурбованість у зв’язку зі значними скороченнями бюджету, виділеного на найважливіші програми агентства з кібербезпеки.

Виступаючи в кулуарах запуску Місяця кібербезпеки 2023, керівник DICT повідомив, що бюджет кібербезпеки для DICT на 2024 рік становить лише 300 мільйонів песо 5,28 мільйона доларів, що значно менше, ніж у попередні роки.

За його словами, бюджет країни на кібербезпеку починався з 1 мільярда песо, а у 2022 і 2023 роках був скорочений, знизивши його до 600 мільйонів песо. Тепер, на 2024 рік, її ще більше зменшено лише до 300 мільйонів песо.

«Оскільки загрози в кіберсфері продовжують розширюватися та зростати, наш бюджет на кібербезпеку продовжує зменшуватися», — сказав він філіппінською мовою». ***(Jay Hilotin. Philippines: Wave of cyberattacks spurs urgent measures to boost***

cybersecurity // Nisr Publishing LLC (https://gulfnews.com/world/asia/philippines/philippines-wave-of-cyberattacks-spurs-urgent-measures-to-boost-cybersecurity-1.1697450124941). 16.10.2023).

***

«Російську розвідку зараз цікавлять конкретні наслідки членства Фінляндії в НАТО, підтримка України та різноманітні способи уникнення санкцій.

Про це заявив очільник фінської поліції безпеки SUPO Антті Пелттарі на пресконференції у четвер, передає Укрінформ з посиланням на Yle.

Він наголосив, що діяльність російських спецслужб у Фінляндії була ускладнена після видворення дипломатів, тому РФ, на його думку, спрямує більше зусиль на кіберпростір. Зокрема, російські хакери посилили Dos-атаки на фінську інфраструктуру, проте Пелттарі запевнив, що зазвичай подібні кібератаки не становлять загрозу для нацбезпеки.

Разом з тим в SUPO підкреслили, що незахищені домашні роутери, підключені до мережі Інтернет, можуть являти собою серйозну загрозу.

Очільник поліції безпеки вважає, що членство Фінляндії в НАТО гарантуватиме захист від «найбільш агресивних форм» впливу з боку РФ.

Як повідомляв Укрінформ, російські хакери у минулий четвер здійснили серію кібератак на сайти Банку Фінляндії, податкової служби країни, та деяких ЗМІ.

Раніше 4 жовтня російська хакерська група NoName 057 (16) атакувала сайти фінської транспортної інфраструктури та банків». ***(Російські шпигуни перемістилися у кіберпростір - служба безпеки Фінляндії // Укрінформ (https://www.ukrinform.ua/rubric-technology/3773239-rosijski-spiguni-peremistilisa-u-kiberprostir-sluzba-bezpeki-finlandii.html). 12.10.2023).***

***

«Кіберзлочинці з рф напали на королівську родину вчора — через кілька днів після того, як король Чарльз засудив війну в Україні. Про це пише The Sun, передає УНН.

Деталі

Зазначається, що пропутінська група KillNet заявила, що у неділю вранці вони вивели з ладу вебсайт royal.uk на 90 хвилин, змусивши керівників палацу залучити своїх експертів з кібербезпеки.

Джерело повідомило: «Це була атака на відмову в обслуговуванні, яка призвела до бомбардування сайту трафіком».

Прихильники монархів, намагаючись увійти, побачили повідомлення «Код помилки тайм-ауту шлюзу 504».

Незабаром після цього KillNet похвалилася в месенджері Telegram, що це справа їхніх рук.

А лідер KillNet — KillMilk — похвалився причетністю до кібератаки у своєму особистому блозі через 20 хвилин після того, як сайт припинив роботу.

Начальники палацу заявили, що особисті облікові записи старших королівських осіб не були зламані, а конфіденційна інформація не була викрадена.

Але легкість того, як було здійснено напад, вразив королівську родину…» ***(https://www.unn.com.ua/uk/news/2048905-rosiyski-khakeri-atakuvali-sayt-monarkhiv-velikoyi-britaniyi). 02.10.2023).***

***

Кібервійна проти держави Ізраїль

«Група хакерів під назвою Killnet, яка ймовірно пов'язана з Кремлем, здійснила кібератаку проти уряду Ізраїлю на тлі ескалації конфлікту, викликаного раптовою атакою ХАМАС у суботу.

У неділю вранці група оприлюднила заяву через Telegram, в якій стверджувала, що уряд Ізраїлю винен у терористичних атаках, сказавши: «Ще в 2022 році ви підтримали терористичний режим України.

«Ви зрадили Росію. Сьогодні Killnet офіційно повідомляє вам про це! Усі урядові системи Ізраїлю будуть піддані нашим атакам!»

Killnet доповнила свою заяву, опублікувавши фотографію, яка показує, що веб-сайт ізраїльського уряду не працює, написавши: «Основний урядовий сайт ізраїльського режиму було вбито!»

Через кілька годин офіційний Telegram Killnet уточнив, що організація виступає не проти ізраїльського народу, а скоріше проти «ізраїльського режиму», який «продався повії НАТО».

У ньому додано: «Мирні жителі Гази та Ізраїлю не мають права віддати своє життя заради виродків з Європи».

Група заперечує, що працювала на Кремль, але експерти Kyiv Post заявили, що наявні докази свідчать про інше.

Двоє старших офіцерів європейської розвідки, які працюють над питаннями кібербезпеки, пов'язаними з Росією, розповіли Kyiv Post, що Killnet тісно пов'язана з російським урядом.

Один із офіцерів розвідки заперечив, що Killnet міг бути просто «піратами», які атакують веб-ресурси ворожих країн за вільного «підтримки» Кремля, сказавши: «Якщо це було так, то чому вони не працюють на російських державні свята? Вони — російський уряд».

Раніше цього року Міністерство охорони здоров'я та соціальних служб США опублікувало звіт, у якому вказано, що Killnet «слід вважати загрозою для уряду та організацій критичної інфраструктури, включаючи охорону здоров'я».

Минулого тижня у відповідь на те, що Міжнародний Червоний Хрест оприлюднив низку «правил взаємодії з хакерами», закликаючи хакерів не атакувати гуманітарні цілі чи лікарні, BBC процитувала реакцію засновника Killnet: «Чому я повинен слухати Червоного? Хрест?»

Хакер із білим капелюхом, який працював над протидією російським хакерським загрозам для американських цілей, сказав Kyiv Post, що Killnet діє для просування інтересів Росії за кордоном, включаючи «високо політизовані та вчасні

атаки, які відбуваються в тандемі з інформаційними операціями, які проводяться урядами БРІКС».

Вони підкреслили, що, хоч і не така відома, як їхні російські колеги Sandworm або Fancy Bear, Killnet є «прогресивною групою, що створює загрози», до якої входять численні суб'єкти Ісламської держави, ісламські недержавні організації та російські групи, які діють під цим прапором Killnet, щоб захопити перевага прикриття «хактивізму».

Вони стверджували, що Killnet «є лише прикриттям для операцій національних держав».

Менш ніж через 16 годин після перших терористичних атак агентство Reuters повідомило, що голова Ліги арабських держав, який займається справами Палестини, вирушив до Москви, оскільки «належні переговори» «необхідні для створення незалежної палестинської держави в межах 1967 зі столицею у Східному Єрусалимі.

На запитання, чи Москва, можливо, сигналізує, що вона стає на бік ХАМАС у конфлікті з Ізраїлем, хакер у білому капелюсі сказав: «Мало того, це свідчить про те, що народ Росії справді зневажає народ Ізраїлю». ***(Jason Jay Smart. Kremlin-Linked Hacker Group Launches Cyber-Attack Against Israel // BIZNESGRUPP TOV (https://www.kyivpost.com/post/22491?utm_source=flipboard&utm_content=KyivPost%2Fmagazine%2FKyiv+Post+Latest+News). 09.10.2023).***

***

«Хакери, які симпатизують ХАМАС, намагаються зробити конфлікт Ізраїлю та Гази наступним фронтом кібервійни.

Хакерські групи, пов'язані з такими країнами, як Іран і Росія, запустили серію кібератак і онлайн-кампаній проти Ізраїлю протягом останнього тижня, деякі з них, можливо, мали місце навіть напередодні удару ХАМАС 7 жовтня.

У Telegram групи хакерів стверджували, що зламали веб-сайти, ізраїльську електромережу, додаток для оповіщення про ракети та систему протиракетної

оборони «Залізний купол». Принаймні одна ізраїльська газета, The Jerusalem Post, визнала, що хакери тимчасово зламали її сайт.

Наскільки далеко та на глибину зайшли кібератаки, невідомо. Але онлайн-кампанії демонструють спроби підсилити фізичну атаку цифровим наступом, потенційно прагнучи відтворити те, як Росія та співчуваючі хактивісти завдали Україні кіберударів у перші дні тієї війни.

Прихильність груп, які скоїли напади, також може дати підказку про те, чи ХАМАС здійснив свою смертоносну атаку самостійно. Хоча немає прямих зв'язків між цими групами та іноземними урядами, деякі з них здійснюють хакерські атаки, які приносять користь країнам, які надають їм притулок, включаючи Іран, який тривалий час підтримує ХАМАС.

Ліз Ву, представник ізраїльської групи кібербезпеки Check Point Software, заявила, що компанія відстежила понад 40 груп, які здійснювали атаки, які перевантажили та порушили роботу понад 80 веб-сайтів, починаючи з дня натиску ХАМАС. Це включало сайти уряду та ЗМІ.

Зломи, ймовірно, відбуваються з-за меж Гази, враховуючи низький доступ до Інтернету ще до ударів, а також через відключення електроенергії та бомбардування з боку Ізраїлю в наступні дні.

Один колишній кіберчиновник із західної країни заявив, що координація кібератаки з вторгненням ХАМАС була б малоймовірною, оскільки бойовики спланували свою атаку за допомогою старомодних методів зв'язку. Співпраця з хакерами в Інтернеті могла спровокувати виявлення ізраїльтян, сказала особа.

«Важко сказати, яке з цих тверджень є правдивим», — сказав Гіл Мессінг, керівник персоналу Check Point. «Іноді бази даних, які вони публікують, переробляються зі старих витоків даних, які тепер вони показують як нові. Жодна з організацій, імовірно пов'язаних із цими витоками даних, не відчула, що це постраждало».

Тим не менш, ці групи мають рівень ноу-хау, який не слід скидати з рахунків, сказав член Комітету з розвідки Палати представників США Джим Хаймс (D-Connect.).

«Хамас і Хезболла, а також підтримувані Іраном хакери набагато кращі, ніж ви могли б подумати», — сказав Гаймс, покидаючи секретний брифінг щодо конфлікту в середу. «Потрібно уважно стежити за кіберсферою».

Досить обмежений масштаб фактичної кібершкоди в Ізраїлі контрастував з полем інтернет-бою під час вторгнення Росії в Україну в 2022 році. Хакери атакували системи зв'язку Kyiv Post і супутникову мережу KA-SAT за кілька годин до того, як російські танки перетнули кордон, спричинивши серйозні перебої в зв'язку, і групи хакерів з обох сторін з того часу продовжували атакувати та порушувати послуги.

Під час атаки 7 жовтня ХАМАС застосував більш конкретну тактику, щоб обійти та зруйнувати величезний ізраїльський апарат спостереження: досліджував місця, де камери були слабкими, руйнував паркани бульдозерами, запускав ракети та знищував безпілотники, перш ніж вони змогли піднятися в повітря.

Ізраїль заявив, що щонайменше 1300 людей загинули внаслідок атаки ХАМАС, тоді як у відповідь ізраїльські авіаудари вбили понад 2000 людей у Газі, за даними місцевих органів охорони здоров'я.

Хронологія страйків

Деякі кібератаки цього тижня мали явні наслідки: ізраїльські ЗМІ повідомили, що міністерство освіти перейшло від Zoom до Google для відеозустрічей після того, як люди, які стверджували, що є бойовиками ХАМАС, піддавали Zoombomb в прямому ефірі. За словами головного редактора Аві Майєра, веб-сайт Jerusalem Post кілька разів замикався та виключався протягом кількох днів після атаки, включаючи кілька годин, коли він був повністю недоступний.

Проросійська група Anonymous Sudan заявила, що запустила розподілену атаку на відмову в обслуговуванні, яка переповнює веб-сайт або програму цифровим трафіком, проти ізраїльської програми Red Alert, яка надає громадянам інформацію про ракети в реальному часі. Фірма з кібербезпеки Group-IB також виявила, що група AnonGhost підробила програму. POLITICO підтвердило повідомлення Group-IB про те, що додаток видалено з магазину Google Play.

Інші напади важко було обґрунтувати. Хакерська група під назвою Cyber Av3ngers, пов'язана з Іраном, заявила, що 6 жовтня вона вразила ізраїльського

постачальника електроенергії та занурила місто Явне в темряву. Прес-секретарі енергокомпанії та міської влади не підтвердили напад.

Невдовзі після цього Cyber Av3ngers, Anonymous Sudan і пов'язана з Росією Killnet також заявили, що зламали веб-сайти мозкового центру Israel Policy Forum і міністерства фінансів країни. Незалежного підтвердження атак не було, і до п'ятниці всі сайти були запущені.

«На даний момент у нас немає доказів того, що існує будь-яка координація між атаками на землі та в кіберпросторі», — сказав Олександр Леслі, аналітик із розвідки загроз у Recorded Future. «Ми вважаємо, що переважна більшість кібератак, за які відповідають хактивістські групи, є опортуністичними та реакційними».

Загроза іранського хакерства

Бойовики ХАМАС, які здійснили напади в Ізраїлі минулих вихідних, підтримуються Тегераном, з яким Ізраїль роками веде тіньові війни. Експерти з безпеки пов'язали принаймні одну антиізраїльську операцію з дезінформації в соціальних мережах цього тижня з Іраном.

Останній виток кіберворожнечі стався після років онлайн-ударів. Іранських хакерів звинуватили в невдалій спробі підвищити рівень хлору в системі водопостачання Ізраїлю в 2020 році. Вірус Stuxnet, виявлений у 2010 році, вважався проектом США та Ізраїлю, спрямованим на саботаж ядерної програми Ірану. Ізраїль також був причетний до кібератаки 2020 року на великий іранський порт.

Маккол про провал ізраїльської розвідки: «Не знаю, як ми його пропустили»

Генерал-лейтенант Чарльз Мур, який до минулого року був заступником директора Кіберкомандування США, сказав: «Зараз я вважаю, що Іран із задоволенням керує та підтримує всі форми операцій, як кібер, так і кінетичних, через своїх довірених осіб».

«Однак, оскільки ізраїльські операції в Газі продовжують розвиватися, це може швидко змінитися», – сказав він, додавши, що очікує «дуже агресивного впливу, пропагандистської кампанії з боку Ірану».

Ізраїль також є важкою мішенню для кіберударів. Вона вважається однією з найрозвиненіших країн у сфері кібербезпеки та є головним центром світової

індустрії стеження. Цього тижня адміністрація Байдена також збільшила кіберпідтримку Ізраїлю. Крім того, ізраїльська технічна спільнота створила власні «громадянські кібербригади» за кілька днів після атаки ХАМАС, повідомляє The Wall Street Journal.

«Питання про те, як ізраїльська та американська розвідка не змогли виявити таку широкомасштабну операцію ХАМАСу, викликало збентеження багатьох людей, як в уряді, так і за його межами», — сказав Мур. «Тим не менш, кіберзбройні сили Ізраїлю є одними з найкращих у світі». ***(Antoaneta Roussi and Maggie Miller. How hackers piled onto the Israeli-Hamas conflict // POLITICO LLC (https://www.politico.com/news/2023/10/15/hackers-israel-hamas-war-00121593?utm_source=flipboard&utm_content=user%2Fpolitico). 15.10.2023).***

***

«Коли справа доходить до передових оборонних технологій, Ізраїль часто був на передовій, маючи найдосконаліше програмне забезпечення для спостереження, як Pegasus. Проте події 7 жовтня показали сувору реальність. Навіть найпередовіші технології можуть бути застані зненацька.

Раптовий удар

Інтенсивність і масштаб нападу ХАМАС на Ізраїль 7 жовтня були не чим іншим, як шокуючими. ХАМАС, який керує Газою, випустив 5000 ракет по Ізраїлю.

Цей повітряний напад був лише одним із аспектів їхньої багатосторонньої стратегії. Бойовики одночасно порушили ізраїльські кордони в різних точках, використовуючи тактику, як парапланеризм, щоб проникнути глибше на територію Ізраїлю.

Зухвалість їхнього несподіваного наземного нападу була очевидною, коли вони лютували через ізраїльські території, що призвело до трагічних втрат людей і викрадення багатьох мирних жителів.

Шпигунське програмне забезпечення Ultimate від NSO Group вийшло з ладу

Pegasus розроблено NSO Group, ізраїльською компанією кіберрозвідки, яка розробляє та продає шпигунське програмне забезпечення державним установам у

всьому світі. Хоча Pegasus — це не просто шпигунське програмне забезпечення, його часто називають вершиною інструментів кібершпигунства. Його дизайн і можливості відображають ретельне розуміння як мобільного програмного забезпечення, так і людської поведінки. Отже, чому розвідка не змогла отримати завчасні попередження від найскладнішого програмного забезпечення для стеження за телефонами у світі, створеного в Ізраїлі? Відповідь на це критичне питання все ще невідома.

Як працює Pegasus

Pegasus — це програмне забезпечення для спостереження, яке може віддалено заражати та контролювати смартфони без відома чи згоди власника. Це золотий стандарт у шпигунстві за телефонами – і крапка. Проникнувши в пристрій, він вибирає потрібні інструменти на основі того, що використовує телефон. Подумайте про це як про швейцарський армійський ніж. Якщо телефон не використовує певну функцію, Pegasus не витягне цей інструмент. Таким чином він краще залишається прихованим, оскільки використовує лише те, що йому потрібно, і не залишає непотрібних підказок.

Що відрізняє Pegasus

Що справді відрізняє Pegasus від інших, так це його здатність атакувати без натискання. Традиційне шпигунське програмне забезпечення часто вимагає від об’єкта помилки, наприклад натискання підозрілого посилання. Однак Пегас може проникнути в пристрій без будь-якого такого введення.

Щоб отримати доступ, він використовує невідомі вразливості, які в програмному забезпеченні називають «нульовими днями». Термін «нульовий день» означає, що розробники мають «нульовий день», щоб вирішити проблему, коли про неї стане відомо. Ці вразливості є дуже цінними для хакерів і часто використовуються під час серйозних кібератак.

Опинившись усередині, його можливості спостереження є величезними. Окрім доступу до повідомлень, електронних листів і дзвінків, він також може записувати розмови, приховано активувати камери та відстежувати рухи користувачів у режимі

реального часу. Потім усі ці дані шифруються та надсилаються на сервер керування, де вони аналізуються та зберігаються.

Обмеження шпигунського ПЗ Pegasus

Зважаючи на все це, останні події в Ізраїлі викликають ще більше здивування. Маючи в своєму розпорядженні такий потужний інструмент, як «Pegasus», нам все ще потрібно зрозуміти, як значна мобілізація ХАМАС у Газі залишилася поза увагою. Це питання не лише підкреслює обмеження навіть найсучаснішого шпигунського програмного забезпечення.

Темна сторона технології Pegasus від NSO Group

NSO Group стверджує, що її технологія використовується лише в законних цілях, таких як боротьба з тероризмом і злочинністю. Однак кілька звітів виявили докази того, що Pegasus використовувався для нападу на правозахисників, журналістів, дисидентів, юристів і політиків у різних країнах. Деякі з цих цілей зазнавали переслідувань, залякувань, арештів, тортур або вбивств.

Таку заяву компанія опублікувала на своєму сайті. Частково в ньому йдеться:

«У нас є найсуворіші у світі програми дотримання законодавства та прав людини, які базуються на американських цінностях, які ми глибоко поділяємо, що вже призвело до численних припинень контрактів з державними установами, які зловживали нашими продуктами».

Ключові висновки Курта

Незалежно від того, наскільки сучасні технології можуть бути, вони не є безпомилковими. Системи на кшталт Pegasus, безсумнівно, є передовими, але вони мають свої власні труднощі. Оскільки країни в усьому світі продовжують покладатися на вдосконалені інструменти спостереження, важливо знати, коли на них можна покластися, а коли вони не зможуть надати достатньо значних даних, щоб попередити про атаку…» ***(Kurt Knutsson. Why Israel's Pegasus spyware was not enough to stop Hamas // FOX News Network, LLC. (https://www.foxnews.com/tech/why-israels-pegasus-spyware-not-enough-stop-hamas?utm_source=flipboard&utm_content=zhogfan%2Fmagazine%2FPOLITICS.WAR.LEGAL.RELIGION). 14.10.2023).***

***

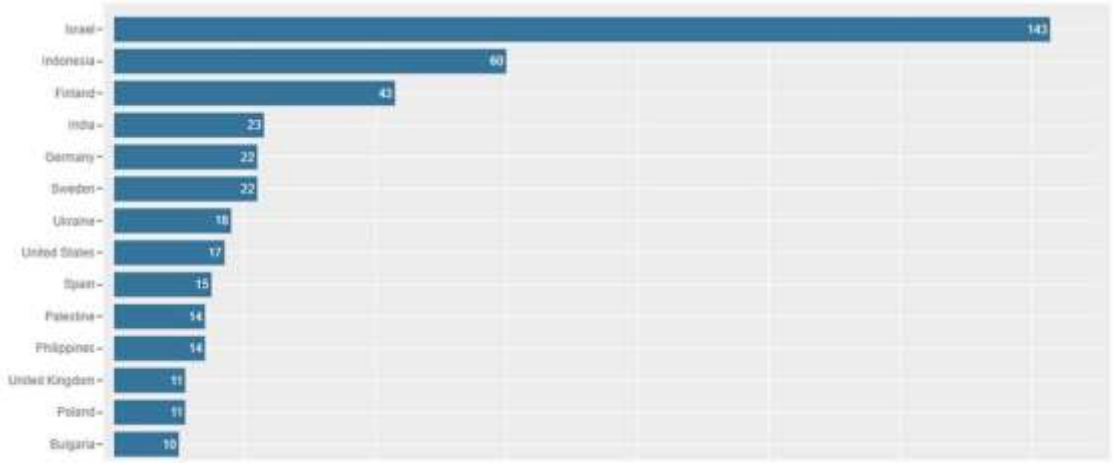
«Війна між ХАМАС та Ізраїлем також вирує у сфері кібербезпеки, оскільки різноманітних зловмисних програм, кампанії з дезінформації та вербування громадянських хакерів. обидві сторони конфлікту спостерігають використання

Важко отримати незалежно перевірену інформацію через динамічну ситуацію, а також через те, що багато ізраїльтян були направлені на дійсну службу з початку війни, що виснажує рівень технічного персоналу. «Більшість співробітників ізраїльських компаній спочатку є резервістами, а тепер готуються до бою», — сказав SiliconANGLE виконавчий директор Horizon2.ai Inc. Снехал Антані.

Дослідники безпеки бачать збільшення кількості кібератак, спрямованих на ізраїльські підприємства та державні установи. «Ми є свідками зростаючої тенденції зусиль з боку супротивників Ізраїлю, як організованих, так і неорганізованих, щодо введення в цей конфлікт аспекту кібератак», — сказав в інтерв'ю Рой Акерман, генеральний директор охоронної фірми Rezonate Inc.

І це не одне. Відповідно до блогу Radware Ltd., «паралельно з вторгненням ХАМАС в Ізраїль ми спостерігали значне зростання кіберагресії проти ізраїльських цілей». Постачальник безпеки Radware знаходиться в Тель-Авіві.

Компанія відстежила кількість розповсюджених атак типу «відмова в обслуговуванні», заявлених на Telegram за перші кілька тижнів жовтня, показуючи, що Ізраїль був мішенню 143 рази (на фото нижче), обидва з боку хакерів, які стверджували, що підтримують палестинські та російські справи. Переважна більшість цих нападів почалася з вторгнення ХАМАС в Ізраїль 7 жовтня.



Дослідження Microsoft бачать подібну картину. У своєму останньому « Звіті про цифрову оборону », опублікованому на початку цього місяця, йдеться про те, що «Ізраїль, безперечно, залишається найбільш об’єктом нападу на Близькому Сході та в регіоні Північної Африки внаслідок великої уваги Ірану до них».

Багато з цих зусиль спрямовані на те, щоб посіяти паніку серед громадян, наприклад, надсилаючи сповіщення з дезінформацією про потенційну загрозу вибуху або ненадійне постачання води. Корпорація Майкрософт виявила, що останнім часом Іран розширив свою цільову спрямованість, включивши країни-члени НАТО на додаток до цілей у США та Ізраїлі.

Прохамасівські групи

Є чотири основні групи хакерів, які послідовно заявляють про свою підтримку ХАМАС: Anonymous Sudan, Killnet, AnonGhost і Storm-1133. Anonymous Sudan спочатку походила з цієї країни, хоча деякі дослідники безпеки кажуть, що група завербувала членів з інших країн, а інші назвали її проросійською групою.

З початку року він проводить різні DDoS-атаки проти кількох західних країн. Його заборонили в Telegram, коли він був націлений на цю платформу минулого місяця. Його останньою мішенню була газета Jerusalem Post, у якої були збої на веб-сайті в перші дні війни, заслугу в розпалюванні якої вважала група Anonymous Sudan.

Друга група – Killnet, яка базується в Росії та стала більш відомою після початку війни в Україні у 2022 році. Вона націлилася на кілька ізраїльських веб-сайтів, у тому числі веб-сайт розвідувального підрозділу Shin Bet, а також інші ізраїльські урядові сайти, наприклад, його головна веб-присутність gov.il.

Незрозуміло, чи цей сайт був переповнений законним трафіком чи став предметом справжньої DDoS-атаки.

Інші дослідники повідомили про посилення атак Killnet минулого тижня. «Тиждень тому ви бачили менше ніж кілька таких за 24 години, а тепер ви бачите кілька за годину», — сказав Йоссі Епплбум, генеральний директор кіберкомпанії Sepio, Wall Street Journal.

Телеметрія Radware спостерігала DDoS-атаки як на прикладному, так і на мережевому рівнях, спровоковані обома групами. Багато з цих атак тривають лише кілька хвилин, перш ніж їх відбивають захисники.

Третім гравцем є група AnonGhost, яка на початку тижня використала вразливість у Red Alert, одному з ізраїльських додатків для Android, які надають геолокаційні оповіщення про ракетні атаки в реальному часі. Дослідники з питань безпеки Group-IB виявили експлойт і опублікували в своєму акаунті X/Twitter. Згодом додаток було видалено з Google Play Store. Є кілька інших додатків Red Alert, які не постраждали та все ще доступні.

Нарешті, є група загроз, яку Microsoft назвала Storm-1133, яка, як вона помітила, спрямована проти ізраїльських енергетичних і телекомунікаційних цілей на початку цього року. Згідно з дослідженням компанії, ця хакерська група була пов’язана з Хамасом і створювала різноманітні проблеми, включаючи бекдори та фішингові приманки. Один не дуже новий підхід полягав у створенні фальшивих профілів LinkedIn під виглядом ізраїльських менеджерів з персоналу та розробників програмного забезпечення, щоб скомпрометувати працівників цільових компаній.

Крім цих зловмисників, існують інші групи, які націлили свою кіберзброю на Ізраїль.

Іран є одним із найактивніших кібератакувальників із сучасними державними групами, які продовжують нападати на цілі по всьому світу. У дослідницькому звіті Microsoft зафіксовано низку перших за минулий рік, у тому числі конкретну цілі щодо деструктивної кібератаки на країну НАТО.

Однак Іран не єдиний. «Очевидно, що інші російські хактивісти також обирають сторону та активно підтримують ХАМАС у їхній війні проти Ізраїлю», —

сказав Маттіас Велен, експерт із розвідки загроз у фірмі з кібербезпеки Truesec AB, у дописі від Time. «Їхні дії більше схожі на опортуністичні страйки».

Деякі атаки є підступними. Журнал повідомляв, що дистанційні уроки студентів були перервані зображенням солдата, який тримає гвинтівку під час одного з їхніх уроків. І є численні зображення, завантажені на різні платформи соціальних медіа, які нібито показують різні події, які є неточними, вирваними з контексту чи відбулися давно. «Ми повинні очікувати високоефективних кампаній з дезінформації, які в поєднанні з кібератаками, які викрадають інформацію або порушують роботу систем, сформують глобальне поле інформаційної битви», — сказав Антані з Horizon2.ai SiliconANGLE.

Проізраїльські групи

За даними кількох джерел, група ізраїльських волонтерів-техніків зібралася для надання гуманітарної допомоги, щоб допомогти в рятувальних роботах. Під назвою «Ізраїльська технічна гвардія» вона допомагає розподіляти медичні та харчові продукти серед переміщених осіб. Багатьом сім'ям доводилося мати справу з тим, що їхніх членів призвали на військову службу (наприклад, мого зятя), або з цивільними особами, яким довелося переїхати в іншу точку країни, щоб бути далі від ракетних атак (наприклад, мій дочка).

«Проізраїльські групи здійснили власні атаки, націлившись на палестинські організації за допомогою кібератак», — в публікації в журналі Fortune зазначається. «Одна група, яка називає себе Індійськими кіберсилами, заявила, що в неділю збила веб-сайт Палестинського національного банку та веб-сайт ХАМАС».

«Той факт, що Іран зазнав невдачі у своїх численних спробах здійснити терористичні напади на ізраїльські та єврейські об'єкти за кордоном, не зменшить його рішучості, і ці зусилля триватимуть у майбутньому», – заявила група дослідників Інституту досліджень національної безпеки. ізраїльський аналітичний центр, написав ще в грудні минулого року. Як виявилося, на жаль, це передбачення справдилося». ***(David Strom. The Hamas-Israeli war is also being fought in cyberspace // SiliconANGLE Media Inc. (https://siliconangle.com/2023/10/12/hamas-israeli-war-also-fought-cyberspace/). 12.10.2023).***

***

«Робота веб-сайтів двох груп допомоги Ізраїлю та Газі була порушена останніми днями після того, як хакери переповнили їх трафіком після серії погроз групи хаквістів через конфлікт, що триває.

Єрусалимська некомерційна організація United Hatzalah, яка надає екстрену медичну допомогу, повідомила, що її веб-сайт був уражений розподіленими атаками на відмову в обслуговуванні (DDoS), які тимчасово сповільнили його здатність отримувати пожертви.

Медична допомога палестинцям (MAP), британська благодійна організація, яка надає екстрену допомогу жителям Гази, у четвер повідомила в дописі на X, раніше Twitter, що її веб-сайт зазнав «кібератаки».

«Надзвичайно розчаровує те, що будь-хто бажає перешкодити роботі гуманітарної організації, особливо під час цієї безпрецедентної гуманітарної кризи», — сказав Рохан Телбот, директор з адвокації та кампаній MAP, у заяві, надісланій електронною поштою.

DDoS — це низькорівнева та зазвичай нескладна атака, призначена для переповнення веб-сайту штучним трафіком, що часто призводить до його збою.

Аналітики безпеки спостерігали за сплеском хакерської діяльності або шпигунської діяльності після нападу бойовиків ХАМАС, у результаті якого за вихідні загинуло понад 1300 ізраїльтян, переважно мирних жителів. За даними влади Гази, у відповідь ізраїльські бомбардування вбили 1800 палестинців.

Збої в роботі веб-сайту United Hatzalah не призвели до втрати даних або пожертвувань, сказав Джеремі Коул, речник групи.

За словами Коула, інший веб-сайт, який імітував United Hatzalah, який з’явився за останні кілька днів і шукав пожертвувань, був закритий.

Незрозуміло, хто стоїть за обома атаками, але різні хакерські групи, багато з яких підтримують ХАМАС, попередили останніми днями в Telegram та інших програмах для обміну повідомленнями про майбутні дії.

«Зараз відбувається багато DDoS-атак, зосереджених на послугах, які шукають люди: служби порятунку, телекомунікаційні компанії, державні служби, засоби масової інформації – усе, що зараз потрібно людям», – сказав Гіл Мессінг з фірми з кібербезпеки Check Point.

Більшість веб-сайтів швидко відновлюються після таких звернень, додав Мессінг». ***(Zeba Siddiqui. Hackers Hit Aid Groups Responding to Israel and Gaza Crisis // U.S. News & World Report L.P. (https://www.usnews.com/news/world/articles/2023-10-13/hackers-hit-aid-groups-responding-to-israel-and-gaza-crisis?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 13.10.2023).***

***

«Кільком ізраїльським лікарням у суботу Національне кіберуправління наказало відключитися від Інтернету на кілька годин через попередження про кібератаки.

Співробітники медичного центру Шеба в Тель-Хашомері, наприклад, отримали повідомлення про те, що «через попередження про кібератаки» доступ до веб-сайтів, а також віддалений доступ до мережі медичного центру «буде вимкнено на наступні кілька годин».

Міністерство охорони здоров'я Ізраїлю оприлюднило офіційну заяву, в якій говориться: «Прагнучи підвищити стійкість економіки, Національний кіберуправління та Міністерство охорони здоров'я вжили заходів для зміцнення лікарень проти атак і перевіряють кожну підозру».

У заяві пояснюється: «У рамках цих зусиль ми проводимо самоініціативні дії, такі як тимчасове розрив інтернет-з’єднання. На даному етапі це не впливає на здатність лікарень функціонувати, і пацієнтів лікували як зазвичай».

За словами джерела з Управління кіберпростору, наразі немає кіберактивності, яка б порушувала роботу лікарень. «Це не Гіллель Яфе чи Мааяней Хайешуа. З початку війни ми також перебуваємо напоготові на кіберфронті, і постійно плануємо ризики, досліджуємо ситуацію та просимо різні установи зробити певні дії. Цього

разу це лікарні, але були й інші інституції, які ми просили провести негайні дії», – розповіло джерело.

Джерело згадало про дві кібератаки, які торкнулися ізраїльських лікарень за останні два роки. Атака, яка закрила медичний центр Гілеля Яффе в комп'ютерній системі Hadera в жовтні 2021 року, змусила персонал і співробітників на кілька тижнів перейти на рукописні нотатки.

Нещодавно кібератака в серпні призвела до вимкнення комп'ютерних систем у медичному центрі Mayanei HaYeshua у Бней-Брак. Хоча атака вплинула лише на адміністративні комп'ютерні системи, «без будь-якої шкоди для лікування та пацієнтів центру», усі комп'ютерні системи лікарні були вимкнені як запобіжний захід». ***(Ido Efrati. Several Israeli Hospitals Asked to Cut Off Internet Access Over Cyberattack Fears // Haaretz Daily Newspaper Ltd. (https://www.haaretz.com/israel-news/2023-10-21/ty-article/.premium/several-israeli-hospitals-asked-to-cut-off-internet-access-over-cyberattack-fears/0000018b-52a7-df6e-a5db-76e7892a0000?utm_source=flipboard&utm_content=Haaretz%2Fmagazine%2FIsrael+and+Middle+East+News). 21.10.2023).***

***

Кіберзахист закладів охорони здоров'я

«…державна медична страхова компанія Філіппін не мала кіберзахисту. Це проклало хакерам шлях до використання мільйонів даних філіппінців і доступу до них. Витік на різні веб-сайти.

У тому ж звіті зазначено, що Філіппінська корпорація медичного страхування з тих пір повідомила своїх понад 36 мільйонів членів, або приблизно третину населення країни, про те, що їхні дані могли бути розкриті, хоча повний масштаб порушення досі невідомий.

Повідомляється, що атака почалася 22 вересня, коли співробітники увімкнули свої комп'ютери, в тому числі необхідні для обробки записів.

Bloomberg взяв інтерв'ю у Ізраеля Паргаса, старшого віце-президента сектору політики фінансування охорони здоров'я, де він заявив, що на екранах комп'ютерів з'явилося повідомлення з групою Medusa, яка бере на себе відповідальність за напад і вимагає 300 000 доларів США в обмін на видалення файлів агентства.

За його словами, постраждали близько 96 комп'ютерів, або приблизно 10% машин агентства в його штаб-квартирі в Манілі, метро Маніла.

Відсутність кіберзахисту

Повідомляється, що термін дії послуг кіберзахисту Philhealth закінчився в травні минулого року, і його не вдалося поновити через перегляд політики закупівель в організації; лише після хакерського інциденту організація зв'язалася з постачальником кіберзахисту, погодившись на 30-денну пробну версію.

Паргас, однак, зазначив, що організація також забезпечила «інші інструменти» для моніторингу майбутніх кібератак і подальшого вдосконалення кібербезпеки, яке буде отримано в майбутньому.

Цей інцидент є останнім у серії кібератак проти урядових установ Філіппін, які привернули увагу до значного ступеня беззахисності країни проти атак на кібербезпеку. Це викликало розслідування та занепокоєння з боку урядових установ і різних груп.

Національна комісія з конфіденційності Філіппін розпочала розслідування, щоб притягнути відповідальних посадових осіб до відповідальності та повністю зрозуміти повний масштаб витоку даних». ***(Aldohn Domingo. Philippine Health Insurer lacked Cyber Protection Software, Hacked for Days // Tech Times LLC. (https://www.techtimes.com/articles/297317/20231009/philippine-health-cyber-protection-software-hacked.htm?utm_source=flipboard&utm_content=other). 09.10.2023).***

***

«Дві лікарні в Нью-Йорку зазнали кібератаки та перенаправляють пацієнтів в інші заклади, повідомили представники лікарні в п'ятницю.

Кібератака вразила комп’ютерні системи в лікарні HealthAlliance у Кінгстоні, а також у лікарні Маргаретвілль і центрі медичної допомоги Mountainside Residential Care Center — усі вони є частиною мережі охорони здоров’я Вестчестерського медичного центру.

Мережа охорони здоров’я планувала вимкнути IT-системи в трьох установах, починаючи з 22:00 п’ятниці, «щоб усунути загрозу та вжити необхідних заходів для повного відновлення нашої безпечної мережі», — йдеться в заяві представників мережі.

Карети швидкої допомоги відводять від лікарні HealthAlliance як запобіжний захід, а деяких поточних пацієнтів виписали в інші заклади, повідомили чиновники.

За словами офіційних осіб, лікарня HealthAlliance та лікарня Margaretville залишаються відкритими, а пацієнтів, які прибули, проведуть лікування, оцінять і або відпустять, або стабілізують і переведуть до інших закладів. Вони додали, що не очікується жодних перебоїв у наданні допомоги в Mountainside Residential Care Center, закладі для медсестер.

Кібератаку розслідують місцеві правоохоронні органи разом з ФБР і незалежною фірмою з кібербезпеки, повідомили представники мережі охорони здоров’я.

Подібна кібератака змусила лікарні в кількох штатах вимкнути свої комп’ютерні системи протягом літа.

Серпнева атака на Prospect Medical Holdings зачепила лікарні в Каліфорнії, Коннектикуті, Пенсільванії, Род-Айленді та Техасі». ***(Cyberattack Hits 2 New York Hospitals, Forces Ambulance Diversions // U.S. News & World Report L.P. (https://www.usnews.com/news/us/articles/2023-10-20/cyberattack-hits-2-new-york-hospitals-forces-ambulance-diversions?utm_source=flipboard&utm_content=seanjkernan%2Fmagazine%2FUS+News). 20.10.2023).***

***

«Згідно з новим аналізом даних, лише у 2023 році понад чверть усіх американців побачили, що їх дані про охорону здоров'я було виявлено під час зламу.

Ця кількість подвоїлася порівняно з минулим роком, що є вражаючим зростанням навіть для індустрії охорони здоров'я, яка протягом тривалого часу була головною мішенню для хакерів через велику кількість особистих даних, які можна викрасти в результаті успішного злому.

Загальна кількість 87 мільйонів пацієнтів зросла порівняно з 37 мільйонами у 2022 році.

Новий аналіз зроблений Atlas VPN, який розглядає дані Управління з громадянських прав Департаменту охорони здоров'я та соціальних служб США, де організації охорони здоров'я повинні публічно повідомляти про порушення, які стосуються 500 або більше пацієнтів.

Відповідно до їхнього звіту, за перші три квартали 2023 року було зареєстровано 480 випадків витоку даних у секторі охорони здоров'я США, порівняно з лише 373 порушеннями за весь 2022 рік.

Двома найбільшими ударами стали порушення HCA Healthcare і Managed Care of North America, в результаті чого були розкриті дані 11 мільйонів і 8,9 мільйонів осіб відповідно.

Загалом цього року постраждали 87 мільйонів пацієнтів, більше чверті з 334,2 мільйона американців у країні втратили свої дані через порушення за останні 9 місяців.

Каліфорнія, Нью-Йорк, Техас, Массачусетс і Пенсільванія були п'ятьма штатами з найбільшою кількістю відкритих файлів пацієнтів. Це не дивно, враховуючи, що щільне населення в цих штатах означало б, що лікарняні системи просто мають більшу кількість даних пацієнтів, які можна втратити.

За збігом обставин лише одному штату США вдалося втекти без будь-яких повідомлень про напади: Вермонту. Atlas VPN зазначає, що «невелике населення штату та відсутність великих міст можуть дозволити йому пройти поза радаром досвідчених хакерів, які шукають максимальну винагороду».

Серед найбільш атакованих штатів кількість організацій охорони здоров'я, які були зламані, коливається від 43 (Каліфорнія) до 14 (Огайо).

Це було важке десятиліття для індустрії охорони здоров'я, коли хвилі пацієнтів з пандемією переважали над персоналом, а потім не менш згубні хвилі хакерів, які продовжують розширювати масштаб своїх порушень. Програмне забезпечення-вимагач було найбільшою проблемою у 2021 році, а тепер загальні зломи опинилися в центрі уваги.

Якщо ви працюєте в сфері охорони здоров'я, ви знаєте, що існує багато запобіжних заходів, які можуть зменшити ваш ризик. Використання антивірусного програмного забезпечення може допомогти, потенційно знизивши ймовірність успішної атаки зловмисного програмного забезпечення на 25%...» ***(Adam Rowe. Healthcare Data Breaches Impacted 25% of Americans in 2023 // Marketing VF Ltd. (https://tech.co/news/healthcare-data-breaches-impact-americans?utm_source=flipboard&utm_content=other). 20.10.2023).***

***

«Серед, здавалося б, нескінченного шквалу кібератак на галузь охорони здоров'я, які призвели до хаосу в лікарнях і час від часу порушували обслуговування пацієнтів, адміністрація Байдена не поспішає розробляти правила, спрямовані на підвищення кіберзахисту галузі.

«Ми розглядаємо всі наші варіанти», — сказала журналістам у середу Андреа Палм, заступник міністра охорони здоров'я та соціальних служб, після спільного проведення круглого столу з кібербезпеки з лідерами галузі. «Є ціла купа речей, які ми розглядаємо, щоб переконатися, що ми всебічно просуваємо цей порядок денний».

Міністерство охорони здоров'я та соціальних служб містить групу агенцій та офісів, які відіграють важливу допоміжну роль, коли йдеться про кібербезпеку охорони здоров'я. Один відділ допомагає галузі підготуватися до кіберінцидентів, а інший засвідчує, що постачальники медичних IT, як-от компанії, що виробляють програмне забезпечення для електронних медичних записів, відповідають вимогам

безпеки. Інша частина відділу контролює дотримання правил безпеки та конфіденційності медичних даних.

З огляду на всі ці напрямки роботи, що збігаються, Служба охорони здоров'я та соціальних служб може бути унікальною серед федеральних агенцій за кількістю потенційних напрямків, якими вона може скористатися для регулювання кібербезпеки в підконтрольному їй сектору. Незрозуміло, чи внутрішні суперечки щодо правильного підходу затримують розробку кіберрегуляторів охорони здоров'я, про які високопоставлений чиновник Білого дому вперше сказав, що вони розглядаються майже рік тому.

Також можливо, що агентство чекає додаткових ресурсів, перш ніж оприлюднити нові амбітні регуляторні зусилля. Health and Human Services «дуже усвідомлює проблеми з ресурсами» та потребу поєднати правила з «всеохоплюючою стратегією, яка приведе нас туди, де ми маємо бути», — сказав Палм The Messenger.

Круглий стіл у середу включав представників асоціацій лікарень і груп співпраці з кібербезпеки, і він дав вищим державним керівникам можливість задати своїм колегам у галузі питаннями про ризики, які їх найбільше хвилюють, і найкращі способи для уряду допомогти усунути прогалини в безпеці, які спричинили натиск дорогих і руйнівних атак програм-вимагачів.

Одна з тем, яка виникла під час обговорення: вразливість сільських лікарень і те, як їхні недоліки в кібербезпеці ставлять під загрозу всю галузь.

«Ми дуже стурбовані, тому що вони є найслабшою ланкою», — сказала Марі Савікіс, віце-президент із питань державної політики Коледжу керівних кадрів у сфері охорони здоров'я, професійної групи для старших IT-посадовців у компаніях охорони здоров'я. Савіцкіс закликав уряд започаткувати регіональні програми навчання або «навчальні табори» для керівників сільських лікарень.

У багатьох сільських лікарнях не вистачає спеціального персоналу з IT або кібербезпеки, а коли вони є, керівники не завжди знають правильні запитання, щоб їм поставити. Допомога цим закладам має починатися з «розуміння того, що ми не матимемо ресурсів» для виконання видів дорогих модернізацій, які іноді потрібні

для впровадження урядових рекомендацій щодо кібербезпеки, сказала Леслі Марш, президент Національної асоціації сільського здоров'я.

У якийсь момент Нік Лейзерсон, помічник національного кібердиректора Білого дому з кіберполітики та програм, запитав представників галузі, як уряд може переконати постачальників медичних послуг у тому, що витрачання грошей на кібербезпеку насправді принесе їм користь у довгостроковій перспективі.

Марк Джарретт, старший віце-президент і головний спеціаліст з якості Northwell Health, сказав, що ключовим є те, щоб кібербезпека стала «постійним» рефреном у дискусіях про догляд за пацієнтами. «Багато лікарень проводять обходи безпеки», — сказав Джарретт. «Чому б вам не зробити кібернетичною частиною ваших раундів безпеки? … Ви повинні опустити це до такого детального рівня».

Савіцкіс закликав Палма доручити федеральним центрам медичної допомоги та медичної допомоги підняти питання кібербезпеки під час розмов з лікарями про виставлення рахунків. Лікарі спілкуються з цим агентством «буквально щодня», сказав Савіцкіс. «Вони мають найбільший канал охоплення».

У своїй роботі з кібербезпеки в секторі охорони здоров'я Health and Human Services співпрацює з Агентством кібербезпеки та безпеки інфраструктури, яке визначило лікарні як одну з трьох пріоритетних спільнот, повних дуже вразливих цілей, поряд із службами водопостачання та школами K-12.

«Зрештою, це питання безпеки пацієнтів», — сказав журналістам у середу заступник директора CISA Нітін Натараджан.

Натараджан, колишній парамедик і командир медичної групи реагування, який керує роботою CISA з кібербезпеки охорони здоров'я, сказав, що HHS був добре підготовлений до співпраці з його командою, щоб надавати поради та підтримку галузі.

Але є одна велика проблема, яку CISA, HHS та їхні партнери в Конгресі досі не вирішили: як зробити оновлення кібербезпеки можливими для тисяч невеликих медичних закладів із недостатнім фінансуванням, які всіяні США.

Один із варіантів: великі лікарняні системи можуть надавати послуги з кібербезпеки — наприклад, сканування мереж на наявність вразливостей і допомогу

у впровадженні виправлень, коли це необхідно — безпосередньо меншим установам у своїх регіонах, можливо, за допомогою федеральних грантів. Натараджан чув деякі дискусії щодо цієї ідеї, подорожуючи країною та зустрічаючись з керівниками охорони здоров'я, хоча CISA чекає, щоб побачити, куди йдуть ці розмови, перш ніж схвалити конкретний підхід до надання цієї вкрай необхідної підтримки, сказав він.

Але Натараджан також сказав, що промисловість не повинна розраховувати на федеральний уряд для отримання всіх грошей, необхідних для виконання цього геркулесового завдання.

«Ми ніколи не будемо фінансувати федеральне фінансування нашого виходу з [ризиків] кібербезпеки», — сказав він The Messenger. «Це мають бути спільні зусилля». ***(Eric Geller. Health Care Hacks Are Proliferating. The White House Is Still Figuring Out What To Do // JAF Communications Inc. (https://themessenger.com/tech/health-care-cybersecurity-hacking-threats-government-industry?utm_source=flipboard&utm_content=TheMessenger%2Fmagazine%2FThe+Messenger+Latest). 26.10.2023).***

***

Захист персональних даних та соціальні мережі

«23andMe, компанія з генетичного тестування, визнала масштабну кібератаку, в результаті якої хакери викрали, опублікували та продали дані близько 1 мільйона людей, Verge повідомляє. Витік даних було виявлено після того, як хакери опублікували базу даних під назвою «Дані ДНК ашкеназі знаменитостей» на форумах темної мережі. База даних містить таку інформацію, як відображувані імена, стать, рік народження та деякі відомості про результати генетичного походження користувачів.

Зокрема, 23andMe — американська біотехнологічна та геномна фірма, яка пропонує послуги генетичного тестування клієнтам, які надсилають зразок слини до її лабораторій і отримують звіт про походження та генетичну схильність.

«Пропонуємо профілі ДНК мільйонів, починаючи від провідних світових бізнес-магнатів і закінчуючи династіями, про які часто говорять у теоріях змови. Кожен набір даних також супроводжується відповідними електронними адресами», — йдеться в одному з дописів на форумі з продажу даних.

Хакер також стверджував, що володіє даними знаменитостей, таких як Марк Цукерберг та Ілон Маск, але це не було підтверджено 23andMe.

Хакер пропонував оптом продавати профілі даних за ціною від 1 до 10 доларів за обліковий запис. Тим часом PCMag повідомив, що в продажу може бути до 7 мільйонів акаунтів.

«Головною цінністю цього злому буде особиста інформація, яка пізніше може бути використана в шахрайстві. Імена, адреси, номери телефонів, загальна особиста інформація – хакери, як правило, продають це шахраям, які потім можуть писати спамові електронні листи, які є більш цілеспрямованими. Це «Шановний Алан», а не «Шановний клієнте», тож ви думаєте, що вони знають, хто ви, і що це має бути законним», — сказав Metro професор Алан Вудворд, фахівець з кібербезпеки з Університету Суррея.

23andMe розглядає витік як достовірний і розслідує інцидент. Говорячи про злом, керуючий редактор 23andMe Скотт Хадлі сказав, що «попередні результати цього розслідування свідчать про те, що облікові дані, які використовувалися під час цих спроб доступу, могли бути зібрані зловмисником із даних, виточених під час інцидентів, пов’язаних з іншими онлайн-платформами, де користувачі переробляли облікові дані для входу». Він додав, що немає ознак «інциденту безпеки в наших системах».

«Ми серйозно ставимося до цієї проблеми та продовжимо наше розслідування, щоб підтвердити ці попередні результати», — йдеться в заяві 23andMe.

«З міркувань обережності ми вимагаємо від усіх клієнтів скинути свої паролі та заохочуємо використовувати багатофакторну автентифікацію (MFA). Якщо ми дізнаємося, що доступ до даних клієнта був отриманий без його авторизації, ми повідомимо його безпосередньо, надавши додаткову інформацію», — додається в заяві». ***(Hackers Claim To Have Stolen Millions Of Users' DNA Data, Sell It Online //***

NDTV (https://www.ndtv.com/feature/hackers-claim-to-have-stolen-millions-of-users-dna-data-sell-it-online-4483462?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 15.10.2023).

***

«Нове дослідження стверджує, що глобальний постачальник CRM зберіг основну базу даних клієнтів незахищеною в загальнодоступній мережі, доступною для всіх, хто знав, де шукати.

База даних містила сотні тисяч записів, багато з яких були особистою та конфіденційною інформацією, яка могла бути використана для крадіжки особистих даних, фішингу та інших форм кіберзлочинності та цифрового шахрайства, хоча, на щастя, немає жодних доказів будь-які порушення, однак.

Цю новину оприлюднив дослідник кібербезпеки Джеремія Фаулер, який виявив незахищену паролем базу даних компанії Really Simple Systems, яка стверджувала, що має близько 18 000 користувачів і клієнтів, включаючи такі організації, як Королівська академія, Червоний Хрест, NHS і IBM.

Фаулер знайшов усілякі формати — зображення, рахунки-фактури, шаблони, а також внутрішні записи Really Simple System. Загалом було понад 2,5 мільйона файлів.dat, понад 50 000 зображень і понад 100 000 рахунків-фактур із іменами клієнтів, адресами та деталями плану CRM. Крім того, в базі даних містилися медичні записи людей, документи, що посвідчують особу, договори на нерухомість, кредитні звіти, юридичні документи, податкові документи, угоди про нерозголошення та навіть претензії щодо втрати працездатності, усі з яких містили ідентифікаційні номери соціального страхування та податкові номери.

«Одна з папок клієнтів містила велику колекцію документів дитячої психологічної експертизи, позначених як конфіденційні», — сказав Фаулер.

Компанії, чиї дані зберігалися в цій базі даних, були розташовані в багатьох країнах світу, включаючи США, Великобританію, Австралію, кілька країн ЄС тощо.

Невдовзі після виявлення бази даних Фаулер зв'язався з компанією, якій знадобилося кілька днів, але зрештою закрили доступ. Немає доказів доступу будь-яких загроз до бази даних у минулому. Компанія Really Simple System повідомила, що звернулася до постраждалих клієнтів із відповідною інформацією». ***(Sead Fadilpašić. This top CRM provider left millions of client files exposed online // Future US, Inc. (https://www.techradar.com/pro/security/this-top-crm-provider-left-millions-of-client-files-exposed-online?utm_source=flipboard&utm_content=other). 09.10.2023).***

***

«Duolingo — одна з найпопулярніших у світі програм для вивчення мов, яка може похвалитися десятками мільйонів активних користувачів щомісяця. Однак на початку 2023 року з'явилася новина про те, що Duolingo зазнало витоку даних, у результаті якого були розкриті дані понад 2,5 мільйонів користувачів.

У результаті злому стався витік загальнодоступної та приватної інформації користувачів, включаючи справжні імена, адреси електронної пошти, номери телефонів і навчальні курси. Ось що вам потрібно знати.

Витік даних Duolingo: що трапилося?

Громадськість дізналася про проблему в січні 2023 року, коли дані з 2,6 мільйонів облікових записів клієнтів були виставлені на продаж на хакерському форумі за 1500 доларів.

Зараз форум закрито. Однак дослідники безпеки з VX-Underground виявили, що дані продаються на новій версії форуму за вісім кредитів на сайті, що означає приблизно 2,13 долара США.

Хакер стверджує, що зібрав дані з викритого API та поділився зразком із 1000 облікових записів. Ймовірно, зловмисник передав адреси електронної пошти з минулих порушень в API, щоб перевірити, чи були вони пов'язані з активними обліковими записами Duolingo, створивши набір даних із загальнодоступними та закритими даними.

Пояснення представника Duolingo полягає в тому, що дані були взяті з інформації загальнодоступного профілю. Однак важко повністю погодитися з цим твердженням, оскільки зібрані дані включали справжні імена користувачів, загальнодоступні логіни, прогрес у вивченні мови та адреси електронної пошти, які зазвичай не є публічними.

Хто постраждав від злому Duolingo?

Згідно з дослідженням Surfshark, витік даних Duolingo найбільше вразив США, вплинувши на майже 1 мільйон облікових записів. Південний Судан посів друге місце зі 175 000 постраждалих облікових записів, за ним йдуть Іспанія (123 000), Франція (105 000) і Великобританія (98 000).

Кожен зламаний обліковий запис електронної пошти мав близько п’яти точок даних, включаючи ім’я, ім’я користувача, зображення профілю, мову та країну. У деяких випадках усі дані користувача були розкриті.

Що далі відбувається зі скопійованими даними?

Брокери даних часто збирають зібрані дані соціальних мереж і продають їх третім особам для різних цілей, зокрема для маркетингу. Однак кіберзлочинці можуть використовувати витік даних користувачів Duolingo для здійснення атак соціальної інженерії, таких як цілеспрямовані фішингові атаки, використовуючи справжні імена та дійсні адреси електронної пошти жертв.

Ті, кого це стосується, можуть отримувати спеціальні фішингові електронні листи, наприклад мовні курси зі знижкою, завдяки витоку імен, прогресу курсу Duolingo та інформації про країну проживання. Ці електронні листи також можуть містити запрошення на подорожі до країн, де розмовляють мовою, яку ви вивчаєте.

Кіберзлочинці також можуть видавати себе за Duolingo та надсилати електронні листи з посиланнями на те, що виглядає як платна версія Duolingo або преміум-курс. Якщо ви клацнете ці посилання та введете платіжні дані, зловмисник може викрасти вашу інформацію.

Як боротися з витоком даних Duolingo

Видалення даних із веб-сайтів і додатків є загальновідомою проблемою багатьох великих технологічних компаній. Наприклад, у квітні 2021 року дані приблизно 500 мільйонів користувачів LinkedIn були зібрані.

Якщо ви підозрюєте, що під час злому стався витік ваших даних, ви можете вжити заходів, щоб усунути це. Одним із них є перевірка того, чи вашу інформацію було скомпрометовано під час відвідування веб-сайту HaveIBeenPwned. Це стверджує, що всі зламані дані Duolingo вже були в його базі даних.

Щоб запобігти фішингу, уважно перевіряйте листи, особливо термінові. Перевіряйте адреси відправників, не натискайте на підозрілі посилання та вкладення та подумайте про встановлення антивірусного програмного забезпечення для посиленого захисту від зловмисного програмного забезпечення у фішингових електронних листах.

Остерігайтеся атак з видаванням себе за іншу особу та ніколи не повідомляйте конфіденційну інформацію, як-от імена користувачів і паролі, електронною поштою, оскільки Duolingo не запитує таку інформацію в електронних листах. Крім того, дотримуйтеся порад постачальника, змініть свій пароль і подумайте про налаштування двофакторної автентифікації.

Що робити, якщо ви не впевнені щодо заходів безпеки, вжитих Duolingo для захисту даних користувачів? А можливо, ви сумніваєтеся в ефективності своїх дій? У такому випадку ви можете спробувати інші програми для вивчення мови.

Захистіть свої дані та зміцніть свій захист

Витоки даних стають все більш поширеними, а викрадені дані можуть служити для різних цілей, від маркетингу до кібератак, включаючи спроби фішингу. Зараз зловмисники мають доступ до багатьох даних користувачів Duolingo, включаючи їхні справжні імена та адреси електронної пошти.

Щоб усунути витоки даних, користувачі повинні вживати профілактичних заходів, зокрема навчитися виявляти потенційні порушення та спроби видати себе за іншу особу та боротися з фішинговими атаками». ***(Denis Manyinsa. Were You Hit by the Duolingo Data Breach? Here's What to Do Next // MUO (https://www.makeuseof.com/hit-by-duoling-data-breach-what-to-do-***

next/?utm_source=flipboard&utm_content=spngbb129%2Fmagazine%2FGosomer+is+Awsomer). 08.10.2023).

***

«Японська електронна компанія Casio Computer Co. Ltd. зазнала витоку даних, і компанія попередила, що дані клієнтів у Японії та за кордоном були викрадені.

Згідно з повідомленням Casio про порушення в середу, яке також містило вибачення, у витоку даних стороння сторона отримала неавторизований доступ до сервера освітнього веб-додатку компанії «ClassPad.net». Порушення призвело до витоку особистої інформації деяких зареєстрованих клієнтів у Японії та за її межами.

Порушення було частково виявлено 11 жовтня, коли співробітник спробував попрацювати в середовищі розробки та виявив, що стався збій бази даних. Потім Casio оцінила помилку, виявивши до 12 жовтня, що особиста інформація була доступна.

Особиста інформація, до якої було отримано доступ, включала імена клієнтів, адреси електронної пошти, країну/регіон проживання, інформацію про покупки, зокрема деталі замовлення та спосіб оплати, а також інформацію про використання послуг.

Було отримано доступ до 91 921 записів, що належать клієнтам у Японії, включаючи фізичних осіб та 1 109 клієнтів навчальних закладів. Крім того, було отримано доступ до 35 049 записів, що належать клієнтам у 148 країнах за межами Японії.

Злом стає ще цікавішим: хоча більшість компаній уникають розголошувати подальші подробиці, наприклад, як зловмисники отримали доступ, Casio не соромилась і заздалегідь визнала, що злом стався через людську помилку.

«Було підтверджено, що деякі налаштування безпеки мережі в середовищі розробки були вимкнені через операційну помилку системи відповідальним відділом і недостатнє операційне управління», — пояснили в компанії. «Casio вважає, що це

було причиною ситуації, яка дозволила зовнішній стороні отримати несанкціонований доступ».

Порушення було обмежено однією базою даних у середовищі розробки, і Casio заявляє, що не має доказів будь-якого несанкціонованого вторгнення в інші активи. База даних, про яку йде мова, залишається в автономному режимі, було зв'язано з правоохоронними та регулюючими органами, і Casio співпрацює із зовнішньою організацією безпеки, щоб провести подальше розслідування та розробити відповідні контрзаходи у відповідь на інцидент.

«Це порушення підкреслює важливість тестування веб-додатків у виробництві», — сказав SiliconANGLE Рей Келлі, співробітник Synopsys Software Integrity Group. «Хоча проведення тестування безпеки додатків на підготовчому етапі виробництва є хорошою практикою безпеки, однак воно не дозволяє додаткам уникнути проблем із безпекою, таких як неправильна конфігурація сервера та мережі або проблеми в ланцюжку постачання через конвеєр збірки, після розгортання у виробництво.»

Роджер Граймс, проповідник захисту на основі даних у тренінговій компанії KnowBe4 Inc., яка займається підвищенням рівня безпеки, сказав, що, оскільки злам стався через помилку гумору, «важливо, щоб будь-які зміни, що впливають на кібербезпеку, перевірялися перед впровадженням і періодично перевірялися всі налаштування безпеки для точність. Це показує важливість контролю змін і конфігурації. Дехто може вважати це «нудними темами», але вони є обов'язковими, якщо очікується, що організація залишатиметься безпечною в довгостроковій перспективі». ***(Duncan Riley. Human error cited as key cause of data breach at Japanese electronics company Casio // SiliconANGLE Media Inc. (https://siliconangle.com/2023/10/19/human-error-cited-key-cause-data-breach-japanese-electronics-company-casio/?utm_source=flipboard&utm_content=SiliconANGLE%2Fmagazine%2FSiliconANGLE). 19.10.2023).***

***

«У п’ятницю, 27 жовтня, корпорація Boeing заявила, що розглядає заяву кіберзлочинної групи Lockbit про те, що у неї була «величезна кількість» конфіденційних даних, викрадених у аерокосмічного гіганта, які вона виклала б в Інтернет, якби Boeing цього не зробила. не заплатити викуп до 2 листопада.

Хакерська група опублікувала годинник зворотного відліку на своєму веб-сайті з витоку даних із повідомленням: «Конфіденційні дані були викрадені та готові до публікації, якщо компанія Boeing не зв’яжеться протягом встановленого терміну!»

«Поки що ми не будемо надсилати списки чи зразки, щоб захистити компанію, АЛЕ ми не будемо зберігати їх у такому вигляді до кінцевого терміну», — заявила хакерська група.

Хакерська група зазвичай розгортає програми-вимагачі в системі організації-жертви, щоб заблокувати її, а також викрадає конфіденційні дані для вимагання.

«Ми оцінюємо цю заяву», - повідомила прес-секретар Boeing електронною поштою.

За даними Агентства з кібербезпеки та безпеки інфраструктури США (CISA), Lockbit була найактивнішою глобальною групою програм-вимагачів минулого року за кількістю жертв, які вона заявила у своєму блозі про витік даних.

За даними CISA в червні, банда, чиє однойменне програмне забезпечення-вимагач вперше було помічено на російськомовних форумах про кіберзлочинність у січні 2020 року, з того часу здійснила 1700 атак на організації США.

Lockbit не повідомив, скільки даних він нібито вкрав у Boeing, або суму викупу. У Boeing не дали жодних коментарів.

Хакерська група також не відразу відповіла на запит про коментар, надісланий на адресу, яку вона вказала на своєму сайті витоку даних». ***(Boeing assessing Lockbit hacking gang threat of sensitive data leak // Rappler (https://www.rappler.com/technology/boeing-assessing-lockbit-hacking-gang-threat-data-leak/?utm_source=flipboard&utm_content=other). 29.10.2023).***

***

«У міру того, як наше суспільство перетворюється на більш пов'язаний світ, важливим компонентом цієї зміни є потреба в безпечному та надійному водінні на наших дорогах. Нещодавній злом автомобіля Tesla менш ніж за дві хвилини французькою охоронною компанією Synacktiv демонструє, наскільки це серйозне занепокоєння: зловмисники змогли зламати кіберконтроль автомобіля, щоб здійснити ряд зловмисних дій, зокрема відкрити багажник автомобіля під час руху та доступу до інформаційно-розважальної системи.

Оскільки на ринок з'являється все більше підключених і автономних транспортних засобів (CAV) і електромобілів (EV), стає зрозуміло, що швидкість виробництва випереджає заходи безпеки. Кібербезпека транспортних засобів часто не враховується в автоматичному розгортанні, навіть незважаючи на те, що пов'язаний характер сучасних транспортних засобів робить їх сприйнятливими до хакерських атак та інших кіберпроблем.

Кібербезпека транспортного засобу є життєво важливою — без неї можливі серйозні травми або навіть летальні випадки. Уявіть наведений вище сценарій Tesla, але гірше: хакер бере під контроль автомобіль і замикає двері, розганяючи автомобіль на шосе. Потім водій або пасажир автомобіля отримує сповіщення на свій мобільний телефон із запитом на програму-вимагач у біткойнах — інакше хакер розіб'є автомобіль на узбіччі дороги.

Це екстремальний сценарій, але такий інцидент із програмним забезпеченням-вимагачем 2.0 можливий сьогодні. Головне питання полягає в тому, чи готові ми ввімкнути керування інцидентами для таких викликів автокібернетики?

Ще одна складна частина цієї проблеми полягає в тому, що кіберризик несе власник або оператор окремих транспортних засобів або, можливо, цілого парку електромобілів. Автопарк може складатися з легкових автомобілів, автобусів або вантажівок, а необхідні засоби контролю кібербезпеки повинні бути на місці, щоб забезпечити більшу кібергігієну цих транспортних засобів.

Оскільки електромобілі — це комп’ютери на колесах, потенційна атака розподіленої відмови в обслуговуванні (DDoS) на кілька транспортних засобів може вивести з ладу цілий парк транспортних засобів на наших дорогах. Уявіть собі сотні транспортних засобів для доставки або критично важливих транспортних засобів, які не працюють, і ці потенційні наслідки.

Робота флоту також залежить від інших критично важливих систем. Кібератака на лікарню в Айдахо на початку цього року, під час якої машини швидкої допомоги були перенаправлені в інші лікарні, демонструє, наскільки важливо захистити всю екосистему автомобіля, а не лише сам транспортний засіб. Ця атака також дозволяє нам уявити, наскільки серйозною вона була б, якби був зворотний сценарій: що, якби сам парк швидкої допомоги був виведений з ладу?

Якщо цього недостатньо, подумайте про крихкий стан нашого поточного ланцюга постачання та всі проблеми, з якими він зіткнувся після пандемії. А тепер уявіть, якби через кібератаку цілий парк доставки зупинився. Ланцюг постачання та транспортна інфраструктура будуть повністю пошкоджені, що призведе до великих економічних збоїв.

Важливо підкреслити, що ці кіберпроблеми зростають багаторазово, оскільки автопарки вантажівок переходять на автономні вантажівки, і це призводить до питань щодо юридичної відповідальності у разі будь-якого кіберінциденту.

Також не можна не помітити збір даних. Дані CAV і EV багаті особистою інформацією (PII), а також можуть містити іншу конфіденційну інформацію, як-от дані платіжних карток або комерційні дані (наприклад, відстеження автопарку та продуктивність). Для забезпечення конфіденційності та дотримання юридичних і договірних зобов’язань необхідно впровадити правила керування даними, щоб забезпечити передачу та зберігання цих даних.

Незважаючи на те, що в багатьох країнах існують загальні мандати щодо кібербезпеки, юрисдикції повинні прийняти законодавчі акти щодо автомобільної кібербезпеки для автомобілів, які рухаються на наших дорогах. Країни активно шукають найкращі способи просування вперед у сфері регулювання транспортних засобів — було наголошено на забезпеченні того, щоб виробники автомобілів

увімкнули кібербезпеку в усіх майбутніх моделях, однак щодо роботи електромобілів політики та найкращі практики все ще повільно розробляються та законодавчо закріплений.

Однією з сфер, на якій потрібно більше уваги, є перспектива власника/оператора як для окремих користувачів, так і для власників автопарків. Як споживачі, ми стурбовані функціями безпеки нашого нового автомобіля, але ми не ставимо жодних питань щодо рівня кібербезпеки автомобіля. Існує потреба в обізнаності користувачів, як і звичайного споживача, про важливість кібербезпеки для безперебійної роботи сучасного автомобіля.

Власники автопарків повинні забезпечити ефективний кіберконтроль. Вони повинні мати інвентаризацію всього програмного забезпечення на своїх транспортних засобах і переконатися, що вони обізнані про вразливі місця та порушення цих програмних програм. Крім того, вони повинні проводити активну оцінку кіберризиків для будь-яких третіх сторін, які розробляють програмне забезпечення для транспортних засобів.

Нарешті, вони повинні здійснювати кібермоніторинг транспортних засобів у режимі реального часу та переконатися, що процеси управління інцидентами діють для пом'якшення будь-яких несприятливих кіберподій. Лише завчасно ввімкнувши це цілісне кіберуправління, ці власники автопарків зможуть вижити в цьому дивовижному новому підключеному світі». ***(AJ Khan. Autonomous Fleets Are Almost Here. Are They Safe From Cyberattacks? // NEWSWEEK DIGITAL LLC (https://www.newsweek.com/autonomous-fleets-are-almost-here-are-they-safe-cyberattacks-opinion-1831474?utm_source=flipboard&utm_content=Newsweekdotcom%2Fmagazine%2FNewsweek). 09.10.2023).***

***

«За останні кілька місяців поява штучного інтелекту змінила те, як люди ведуть своє повсякденне життя. І хоча більшість із цих досягнень покращили та покращили те, як люди роблять речі, ця технологія також на радарі хакерів.

Згідно з новим звітом Microsoft, хакери тепер використовують складні методи на основі штучного інтелекту, щоб зробити свої атаки більш смертоносними та непомітними. Крім того, компанія розповіла, що хакери використовують існуючі генеративні інструменти ШІ та нові чат-боти для розгортання цих атак на нічого не підозрюючих користувачів.

«Кіберзлочинці та національні держави використовують штучний інтелект, щоб покращити мову, яку вони використовують у фішингових атаках, або зображення в операціях впливу», — заявив Том Берт, CVP з питань безпеки та довіри клієнтів Microsoft.

У звіті детально описується перехід хакерів від шифрування даних із зламаних мереж до шифрування даних віддалено, посилаючись на те, що до 60% атак, керованих людьми, виявлених Microsoft за минулий рік, використовували цей підхід. Такий підхід ускладнює для компаній пом’якшення проблеми, оскільки він прикриває сліди хакера, залишаючи холодний слід.

Згідно зі звітом, загальні атаки з викраденням даних досягли найвищого рівня за весь час, подвоївшись з листопада 2022 року по червень 2023 року. Для тих, хто не знайомий з цією ставкою, це, по суті, прийом, який використовують хакери для викрадення приватної інформації та даних, які потім використовували як приманку для вимагання викупу від постраждалих.

Технологічний гігант також повідомив про 200%-ве зростання кількості атак, керованих людьми, у період з вересня 2022 року по червень, посилаючись на те, що вони налаштовані для адаптації до певного середовища, на відміну від автоматизованих прийомів. Також спостерігається зростання кількості хакерів, які викрадають інформацію в організацій і використовують цю інформацію для вимагання грошей, погрожуючи оприлюднити або навіть продати її громадськості, якщо вони не підкоряться.

Натомість організації також підбирають технологію штучного інтелекту та використовують її, щоб розробити вогнестійкі інструменти, які можна використовувати для боротьби з цими складними кампаніями та хитрощами, розгорнутими зловмисниками, згідно з матеріалом WSJ.

Виступаючи на мережевому саміті WSJ CIO, виконавчий директор компанії Deep Instinct, яка займається кібербезпекою зі штучним інтелектом, Лейн Бесс зазначив, що важче пом'якшити атаки на основі ШІ, які використовують хакери.

Очевидно, що хакери стають більш креативними і тепер використовують технологію штучного інтелекту, щоб розробити витончені та складні методи розгортання своїх атак. Це викликає занепокоєння серед організацій і навіть уряду. Отже, існують плани щодо розробки технологій на основі ШІ, які використовуватимуться для протидії цим атакам…». ***(Kevin Okemwa. Unsurprisingly, cybercriminals are using generative AI like ChatGPT and Bing to refine their phishing attacks on you // Future US, Inc. (https://www.windowscentral.com/software-apps/unsurprisingly-cyber-criminals-are-using-ai-to-refine-phishing-attacks?utm_source=flipboard&utm_content=WindowsCentral%2Fmagazine%2FWindows+Central%3A+Start+Menu). 06.10.2023).***

***

«Оскільки штучний інтелект все глибше вплітається в структуру національної оборони, Агентство національної безпеки США оприлюднило спеціальний центр безпеки ШІ. Директор АНБ, генерал Пол Накасоне, який покидає свою посаду, оголосив про цей стратегічний крок у четвер.

Новий підрозділ штучного інтелекту буде розташовано в ширшій структурі Центру співпраці з кібербезпеки, зв'язку, де АНБ співпрацює з приватними організаціями та глобальними союзниками. Associated Press повідомляє, що метою є зміцнення кіберзахисту нації, особливо в умовах нависаючих загроз з боку таких держав, як Китай і Росія.

На недавньому заході для преси Накасоне висловив занепокоєння з приводу лідерства США у сфері штучного інтелекту, особливо щодо зростаючих можливостей Пекіна в кіберпросторі. «Сьогодні ми зберігаємо перевагу в області штучного інтелекту в Сполучених Штатах», — сказав він. «Цю перевагу ШІ не слід сприймати як належне».

ШІ та глобальний ландшафт кібербезпеки

З огляду на те, що на горизонті президентські вибори в США 2024 року, Накасоне підтвердив, що поки що немає жодних доказів спроб втручання таких великих супротивників, як Росія чи Китай. Однак він наголосив на зобов'язанні США забезпечити глобальні вибори у партнерстві з міжнародними союзниками.

У Китаю були явні кіберамбіції, нещодавні дії натякали на спроби скомпрометувати військовий зв'язок США. І США, і Японія висловили тривогу щодо кібератак Китаю на їхні оборонні інфраструктури.

Що стосується штучного інтелекту, Накасоне пояснив роль технологій в аналізі загроз.

«ШІ допомагає нам, але наші рішення приймають люди. Ця різниця має вирішальне значення", - сказав він. «Ми дійсно бачимо допомогу від штучного інтелекту. Але врешті-решт рішення будуть приймати люди та люди в циклі».

Новий центр штучного інтелекту співпрацюватиме з різними секторами США, включаючи наукові установи, дослідницькі лабораторії, Міністерство оборони та глобальних партнерів.

Поки АНБ готується до переходу керівництва, генерал-лейтенант ВПС Тімоті Го готовий прийняти кермо влади від Накасоне, наглядаючи як за АНБ, так і за Кіберкомандуванням США». ***(Maxwell William. NSA launches AI security center amid growing cyber threats // ReadWrite, INC (https://readwrite.com/nsa-launches-ai-security-center-amid-growing-cyber-threats/). 01.10.2023).***

***

«Гостьовий документ від NCC Group досліджує, як ШІ трансформує кібербезпеку, що глобальні регулятори роблять у відповідь і що все це означає для компаній, які розробляють стратегії ШІ.

Що означає ШІ для кібербезпеки?

Безпека систем штучного інтелекту (ШІ) — це сфера, яка постійно розвивається, і сучасні технології постійно розвиваються в темпі, оскільки ШІ застосовується в широкому діапазоні секторів і областей застосування. ШІ надає можливості як супротивникам, так і захисникам. Крім того, це створює нові ризики

для бізнес-процесів і безпеки даних, а також для безпеки при використанні в кіберфізичних системах, таких як автономні транспортні засоби. Експоненціальне впровадження та вплив штучного інтелекту в усіх секторах і технологіях підштовхує штучний інтелект ще більше до глобальних регуляторних планів, намагаючись отримати контроль над проблемами безпеки, безпеки та етики, пов'язаними з використанням штучного інтелекту.

Ці нові виклики необхідно враховувати при розробці стратегії безпеки для розробки або використання штучного інтелекту, гарантуючи, що користувачі зможуть отримати переваги, які приносить штучний інтелект, водночас керуючи ризиками на прийнятному рівні.

Процеси та політику управління ризиками необхідно адаптувати й оновлювати, щоб співробітники усвідомлювали свої обов'язки перед обличчям цих нещодавно доступних і спокусливих інструментів, а також щоб нові ризики, пов'язані з широким впровадженням штучного інтелекту, були зрозумілі, повідомлені та належним чином пом'якшені. NCC Group опублікувала цей офіційний документ, щоб допомогти тим, хто хоче краще зрозуміти, як штучний інтелект застосовується до кібербезпеки. У документі подано короткий опис того, як штучний інтелект може використовуватися як кіберпрофесіоналами, так і зловмисниками, ризикам, яким піддаються системи штучного інтелекту, проблемам безпеки, конфіденційності та етики, а також тому, як розвивається нормативно-правовий ландшафт для вирішення цих викликів. Для зацікавлених читачів ми також включили розділи про термінологію та технології штучного інтелекту та короткий виклад досліджень, опублікованих у цьому розділі NCC Group. Ми сподіваємося, що ця інформація стане в нагоді фахівцям із безпеки та керівникам вищої ланки, які прагнуть познайомитися зі сферою штучного інтелекту та кібербезпеки, допомагаючи зрозуміти нові ризики та загрози в цій сфері та те, як вони можуть вплинути на організації. Ми сподіваємося, що ця стаття також буде корисною для розробників, які хочуть зрозуміти випадки використання кібербезпеки для ШІ.

У цьому білому документі

Ми надаємо огляд технологій, що лежать в основі штучного інтелекту, детально описуємо загальні позитивні та негативні випадки використання та наслідки штучного інтелекту, перш ніж заглибитися в конкретні випадки використання штучного інтелекту в кібербезпеці.

Потім ми розглядаємо кіберзагрози для систем на основі штучного інтелекту та представляємо погляд на глобальне нормативне середовище штучного інтелекту, що формується, і що це означає для організацій, які прагнуть використовувати штучний інтелект.

Ми закінчуємо рекомендаціями щодо безпечного, безпечного та сумісного використання ШІ.

Ви отримаєте знання з провідних ресурсів у всьому світі, включно з нашими власними первинними дослідженнями, і підете з кращим розумінням ризиків і переваг для вашої організації. Знайдіть важливе розуміння світу безпеки штучного інтелекту, що розвивається, з наступальної та оборонної точок зору. Оскільки уряди в усьому світі запроваджують правила та законодавство, наші експерти інформують вас про останні новини». ***(Safety, Security, Privacy & Prompts: Cyber Resilience in the Age of Artificial Intelligence // techUK (https://www.techuk.org/resource/safety-security-privacy-prompts-cyber-resilience-in-the-age-of-artificial-intelligence.html). 05.10.2023).***

***

Широкий діапазон підключених пристроїв матиме право на отримання мітки, яка також включатиме сканований код, що посилається на спеціальну інформацію про безпеку пристрою та нещодавно створений реєстр кваліфікованих пристроїв IoT. У той час як багато хто проголошує ці зусилля для більшої прозорості та навчання споживачів, інші висловлюють занепокоєння щодо обсягу та реалізації нової програми.

Фон

Посилаючись на залежність споживачів від підключених пристроїв, які є частиною нашого повсякденного життя, FCC опублікувала Повідомлення про

запропоновану нормотворчість щодо створення позначки IoT, яка «допоможе споживачам порівнювати пристрої IoT і приймати обґрунтовані рішення про покупку, спонукатиме споживачів купувати пристрої з більшою безпекою, стимулюватиме виробники повинні відповідати вищим стандартам кібербезпеки, щоб задовольнити ринковий попит, і заохочувати роздрібних торговців продавати безпечні пристрої». Білий дім привітав ці зусилля щодо створення нового «Знака кібердовіри США», назвавши це останнім із серії дій адміністрації для захисту працьовитих сімей. Очікується, що програма буде запущена в 2024 році.

Обсяг пристроїв і продуктів

Нова програма маркування охоплюватиме розумні пристрої, починаючи від медичних пристроїв, фітнес-трекерів, GPS-трекерів, підключених до Інтернету пристроїв, персональних цифрових помічників, підключених до Інтернету камер домашнього спостереження, голосових пристроїв для покупок, маршрутизаторів для домашнього офісу, механізмів відкривання дверей гаража та радіоняні будуть включені в цю нову програму. Федеральна комісія з зв'язку (FCC) пропонує визначити придатний пристрій IoT як: (1) пристрій, підключений до Інтернету, здатний навмисно випромінювати радіочастотну енергію, який має принаймні один перетворювач (датчик або виконавчий механізм) для безпосередньої взаємодії з фізичним світом у поєднанні з (2) на принаймні один мережевий інтерфейс (наприклад, Wi-Fi, Bluetooth) для взаємодії з цифровим світом. Це визначення охоплює пристрій IoT і будь-які додаткові компоненти продукту (сервер, шлюз, мобільний додаток тощо). Федеральна комісія зв'язку хоче отримати коментарі щодо того, чи повинна програма зосереджуватися на продуктах або пристроях Інтернету речей для споживчого використання чи включати «корпоративні» пристрої або продукти, призначені для промислового чи бізнес-використання.

Критерії кібербезпеки IoT

FCC обговорює використання базових критеріїв кібербезпеки, зокрема, Рекомендованих критеріїв Національного інституту стандартів і технологій (NIST) для маркування кібербезпеки для споживчих продуктів Інтернету речей (IoT), для запропонованої програми маркування. Звідти FCC пропонує скликати організації зі

стандартизації, галузеві групи та державні установи для розробки вимог щодо безпеки IoT і програми оцінки відповідності.

Етикетка

Етикетка складатиметься зі знака сертифікації, який вказуватиме на те, що продукт або пристрій відповідає базовим стандартам кібербезпеки споживчого Інтернету речей FCC, і коду, який можна сканувати, спрямовуючи споживача до більш детальної інформації про продукт. Федеральна комісія зв'язку США (FCC) хоче дати коментар щодо того, де слід прикріпити етикетку та яку інформацію про пристрій слід пов'язувати з QR-кодом. FCC пропонує, щоб виробник розкривав гарантований мінімальний час підтримки для пристрою чи продукту. FCC також пропонує, щоб мітка була посиланням на новий реєстр IoT, де громадськість могла б отримати доступ до каталогу пристроїв, схвалених відповідно до програми, і переглянути доступну для пошуку інформацію про безпеку IoT.

Демонстрація відповідності

NPRM передбачає створення органів авторизації маркування кібербезпеки, також відомих як CyberLAB (за моделлю органів сертифікації телекомунікацій), які б тестували та оцінювали пристрої та продукти IoT. Такі CyberLAB будуть оцінені, акредитовані та визнані FCC або іншою третьою стороною. Компанії повинні будуть щорічно подавати заявку на знак, щоб продемонструвати постійну відповідність вимогам. Федеральна комісія з зв'язку (FCC) хоче отримати коментарі щодо виконання вимог програми маркування.

Ключові питання

Незважаючи на те, що багато хто аплодує Федеральній комісії зв'язку США (FCC) за те, що вона допомогла зробити пристрої IoT більш безпечними та надати споживачам більше інформації, питання щодо програми залишаються.

По-перше, дехто висловив занепокоєння щодо застосування цієї програми FCC до продуктів, які вже підпадають під інші режими. Наприклад, медичні пристрої вже регулюються іншими агенціями, такими як Управління з контролю за продуктами й ліками (FDA), і вже мають відповідати певним стандартам кібербезпеки. У той час як FDA, ймовірно, не заперечуватиме проти додавання мітки IoT до ярлика

медичного пристрою, за умови, що це не буде розглядатися як фальшиве або оманливе, таке маркування та тестування, що стоїть за ним, щоб продемонструвати відповідність, навряд чи будуть достатніми для задоволення вимог FDA щодо кібербезпеки. Увага до ризиків кібербезпеки та засобів контролю в медичних пристроях зростає, і FDA також посилило свою увагу. Минулого місяця FDA завершило свою інструкцію щодо «Кібербезпеки в медичних пристроях: міркування щодо системи якості та вміст передпродажних матеріалів» і вказало на свій намір відмовитися приймати маркетингові матеріали без необхідної інформації та даних про кібербезпеку. У міру того, як дані та тестування, необхідні для підтримки маркування IoT, відрізняються, чи потрібно буде компаніям медичних пристроїв генерувати ще більше даних про кібербезпеку, щоб отримати маркування IoT, чи даних, які генеруються для FDA, буде достатньо для задоволення обох вимог? Крім того, існує велика кількість програмних продуктів, які продаються на власний розсуд FDA і тому не відповідають стандартам FDA. Чи існує ризик того, що випуск маркування IOT буде розглядатися як певний урядовий дозвіл, який FDA може розглядати як потенційно оманливий, тим самим знижуючи рівень комфорту Агентства через відсутність активного регулювання цих типів продуктів? Для виробників медичних пристроїв буде важливо мати ясність щодо того, як ці два режими поєднуються, коли йдеться про один продукт.

По-друге, є побоювання, що ця «добровільна» програма з часом може стати обов’язковою та надто директивною.

По-третє, деякі наполягають на безпечних гаванях, тобто отримання ярлика служитиме захистом від відповідальності за збитки, спричинені кіберінцидентом.

Ці та інші питання необхідно буде офіційно порушити, щоб FCC врахувала їх при розробці остаточного правила.

Наступні кроки

Зацікавлені сторони, включаючи виробників і постачальників пристроїв, повинні проаналізувати цей NPRM і розглянути питання про надання FCC відгуків щодо пропозиції. Початкові коментарі щодо NPRM мали бути надіслані 9 жовтня, а коментарі – відповідь 10 листопада 2023 року. Після завершення періоду коментарів

зацікавлені сторони можуть подати документи ex parte у реєстр або запросити зустрічі з FCC для обговорення відповідних питань». ***(Katy Milner, Jodi Scott. FCC proposes a new cybersecurity labeling program for Internet of Things devices // Hogan Lovells International LLP (https://www.engage.hoganlovells.com/knowledgeservices/news/fcc-proposes-a-new-cybersecurity-labeling-program-for-internet-of-things-devices). 12.10.2023).***

***

«ШІ швидко стає центром уваги експертів галузі та регуляторів. Зростає занепокоєння, що зловмисники можуть використовувати штучний інтелект для посилення фішингових кампаній, розробки вдосконаленого зловмисного програмного забезпечення та втручання в інші технологічні порушення.

Однак, з іншого боку, штучний інтелект виявився неоціненним у зміцненні захисту кібербезпеки. Яскравим прикладом є те, як штучний інтелект було ефективно використано в Україні для протидії російським кібератакам. Очікується, що розвиток кіберзахисту, керованого штучним інтелектом, матиме вирішальне значення для стримування наростаючої хвилі кібератак.

Нещодавній звіт Microsoft Digital Defense Report підкреслює мінливий ландшафт загроз, наголошуючи на критичній необхідності тіснішої співпраці між державним і приватним секторами. Таке партнерство має вирішальне значення для створення середовища, яке підтримує глобальну кібербезпеку та інновації.

Перехід до кіберзлочинності як послуги

Отримані дані свідчать про те, що кіберзлочинці все частіше використовують модель кіберзлочинності як послуги, організовуючи масштабний фішинг, крадіжку особистих даних і розподілені атаки на відмову в обслуговуванні (DDoS). Злочинці удосконалили свою тактику, навчившись обходити багатофакторну автентифікацію для здійснення точних атак. Вимагання даних також зростає, причому з листопада 2022 року спостерігався значний сплеск потенційних випадків викрадання даних, що вказує на несанкціоновану передачу даних.

Примітно, що 13% ініційованих людьми атак програм-вимагачів, які переросли до фази викупу, включали певний елемент викрадання даних. За допомогою сповіщень, надісланих клієнтам, експерти Microsoft Defender визначили домінуючі кіберзагрози цього року:

Атаки на ідентифікацію

Порушення особистих даних проявлялося в різних формах: традиційні атаки грубою силою, складні стратегії розпилення паролів, які охоплюють різні країни та IP-адреси, а також тактика противника посередині (AiTM). Дані Microsoft Entra, спеціалізованого аналітичного підрозділу Microsoft, малюють жахливу картину: тривожне зростання кількості спроб злому порівняно з тим самим періодом 2022 року. Спроби зросли з приблизно 3 мільярдів на місяць до 30 мільярдів, що означає 4000 спроб зламу паролів. Хмарні ідентифікатори Microsoft за секунду.

Ключовою причиною цих порушень є слабкі заходи безпеки, які впроваджуються багатьма, особливо в освітньому секторі. Декілька установ не помічають важливості багатофакторної автентифікації (MFA), що робить їхніх користувачів уразливими до фішингу, підміни облікових даних і атак грубої сили.

Незважаючи на те, що MFA запроваджує додатковий рівень захисту, це не повністю відлякує зловмисників. Зловмисники розробили тактику обходу MFA, включаючи використання ботів з одноразовим паролем (OTP-ботів) для несанкціонованого доступу до облікового запису. Ці боти обманом змушують користувачів ділитися своїми одноразовими паролями, отриманими через SMS, програми автентифікації або електронні листи. Як тільки кіберзлочинці отримують OTP, вони отримують безперешкодний доступ.

Еволюція програм-вимагачів в епоху кібербезпеки та ШІ

Стратегії програм-вимагачів розвиваються, і зловмисники більше схиляються до ручних атак, використовують методи скритності та викрадають дані, щоб посилити вимоги щодо викупу. Кіберзлочинці відточують свої навички, тому користувачам стає дедалі складніше виявляти шахрайство, поки не буде завдано шкоди.

У звіті «Інциденти з програмами-вимагачами» визначаються як будь-які виявлені дії, пов’язані з програмами-вимагачами, зірвані або призвели до сповіщень. Це охоплює різні етапи атаки програм-вимагачів. Було окремо відзначено одну великомасштабну атаку програмного забезпечення-вимагача, спрямовану на кінцеві пристрої організації та хмарну інфраструктуру.

Корпорація Майкрософт визначила організацію, що стоїть за цією великою кампанією, як Mango Sandstorm. Його підхід був багатогранним і впливав як на фізичні, так і на хмарні системи. Зловмисники підвищили привілеї доступу, видаливши критичні дані та забезпечивши тривалу неавторизовану присутність у мережах за допомогою підробки програм OAuth.

Також помітно збільшилася кількість фішингових атак, спрямованих на компрометацію пристрою та крадіжку особистих даних за допомогою фішингу AiTM. Це передбачає викрадення постачальників для фішингу та неправомірне використання справжніх послуг для обману цілей.

Наростаюча хвиля фішингових атак AiTM: де зустрічаються кібербезпека та ШІ

Історично склалося так, що зловмисники використовували AiTM для захоплення облікових даних, розповсюдження зловмисного програмного забезпечення або накопичення особистих даних і файлів cookie сеансу. Корпорація Майкрософт спостерігала постійне зростання кількості фішингових кампаній AiTM, у деяких інцидентах були розіслані мільйони фішингових електронних листів за один день. Ця тенденція почалася у вересні 2021 року та значно посилилася до середини липня 2022 року, що підкреслює широкі спроби обійти МЗС.

Під час атаки AiTM зловмисник створює зворотний проксі-сервер між жертвою та законною сторінкою входу. Хоча зворотні проксі-сервери можуть підвищити безпеку, вони також можуть бути використані для зловмисних цілей. У сценаріях AiTM жертвам надається фальшива сторінка входу. На відміну від традиційного фішингу, окремий сервер, який належить зловмиснику, використовується для передачі викрадених облікових даних, ініціюючи виклик MFA.

Корпорація Майкрософт відстежує різні групи загроз, пов’язані з інструментами та службами фішингу AiTM, включно з відомими хакерами, використовуючи різні платформи. Шкідливі інструменти були розпізнані як Caffeine (пов’язаний зі Storm-0867), EvilProxy (пов’язаний зі Storm-0835) і NakedPages (пов’язаний зі Storm-1101). Спроби фішингу AiTM були пов’язані з поки що невідомими інструментами чи службами.

Інші інструменти, такі як Evilginx2, Modlishka та Muraena, є загальнодоступними. Їм не вистачає деяких повних функцій, які є в платних версіях. Завдяки впровадженню фішингових наборів AiTM для фішингу як послуги ширше коло загрозливих суб’єктів тепер має доступ до розширених інструментів, таким чином знижуючи бар’єр входу та підвищуючи ефективність атак.

Caffeine, EvilProxy і NakedPages спільно обслуговують сотні клієнтів, а кіберзлочинці сплачують ліцензійні збори в розмірі від 200 до 1000 доларів США щомісяця за підтримку щоденних операцій фішингу. З багатьма загрозами, які використовують ці платформи, виявлення окремих винуватців стає проблемою. Зараз акцент робиться на моніторингу цих служб, припиненні їхньої зловмисної діяльності та зміцненні захисту користувачів.

Компроміс ділової електронної пошти: прихована небезпека

Компроміс ділової електронної пошти (BEC) передбачає використання кіберзлочинцями різноманітних стратегій, від перехоплення розмов електронною поштою до розповсюдження спаму та боротьби з фінансовими шахрайствами. Хакери надсилають оманливі електронні листи зі шкідливими посиланнями та файлами зі зламаного ідентифікатора електронної пошти своїм контактам. Законна поява внутрішніх фішингових електронних листів спонукає багатьох одержувачів до ненавмисного взаємодії зі шкідливим вмістом.

Експерти Microsoft Defender помітили, що ці зловмисники часто створюють фальшиві ланцюжки електронної пошти, використовуючи маску справжнього ділового спілкування, щоб заманити нічого не підозрюючих жертв. Поєднання точної бізнес-термінології, здавалося б легітимних файлів і знайомства з

відправником робить ці електронні листи особливо переконливими і, отже, більш небезпечними.

Постійна тенденція зламу бізнес-електронної пошти також виявила ще один тривожний фактор: легкість, з якою кіберзлочинці можуть орендувати або купувати облікові записи електронної пошти з високою репутацією. Використовуючи такі облікові записи, зловмисники можуть обходити звичайні фільтри електронної пошти, забезпечуючи вищий рівень успішності своїх кампаній.

Кілька форумів про кіберзлочинність пропонують на продаж такі облікові записи електронної пошти з високою репутацією. Ставка для цих облікових записів зазвичай залежить від передбачуваної репутації та вихідного домену. Наприклад, облікові записи в освітніх або державних сферах можуть мати вищу ціну через їх природну надійність для одержувачів електронної пошти.

Контрзаходи на основі ШІ: потреба часу

Крім того, ландшафт зловмисного програмного забезпечення зазнав еволюції. Хоча інструменти виявлення зловмисного програмного забезпечення на основі сигнатур довели свою ефективність, сучасні кіберзлочинці часто використовують поліморфне зловмисне програмне забезпечення, яке змінює свій підпис, щоб уникнути виявлення. Проти таких загроз рішення на основі штучного інтелекту, які зосереджені на поведінковій аналітиці та евристичних шаблонах, демонструють багатообіцяючі результати. Ці інструменти безпеки наступного покоління не просто залежать від відомих сигнатур, але й оцінюють поведінку програмного забезпечення та процесів, щоб виявити будь-які дивні моделі, що вказують на зловмисну діяльність.

Враховуючи зростаючі загрози, очевидною є першорядна важливість співпраці між галузями промисловості, державними органами та приватними особами. Спільні знання, об’єднані ресурси та колективний інтелект можуть стати потужним захистом від складних стратегій сучасних кіберзлочинців.

Для організацій багаторівневий підхід до безпеки більше не є необов’язковим, а необхідним. Це включає використання передових інструментів на основі штучного інтелекту та виховання культури обізнаності про кібербезпеку серед співробітників.

Регулярні тренінги, імітаційні тести на фішинг і зворотній зв'язок у реальному часі можуть значно підвищити захист організації, перетворивши її персонал із потенційно вразливих місць на засоби безпеки.

Підсумовуючи, хоча штучний інтелект продовжує залишатися двосічним мечем у сфері кібербезпеки, його потенціал як потужного механізму захисту не можна ігнорувати. У той час, коли ми перебуваємо в епосі цифрових загроз, ми повинні зосередитися на використанні позитивних аспектів штучного інтелекту, сприянні глобальному співробітництву та створенні надійних систем, стійких до нових стратегій кіберсупротивників». ***(Muhammad Zulhusni. Ransomware & more: How cybersecurity and AI shape the digital realm // Tech Wire Asia (https://techwireasia.com/2023/10/microsoft-how-cybersecurity-and-ai-transform-threats-into-defenses/). 11.10.2023).***

***

«Канадські генеральні директори дедалі більше стурбовані готовністю своїх організацій до кібербезпеки, оскільки поява генеративного штучного інтелекту (ШІ) розглядається як загроза, що насувається.

Про це свідчить останній прогноз генерального директора KPMG, згідно з яким дев'ять із десяти керівників стурбовані тим, що поява генеративного штучного інтелекту може зробити їхні організації більш сприйнятливими до злому.

Хоча деякі генеральні директори визнавали потенціал генеративного штучного інтелекту, лише 8% назвали покращені можливості реагування на кібератаки перевагою впровадження цієї технології.

Тим часом 25% сказали, що вони стурбовані тим, що використання генеративного штучного інтелекту може призвести до проблем із відповідністю та безпекою, наприклад, до супротивників, озброєних штучним інтелектом.

Хартадж Ніджар, партнер і національний лідер канадської практики кібербезпеки KPMG, сказав, що це побоювання щодо генеративного штучного інтелекту зрозуміле, оскільки може бути важко оцінити, як такі технології можуть вплинути на стан кібербезпеки організації.

«Генеративний штучний інтелект може допомогти організаціям підвищити рівень безпеки та підвищити при цьому ефективність», — сказав він. «Однак реальність полягає в тому, що кіберзлочинці також збільшать використання генеративного штучного інтелекту у своїх стратегіях атак, і вони можуть набагато швидше впровадити цю технологію, ніж великі організації».

Ключ до кіберготовності до генеративних атак з підтримкою ШІ

У своєму опитуванні понад 1300 лідерів канадського бізнесу KPMG виявила, що лише 56% вважають, що їхні компанії належним чином готові до кібератак.

Менше 5% опитаних заявили, що їх організація «дуже добре підготовлена» до кібератаки.

Що стосується генеральних директорів, які вказали, що їхні організації недостатньо готові до кібератаки, основні причини включали:

Застарілі технологічні системи або інфраструктура (38%).

Зростання досвідченості кіберзлочинців (25%).

Відсутність інвестицій у кіберзахист (19%).

Ніджар попередив, що організації, швидше за все, побачать більш генеративні атаки з підтримкою штучного інтелекту, «зокрема через соціальну інженерію, де можна розгортати глибокі фейки, щоб обдурити співробітників, щоб вони зламали дані компанії та обійшли традиційні методи доступу».

Він підкреслив важливість готовності до загрози, що розвивається, шляхом створення «надійного захисту», включаючи інвестиції в технології кібербезпеки та навчання персоналу.

«Організації з сильними засадами кібербезпеки будуть краще оснащені для боротьби з невідомими ризиками технологій, що розвиваються, таких як генеративний ШІ», — сказав Ніджар». ***(Mika Pangilinan. Generative AI raises concerns about cybersecurity – survey // KM Business Information Canada Ltd. (https://www.insurancebusinessmag.com/ca/news/cyber/generative-ai-raises-concerns-about-cybersecurity--survey-464658.aspx). 27.10.2023).***

***

«Перший у своєму роді звіт попереджає, що ChatGPT та інші системи штучного інтелекту можуть бути використані для здійснення кібератак і виведення з ладу інших комп'ютерних систем.

Дослідники з Університету Шеффілда виявили вразливість шести комерційних інструментів ШІ, успішно атакувавши кожен з них.

Експерти виявили, що вони можуть створювати шкідливий код, якщо ставити конкретні запитання різним платформам.

Після виконання код може призвести до витоку конфіденційної інформації та перервати або навіть знищити служби.

Робота команди вже була використана для зміцнення комерційних платформ штучного інтелекту, хоча вони попереджають, що оновлені кіберстратегії постійно розробляються.

Дослідження, проведене вченими з Департаменту комп'ютерних наук Шеффілда, є першим, хто показує, що системи Text-to-SQL – штучний інтелект, який дозволяє людям здійснювати пошук у базах даних, ставлячи запитання простою мовою, яка використовується в багатьох галузях промисловості. використовуватися для атаки на комп'ютерні системи в реальному світі.

Їхні висновки показали, як штучний інтелект можна проникнути та маніпулювати ним, щоб допомогти викрасти конфіденційну інформацію, підробити або знищити цілі бази даних або навіть вивести з ладу служби за допомогою атак типу «відмова в обслуговуванні».

Команда виявила вразливі місця в шести комерційних інструментах ШІ: ChatGPT; BAIDU-UNIT – провідна китайська платформа, яку використовують клієнти в галузях, включаючи електронну комерцію, банківську справу, журналістику, телекомунікації, автомобільну та цивільну авіацію; AI2SQL; AIHELPERBOT; Text2SQL і ToolSKE.

У Baidu-UNIT – додатку для налаштування діалогу для спрощеної китайської – вчені змогли отримати доступ до конфіденційних конфігурацій сервера Baidu та вивели з ладу один серверний вузол.

«Насправді багато компаній просто не знають про такі типи загроз, і через складність чат-ботів, навіть у спільноті, є речі, які не повністю зрозумілі», — сказав Сютан Пенг, докторант Університету Шеффілда. який співкерував дослідженням.

Наразі ChatGPT приділяється багато уваги.

«Це автономна система, тому ризики для самої служби мінімальні, але ми виявили, що її можна обманом створити шкідливий код, який може завдати серйозної шкоди іншим службам».

Результати дослідження, представлені на Міжнародному симпозіумі з розробки надійності програмного забезпечення (ISSRE) у Флоренції, Італія, на початку цього місяця, також підкреслюють небезпеку того, як люди використовують ШІ для вивчення мов програмування, щоб вони могли взаємодіяти з базами даних.

«Ризик таких ШІ, як ChatGPT, полягає в тому, що все більше і більше людей використовують їх як інструменти підвищення продуктивності, а не як розмовного бота, і саме тут наше дослідження показує вразливість», — додав пан Пенг.

«Наприклад, медсестра може попросити ChatGPT написати команду SQL, щоб вони могли взаємодіяти з базою даних, наприклад тією, яка зберігає клінічні записи.

«Як показано в нашому дослідженні, код SQL, створений ChatGPT, у багатьох випадках може бути шкідливим для бази даних, тому медсестра в цьому сценарії може викликати серйозні збої в управлінні даними, навіть не отримавши попередження».

У рамках дослідження дослідницька група також виявила, що можна запускати прості бекдор-атаки, такі як встановлення «троянського коня» в моделях Text-to-SQL шляхом отруєння навчальних даних.

Така атака не вплине на продуктивність моделі загалом, але її можна спровокувати в будь-який момент і завдати реальної шкоди кожному, хто її використовує.

Доктор Марк Стівенсон, старший викладач дослідницької групи з обробки природної мови в Університеті Шеффілда, сказав: «Користувачі систем Text-to-SQL повинні знати про потенційні ризики, висвітлені в цій роботі.

«Великі мовні моделі, такі як ті, що використовуються в системах Text-to-SQL, надзвичайно потужні, але їх поведінка складна, і її важко передбачити.

«В Університеті Шеффілда ми зараз працюємо над тим, щоб краще зрозуміти ці моделі та дозволити безпечно реалізувати їхній потенціал».

Дослідники вже працюють разом із зацікавленими сторонами в індустрії кібербезпеки, щоб усунути вразливості, які виявило їхнє дослідження, оскільки системи Text-to-SQL стають все більш і більш широко використовуваними в суспільстві.

Їх роботу вже відзначила китайська платформа Baidu, Центр реагування на безпеку якої оцінив виявлені вразливості як дуже небезпечні.

Відтоді компанія звернула увагу та усунула всі повідомлені вразливості та навіть виплатила вченим винагороду за їх новаторську роботу.

Тепер дослідники сподіваються, що виявлені ними вразливості послужать закликом до спільнот обробки природної мови та кібербезпеки для виявлення та вирішення проблем безпеки, які досі залишалися непоміченими.

«Наші зусилля визнаються галуззю, і вони дотримуються наших порад щодо усунення цих недоліків безпеки», — сказав пан Пен.

«Однак ми відкриваємо двері на нескінченній дорозі – тепер нам потрібно побачити великі групи дослідників, які створюють і тестують виправлення для мінімізації ризиків безпеки через спільноти з відкритим кодом.

«Зловмисники завжди розроблятимуть більш просунуті стратегії, а це означає, що стратегії безпеки повинні йти в ногу.

«Для цього нам потрібна нова спільнота для боротьби з цими атаками нового покоління». ***(James Gamble. Hackers can use ChatGPT to steal your private data // Associated Newspapers Limited (https://metro.co.uk/2023/10/24/hackers-can-use-chatgpt-to-steal-your-private-data-says-new-study-19712353/?utm_source=flipboard&utm_content=RBenoit2014%2Fmagazine%2FSECURITY+%2F+PRIVACY+%2F+MALWARE+%2F+VULN+%2F+FRAUD+%2F+SURVEILLANCE++%2F+MCA+%2F+SAFETY). 24.10.2023).***

***

«Google вживає заходів для усунення кіберризиків, пов'язаних із генеративним штучним інтелектом (GenAI), розширюючи свою схему винагород за помилки, Vulnerability Rewards Program (VRP), щоб охопити сценарії атак, специфічні для генеративного штучного інтелекту.

Лорі Річардсон, віце-президент із питань довіри та безпеки, і Роял Хансен, віце-президент із конфіденційності, безпеки та техніки безпеки, заявили, що фірма вважає, що такий крок не лише швидше висвітлить потенційні проблеми безпеки та зробить штучний інтелект безпечнішим для всіх, але заохочувати ширшу спільноту проводити додаткові дослідження щодо безпеки та захисту ШІ.

«У рамках розширення VRP для ШІ ми по-новому дивимося на те, як слід класифікувати помилки та повідомляти про них. «Генеративний штучний інтелект викликає нові та інші проблеми, ніж традиційна цифрова безпека, наприклад, потенційна можливість несправедливого упередження, маніпуляції моделлю або неправильної інтерпретації даних [або] галюцинацій», — сказали вони.

«Оскільки ми продовжуємо інтегрувати генеративний штучний інтелект у нові продукти та функції, наші команди з довіри та безпеки використовують десятиліття досвіду та використовують комплексний підхід, щоб краще передбачати та перевіряти ці потенційні ризики.

«Але ми розуміємо, що зовнішні дослідники безпеки можуть допомогти нам знайти та усунути нові вразливості, які, у свою чергу, зроблять наші генеруючі продукти штучного інтелекту ще безпечнішими та надійнішими. У серпні ми приєдналися до Білого дому та колег з галузі, щоб дати можливість тисячам сторонніх дослідників безпеки знайти потенційні проблеми на найбільшому загальнодоступному заході DEF CON Generative AI Red Team.

«Тепер, оскільки ми розширюємо програму винагород за помилки та випускаємо додаткові вказівки щодо того, що ми хочемо шукати дослідникам безпеки, ми ділимося цими вказівками, щоб будь-хто міг побачити, що «в межах». Ми очікуємо, що це спонукає дослідників безпеки виявляти більше помилок і

прискорить досягнення більш безпечного та безпечного генеративного штучного інтелекту», – сказали вони.

У той же час Google також запроваджує нові заходи для кращого захисту ланцюга поставок штучного інтелекту, оголошуючи про ряд удосконалень у своїй Secure AI Framework (SAIF), яку вона запустила в червні 2023 року.

SAIF був розроблений, щоб підтримати галузь у створенні надійних додатків штучного інтелекту, основним принципом якого є безпека критичних компонентів ланцюга поставок, що забезпечує їх захист від таких загроз, як підробка, отруєння даних і створення шкідливого вмісту.

Крім того, Google зараз розширює свою роботу з безпеки відкритого коду та спирається на попередню співпрацю з Open Source Security Foundation. Завдяки цьому партнерству власна команда Google з безпеки з відкритим вихідним кодом (GOSST) використовуватиме структуру SLSA для покращення стійкості ланцюгів постачання, а Sigstore – для перевірки того, що програмне забезпечення в ланцюжку постачання ШІ відповідає його заявам. Google уже зробив доступними прототипи для перевірки атестації за допомогою SLSA та підписання моделі за допомогою Sigstore.

«Це перші кроки до забезпечення безпечної та надійної розробки генеративного штучного інтелекту, і ми знаємо, що робота тільки починається», — сказали Річардсон і Хансен.

«Ми сподіваємося, що, заохочуючи більше досліджень у сфері безпеки, одночасно застосовуючи безпеку ланцюга постачання до штучного інтелекту, ми започаткуємо ще більшу співпрацю з спільнотою безпеки з відкритим кодом та іншими представниками галузі, і зрештою допоможемо зробити ШІ безпечнішим для всіх».

Дослідник безпеки Endor Labs Хенрік Плейт, який спеціалізується на безпеці програмного забезпечення з відкритим вихідним кодом (OSS) і штучному інтелекті, прокоментував: «Застосування тих самих принципів безпеки та, де це можливо, інструментів для штучного інтелекту/ML — це чудова можливість розробляти безпечні системи з нуля.

«Порівняно з новим простором штучного інтелекту/ML, OSS або розробка програмного забезпечення на основі компонентів існує протягом більш тривалого періоду часу, що іноді ускладнює впровадження безпеки в усталені технології без порушення існуючих процесів розробки та розповсюдження програмного забезпечення.

«Існує багато спільного між створенням і спільним використанням компонентів програмного забезпечення та артефактами AI/ML: навчальні дані можна порівняти із залежностями програмного забезпечення, навчену модель із бінарними артефактами, а реєстри артефактів, такі як Maven Central або PyPI, із реєстрами моделей, такими як Hugging Face. І з точки зору розробників, які використовують моделі сторонніх розробників, ці моделі можна розглядати як будь-яку іншу залежність вище за течією.

«Деякі атаки також дуже схожі, наприклад, десеріалізація даних із ненадійних джерел, яка вже деякий час переслідує деякі екосистеми OSS: серіалізовані моделі ML також можуть містити шкідливий код, який виконується після десеріалізації (проблема відомого формату серіалізації pickle вже представлений на BlackHat 2011). Hugging Face і проекти з відкритим кодом намагаються вирішити це за допомогою спеціальних сканерів моделей». ***(Alex Scroxton. Google launches bug bounties for generative AI attack scenarios // TechTarget (https://www.computerweekly.com/news/366557318/Google-launches-bug-bounties-for-generative-AI-attack-scenarios?utm_source=flipboard&utm_content=jazzilla%2Fmagazine%2FAI+TODAY+AI). 27.10.2023).***

***

«…Згідно з нещодавнім звітом Upstream Security, у період з 2019 по 2020 рік кількість інцидентів, пов'язаних із кібербезпекою автомобілів, зросла на 99%. До 2022 року кількість випадків атак на автомобільні API зросла на 380%, що становить 12% від загальної кількості зареєстрованих інцидентів. незважаючи на передові заходи кібербезпеки, які застосовуються виробниками оригінального

обладнання. Ці загрози, що стосуються автомобільної кібербезпеки, охоплюють широкий спектр нападів, починаючи від віддаленого використання та витоку даних до атак програм-вимагачів і навіть фізичних маніпуляцій з компонентами автомобіля. Оскільки технологічний прогрес продовжується, підтримання високого рівня пильності в автомобільному секторі для розпізнавання та пом’якшення цих загроз залишається першорядним.

Вплив кібератаки

Витоки даних в автомобільному секторі почастішали, особливо за участю відомих виробників і брендів. Раніше цього року стався витік даних клієнтів Toyota у Японії, які були загальнодоступними протягом десяти років через просту технічну помилку. Понад два мільйони клієнтів отримали дані — це майже вся клієнтська база, яка підписалася на основні платформи хмарних сервісів Toyota з 2012 року.

Тоді відомого автомобільного продавця Арнольда Кларка шантажували хакери після витоку даних. Повідомлялося, що їхні адреси, паспорти та номери національного страхування потрапили в темну мережу після кібератаки на гіганта роздрібної торгівлі автомобілями.

Нещодавно компанія Tesla оприлюднила витік даних, який торкнувся приблизно 75 000 людей. Примітно, що це результат витоку інформації інформатора, а не зловмисної кібератаки. Скомпрометована інформація включає імена, контактну інформацію та трудові записи, пов’язані з нинішніми та колишніми працівниками, а також банківські дані клієнтів, секрети виробництва та скарги клієнтів щодо систем допомоги водієві.

Наведені вище приклади лише малюють поверхню величезної та заплутаної проблеми, ілюструючи, наскільки різні підприємства в автомобільному секторі знаходяться під загрозою. Очікується, що ці напади матимуть негативні наслідки кількома способами.

У разі витоку даних у виробника або роздрібного продавця автомобілів величезний обсяг ідентифікаційної інформації клієнтів, що знаходиться під загрозою, може серйозно підірвати довіру споживачів до бренду. Крім того, компрометація конфіденційних бізнес-даних, включаючи інтелектуальну власність,

фінансову інформацію та майбутні стратегії, становить значну загрозу, потенційно призводячи до втрати будь-якої конкурентної переваги, яку компанія могла мати.

Крім того, фінансовий збиток від кібератаки може бути дорогим, за останніми оцінками, середня вартість витоку даних становить 3,4 мільйона фунтів стерлінгів (4,2 мільйона доларів США). Після успішної атаки проведення аудиту та виправлення слабких місць може збільшити витрати, які компанія спочатку не врахувала.

Крім того, автомобільна компанія, яка стає об'єктом кібератаки або зазнає порушення даних, може зіткнутися з фінансовими штрафами відповідно до Загального регламенту захисту даних (GDPR) і європейських правил кібербезпеки. Ці нормативні акти, зокрема, включають Директиву про мережеві та інформаційні системи (NIS), яка наразі переходить до Директиви NIS2, яка має створити розширену структуру кібербезпеки ЄС, яка також охоплює галузь автомобільного транспорту. Крім того, очікується, що регуляторний орган проведе розслідування щодо дотримання компанією нормативних протоколів, визначаючи та підкреслюючи будь-які випадки, коли компанія не відповідає встановленим вимогам.

Дані, конфіденційність і підключені автомобілі

Ще одним зростаючим елементом автомобільної промисловості є ринок підключених автомобілів, який набирає обертів. Прогнозується, що до 2028 року його вартість зросте майже до 192 мільярдів доларів США. Навіть звичайні неелектричні транспортні засоби тепер містять широкий набір мікрочіпів, які контролюють широкий спектр функцій, починаючи від розваг і систем кондиціонування повітря до критичних операцій, таких як уникнення зіткнень, допомога в смузі руху та гальмування.

Природно, що зі збільшенням обчислювальної потужності та використання цих транспортних засобів зростає і кількість даних. Сучасні транспортні засоби більше схожі на комп'ютери з колесами. Ці транспортні засоби також мають низку інтелектуальних датчиків у ключових областях для збору великої кількості даних, які аналізують температуру шин, швидкість, GPS, а також рівень масла та води; деякі

автомобілі навіть контролюють пульс водіїв. Потім уся ця інформація використовується виробниками, які можуть контролювати інтервали обслуговування, якість продукції та продуктивність. Якщо ці дані не будуть належним чином анонімні або захищені, вони стануть потенційною мішенню для кіберзлочинців.

Найкращі практики безпеки даних

Отже, як автомобільна промисловість може ефективно продовжувати бізнес, зберігаючи безпеку даних для клієнтів?

Найважливішим для будь-якої організації є ознайомлення з даними, які вона обробляє, і усвідомлення регуляторних наслідків, пов'язаних з такою діяльністю. Можливо, конфіденційна інформація збирається незахищеним способом або без справжньої потреби. Після того, як склад інвентаризації даних компанії з'ясований, стає критично важливим визначити, які дані є конфіденційними, які потребують захисту, а які є поверхневими.

Здатність точного визначення місцезнаходження даних у будь-який момент часу має першочергове значення. Розуміння важливості цього у внутрішніх системах є ключовим кроком до забезпечення безпеки даних. Компанії повинні ініціювати захист будь-якого екземпляра конфіденційних даних із початкової взаємодії та підтримувати цей захист протягом усього життєвого циклу.

У сучасну цифрову епоху недостатньо простого розміщення маси даних на хмарному сервері, захищеному паролем, або покладатися виключно на захист периметра; ці заходи являють собою мінімум. Що справді є необхідним для захисту конфіденційних даних, так це стратегія безпеки, орієнтована на дані. Це передбачає зміцнення самих даних, а не зосередження лише на їх контейнері. Такі методи, як токенізація та псевдонімізація, які приховують дані, стають потужними інструментами в боротьбі за конфіденційність даних.

Ці методи працюють шляхом заміни регульованих даних «токеном», щоб полегшити аналіз даних для маркетингових або наукових програм. Винятковим аспектом є те, що токенізація робить інформацію безцінною для кіберзлочинців і

неавторизованих осіб, оскільки дані не залишаються у відкритому тексті, таким чином усуваючи фінансовий стимул для кібератаки на компанію.

Співпрацюючи з досвідченим технологічним партнером, який пропонує безперервну ідентифікацію даних, категоризацію та захист у всіх середовищах, організації в автомобільній промисловості можуть встановити надійну позицію для всіх даних, які обробляються. Зрештою, у цьому новому, керованому даними світі, автовиробники відповідають не лише за безпеку транспортних засобів». ***(Erfan Shadabi. How will cyber security evolve in the data-driven world? // Automotive World Ltd (https://www.automotiveworld.com/articles/how-will-cyber-security-evolve-in-the-data-driven-world/). 26.10.2023).***

***

Кіберзлочинність та кібертероризм

«Під час нещодавнього інциденту з кібербезпекою форум спільноти платформи Web3 Galxe Protocol став жертвою зловмисної атаки на записи системи доменних імен (DNS), що призвело до значних фінансових втрат. Атака, яка сталася 6 жовтня, призвела до перебоїв у роботі платформи приблизно на годину. Galxe Protocol звернувся до соціальних мереж, щоб попередити своїх користувачів і порадити не відвідувати його веб-сайт, доки ситуація не буде вирішена. На даний момент платформа ще не підтвердила, що вона повністю безпечна для використання, і деякі звіти вказують на те, що Google заблокував доступ до сайту.

Протокол Galxe зазнає DNS-атаки та постійних втрат

Серйозність зламу стала очевидною, коли криптодетектив ZachXBT повідомив, що зловмисники перенаправили записи DNS Galxe на фішинговий веб-сайт, спрямований на викачування криптовалютних гаманців користувачів. Зловмисникам вдалося викрасти кошти користувачів Galxe, і навіть після того, як платформа відновила свій веб-сайт, експлойт продовжив збирати кошти, накопичивши близько 160 000 доларів США до 17:15 UTC, за даними DeBank.

Більше того, ZachXBT припустив потенційний зв’язок між цією атакою на протокол Galxe та попереднім інцидентом із залученням протоколу Balancer 19 вересня. Протокол Balancer зазнав подібної атаки DNS, що призвело до збитків у розмірі 238 000 доларів США. Команда Balancer визначила цей інцидент як атаку соціальної інженерії на її DNS-сервер, імовірно організовану системою зливу крипто-гаманців, відомою як Angel Drainer. Фахівці з безпеки компанії SlowMist, що спеціалізується на блокчейні, висунули підозри, що зловмисник мав зв’язки з Росією.

Зростаючі втрати проектів Web3 підкреслюють зростаючий ландшафт загроз

Напад на протокол Galxe є лише одним із прикладів тривожної тенденції в екосистемі Web3. Недавній звіт платформи кібербезпеки Immunefi показує значне збільшення збитків для проектів Web3 протягом третього кварталу 2023 року порівняно з тим же періодом попереднього року. У звіті зазначено, що кількість атак на проекти Web3 зросла з 30% до 76% порівняно з минулим роком, а загальні збитки протягом третього кварталу 2023 року склали майже 686 мільйонів доларів.

Найзначніші втрати за цей період пов’язані зі зломом Mixin, який стався 25 вересня. Ці зростаючі втрати підкреслюють зростаючі проблеми, з якими стикаються платформи Web3 у захисті своїх активів і даних користувачів від невпинної хвилі кібератак.

Відповідь Galxe Protocol і поточні розслідування

На тлі заворушень представник Galxe Protocol опублікував заяву, запевнивши користувачів щодо безпеки їхніх коштів та інформації. У заяві уточнюється, що веб-сайт Galxe залишається в автономному режимі, доки правильні записи DNS не будуть поширені у всьому світі. Примітно, що платформа відновила право власності на домен 6 жовтня о 9 ранку за тихоокеанським стандартним часом і посилила безпеку свого облікового запису через службу реєстрації доменів Dynadot.

Крім того, Протокол Galxe вжив активних заходів для вирішення ситуації шляхом взаємодії з відповідними правоохоронними органами. Ця співпраця підкреслює серйозність інциденту та прагнення платформи притягнути зловмисників до відповідальності за свої дії.

Висновок

Нещодавня атака DNS на протокол Galxe служить яскравим нагадуванням про постійні загрози, з якими стикаються платформи Web3 і ширша екосистема криптовалют. Оскільки проекти Web3 продовжують розвиватися та розширюватися, так само розвиваються і тактики зловмисників, які прагнуть використовувати вразливості. Поточне розслідування цього інциденту, швидше за все, проллє більше світла на винних у атаці та може призвести до посилених заходів безпеки в спільноті Web3 для захисту від майбутніх загроз». ***(Haseeb Shaheen. Web3 platform Galxe Protocol experiences DNS attack, Suffers Over $150K in losses // cryptopolitan (https://www.cryptopolitan.com/web3-platform-galxe-protocol-dns-attack/?utm_source=flipboard&utm_content=Cryptopolitan%2Fmagazine%2FLatest+Crypto+and+Blockchain+News). 07.10.2023).***

***

«Кібератаки завдають величезної шкоди цільовим компаніям. Лише в Німеччині 22% усіх логістичних компаній зазнали кібератак у 2022 році. У ЄС рівень атак становить ймовірно, буде принаймні порівняно високим, але, швидше за все, навіть вищим. Моріс Тельтшер, генеральний директор INVENTRY GmbH, представив цифри щодо цієї важливої проблеми безпеки та інші факти про кіберзлочинність на нещодавній мережевій події Riege Software у Дюссельдорфі.

Загалом експерти INVENTRY опитали 500 логістичних компаній, зробивши результати дуже репрезентативними. Тим не менш, ці результати викликали ще більше занепокоєння, ніж згадані вище цифри Експерт з питань безпеки Тельтшер доповів 90+ учасникам зустрічі Riege Software: 95% компаній, які брали участь у розслідуванні, не змогли працювати в Інтернеті через успішна хакерська атака. Вони були офлайн в середньому тридцять днів, що призвело до значного економічного збитку. Особливе занепокоєння викликає те, що майже всі вони мали уразливості в їхніх системах безпеки даних, які хакери змогли використати у власних цілях. Те, що може повторитися в майбутньому, якщо недоліки не будуть усунуті та кібер безпека не покращена. Загалом це було правдою для тривожних 95% опитаних компаній.

Платити викуп дорого і допомагає лише в обмеженій мірі

Ці цифри також змушують людей сісти й звернути увагу: щоб відновити їхні дані від хакерів, злочинцям було сплачено викуп у середньому 252 000 євро. І 46% усіх зламаних компаній вирішили це зробити заплатити за повернення своїх даних. З одного боку, це зрозуміло, оскільки рівень виявлення хакерських атак становить менше одного відсотка. З іншого боку, повернення даних після викупу було платний не гарантує, що він не буде витік до громадськості через інші канали. Це пов'язано з тим, що хакери зазвичай розміщують важливу інформацію в темній мережі, де інші можуть її підхопити, наприклад повідомив експерт з безпеки.

Кібератаки – ще один засіб ведення війни

Деякий час кібератаки на західні компанії здійснюють переважно російські групи. Вони не так зацікавлені у викупах, ніж у завданні шкоди економіці. Це шоу сила та спроба принизити компанії, що базуються в ЄС – ще одна лінія конфлікту в боротьбі Кремля із західною системою.

Компанії, які мають велику кількість постачальників, такі як Airbus, яку Тельтшер навів як приклад, особливо піддаються високому ризику. Ці постачальники часто є шлюзом для крадіжки даних і розміщення зловмисного програмного забезпечення, оскільки їхні системи безпеки легше зламати, ніж власні системи виробника літака та спеціаліста з оборони.

Три важливі запобіжні заходи

Захисні заходи, які він рекомендує, включають ефективний брандмауер, який блокує несанкціонований трафік, часту зміну пароля, підтвердження ідентифікації за допомогою двофакторної автентифікації, регулярну навчання, включаючи підвищення кваліфікації для співробітників, і плани дій на випадок успішної або частково успішної хакерської атаки. Підсумовуючи, компанії повинні мати три стовпи обов'язково врахуйте, коли мова заходить про покращення кібербезпеки: 1. Профілактика шляхом впровадження високих стандартів безпеки, включаючи інформування працівників, 2. Резервне копіювання даних із щоденними оновленнями та нарешті - щоб запобігти гірким і дорогим наслідкам – 3. Створення та оновлення плану на випадок надзвичайних ситуацій». ***(Heiner Siegmund. Cyber***

Security is not yet on everybody's mind // CargoForwarder Global (CFG) (https://www.cargoforwarder.eu/2023/10/08/cyber-security-is-not-yet-on-everybody-s-mind/). 08.10.2023).

***

«Згідно з опитуванням про порушення кібербезпеки за 2023 рік, опублікованим Департаментом науки, інновацій і технологій 19 квітня 2023 року, 32% компаній постраждали від кіберзлому або атаки за останні 12 місяців. Для великих підприємств цей показник вищий і становить 69%. Подальші дослідження вказують на те, що пенсійні схеми Великої Британії мали найбільше зростання, повідомляючи про збільшення кількості повідомлень про порушення даних до Управління інформаційного комісара на 4000%, з шести у 2021/22 до 246 у 2022/23. Ці статистичні дані чітко показують, що кібератаки залишаються ключовим ризиком для бізнесу в усіх секторах, і пенсійна галузь не є винятком.

Через те, що вони зберігають значні обсяги особистих і конфіденційних даних, пенсійні схеми є ключовими цілями для цих атак. Наслідки успішних кібератак на пенсійні схеми можуть бути серйозними, завдаючи шкоди репутації постачальників і фінансових втрат членам. Такі інциденти також можуть викликати судові позови з боку членів і накласти на постачальників значні регулятивні штрафи за певних обставин серйозного порушення. Офіс уповноваженого з питань інформації (ICO), зокрема, має повноваження накладати штрафи на суму до 17,5 мільйонів фунтів стерлінгів або еквівалент до 4% річного обороту – залежно від того, яке значення є вищим.

Ця зростаюча загроза чітко показує, що існує потреба в надійних заходах безпеки в рамках пенсійних схем, і тому довіреним особам і менеджерам схем необхідно вжити заходів для захисту своїх учасників від таких атак.

У цьому матеріалі ми досліджуємо загрози кібербезпеці, з якими стикається пенсійний сектор Великобританії, і обговорюємо, які кроки можуть вжити довірені особи, щоб захистити своїх членів і активи від цього ризику. Ми також заглиблюємось у практичні вказівки, видані регуляторними органами, такими як

Пенсійний регулятор (TPR), спрямовані на захист цих важливих пенсійних фондів від кіберзагроз.

Типи кіберзагроз для пенсійних схем

Пенсійні схеми стикаються зі значними загрозами через різні форми кібератак, причому найбільше занепокоєння викликають фішинг і атаки програм-вимагачів.

Фішингові атаки включають шахраїв, які обманом змушують людей розголошувати конфіденційну інформацію. Це може бути неймовірно шкідливим для пенсійних схем, оскільки, якщо така інформація буде надана, це може призвести до того, що зловмисники отримають доступ до реквізитів рахунків пенсійної схеми, куди вони потенційно можуть перенаправити кошти або зробити несанкціоноване зняття. Це також може бути проблематичним для постачальника схеми, оскільки успішна фішингова атака може завдати шкоди його репутації та ускладнити залучення нових учасників.

Атаки програм-вимагачів — це коли зловмисник може заблокувати доступ до критично важливих систем, доки не буде сплачено викуп. Це часто робить зловмисник, який розгортає шкідливе програмне забезпечення, яке може проникати та шифрувати дані в мережі. Зазвичай зловмисники просять сплатити викуп у криптовалюті, яку важче відстежити, і натомість вони нададуть ключ розшифровки. Якщо цей ключ не надано, це може означати, що ця інформація остаточно втрачена.

Поточний нормативний ландшафт і вказівки

Як згадувалося вище, фінансові втрати для зацікавлених сторін, репутаційна шкода для постачальників схем і потенційні регулятивні штрафи через недотримання законів про захист даних чітко вказують на те, що довірчі особи та постачальники схем повинні надавати пріоритет кібербезпеці.

TPR виклав свої очікування щодо довірених осіб у новому проекті єдиного кодексу правил. Хоча цей кодекс ще не набув чинності та є ранньою версією, розробленою з метою використання в консультаціях щодо нового кодексу практики, він повторює положення, висловлені раніше TPR у своїх інструкціях щодо кібербезпеки для пенсійних схем, опублікованих у квітні 2018 року.

У цьому проекті кодексу TPR чітко пояснює, що довірчі особи та менеджери схем несуть відповідальність за безпеку інформації та активів схем, а також зобов'язані за законом використовувати адекватні засоби внутрішнього контролю для роботи своєї схеми.

Таким чином, слід вжити заходів для підвищення кіберстійкості. TPR визначив заходи, які довірені особи повинні враховувати під час (i) оцінки кіберризиків і (ii) управління кіберризиками. Їх можна підсумувати нижче:

Оцінка кіберризику

Знання та розуміння: довірені особи повинні розуміти кіберризики, пов'язані з їх схемою.

Конфіденційність і цілісність: довірені особи повинні визнавати необхідність збереження конфіденційності, цілісності та доступності систем, які обробляють персональні дані.

Визначені ролі та обов'язки: між постачальниками мають бути визначені чіткі ролі для виявлення кіберризиків і порушень, а також реагування на інциденти.

Ведення реєстру ризиків: кіберризики мають бути частиною реєстру ризиків і регулярно переглядатися.

Оцінка вразливості: слід проводити регулярні оцінки вразливості до кіберінцидентів щодо ключових функцій схеми, систем, активів (включаючи дані) і постачальників послуг.

Доступ до спеціалізованих навичок: довіреним особам слід розглянути можливість залучення спеціалістів, щоб розуміти ці ризики та ефективно керувати ними.

Оновлення елементів керування системою: переконайтеся, що засоби керування системою, такі як брандмауери та антивірусне програмне забезпечення, оновлені.

Управління кіберризиками

Регулярне резервне копіювання: переконайтеся, що критичні системи та дані регулярно створюють резервні копії.

Політика використання пристрою: установіть правила використання пристрою, включаючи сценарії домашньої та мобільної роботи.

Політика та засоби керування даними: запроваджуйте політики контролю доступу, захисту, використання та передачі даних відповідно до чинних законів про захист даних.

Ефективність політики: вжийте необхідних заходів, щоб гарантувати, що ця політика залишатиметься ефективною з часом.

Повідомлення про порушення: мати вказівки щодо того, коли про порушення потрібно повідомляти ICO.

План реагування на інциденти: Дотримуйтесь плану, у якому описано кроки, вжиті під час будь-якого інциденту, щоб забезпечити безпечне та швидке відновлення операцій – дізнайтеся більше в розділі «Планування безперервності».

Оцінка засобів контролю постачальників послуг: переконайтеся, що постачальники послуг, які беруть участь у запущених схемах, мають надійні заходи кібербезпеки.

Отримання регулярних звітів: отримуйте періодичні звіти від персоналу/постачальників послуг про будь-які виявлені ризики чи інциденти, які мали місце.

Дотримуючись цих вказівок, пенсійні схеми можуть значно зменшити свій вплив на потенційні кіберзагрози, загалом забезпечуючи кращий захист інтересів членів від еволюції цифрових загроз.

Окрім вищезазначеного, TPR чітко дав зрозуміти, що керівні органи також повинні знати про свої обов’язки відповідно до Загального регламенту захисту даних Великобританії (GDPR). ICO забезпечує виконання GDPR і передбачає, що постачальники схем мають певні зобов’язання повідомляти про порушення даних протягом 72 годин після того, як їм стало відомо про будь-які порушення персональних даних.

Висновок

У середовищі кіберзагроз, що постійно змінюється, пильність є важливою, особливо в пенсійній індустрії, яка захищає не лише значні фінансові активи, а й

величезні обсяги конфіденційних персональних даних. Тому для довірених осіб і постачальників схем вкрай важливо бути в курсі останніх тенденцій кібербезпеки та потенційних вразливостей – вони повинні переконатися, що вони тримають в курсі регуляторних вказівок, щоб підвищити свою кіберстійкість і оцінити свій підхід до політики управління ризиками». ***(Alan Cronin. Cyberattacks and pension schemes: understanding the risks and guidance // Dentons (https://www.ukemploymenthub.com/cyberattacks-and-pension-schemes-understanding-the-risks-and-guidance/#page=1). 03.10.2023).***

***

«…Уряди збираються у Відні 19 жовтня для обговорення глобальної угоди про кіберзлочинність. Але замість того, щоб дотримуватися поставленого завдання – сприяння глобальному досвіду та співпраці в боротьбі з кіберзлочинністю – запропонована угода передбачає широкі повноваження для розслідування практично будь-якого кримінального правопорушення, яке можна уявити, навіть якщо технології взагалі не задіяні.

Цей хибний підхід сприятиме транскордонним репресіям. І це ускладнить розслідування реальних кіберзлочинів.

Незаплановані переговори ООН за закритими дверима у Відні є останньою спробою подолати розбіжності між урядами щодо сфери дії договору та щодо того, яку роль, якщо взагалі мають відігравати права людини, не лише у розробці договору, а й у його виконанні. і остаточне виконання.

Основним питанням розбіжностей було те, чи повинен запропонований договір охоплювати лише правопорушення, пов’язані з комп’ютерами, як-от атаки на комп’ютерні дані чи системи, чи більшу групу злочинів, вчинення яких здійснюється за допомогою технологій.

З’являється пакет компромісів, який викликає серйозне занепокоєння, який передбачав би кримінальну відповідальність за відносно вузький перелік правопорушень в обмін на міжнародну співпрацю щодо будь-якої діяльності, яку уряд криміналізує всередині країни, яка передбачає покарання у вигляді принаймні

3 або 4 років позбавлення волі. Цей підхід жертвує правами людини заради досягнення консенсусу.

Уряди в усьому світі криміналізують можливість вільно говорити, виражати невідповідну сексуальну орієнтацію чи гендерну ідентичність або мирно протестувати, що є грубим порушенням прав людини. Людей засуджували до значних термінів ув'язнення або навіть засуджували до смертної кари за критику своїх урядів у соціальних мережах.

ЛГБТ-людей затримували та навіть катували через їхню сексуальну орієнтацію чи гендерну ідентичність; махання райдужним прапором на концерті або наявності облікового запису в додатку для знайомств для осіб однієї статі може бути достатньо, щоб викликати переслідування, замасковане під кримінальне переслідування. У сучасному світі ці та інші дії залишають цифрові сліди, які найчастіше знаходяться в іншій юрисдикції.

Вимагаючи взаємної правової допомоги щодо цих та інших «злочинів», запропонована угода запрошує уряди сприяти порушенням прав людини в усьому світі, надаючи повноваження зі спостереження за транскордонними розслідуваннями за допомогою безпрецедентного багатостороннього інструменту.

Уряди стверджують, що запропонована угода може вирішити проблеми з правами людини, дозволяючи їм відмовляти в проханнях про співпрацю, якщо основна діяльність, яка розслідується, захищена правами людини, якщо вона політично вмотивована або якщо вона не є злочином у їхніх кордонах.

Хоча включення всіх цих підстав для відмови було б корисним, запропонована структура продовжувала б загрожувати правам людини, підриваючи мету договору – боротьбу зі справжньою кіберзлочинністю.

По-перше, підстави для відмови є дискреційними. Навіть уряди, які мають потужний захист свободи слова та приватного життя вдома, виявилися ненадійними захисниками прав, коли йдеться про міжнародну співпрацю, наприклад, в ім'я боротьби з тероризмом.

У випадках, коли країни, що співпрацюють, визнають кримінальною відповідальність за поведінку, яка захищається правами людини, цей договір у його

нинішній редакції забезпечить правову основу та законну основу в міжнародному праві для спільних зловживань цих урядів.

По-друге, з практичної точки зору ця пропозиція перевантажить і без того перенапружену систему взаємної правової допомоги, що призведе до ще більших затримок і відставання. Відкриття взаємної правової допомоги для такого широкого кола правопорушень замість зосередження ресурсів на справжніх кіберзлочинах збільшить і без того значні затримки.

Більше навантаження на системи взаємної співпраці також ускладнить здатність органів влади виявляти порушення прав людини під час обробки запитів. Це підвищить вірогідність того, що співпраця може призвести до ідентифікації або визначення місцезнаходження людини, яка втекла з країни, щоб уникнути насильства, що призвело до переслідувань, тортур, зникнення або навіть смерті.

Нарешті, оскільки дані дедалі більше зберігаються в кількох юрисдикціях, ймовірність того, що уряди скористаються своїм правом відмовити у взаємній правовій допомозі на підставі прав людини, є в кращому разі малою. Історично глобальне зберігання даних було зосереджено в кількох країнах.

Але в останні роки відбувся зсув у бік локалізації зберігання даних у країнах по всьому світу, і хмарні провайдери активно розширюють свою діяльність і послуги в нових регіонах, у тому числі в країнах із кричущими порушеннями прав людини.

Будапештська конвенція про кіберзлочинність, розроблена в 2001 році, використовує такий же широкий підхід до збору доказів. Але на момент його прийняття електронні докази відігравали обмежену роль у кількох технологічних правопорушеннях.

Наслідки повторення цього підходу в глобальному договорі через два десятиліття з державами-учасницями, які мають дуже різні підходи до захисту та гарантій прав людини, будуть набагато суворішими та масштабнішими.

За відсутності надійних гарантій, обмеженої сфери застосування та зобов’язань дотримуватися міжнародного права прав людини, включно з відмовою в розслідуваннях, які суперечать правам людини, ця угода спрямована на сприяння зловживанням у глобальному масштабі.

Урядам слід відмовитися від будь-яких подібних компромісів і забезпечити, щоб ця угода підвищувала, а не жертвувала нашими найважливішими правами». ***(Deborah Brown and Katitza Rodriguez. UN cybercrime treaty: A menace in the making // EURACTIV MEDIA NETWORK BV (https://www.euractiv.com/section/cybersecurity/opinion/un-cybercrime-treaty-a-menace-in-the-making/?utm_source=flipboard&utm_content=EURACTIV%2Fmagazine%2FEURACTIV). 16.10.2023).***

***

«Google, Microsoft, Cloudflare і гігант електронної комерції Amazon завадили атаці, яку рекламують як найбільшу в історії атаку на розподілену відмову в обслуговуванні (DDoS), і це навіть не близька річ.

Вважається, що розмір атаки, яка відбулася протягом останніх двох місяців, більш ніж у сім разів перевищує попередній рекорд DDoS. Google заявляє, що застосував «нові» методи, щоб спробувати порушити роботу кількох служб інтернет-інфраструктури.

Протягом останніх двох років відбулася низка потужних DDoS-атак, що викликає занепокоєння, враховуючи, що будь-яка підключена до Інтернету компанія чи організація може бути вразливою до атаки такого роду.

Google відстежує найбільшу атаку в історії

Команда реагування на DDoS-атак Google, а також Microsoft, Cloudflare та AWS показали, що всі вони зробили свій внесок у подолання найбільшої DDoS-атаки в Інтернеті.

Цього тижня технічний гігант повідомив у своєму блозі, що на піку атака досягала 398 мільйонів запитів на секунду.

Кількість запитів, створених протягом двох хвилин під час цієї атаки, перевищила загальну кількість переглядів статей Вікіпедії, отриманих у листопаді.

Однак інші компанії, які займаються пом’якшенням атаки, пропонують дещо інші цифри: Cloudflare показує 201 мільйон обертів за секунду, а Amazon – 115

мільйонів обертів за секунду на піку. Усі три цифри наразі можна вважати рекордними.

У Google стверджують, що атаку було організовано «з використанням нової техніки «швидкого скидання», яка використовує мультиплексування потоків, функцію широко поширеного протоколу HTTP/2».

HTTP/2 прискорює час завантаження веб-сайту, дозволяючи надсилати декілька запитів через одне з'єднання одночасно. DDoS-атака, про яку йде мова, ефективно автоматизувала цей процес і повторювала його знову і знову.

Що таке DDoS-атака і чому вони відбуваються?

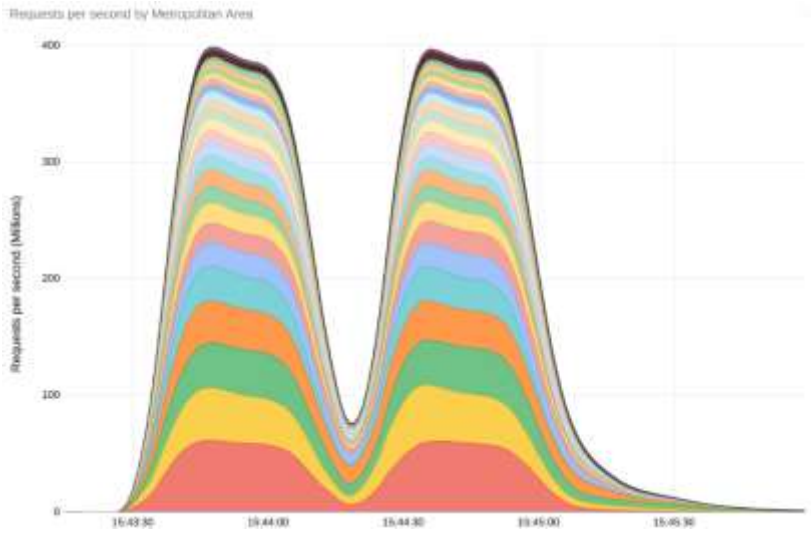
У розподілених атаках на відмову в обслуговуванні зловмисник використовує безліч обчислювальних ресурсів, часто з віддалених місць, і направляє величезну кількість запитів на певний сервер або мережу, наприклад, на веб-сайт. Іноді для цієї мети використовуються армії ботів або «ботнети».

Мета полягає в тому, щоб перевантажити цільовий сервер запитами в надії, що він вийде з ладу, і власники будуть змушені вивести його з мережі або вимкнути. DDoS-атаки відрізняються від подібних до атак програм-вимагачів тим, що вони насправді не передбачають злому будь-чого – головне – створити якомога більше хаосу.

DDoS-атаки зазвичай використовуються, щоб відвернути увагу від інших більших, складніших атак, націлених на ту саму мережу, або щоб певна компанія чи організація була змушена виділяти значні захисні ресурси для боротьби з нею, що робить їх більш вразливими до наступних атак, які ще не відбулися. бути оплаченим.

DDoS-атаки продовжують зростати

Як ми вже згадували, DDoS-атака, запущена в серпні та вересні цього року, досягла піку приблизно в 398 мільйонів обертів за секунду:



Це перевершує попередній рекорд запитів у 71 мільйон обертів за секунду, зафіксований під час атаки, що відбулася на початку цього року, пом'якшеної Cloudflare.

Сама ця атака була значно більшою, ніж найбільша DDoS-атака 2022 року, яка, за словами Google, досягла піку в 46 мільйонів обертів за секунду. Це був другий випадок, коли рекорд було побито минулого року, коли Cloudflare зупинив DDoS-атаку, досягнувши піку 26 мільйонів обертів за секунду на початку червня 2022 року.

Google каже, що експоненціальне зростання розміру цих атак є «меншим занепокоєнням, хоча й проблематичним», якщо взяти до уваги швидкість, з якою зростає Інтернет». ***(Aaron Drapkin. Microsoft and Google Halt "Largest" Cyberattack on Record // Marketing VF Ltd. (https://tech.co/news/microsoft-google-halt-largest-cyberattack?utm_source=flipboard&utm_content=waral01%2Fmagazine%2FRumors+Of+War). 11.10.2023).***

***

«Підприємства та інші організації в Канаді беруть участь у «гонці озброєнь у сфері кібербезпеки», оскільки вони намагаються випередити кіберзлочинців, оснащених новими складними інструментами та методами для зламу систем безпеки та викрадення даних.

У цій конкуренції зловмисники дедалі більше переважають, каже Іво Вінс, технічний директор відділу кібербезпеки компанії CDW Canada, яка надає IT-

рішення та послуги для компаній у таких сферах, як кібербезпека, цифрова інфраструктура та хмарні технології.

«Ця триваюча «гонка кіберозброєнь» має високі ставки, і ризики відставання є більшими, ніж будь-коли», — каже він. «Дослідження CDW показують, що ми спостерігаємо перехід від обсягу до якості кібератак; хоча загальна кількість атак зменшилася, кількість успішних інцидентів зростає. Іншими словами, зловмисники стають кращими у зламуванні IT-систем і завданні шкоди».

Відповідно до канадського дослідження кібербезпеки CDW за 2023 рік, ексфільтрації (захоплення та/або видалення даних) підскочили з середнього 13 інцидентів на організацію у 2022 році до 30 у 2023 році. Так само зросла кількість проникнень (вставлення шкідливого програмного забезпечення та/або інших активів). з 11 інцидентів у 2022 році до понад 28 у 2023 році.

Крім того, кібератаки мають значно кращий «показник» (кількість успішних атак, які стали інцидентом), ніж у попередні роки. У 2023 році від 7 до 10 відсотків усіх кібератак у різних галузях і розмірах організацій були успішними.

«Підприємства та організації змушені інвестувати в більш прогресивні заходи кібербезпеки, щоб випереджати загрози, що наростають з боку кіберзлочинців», — каже пан Вінс.

Кіберзлочинці процвітають у поточному бізнес-ландшафті

Після пандемії компанії швидко перейшли до гібридної роботи, цифрових послуг і впровадження пристроїв Інтернету речей (IoT). Величезне зростання клієнтських обчислювальних пристроїв, серверів і пристроїв Інтернету речей означає, що організації мають «розширену поверхню для атаки», що створює більше точок входу для зловмисників.

«Коли організаціям довелося перейти на віддалену роботу та забезпечити доступ до своїх систем звідусіль, перехід до хмари був простим і швидким рішенням», — пояснює пан Вінс. «По суті, за одну ніч ми змогли продовжити роботу, як і раніше, але, оскільки ми рухалися зі швидкістю, ми не запровадили необхідні засоби кіберзахисту».

Захист хмарних технологій вимагає іншого набору навичок у команді безпеки та іншого набору процесів, каже він, додаючи, що команди з кібербезпеки вже були перевантажені до цієї величезної трансформації. Через терміновість організації застосували підхід «спочатку зміна, а потім захист».

«Бізнес розвивається швидше, ніж інвестиції в кібербезпеку», — каже пан Вінс. «Тепер такі технології, як хмара та IoT, стали важливими для сучасних бізнес-функцій, водночас створюючи середовище, у якому кіберзлочинці можуть процвітати».

Виявлення загрози та реагування не виконуються

Канадське дослідження кібербезпеки 2023 року показало, що можливості канадських організацій у виявленні кіберзагроз і реагуванні на них не відповідають необхідним.

«Тенденція до затримки реагування безумовно погіршується, зокрема для малих і середніх організацій, які часто не мають планування та процесів, щоб реагувати на ці атаки», – каже пан Вінс. Це має хвилевий ефект, оскільки менші підприємства часто є постачальниками для великих організацій, тому вплив порушення однієї компанії може значно поширитися, каже він.

Відповідно до дослідження, середній час, який потрібен канадським організаціям для виявлення кіберінциденту, становить 7,1 дня, тоді як середній час реагування більш ніж вдвічі довший – 14,9 дня. Середній час відновлення після кіберінциденту становить 25,6 дня.

У середньому проходить 48 днів, перш ніж організація вирішить кіберінцидент.

«Це довгий час для бізнесу, коли послуги чи продукти недоступні, або, що ще гірше, коли хтось має повну свободу дій у їхніх системах і має доступ до цінних корпоративних ресурсів», — каже пан Вінс.

Наслідки дорого коштують, додає він. «Будь-яка затримка виявлення та часу реагування, пов’язана з кібератаками, піддає канадським організаціям підвищений ризик регулятивних штрафів, втрати довіри клієнтів і більших витрат на відновлення після інцидентів безпеки».

Рішення: випередження в гонці кіберозброєнь

Кіберзловмисники все частіше використовують штучний інтелект (AI) і автоматизацію у своїх пошуках доступу та викрадення особистих, фінансових чи інтелектуальних даних або для порушення бізнес-процесів за допомогою програм-вимагачів і розподілених атак типу «відмова в обслуговуванні» (DDoS).

Ці передові технології також доступні для організацій, які прагнуть захистити свої дані та операції, каже пан Вінс, і найважливішим наступним кроком є розширення розробки та впровадження.

Технології є одним з аспектів кіберзахисту, але він наголошує, що організаціям також необхідно вдосконалювати свої процеси та підтримку, яку вони надають своїм працівникам, щоб допомогти їм уникнути дорогих помилок.

Рішення, які допоможуть організаціям перемогти в кібергонці озброєнь, включають наступне:

Використовуйте виявлення загроз на основі штучного інтелекту, а також автоматизовані та організовані механізми реагування.

Розробіть план реагування на інцидент із політикою та процедурами для оцінки, стримування та відновлення після інциденту безпеки.

Використовуйте автоматизовані процеси та переконайтеся, що у груп безпеки є розробники, які можуть створити автоматизацію в середовищі.

Оскільки кіберзлочинці стають все більш вправними у представленні фішингових повідомлень, які виглядають цілком законними, повідомте співробітникам, на що слід звернути увагу, і нагадайте їм вжити додаткових заходів, щоб перевірити, що є справжнім, а що — підробкою.

Хоча ці рішення можуть здаватися очевидними для працівників галузі, швидкість, з якою розвивається гонка кіберозброєнь, може бути надзвичайною для організацій. Крім того, складно мати власні ресурси та досвід, щоб випередити ці загрози.

Партнерство зі сторонніми постачальниками рішень для кібербезпеки — найкращий спосіб забезпечити безпеку мереж організацій, пояснює пан Вінс. «Витонченості сучасних кіберзагроз достатньо, щоб не дати спати вночі. Саме тут

на допомогу приходять сторонні IT-експерти. Їх робота полягає в тому, щоб глибоко зрозуміти ландшафт загроз, дозволяючи організаціям зосередитися на веденні свого бізнесу без додаткових турбот». ***(As threats increase, Canadian organizations need to take action to stay ahead in the cybersecurity arms race // The Globe and Mail Inc. (https://www.theglobeandmail.com/business/adv/article-as-threats-increase-canadian-organizations-need-to-take-action-to-stay/). 10.10.2023).***

***

«У цифровому ландшафті, де межа між реальністю та віртуальною реальністю часто стирається, загрози кібербезпеці виникли як сучасна Гідра. З кожною відрубаною головою проростають ще дві, зростаючи в інтенсивності та витонченості. Глобальні компанії опиняються в ескалації гонки озброєнь проти безликих злочинців, боротьбі, яка виходить за межі залів засідань і в царство одиниць і нулів.

Картування ландшафту загроз

Зростання частоти кібератак є жахливою реальністю, яка підкреслює нашу зростаючу залежність від цифрової інфраструктури. Поле битви величезне, націлені на підприємства будь-якого розміру в різних галузях. Зброя вибору? Атаки програм-вимагачів, коли зловмисники використовують передові методи для проникнення в системи, шифрування конфіденційних даних і утримання їх у заручниках, вимагаючи значні викупи за їх оприлюднення. Це гра з високими ставками, де кубики завантажуються на користь зловмисників, які залишаються прикритими шарами цифрової анонімності.

Наслідки: підрахунок вартості

Кожне порушення системи кібербезпеки є сильним ударом по фінансовому нутру організації. Дослідження IBM малює похмуру картину, оцінюючи середню вартість витоку даних у 2020 році в 3,86 мільйона доларів. Наслідки виходять за межі негайного реагування на інцидент, перетворюючись у вир судових зборів, репутаційної шкоди та витрат на відновлення. Малі та середні підприємства (МСП)

несуть на собі основний тягар цих атак, часто не маючи необхідних ресурсів, щоб впоратися з штормом.

Кіберзлочинці: Майстри маскування

Кожен новий світанок приносить із собою вдосконалені тактики, які використовують кіберзлочинці. Їхній спосіб дії — адаптивність, використання вразливостей із безжальною точністю. Фішингові атаки, під час яких зловмисники маскуються під довірених осіб, щоб обманом змусити жертв розкрити конфіденційну інформацію, стають все більш витонченими. Соціальна інженерія, використання особистої інформації для цілеспрямованих атак і використання платформ соціальних медіа для збору розвідувальної інформації стали загальноприйнятою тактикою, через що підприємствам стає дедалі складніше створювати надійний захист.

Внутрішня загроза

Хоча розповідь часто зосереджується на зовнішніх загрозах, внутрішні вразливості є не менш критичними. Співробітники можуть несвідомо стати найслабшою ланкою в ланцюжку кібербезпеки організації через навмисні дії або помилки, які нічого не підозрюють. Випадки, коли незадоволені працівники злили конфіденційну інформацію або стали жертвою тактики соціальної інженерії, підкреслюють необхідність для компаній звертати увагу на ризики безпеки.

Проактивна позиція: шлях вперед

Перед лицем зростаючих загроз бізнес повинен зайняти активну позицію. Це передбачає інвестиції в надійні заходи кібербезпеки, розробку комплексних планів реагування на інциденти та сприяння культурі обізнаності щодо кібербезпеки через регулярне навчання та навчання. Співпраця та обмін інформацією в рамках спільноти кібербезпеки також відіграють вирішальну роль, дозволяючи компаніям випереджати нові загрози та колективно зміцнювати свій захист. Хоча виклики страшні, шлях до стійкості ясний. Це шлях, який вимагає пильності, передбачення та непохитної відданості захисту цифрової сфери, де наше життя все більше переплітається». ***(Navigating the Cybersecurity Minefield: A Global Business Endeavor***

// Microsoft (https://www.msn.com/en-xl/news/other/navigating-the-cybersecurity-minefield-a-global-business-endeavor/ar-AA1il9oM). 17.10.2023).

***

«Міжнародний кримінальний суд (ICC), єдиний у світі постійний міжнародний суд із мандатом розслідувати та переслідувати геноцид, злочини проти людства та військові злочини, визначив, що кібератака на його системи у вересні була спробою шпигунства.

Суд зі штаб-квартирою в Гаазі, Нідерланди, підтвердив минулого місяця, що хакери проникли в його мережу. В оновленому повідомленні, опублікованому в п'ятницю, МКС заявив, що з тих пір він визначив, що цей інцидент був «цілеспрямованою та витонченою атакою» з «метою шпигунства».

«Тому напад можна тлумачити як серйозну спробу підірвати мандат суду», – сказав суд.

ICC, який зберігає конфіденційну інформацію, пов'язану з передбачуваними військовими злочинами, і дані про свідків, які можуть опинитися під загрозою, якщо їхні особи будуть розкриті, заявив, що ще не визначив, чи був доступ до будь-яких даних або їх викрадення під час кібератаки.

«Якщо будуть знайдені докази того, що конкретні дані, довірені Суду, були скомпрометовані, Суд негайно зв'яжеться безпосередньо з постраждалими особами», — заявив ICC. Суд ще має підтвердити конкретний характер кібератаки, наприклад, чи було розгорнуто шкідливе програмне забезпечення.

Речник ICC Соня Робла не відразу відповіла на запитання TechCrunch.

Суд заявив, що він ще не підтвердив, хто стоїть за кібератакою, але зазначив, що він очікує, що він зіткнеться з кампаніями дезінформації, націленими на ICC та його посадових осіб у спробі делегітимізувати його діяльність.

У своїй заяві ICC зазначив, що кібератака сталася в період «більш широких і підвищених проблем безпеки» для суду. Після того, як МКС видав ордери на арешт президента Росії Володимира Путіна, Росія у відповідь видала ордери на арешт

президента МКС, їхнього заступника, головного прокурора та одного з головуючих суддів.

У той же час ICC заявив, що зазнав «щоденних і наполегливих спроб» атакувати та порушити роботу його систем.

У відповідь на безпрецедентну вересневу кібератаку ICC заявив, що посилює свої гарантії кібербезпеки, що включатиме зміцнення системи управління ризиками та забезпечення наявності процедур для захисту від будь-якого потенційного ризику для жертв і свідків». ***(Carly Page. International Criminal Court says cyberattack was attempted espionage // Yahoo (https://techcrunch.com/2023/10/20/war-crimes-tribunal-cyberattack-espionage-russia/?utm_source=flipboard&utm_content=MattMagnuson%2Fmagazine%2FPUTIN%E2%80%99S+REACH%2C+RUSSIA%2C+%26+UKRAINE). 20.10.2023).***

***

«Okta каже, що зловмисники отримали доступ до файлів, що містять файли cookie та токени сеансу, завантажені клієнтами в її систему управління підтримкою після того, як зламали її за допомогою вкрадених облікових даних.

«Зловмисник зміг переглянути файли, завантажені певними клієнтами Okta в рамках нещодавніх звернень у службу підтримки», — сказав головний спеціаліст служби безпеки Okta Девід Бредбері.

«Слід зазначити, що система управління справами служби підтримки Okta відокремлена від робочої служби Okta, яка повністю працює і не зазнала жодного впливу».

CSO Okta додав, що цей інцидент не вплинув на систему керування справами Auth0/CIC. Okta повідомила всіх клієнтів, чиє середовище Okta або запити служби підтримки постраждали від інциденту. Це не стосується тих, хто не отримав сповіщення.

Розкрито маркери сеансу та файли cookie

Незважаючи на те, що компанія ще не надала подробиць про те, яка інформація про клієнтів була розкрита або доступна під час порушення, система керування

зверненнями до служби підтримки, зламана під час цієї атаки, також використовувалася для зберігання архівних файлів HTTP (HAR), які використовуються для реплікації помилок користувача чи адміністратора для усунення різних несправностей. проблеми, про які повідомляють користувачі.

Вони також містять конфіденційні дані, такі як файли cookie та маркери сеансу, які зловмисники можуть використовувати для викрадення облікових записів клієнтів.

«Файли HAR представляють собою записи активності браузера та, можливо, містять конфіденційні дані, включаючи вміст відвіданих сторінок, заголовки, файли cookie та інші дані», — пояснює Okta на своєму порталі підтримки.

«Хоча це дозволяє співробітникам Okta копіювати діяльність браузера та вирішувати проблеми, зловмисники можуть використовувати ці файли, щоб видати себе за вас».

Під час розслідування інциденту компанія працювала з постраждалими клієнтами та відкликала токени сесії, вбудовані в спільні файли HAR. Тепер він радить усім клієнтам очистити свої файли HAR перед наданням доступу, щоб переконатися, що вони не включають облікові дані та файли cookie/токени сеансу.

Okta також поділився списком індикаторів компрометації, помічених під час розслідування, включаючи IP-адреси та інформацію про агент користувача веб-браузера, пов’язану зі зловмисниками.

Представник Okta не відповів на запитання щодо дати порушення та кількості клієнтів, які постраждали, коли BleepingComputer звернувся раніше сьогодні.

Натомість речник сказав, що система підтримки «є окремою від виробничої служби Okta, яка повністю працює та не зазнала жодного впливу. Ми повідомили постраждалих клієнтів і вжили заходів для захисту всіх наших клієнтів».

Порушення виявлено BeyondTrust після спроби порушення

BeyondTrust каже, що це був один із постраждалих клієнтів і надав додаткову інформацію про інцидент.

Команда безпеки BeyondTrust виявила та заблокувала спробу входу у внутрішній обліковий запис адміністратора Okta 2 жовтня за допомогою файлу cookie, викраденого із системи підтримки Okta.

Незважаючи на те, що BeyondTrust зв'язався з Okta і надав їм дані судової експертизи, які свідчать про те, що їхню організацію підтримки було зламано, Okta знадобилося більше двох тижнів, щоб підтвердити порушення.

«2 жовтня ми висловили занепокоєння з приводу злому Okta. Не отримавши підтвердження від Okta про можливе порушення, ми продовжували ескалацію в Okta до 19 жовтня, коли керівництво служби безпеки Okta повідомило нас, що вони дійсно зазнали порушення, і ми були один з їхніх постраждалих клієнтів", - повідомили в BeyondTrust.

BeyondTrust каже, що атаку вдалося запобігти «контролю спеціальної політики», але через «обмеження в моделі безпеки Okta» зловмисник зміг виконати «кілька обмежених дій».

Незважаючи на це, компанія каже, що зловмисник не отримав доступу до жодної з її систем, і її клієнти не постраждали.

BeyondTrust також поділився наступною хронологією атаки:

2 жовтня 2023 р. – виявлено та усунено атаку, орієнтовану на ідентифікацію, на внутрішній обліковий запис адміністратора Okta та попереджено Okta

3 жовтня 2023 р. – звернувся до служби підтримки Okta з проханням передати цю інформацію команді безпеки Okta, отримавши початкову криміналістику, яка вказує на компрометацію в організації підтримки Okta

11 жовтня 2023 року та 13 жовтня 2023 року – провели сеанси Zoom з командою безпеки Okta, щоб пояснити, чому ми вважаємо, що вони можуть бути скомпрометовані

19 жовтня 2023 р. – Керівництво служби безпеки Okta підтвердило внутрішнє порушення, і BeyondTrust був одним із постраждалих клієнтів.

Cloudflare також постраждав

У середу, 18 жовтня 2023 року, Cloudflare також виявила на своїх серверах зловмисну активність, пов'язану зі зломом Okta.

«Хоча це був тривожний інцидент безпеки, виявлення в режимі реального часу та швидке реагування нашої групи реагування на інциденти безпеки (SIRT) увімкнули стримування та мінімізували вплив на системи та дані Cloudflare», — заявили в компанії.

«Ми перевірили, що ця подія не вплинула на інформацію або системи клієнтів Cloudflare».

Зловмисники використали токен автентифікації, вкрадений із системи підтримки Okta, щоб перейти до примірника Okta Cloudflare за допомогою відкритого сеансу з правами адміністратора.

Cloudflare зв’язалася з Okta щодо інциденту за 24 години до того, як їх сповістили про злам, який вплинув на системи Okta.

«Схоже, що в нашому випадку зловмисник зміг викрасти токен сеансу з квитка служби підтримки, створеного співробітником Cloudflare. Використовуючи токен, отриманий з Okta, зловмисник отримав доступ до систем Cloudflare 18 жовтня», Cloudflare сказав.

«У цій складній атаці ми помітили, що зловмисники скомпрометували два окремих облікові записи співробітників Cloudflare на платформі Okta».

Кілька інцидентів безпеки менш ніж за 2 роки

Минулого року Okta розкрила, що деякі дані її клієнтів були розкриті після того, як група вимагачів даних Lapsus$ отримала доступ до її адміністративних консолей у січні 2022 року.

Одноразові паролі (OTP), які надсилаються клієнтам Okta через SMS, також були викрадені групою загроз Scatter Swine (також відомою як 0ktapus), яка зламала хмарну комунікаційну компанію Twilio у серпні 2022 року.

Провайдер послуг аутентифікації Auth0, який належить Okta, також повідомив у вересні, що деякі старіші сховища вихідного коду були викрадені з його середовища невідомим методом.

Okta розкрила власний інцидент з крадіжкою вихідного коду в грудні після того, як приватні репозиторії GitHub компанії були зламані». ***(Sergiu Gatlan. Okta says its support system was breached using stolen credentials // Bleeping Computer®***

LLC (https://www.bleepingcomputer.com/news/security/okta-says-its-support-system-was-breached-using-stolen-credentials/?utm_source=flipboard&utm_content=HamsterBoomer%2Fmagazine%2FCYBERSECURITY-DATA+BREACH). 20.10.2023).

***

«Кілька бельгійських державних веб-сайтів, постраждалих від імовірної кібератаки DDOS у неділю, знову стали доступними на світанку в понеділок.

Веб-сайти Федеральної державної служби фінансів, канцелярії прем'єр-міністра та монархії були доступні близько 04:00 у понеділок вранці, повідомляє Belga. Однак веб-сайт Сенату все ще був недоступний.

У неділю проблеми з IT порушили роботу кількох веб-сайтів державних послуг. Зокрема, FPS Finance повідомила про «хакерську атаку» через X (раніше Twitter).

Кілька веб-сайтів бельгійських установ вже стали жертвами кібератаки DDOS (відмова в обслуговуванні) минулого четверга. Сайти королівського палацу, прем'єр-міністра та сенату були тимчасово недоступні.

Замість домашньої сторінки було розміщено повідомлення англійською мовою про допомогу Бельгії Україні, включаючи обіцянку в середу надіслати F-16 до 2025 року». ***(Cyberattack targets Belgian public service websites for second time in a week // The Brussels Times (https://www.brusselstimes.com/belgium/743890/cyberattack-targets-belgian-public-service-websites-for-second-time-in-a-week). 16.10.2023).***

***

«З розвитком технологій розвиваються і методи, які використовують кіберзлочинці. Кібершантаж, форма цифрового здирництва, зростає в усьому світі, і ОАЕ не є винятком. Багато людей стали жертвами цих злочинів.

Для боротьби з цією зростаючою загрозою важливо розуміти правову базу та заходи, викладені в Законі ОАЕ про кіберзлочинність (Федеральний декрет-закон № 34/2021), і вживати заходів, щоб захистити себе від того, щоб стати жертвою кібер-

шантажу. Оскільки випадки кібершантажу стрімко зростають у всьому світі, важливо розуміти, як захистити себе.

Розуміння кібершантажу згідно з Федеральним указом-законом № 34/2021:

Кібершантаж — це різновид кіберзлочинності, коли зловмисники використовують цифрові платформи, щоб маніпулювати окремими особами чи організаціями, погрожувати їм або примушувати їх. Ці погрози часто супроводжуються вимогами, що варіюються від фінансового вимагання до шкоди репутації.

Кібершантажисти впливають на конфіденційну інформацію чи компрометуючі матеріали, щоб змусити своїх жертв підкоритися.

Стаття 2 закону стосується хакерства та є ще одним аспектом кіберзлочинності, на який поширюється дія закону. Зловмисники зламують особисту інформацію та конфіденційні дані людей через електронні носії, які згодом використовують як важіль для шантажу.

Це включає несанкціонований доступ до веб-сайтів, електронних інформаційних систем, інформаційних мереж або методів інформаційних технологій. Особам, яких визнають винними, може загрожувати затримання та/або штраф у розмірі від 100 000 до 500 000 дирхамів ОАЕ, залежно від тяжкості злому та його наслідків.

У статті 13 йдеться про незаконний збір та обробку персональних даних та інформації, що викликає серйозне занепокоєння у сфері кіберзлочинів. Порушникам загрожує затримання та/або штраф у розмірі від 50 000 до 500 000 дирхамів ОАЕ.

Згідно зі статтею 42, яка конкретно стосується електронного вимагання та погроз, кожному, хто вимагає іншу особу або погрожує іншій особі, щоб спонукати її вчинити або відмовитися від дії, використовуючи інформаційну мережу або метод інформаційних технологій, може загрожувати ув’язнення на строк до двох років та/ або штраф у розмірі від 250 000 до 500 000 дирхамів ОАЕ.

Якщо погроза передбачає вчинення злочину або заподіяння шкоди честі чи репутації та супроводжується явним чи неявним проханням виконати дію чи

утриматися від неї, покаранням може бути тимчасове позбавлення волі на строк до 10 років.

Стаття 44 закону присвячена порушенням приватного життя та несанкціонованому розголошенню особистої інформації. Особам, які займаються такою діяльністю, може загрожувати затримання на термін не менше шести місяців та/або штраф у розмірі від 150 000 до 500 000 дирхамів ОАЕ.

Усвідомлюючи нагальність боротьби з кіберзлочинами, такими як кібершантаж, уряд ОАЕ запровадив Федеральний декрет-закон № 34/2021. Цей комплексний закон забезпечує надійну основу для боротьби з широким спектром кіберзлочинів, включаючи кібершантаж.

Основні положення щодо боротьби з кібершантажем:

Звільнення від покарання (стаття 61): ця стаття дозволяє пом'якшити або зняти покарання для осіб, які повідомляють владі про кіберзлочини, включно з кібершантажем.

Накази про виправлення, призупинення, перехоплення та обмеження доступу (стаття 62): Компетентні органи мають право видавати накази щодо протиправного вмісту або підроблених даних, пов'язаних із кібершантажем. Ці накази можуть включати призупинення веб-сайтів, перехоплення комунікацій або обмеження доступу у разі виявлення зловмисних дій.

Скарги та оскарження наказів (стаття 63): Будь-яка особа, яка отримала накази, пов'язані з кібершантажем, може подавати скарги та апеляції протягом певного періоду часу. Це гарантує людям справедливий процес оскарження несправедливих наказів.

Посадові особи судового контролю (стаття 70): призначення працівників на посади службових осіб судового контролю надає їм повноваження оперативно припиняти дії, пов'язані з кібершантажем. Це дає правоохоронним органам повноваження вживати оперативних заходів проти порушників.

Застосування більш суворого покарання (стаття 72): Важливо, що закон роз'яснює, що покарання, визначені в ньому, не перешкоджають застосуванню

більш суворих покарань, визначених в інших законах. Це підкреслює серйозність, з якою в ОАЕ сприймають кібершантаж.

Покарання за кібершантаж:

Згідно з Федеральним указом-законом № 34/2021 покарання за кібершантаж можуть включати затримання, штрафи від 250 000 до 500 000 дирхамів ОАЕ або навіть тимчасове ув'язнення на строк до 10 років.

Захист себе від кібершантажу:

Щоб запобігти загрозам кібершантажу та захиститися від них, окремі особи та організації в ОАЕ повинні вживати активних заходів:

Будьте в курсі: ознайомтеся із законодавством ОАЕ щодо боротьби з кіберзлочинністю, зокрема Федеральним указом-законом № 34/2021. Усвідомлення цих законів є вашою першою лінією захисту.

Посилення кібербезпеки: інвестуйте в потужні заходи кібербезпеки, щоб захистити свою цифрову присутність. Регулярно оновлюйте паролі, використовуйте шифрування та встановлюйте надійне антивірусне програмне забезпечення.

Застереження: будьте обережні, надаючи особисту або конфіденційну інформацію в Інтернеті. Кібершантажисти часто використовують таку інформацію як важелі.

Повідомте про підозрілу активність: якщо ви зазнали будь-якої форми кібершантажу або вважаєте, що стали жертвою, негайно повідомте про це відповідним органам. Закон заохочує співпрацю та захищає тих, хто виступає.

Підсумовуючи, кібершантаж викликає дедалі більше занепокоєння в ОАЕ, але після введення в дію Федерального указу-закону № 34/2021 країна зміцнила свій захист від цієї загрози. Пильність і обізнаність — ваша найпотужніша зброя в боротьбі з кібершантажем». ***(Dr. Hassan Elhais. Cyber blackmail is increasing in the UAE: learn how to protect Yourself // Hassan Elhais (https://www.professionallawyer.me/legal-articles/criminal-law/cyber-blackmail-is-increasing-uae-learn-how-to-protect-yourself). 23.10.2023).***

***

«Кібербезпека має першочергове значення як для компаній, так і для окремих осіб, оскільки щомісяця з'являється все більше загроз. Отже, якщо ви хочете залишатися в безпеці, важливо розуміти, як змінюється ландшафт кібербезпеки.

З наближенням 2024 року існує низка тенденцій і прогнозів у сфері кібербезпеки, про які слід знати.

1. Збільшення кількості атак за допомогою ШІ

Протягом 2022 і 2023 років ми бачили, наскільки розвинені зараз системи ШІ. Найвідомішим сервісом на основі ШІ, запущеним у цей час, є ChatGPT, інструмент обробки мови на базі штучного інтелекту. Невдовзі після його запуску почали з'являтися історії про те, що кіберзлочинці використовують ChatGPT для створення шкідливих програм. Хоча зловмисне програмне забезпечення лише здавалося простим сценарієм на основі Python, воно показало, що ШІ насправді можна використовувати зловмисно.

Але ChatGPT не закінчується. Сьогодні існує незліченна кількість інструментів штучного інтелекту, які постійно розробляються, тому ми не знаємо, як більш просунуту версію такого програмного забезпечення можна використовувати для скоєння кіберзлочинів.

В Оцінці загрози Міністерства внутрішньої безпеки за 2024 рік зазначено, що кіберзлочинці продовжуватимуть «розробляти нові інструменти та доступи, які дозволять їм скомпрометувати більше жертв і забезпечать масштабніші, швидші, ефективніші та більш обхідні кібератаки».

У цьому ж звіті також зазначено, що:

Поширення та доступність нових кібер-інструментів та інструментів штучного інтелекту, ймовірно, допоможе цим гравцям посилити їхні зловмисні інформаційні кампанії, дозволяючи створювати недорогий синтетичний текстовий, графічний та аудіоконтент вищої якості.

Схоже, що подальше впровадження та розвиток штучного інтелекту становитиме загрозу нашій кібербезпеці, хоча ступінь, до якої це вплине на нас, ще не встановлено.

2. Збільшення кількості атак на цифровий ланцюг поставок

Ланцюг постачання утворює основу комерційного світу. Без цієї важливої галузі ефективне виробництво та доставка продукції по всьому світу було б майже неможливим.

Серйозність впливу ланцюга постачання робить його привабливою мішенню для кіберзлочинців. Із зростанням попиту на масове виробництво та глобальні доставки зростає й вплив хакерських систем на системи постачання.

За даними Cybersecurity Hub, за останні три роки кількість атак на ланцюги поставок зросла на 74 відсотки. На сайті також повідомляється, що для виявлення атаки на ланцюжок поставок потрібно в середньому 287 днів, що дає зловмисникам достатньо часу для викрадення даних або порушення роботи служб. У 2024 році ми можемо спостерігати зростання кількості атак на ланцюги поставок або навіть ускладнюватися.

3. Подальше впровадження систем нульової довіри

Системи нульової довіри не покладаються на жодного користувача чи групу користувачів для автентифікації, моніторингу чи зберігання даних. Крім того, кожен користувач, присутній у системі з нульовою довірою, повинен авторизувати доступ новому користувачеві, інакше система залишається закритою для цієї особи. Коротше кажучи, система нульової довіри створена для того, щоб не довіряти одній людині. Усі користувачі вважаються ненадійними, якщо автентифікацію не надають інші користувачі.

З точки зору кібербезпеки, система нульової довіри може бути величезною перевагою. Багато поточних мереж — будь то ті, що використовуються для зберігання даних, соціальних комунікацій, обміну медіафайлами чи розміщення серверів — не створені для забезпечення нульової довіри. Це означає, що система довіряє певним користувачам. Якщо певний користувач виявляється зловмисним і система вже вирішила йому довіряти, стають можливими кібератаки.

Системи нульової довіри також забезпечують детальний доступ і контроль. Це означає, що ніхто ніколи не має контролю або доступу до більшості даних і влади в мережі. Кожному користувачеві надається інформація в строгому порядку.

Блокчейни працюють аналогічно, при цьому потужність і дані розподіляються по мережі децентралізованим способом.

4. Подальше використання EV Security Systems

Пройшли ті часи, коли автомобіль був просто механічним транспортним засобом з радіо. Тепер ми можемо використовувати Bluetooth, Wi-Fi і навіть NFC у своїх автомобілях. Ці бездротові з'єднання разом із використанням програмного забезпечення відкрили двері для кіберзлочинців.

Особливо це стосується електромобілів. Багато електромобілів розроблено з високотехнологічними функціями, такими як дверні замки на основі NFC, виявлення небезпек AI, можливості Wi-Fi, додатки для заряджання та багато іншого. Використовуючи такі функції, можна здійснити як віддалені, так і короткочасні зломи, піддаючи ризику власників електромобілів та інших водіїв.

Наприклад, хакер може використовувати зарядний пристрій для електромобілів, щоб отримати доступ до інформації про певний транспортний засіб. Коли EV під'єднується до зарядного пристрою, вони обмінюються інформацією, наприклад, скільки енергії постачається, як довго заряджався EV і навіть платіжною інформацією власника (якщо зарядний пристрій EV пов'язано з додатком для заряджання користувача). Якщо в зарядній станції є вразливість програмного забезпечення, хакер може скористатися нею та проникнути в з'єднання між електромобілем і зарядним пристроєм. Тут можна викрасти місцезнаходження користувача, платіжні реквізити та інші дані.

Це лише один із численних хаків для електромобілів типів можливих. Щоб уникнути цього, виробники електромобілів повинні ретельно перевірити своє програмне забезпечення, щоб переконатися, що вразливі місця не залишаються позаду в коді.

5. Покращений розумний дім та безпека Інтернету речей

Пристрої IoT роблять наше повсякденне життя можливим. Незалежно від того, чи використовуєте ви свій смартфон, розумну колонку, розумний годинник або щось подібне, IoT полегшує ваші дії. Коротше кажучи, IoT — це загальний термін, що охоплює всі взаємопов'язані пристрої. Ця мережа пов'язаних «речей» формує

власний Інтернет речей (IoT). Саме ця розширена підключеність, що формує Інтернет речей, привабила кіберзлочинців.

Причина цього схожа на підвищену увагу до злому електромобілів. Пристрої IoT не тільки покладаються на програмне забезпечення, але й використовують бездротові з'єднання для зв'язку один з одним. Ці два елементи залишають відкритими двері для експлойтів, будь то через уразливості програмного забезпечення, зловмисне програмне забезпечення або внутрішні актори.

Згідно зі звітом Statista, глобальні кібератаки IoT зросли більш ніж на 243 відсотки між 2018 і 2022 роками, з 32,7 мільйонів атак на рік до шокуючих 112,29 мільйонів.

Очікується, що через цю зростаючу загрозу безпека розумного дому та Інтернету речей покращиться протягом 2024 року. Надання виправлень для вразливостей, надання додаткових функцій безпеки (таких як шифрування та двофакторна автентифікація) і проведення регулярних перевірок коду – все це може допомогти впоратися кібератак, спрямованих на пристрої Інтернету речей і розумні будинки.

6. Подальше використання хмарних платформ

Цілком ймовірно, що у вас уже є дані, які зберігаються на хмарній платформі, наприклад Microsoft OneDrive або Google Drive. Ці платформи непросто зламати, але натовпи даних, які вони зберігають, роблять їх дуже прибутковими цілями для хакерів.

Хоча хмарні платформи, безсумнівно, є зручним варіантом зберігання, можливість отримати доступ до даних будь-де за допомогою правильних облікових даних створює проблему. Якщо хакеру вдасться отримати доступ до чийогось облікового запису, він зможе переглянути будь-які дані, що зберігаються в цьому обліковому записі — робочі документи, фотографії, що посвідчують особу, фотографії та відео, фінансову інформацію чи будь-що інше.

Оскільки цей горщик із золотом даних чекає на кіберзлочинців, не дивно, що вони роблять усе можливе, щоб проникнути всередину. Хоча хмарні платформи часто оснащені різними функціями безпеки, вони не є непроникними, і величезна

кількість даних, які сьогодні зберігаються на цих платформах, робить їх все більш привабливими для хакерів.

7. Продовження тематичних шахрайств електронною поштою

Не бракує шахраїв, які хочуть отримати прибуток на поточних подіях. Ми бачили безліч шахрайських дій через пандемію COVID-19, але на цьому все не закінчилося. Російсько-українська війна та ізраїльсько-палестинський конфлікт також використовувалися протягом 2023 року, щоб вичавити гроші з жертв за допомогою соціальної інженерії.

Наприклад, шахрай може надіслати потенційній жертві електронний лист, видаючи себе за представника благодійної організації. Вони містять посилання на сторінку пожертв, щоб одержувач міг надати трохи грошей на справу. Але насправді благодійна допомога або вигадана, або відправник видає себе за співробітника відомої благодійної організації. Можливо, шахрай шукає одноразовий платіж, але він також може надати посилання на фішинговий сайт, призначений для викрадення платіжних даних жертви. У будь-якому випадку одержувач зрештою програє.

Оскільки ми продовжуємо спостерігати все більше конфліктів, трагедій і скандалів, немає сумніву, що кіберзлочинці й надалі намагатимуться нажитися на труднощах інших людей.

Кожен рік приносить нові загрози кібербезпеці

Оскільки 2023 рік добігає кінця, важливо пам’ятати про основні тенденції безпеки та прогнози 2024 року. Залишившись грамотним у питаннях безпеки, ви зможете відбивати загрози та краще підготуватися до зловмисних кампаній. Ніхто не знає напевно, що принесе 2024 рік для сфери кібербезпеки, але варто пам’ятати про вищесказане, оскільки вони, швидше за все, з’являться». ***(Katie Rees. 7 Cybersecurity Trends and Predictions for 2024 // www.makeuseof.com (https://www.makeuseof.com/cybersecurity-trends-predictions-next-year/). 25.10.2023).***

***

«Згідно зі звітом CyberSecurity Malaysia, урядовий сектор зазнав найбільшої кількості витоків даних, тоді як телекомунікаційний сектор став найбільшим витоком даних у першій половині року.

У середньорічному звіті про загрози за 2023 рік сказано, що на державний сектор припадає 22% зломів, за ним йдуть телекомунікації з 9%.

На сектор освіти та роздрібної торгівлі припадає по 6%, тоді як на ряд інших секторів припадає решта 48%.

Національне спеціалізоване агентство з кібербезпеки при Міністерстві зв'язку та цифрових технологій заявило, що урядові міністерства та відомства «піддаються значним кіберризикам, включаючи вразливе програмне забезпечення, слабкий контроль доступу, розкриття даних та інші критичні проблеми».

Він рекомендував провести комплексну оцінку для всіх державних установ, пропонуючи охопити веб-інфраструктуру та інфраструктуру хостингу, центри обробки даних, внутрішні системи та всю екосистему міністерства.

«З даних ми бачимо, що 71% цих інцидентів пов'язані з панеллю адміністратора/панеллю C, даними клієнтів і витоком конфіденційних даних», – йдеться в повідомленні.

Що стосується обсягу витоку даних, агентство заявило, що було виявлено «приголомшливу кількість 842,84 ГБ», причому сектор телекомунікацій очолив список (424,92 ГБ), за ним йдуть державні сектори (291,49 ГБ), банківська справа (62,46 ГБ), IT-сфера. (14,60 ГБ) та інші (49,37 ГБ).

«Викликає тривогу те, що 36,96% TA (акторів загрози) займаються продажем витоку даних. Ще більше занепокоєння викликає той факт, що 63,04% цих TA беруть участь у боротьбі за обмін даними.

«Це може означати низку подальших сценаріїв – від публічних витоків, які покликані завдати шкоди репутації, до обміну між мережами TA для більш широкого використання», – йдеться у звіті CyberSecurity Malaysia…

Він назвав LeakBase, DeltaBoys, Desorden, Actifedot і Juliay п'ятіркою найпоширеніших загроз, які розкривають конфіденційні дані країни.

«З цих секторів ми бачимо три сектори, які є найбільш вразливими: уряд, телекомунікації, логістика, транспорт і банківська справа.

«Ці сектори вважаються прибутковими для ТА, оскільки дані цих секторів вважаються більш впливовими з точки зору рівня чутливості даних і з точки зору обсягу цих даних», — йдеться в повідомленні.

Тільки в січні, за підрахунками агентства, понад 40 мільйонів записів було виточено в результаті різних інцидентів з витоком даних, загальним розміром 13 ГБ, за участю восьми державних установ і дев'яти приватних організацій.

Кількість повідомлень про інциденти також значно зросла: з 29 за третій тиждень січня до 48 за наступний тиждень.

У лютому було зафіксовано найбільшу кількість інцидентів – 197, з витоком понад 28 мільйонів записів, або розміром 33 ГБ, за участю дев'яти державних і дев'яти приватних організацій.

У наступні місяці кількість повідомлень про інциденти зменшилася.

У червні було підраховано, що стався витік 823 880 записів із розміром даних 417,59 ГБ, за участю шести державних установ і 20 приватних організацій.

Агентство повідомило, що дані були зібрані з соціальних мереж, онлайн-новин, платформ аналізу кіберзагроз і темних форумів». ***(Angelin Yeoh. CyberSecurity Malaysia report: Government sectors suffered most data breaches, while telcos spilled over 400GB of data in H1 2023 // Star Media Group Berhad (https://www.thestar.com.my/tech/tech-news/2023/10/25/cybersecurity-malaysia-report-government-sectors-suffered-most-data-breaches-while-telcos-spilled-over-400gb-of-data-in-h1-2023). 25.10.2023).***

***

«Жовтень призначений для підвищення обізнаності про кібербезпеку, але захист від кібератак – це завдання 24/7. Згідно зі звітом Fortinet 2023 Cybersecurity Skills Gap, більшість організацій (80%) зазнали кібератак протягом попередніх 12 місяців, і майже половина з них втратили понад 1 мільйон доларів США.

Причина очевидна. Кіберзлочинці більш досвідчені, використовують нові технології та стратегії для розвитку та монетизації атак. Зловмисники також все частіше атакують критично важливу інфраструктуру, служби та уряди, що має різноманітні наслідки та підвищує ризик для життя та засобів до існування

Знищення цих злочинних організацій вимагає розуміння ризиків, знання ефективних профілактичних заходів і доступу до кваліфікованих професіоналів для впровадження стратегій і технологій захисту критично важливих систем.

Розуміння ризику

Кіберзлочинність – це великий бізнес. Злочинні мережі тепер можуть пропонувати злочинність як послугу, яка підтримується складними бізнес-структурами. Розуміння того, як ці мережі працюють, допомагає захисникам кількісно оцінити ризик. Хоча ідеального вимірювання не існує, сектор кібербезпеки працює над тим, щоб зрозуміти масштаби загрози.

Нещодавно Fortinet, Banco Santander, Microsoft і PayPal запустили «Атлас кіберзлочинності» — спільну ініціативу, яка надає галузевим, правоохоронним і державним установам доступ до екосистем та інфраструктури кіберзлочинців, щоб допомогти зруйнувати та демонтувати ці мережі.

У зв’язку зі збільшенням масштабів і наслідків кібератак звіт Всесвітнього економічного форуму показує, що більшість керівників бізнесу та кібербезпеки (91%) вважають, що катастрофічна кіберподія може статися протягом наступних двох років. Захист від атак вимагає відстеження ефективності дій, спрямованих на запобігання або припинення атак, що допомагає визначити найкращі практики та розвивати підходи.

Існують ресурси, які допомагають організаціям, у тому числі двічі на рік звіт Fortinet Global Threat Landscape, дослідження IBM щодо витрат на порушення даних і звіт Verizon про розслідування витоку даних. Кожен забезпечує регулярну перевірку, що дає змогу спільноті кібербезпеки відстежувати тенденції.

На батьківщині Канадський центр кібербезпеки та RCMP опублікували базову оцінку кіберзагроз щодо кіберзлочинності. Оцінка стосується найбільш значущих

тактик кіберзлочинності, методів і характеру глобальної загрози, зосереджуючись на наслідках для Канади.

У міру появи більш надійних даних спільнота кібербезпеки повинна встановити стандартні визначення та способи звітування про статистику кіберзлочинності. Ця консолідація спростить розкриття інформації організаціям, які вживають захисних заходів.

Заповнення прогалини

Незважаючи на зростання загроз, існує глобальна прогалина в навичках кібербезпеки, що ставить під загрозу організації, уряди та громадян. Відповідно до звіту Fortinet Skills Gap, майже 70 відсотків керівників безпеки кажуть, що їхні організації стикаються з додатковими ризиками через цю нестачу.

Проблема полягає в двох аспектах: галузь змінюється з шаленою швидкістю, вимагаючи постійного підвищення кваліфікації, і не вистачає кваліфікованих людей, щоб заповнити відкриті посади. Найскладніші посади для заповнення часто зосереджені на сферах значного ризику або зростання, таких як хмарна безпека, операції безпеки, мережева безпека та аналіз загроз і зловмисного програмного забезпечення.

Державний, приватний і академічний сектори повинні знайти нових учасників у сфері кібербезпеки, залучаючи недостатньо представлені групи. У той же час існуючі фахівці з кібербезпеки також повинні будуть підвищити кваліфікацію, щоб керувати організаційними ризиками та адаптуватися до нових технологій і автоматизації.

Навчання

Організації можуть почати усувати прогалину в навичках за допомогою доступних програм навчання та сертифікації з кібербезпеки. Сертифікація дозволяє професіоналам вдосконалювати свої навички та випереджати мінливий ландшафт загроз. Такі програми, як сертифікація експертів з мережевої безпеки Fortinet Training Institute (NSE), пропонують спеціалізовані курси навчання, щоб професіонали та роботодавці могли легко виявляти певні прогалини.

Fortinet Training Institute зосереджується на розширенні доступу до навчання з кібербезпеки, щоб усунути прогалину в навичках галузі. Fortinet пообіцяв навчити мільйон людей кібербезпеці до 2026 року, використовуючи свою відзначену нагородами навчальну програму, співпрацюючи з академічними партнерами та збільшуючи кількість викладачів, здатних проводити її багаторівневі програми сертифікації.

Fortinet також пропонує навчання для персоналу, не пов'язаного з безпекою та IT-спеціалістами, що є важливою інвестицією, враховуючи останній звіт Fortinet щодо безпеки та навчання, згідно з яким 56 відсотків керівників організацій вважають, що їхнім співробітникам бракує знань, коли йдеться про кібербезпеку. Один із способів вирішити цю проблему – забезпечити цільове навчання. Наприклад, Fortinet пропонує орієнтовану на освіту версію своєї служби безпеки та навчання для шкільних округів K-12, щоб покращити навички викладачів і персоналу з кібербезпеки та зменшити кіберризик. Нещодавно вони розширили програму до Канади та забезпечуватимуть безкоштовне навчання англійською та французькою мовами для 300 шкільних рад та 1700 приватних шкіл по всій країні.

Усунення прогалин у безпеці вимагає багатогранного підходу. Співтовариство кібербезпеки має кількісно визначити ризик, щоб краще зрозуміти ландшафт загроз. Він також повинен кількісно оцінити реакцію на загрози, щоб визначити найкращі практики та найефективніші рішення проти кібератак. Успіх вимагає зосередження на розширенні кадрового резерву та відданості підвищенню кваліфікації та навчанню. Швидке зростання злочинних мереж, дедалі складніші атаки та навіть вплив цифрової трансформації можуть зробити це складним завданням. Проте організації можуть зменшити ризик, використовуючи надійні програми навчання та сертифікації для підвищення кваліфікації персоналу та усунення пріоритетних прогалин у своїх командах безпеки та мереж». ***(Rob Rashotte. Conquering the Cybersecurity Gap // IT World Canada (https://www.itworldcanada.com/sponsored/conquering-the-cybersecurity-gap). 25.10.2023).***

***

«Корпорація Майкрософт опублікувала детальний профіль англомовного загрозливого актора з розширеними можливостями соціальної інженерії, який він відстежує як Octo Tempest, який націлений на компанії у вимаганні даних і атаках програм-вимагачів.

Атаки Octo Tempest постійно розвивалися з початку 2022 року, розширюючи їх націлювання на організації, що надають кабельні телекомунікаційні, електронні та технічні послуги, а також співпрацюють із групою програм-вимагачів ALPHV/BlackCat.

Від крадіжки облікового запису до програм-вимагачів

Спочатку помічено, що зловмисник продає SIM-карти та краде облікові записи високопоставлених осіб із криптовалютними активами.

Наприкінці 2022 року Octa Tempest перейшла до фішингу, соціальної інженерії, масового скидання паролів для клієнтів зламаних постачальників послуг і крадіжки даних.

Раніше цього року група загроз атакувала компанії в сферах ігор, гостинності, роздрібної торгівлі, виробництва, технологій і фінансів, а також постачальників керованих послуг (MSP).

Ставши філією ALPHV/BlackCat, Octa Tempest розгорнула програму-вимагач як для крадіжки, так і для шифрування даних жертви…

Група використала накопичений досвід для створення більш просунутих і агресивних атак, а також почала монетизувати вторгнення, вимагаючи жертв після викрадення даних.

У Microsoft кажуть, що Octo Tempest також використовував прямі фізичні загрози в деяких випадках, щоб отримати логіни для посилення атаки.

Згідно з дивним поворотом подій, Octo Tempest стала афілійованою компанією ALPHV/BlackCat ransomware-as-a-service (RaaS), повідомляє Microsoft, і до червня вони почали розгортати програми-вимагачі Windows і Linux, зосереджуючись на VMware ESXi. останнім часом...

Недавні атаки цієї групи спрямовані на організації в різних секторах, включаючи ігри, природні ресурси, готельний бізнес, споживчі товари, роздрібну торгівлю, постачальників керованих послуг, виробництво, право, технології та фінансові послуги.

Octo Tempest TTP

Корпорація Майкрософт вважає, що Octo Tempest — це добре організована група, до складу якої входять члени з великими технічними знаннями та кілька операторів ручної роботи з клавіатурою.

Хакери часто отримують початковий доступ за допомогою розширеної соціальної інженерії, яка спрямована на облікові записи технічних адміністраторів (наприклад, персонал служби підтримки та довідкової служби) з достатніми дозволами для подальшої атаки.

Вони досліджують компанію, щоб визначити цілі, яких вони можуть видати за себе до рівня імітації мовних моделей людини під час телефонних дзвінків.

Таким чином вони обманом змушують технічних адміністраторів скинути паролі та скинути методи багатофакторної автентифікації (MFA).

Інші методи початкового доступу включають:

обманом змусити ціль встановити програмне забезпечення для віддаленого моніторингу та керування

викрадення логінів через фішингові сайти

купівля облікових даних або токенів сесії в інших кіберзлочинців

СМС-фішингові співробітники з посиланнями на підроблені портали входу, які перехоплюють облікові дані

SIM-заміна або переадресація

Прямі погрози розправою

Отримавши достатній доступ, хакери Octo Tempest починають етап розвідки атаки, перераховуючи хости та служби та збираючи інформацію, яка дозволить зловживати законними каналами для просування вторгнення…

Потім Octo Tempest переходить до вивчення інфраструктури, перераховуючи доступ і ресурси в хмарних середовищах, сховищах коду, серверах і системах керування резервним копіюванням.

Щоб підвищити привілеї, зловмисник знову звертається до соціальної інженерії, заміни SIM-карти або переадресації виклику та ініціює самостійне скидання пароля облікового запису цілі.

Під час цього кроку хакери зміцнюють довіру з жертвою, використовуючи скомпрометовані облікові записи та демонструючи розуміння процедур компанії. Якщо у них є обліковий запис менеджера, вони самі погоджують запити на збільшення дозволів.

Поки вони мають доступ, Octo Tempest продовжує шукати додаткові облікові дані для розширення свого охоплення. Вони використовують такі інструменти, як Jercretz і TruffleHog, щоб автоматизувати пошук відкритих ключів, секретів і паролів у сховищах коду.

Щоб зберегти свої сліди прихованими, хакери також атакують облікові записи співробітників служби безпеки, що дозволяє їм відключати продукти та функції безпеки…

За словами Microsoft, Octo Tempest намагається приховати свою присутність у мережі, пригнічуючи сповіщення про зміни та змінюючи правила поштової скриньки, щоб видаляти електронні листи, які можуть викликати у жертви підозри щодо порушення.

Дослідники надають наступні додаткові інструменти та методи, які Octo Tempest використовує у своїх атаках:

інструменти з відкритим кодом: ScreenConnect, FleetDeck, AnyDesk, RustDesk, Splashtop, Pulseway, TightVNC, LummaC2, Level.io, Mesh, TacticalRMM, Tailscale, Ngrok, WsTunnel, Rsocx і Socat

розгортання віртуальних машин Azure для забезпечення віддаленого доступу через установку RMM або модифікацію наявних ресурсів через послідовну консоль Azure

додавання методів MFA до існуючих користувачів

за допомогою інструменту тунелювання Twingate, який використовує екземпляри контейнера Azure як приватний з'єднувач (без доступу до загальнодоступної мережі)

Хакери також переміщують викрадені дані на свої сервери за допомогою унікальної техніки, яка включає Azure Data Factory і автоматизовані конвеєри, щоб поєднуватися з типовими операціями з великими даними.

Щоб експортувати бібліотеки документів SharePoint і швидше передати файли, зловмисник часто реєстрував законні рішення для резервного копіювання Microsoft 365, такі як Veeam, AFI Backup і CommVault.

Корпорація Майкрософт зазначає, що виявлення або полювання на цього загрозливого актора в середовищі є нелегким завданням через використання соціальної інженерії, методів життя поза межами землі та різноманітних інструментів.

Однак дослідники надають набір загальних вказівок, які можуть допомогти виявити зловмисну активність, яка починається з моніторингу та перегляду процесів, пов'язаних із ідентифікацією, середовищ Azure та кінцевих точок.

Octo Tempest має фінансову мотивацію та досягає своїх цілей шляхом крадіжки криптовалюти, вимагання крадіжки даних або систем шифрування та вимагання викупу». ***(Ionut Ilascu. Microsoft: Octo Tempest is one of the most dangerous financial hacking groups // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/microsoft-octo-tempest-is-one-of-the-most-dangerous-financial-hacking-groups/?utm_source=flipboard&utm_content=lks2017%2Fmagazine%2FInet+Scams%2FComputing+Tips%2FTech+Updates%2FInteresting+Snippets+from+the+Ether). 26.10.2023).***

***

«Казино тільки оговтуються від кібератаки, яка завдала шкоди об'єктам MGM Resorts (MGM) на Лас-Вегас-Стріп минулого місяця. Але тепер нова інформація від компанії проливає більше світла на те, наскільки згубною була атака.

Відповідальність за кібератаку 11 вересня взяла на себе група хакерів, відома як Scattered Spider, підгрупа більшої злочинної організації, відомої як ALPHV. Його атака програм-вимагачів закрила все, від служб бронювання готелів до банкоматів і ігрових автоматів у власності MGM.

У нормативній заявці до Комісії з цінних паперів і бірж MGM визнала, що хакери отримали деяку особисту інформацію, що належить клієнтам, які здійснювали операції з компанією до березня 2019 року.

Ця інформація включає імена, контактну інформацію, стать, дати народження та номери водійських прав. Для деяких хакери навіть змогли зібрати номери соціального страхування та паспортів під час атаки. Однак компанія також заявляє, що не вважає, що паролі клієнтів, номери банківських рахунків або дані платіжних карток були отримані злочинцями.

Для інвесторів компанія заявляє, що, на її думку, атака матиме негативний вплив на результати третього кварталу 2023 року, головним чином на операції в Лас-Вегасі, на суму близько 100 мільйонів доларів.

MGM каже, що рівень заповнюваності протягом місяця знизився приблизно на 5% до 88% порівняно з попереднім роком.

«Хоча на даний момент Компанія вважає, що її страхування кібербезпеки буде достатньо для покриття фінансових наслідків для її бізнесу в результаті операційних збоїв, одноразових витрат, описаних вище, і майбутніх витрат, повний обсяг витрат і пов'язані з ними наслідки це питання не було вирішено», - йдеться у заяві MGM.

Акції MGM впали на 18,5% між 11 вересня та закриттям у четвер. (У п'ятницю акції зросли на 4,9% до 36,48 доларів США». ***(Tony Owusu. Las Vegas Strip icon confirms astronomical financial toll from recent cyberattack // The Arena Media Brands, LLC (https://www.thestreet.com/travel/las-vegas-strip-icon-confirms-astronomical-***

financial-toll-from-recent-cyberattack?utm_source=flipboard&utm_content=TheStreet%2Fmagazine%2FMeme+Stocks). 06.10.2023).

***

«Попри те, що одна із хакерських груп погодилася слідувати новому зведенню кіберправил, на вихідних вона заявила, що почала атаку на сайт королівської сім'ї в Британії.

Українські та російські хакери домовилися знизити рівень кібератак і дотримуватися нового зведення правил, який має назву Женевський кодекс кібервійни. Про це повідомляє британське Express.

Як пише видання, таке прагнення врегулювати діяльність тисяч людей, що входять до патріотичних кібергруп, спочатку було визнано неможливим. Критика цих дій посилилася після того, як низка активістів заявили, що не дотримуватимуться правил. Однак дві найбільші групи хакерів, які брали участь у війні проти України, пообіцяли деескалацію кібератак, особливо якщо це стосується цивільних об'єктів і мирного населення.

«Після вторгнення в Україну спостерігався постійний потік руйнівних кібератак на державні служби як в Україні, так і в Росії з різним ступенем впливу. Групи хактивістів використовували здебільшого прості форми кібератак, але успішно на певний час порушували роботу банків, компаній, аптек, лікарень, залізничних мереж і цивільних державних послуг для громадян України та Росії», — пише BBC News, випереджаючи інтерв'ю з лідером сумнозвісної проросійської хакерської групи Killnet.

Як зазначає видання, не маючи особливих цілей в уряді та армії, хакери, тим не менш, насолоджувалися тим, що провокували негаразди в суспільстві для просування своїх інтересів, часто збираючи гнівні пости в соціальних мережах від тих, хто постраждав від їхніх хакерських атак.

Хакерська група Killnet — що важливо знати

Killmilk, як його називають, заснував групу Telegram для Killnet незабаром після вторгнення в Україну. Зараз у цієї групи 90 000 підписників. Групу звинувачували в тісних зв'язках із Кремлем, але вона завжди це заперечувала.

У квітні Національний центр кібербезпеки Великої Британії назвав такі групи, як Killnet, новою загрозою, з якою стикаються союзники України, попередивши британські підприємства про зростання атак з їхнього боку. Однак зараз чиновники вірять, що якщо Killnet дотримається свого слова, то кібератаки на цивільні об'єкти, зокрема на об'єкти союзників України, припиняться.

У бесіді з BBC лідер Killnet заявив, що він «згоден з умовами і правилами Червоного Хреста, і нехай це стане першим кроком від Killnet до миру».

ІТ-армія України також заявила, що дотримуватиметься восьми правил МКЧХ. Група, у Telegram-каналі якої налічується 160 000 учасників, також націлена на державні служби, як-от залізничні системи і банки. Проте її представник повідомив BBC News, що група «докладе всіх зусиль, щоб дотримуватися правил», навіть незважаючи на те, що це може поставити їх у невигідне становище порівняно з противниками. Наприклад, він додав, що напади на об'єкти охорони здоров'я завжди були для них червоною лінією.

«Ця новина означає, що, ймовірно, відбудеться значне скорочення кількості кібератак, оскільки групи обмежують свою діяльність офіційними або військовими цілями. Проте інші групи хактивістів, що працюють під іншими патріотичними або етичними гаслами, заявили, що взагалі будуть ігнорувати правила», — уточнює BBC.

Женевський кодекс кібервійни — що про нього відомо

Нещодавно Міжнародний комітет Червоного Хреста (МКЧХ) опублікував список правил для цивільних хакерів — перший і єдиний у своєму роді.

Його назвали Женевським кодексом кібервійни, і він охоплює вісім правил, що забороняють, серед іншого, напади на лікарні та поширення загроз, спрямованих на розпалювання терору серед цивільного населення.

Відповідно до міжнародного гуманітарного права діють такі правила:

Не спрямовувати кібератаки на цивільні об'єкти.

Не використовувати шкідливе ПЗ або інші інструменти чи методи, які поширюються автоматично і завдають шкоди військовим і цивільним об'єктам без розбору.

Плануючи кібератаку на військовий об'єкт, зробити все можливе, щоб уникнути або звести до мінімуму наслідки, які хакерська операція може спричинити на цивільне населення.

Не проводити жодних кібероперацій проти медичних і гуманітарних об'єктів.

Не проводити кібератаки на об'єкти, необхідні для виживання населення або здатні вивільнити небезпечні сили.

Не погрожувати насильством з метою посіяти терор серед цивільного населення.

Не підбурювати до порушень міжнародного гуманітарного права.

Дотримуватися цих правил, навіть якщо противник цього не робить.

У вересні Фокус писав, що хакери зламали сайти російської партії «Единая Россия». На її порталах з'явилася інформація про втрати ЗС РФ у війні з Україною, а також іронічні заклики голосувати за партію, яка розкрадає країну і вбиває її громадян…» ***(Тетяна Заремба. Хакери з РФ пообіцяли дотримуватися «Женевського кодексу кібервійни»: що відомо // Фокус (https://focus.ua/uk/digital/597590-hakeri-z-rf-poobicyali-dotrimuvatisya-zhenevskogo-kodeksu-kibervijni-sho-vidomo). 06.10.2023).***

***

«Пов’язана з Північною Кореєю хакерська компанія Lazarus Group активно використовує програми Trojanized Virtual Network Computing (VNC) для націлювання на професіоналів оборонної та ядерної промисловості, що є частиною поточної схеми, відомої як Operation Dream Job.

Цільовими підприємствами є переважно підприємства, які безпосередньо займаються оборонним виробництвом, у тому числі ті, що виробляють

радіолокаційні системи, безпілотні літальні апарати, військові транспортні засоби, кораблі та зброю.

Відповідно до звіту Kaspersky про тенденції розвитку стійких загроз (APT) за третій квартал 2023 року, зловмисники використовують платформи соціальних мереж, щоб заманити шукачів роботи в активацію цих шкідливих програм.

Троянізовані програми VNC створені для роботи непомітно, щоб уникнути виявлення механізмів безпеки, заснованих на поведінці.

Після активації користувачем ці мерзенні програми завантажують додаткове корисне навантаження, порушуючи цільову систему або мережеву інфраструктуру...

У ширшому контексті група Lazarus є частиною групи північнокорейських груп загрози, включаючи APT37, APT43, Kimsuky та її власні підгрупи Andariel і BlueNoroff.

Ці групи адаптувалися та розвивалися, як зазначає Mandiant, що належить Google, розробляючи спеціальне шкідливе програмне забезпечення для багатьох платформ, включаючи Linux і macOS.

Це свідчить про ширший зсув у тактиці, техніках і процедурах, які використовують північнокорейські хакерські організації, що робить атрибуцію дедалі складнішою.

Варто відзначити, що ці досягнення супроводжувалися підвищеною увагою до розробки зловмисного програмного забезпечення для macOS, особливо націленого на високоцінних людей у сфері криптовалют і блокчейнів, повідомляє Mandiant». ***(North Korean hackers compromise defence and nuclear sectors with trojanized apps // Fusion Media Limited (https://au.investing.com/news/stock-market-news/north-korean-hackers-compromise-defence-and-nuclear-sectors-with-trojanized-apps-3005514?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 19.10.2023).***

***

«На війні є правила. Міжнародне гуманітарне право регулює, що можуть і чого не можуть робити комбатанти з метою захисту цивільних осіб і обмеження страждань.

Більшість із цих законів були розроблені протягом 19-го та 20-го століть. Але в наше століття з'явився новий тип поля бою: сфера кібератак, цифрових кампаній та інформаційних онлайн-операцій. Усе це відіграло підвищену роль у війні Росії в Україні та, дедалі більше, у поточному конфлікті Ізраїлю та ХАМАС.

Існує стійкий міф, що кіберпростір – це беззаконний дикий захід. Це не може бути далі від істини. Існує чіткий міжнародний консенсус щодо того, що існуючі закони війни застосовуються онлайн.

За останній місяць ми побачили три значні події в цій сфері. Правила для «цивільних хакерів» почали набирати обертів. Новий міжнародний гуманітарний звіт рекомендує урядам, технологічним компаніям та іншим шляхи подальших дій. І Міжнародний кримінальний суд вперше заявив, що вважає кібервійну під своєю юрисдикцією.

Правила для хактивістів

4 жовтня 2023 року двоє радників Міжнародного комітету Червоного Хреста запропонували набір правил для «цивільних хакерів» під час війни. Пропозиції включають такі речі, як «не проводити жодних кібероперацій проти медичних і гуманітарних закладів» і «під час планування кібератаки на військовий об'єкт зробіть усе можливе, щоб уникнути або мінімізувати вплив вашої операції на цивільних осіб».

Автори мотивувалися доказами онлайн-атак, які порушили роботу банків, компаній, аптек, лікарень, залізничних мереж і цивільних державних служб.

Кібернетичні, цифрові та інформаційні операції, які використовуються поряд із «реальними» військовими операціями, стали популярними під час війни Росії в Україні. Багато операцій проводяться цивільними групами, формально не пов'язаними з військовими.

Ці маневри не є вражаючими. Однак, як сказав Джеремі Флемінг (колишній керівник GCHQ, електронного шпигунського агентства Великобританії):

Ми ніколи не розуміли, що катастрофічна кібератака була центральною частиною використання Росією наступальної кібератаки у своїй військовій доктрині. Думати інакше означає неправильно оцінювати вплив кібернетики на військові кампанії. Це не означає, що ми не бачили кібернетики в цьому конфлікті. У нас є – і багато.

Після публікації запропонованих правил для цивільних хакерів сталося щось надзвичайне.

Дві з найбільших хактивістських груп, які активно беруть участь по різні боки війни в Україні, — пов'язана з Росією Killnet та Українська ІТ-армія. Представники обох груп пообіцяли ВВС, що вони будуть дотримуватися правил.

Цифрові загрози під час збройного конфлікту

Дотримуватися законів війни в кіберпросторі мають не лише актори в Україні та не лише хактивістські групи.

18 жовтня Міжнародний комітет Червоного Хреста опублікував остаточний звіт своєї глобальної консультативної ради щодо цифрових загроз під час збройних конфліктів.

Звіт є підсумком дворічної роботи. Рада складається з різноманітної групи експертів, що охоплюють геополітичний спектр, включаючи Сполучені Штати, Росію, Китай, Південну Африку, Мексику, Індію та Австралію (включаючи мене).

Ми працювали над «міжнародним консенсусом щодо того, що встановлені принципи та правила [міжнародного гуманітарного права] застосовуються до всіх форм ведення війни та всіх видів зброї, будь то нова чи стара, цифрова чи фізична».

Щоб захистити цивільне населення від цифрових загроз, звіт містить 25 орієнтованих на дії рекомендацій для воюючих сторін, держав, технологічних компаній і гуманітарних організацій.

Починаючи з 2013 року, домовленості, укладені в Організації Об'єднаних Націй, визнають, що чинне міжнародне право застосовується до дій держав у кіберпросторі.

У 2021 році Росія, Китай, США, Австралія та всі країни ООН пішли ще далі, прямо визнавши застосування законів війни до кібероперацій.

Міжнародний Комітет Червоного Хреста – його місія полягає в «запобіганні страждань шляхом просування та зміцнення гуманітарного права та універсальних гуманітарних принципів» – також неодноразово підтверджував це, в тому числі у звітах, наведених вище.

Міжнародний кримінальний суд бере свою думку

Звичайно, погодження з правилами не заважає безвідповідальним особам їх порушувати. І тут виникає третя важлива подія.

У вересні 2023 року Карім А. А. Хан, прокурор Міжнародного кримінального суду, повідомив, що суд почне «збирати та перевіряти» докази кібервійни. Він також розглядатиме «зловживання Інтернетом для посилення мови ненависті та дезінформації, що може сприяти або навіть безпосередньо призводити до виникнення жорстоких злочинів».

Це перший раз, коли Міжнародний кримінальний суд прямо вказав, що кібервійна та зловживання Інтернетом підпадають під його юрисдикцію. Це сповіщає уряди, військові, технологічні компанії та хакерів, що вони не діють безкарно в кіберпросторі.

Оскільки війна в Україні затягується, а конфлікт між Ізраїлем і ХАМАС загострюється (зокрема, зростає кількість повідомлень про хактивізм), усім сторонам було б добре подумати, що правила кібервійни чіткі.

Бомби чи байти, ракети чи зловмисне програмне забезпечення, застосовується міжнародне гуманітарне право». ***(Johanna Weaver. Governments and hackers agree: the laws of war must apply in cyberspace // The Conversation Media Group Ltd (https://theconversation.com/governments-and-hackers-agree-the-laws-of-war-must-apply-in-cyberspace-216202?utm_source=flipboard&utm_content=Farawayman%2Fmagazine%2FMilitary+Technology). 25.10.2023).***

***

«…Відповідно до нового звіту, опублікованого цього тижня, компанія з кібербезпеки Human Security виявила докази того, що кілька моделей приставок Android TV і принаймні один планшет були заражені прямо з коробки небезпечними бекдорами прошивки, які важко виявити і ще важче видалити. Відповідно до звіту, опублікованого Wired Human Security виявила щонайменше 74 000 мобільних телефонів, планшетів і підключених телевізійних приставок Android, які мають ознаки зараження по всьому світу., дослідники виявили ознаки того, що це може вплинути на щонайменше 200 різних моделей пристроїв Android.

Загалом дослідники виявили вісім пристроїв, які, як відомо, мають встановлені бекдори — сім ТВ-приставок, T95, T95Z, T95MAX, X88, Q9, X12PLUS і MXQ Pro 5G, а також планшет J5-W. Усі пристрої мають широку та різноманітну базу користувачів від дому та бізнесу до шкіл у США

«Це справді розповсюджений спосіб шахрайства», — сказав CISO Human Security Гевін Рейд в інтерв'ю Wired. Він додав, що правоохоронні органи вже отримали всю зібрану інформацію про об'єкти, де могли бути виготовлені пристрої.

Ось як працює схема. Пристрої створені в Китаї, де на певному етапі комерційного ланцюжка поставок перед їх доставкою торговим посередникам або магазинам встановлюється бекдор прошивки на основі шкідливого програмного забезпечення. Бекдор побудований на основі шкідливого програмного забезпечення Triada, «завантажувача», основною метою якого є створення бекдору, через який можна завантажувати та інсталювати інші шкідливі програми. Ці бекдори, які отримали назву Badbox, пов'язані з глобальною мережею шахрайства та кіберзлочинності.

«Без відома користувача, коли ви підключаєте цю штуку, вона переходить до командно-контрольної системи (C2) у Китаї, завантажує набір інструкцій і починає робити купу поганих речей», — сказав Рід виданню.

Потім хакери використовують цей доступ до скомпрометованих пристроїв для здійснення різних типів шахрайства, включаючи рекламне шахрайство, створення

підроблених облікових записів Gmail і WhatsApp і віддалене встановлення коду, пояснюється у звіті Human Security. Група, яка стоїть за схемою, комерційно продає доступ до приватних мереж і стверджує, що має доступ до мільйонів мобільних IP-адрес.

Фірма з кібербезпеки повідомляє, що оператори BadBox вивели з ладу свої командно-контрольні сервери, нібито для адаптації та обходу захисних заходів під час посиленого контролю. Занепокоєним споживачам слід уникати використання заражених пристроїв, оскільки зловмисне програмне забезпечення знаходиться в розділі прошивки, через що його надзвичайно важко видалити, якщо у вас немає певних технічних знань.

«Ви можете думати про ці Badboxes як про сплячі клітини. Вони просто сидять і чекають наборів інструкцій», — сказав Рейд Wired. Усім, хто шукає нову телевізійну трансляцію, він порадив обирати знайомі бренди під час купівлі нових продуктів і зупинятися на пристроях перевірених виробників». ***(Alyse Stanley. Thousands of Android TV boxes infected with dangerous malware linked to fraud // Future US, Inc. (https://www.tomsguide.com/news/thousands-of-android-tv-boxes-infected-with-dangerous-malware-linked-to-fraud?utm_source=flipboard&utm_content=TomsGuide%2Fmagazine%2FTom%27s+Guide%3A+Full+Edition). 08.10.2023).***

***

«Глобальне розслідування, опубліковане в четвер щодо Intellexa, альянсу компаній із цифрової зброї та спостереження, що належать ізраїльтянам, але діють за межами Ізраїлю, показує, як компанія продавала своє шпигунське програмне забезпечення до Єгипту, де воно використовувалося проти критиків режиму. Згідно з розслідуванням, Intellexa також представила свої можливості Саудівській Аравії, Малайзії, Камеруну, Маврикію, Сьєрра-Леоне та іншим.

Викриття є частиною розслідування «Файлів хижаків», яке базується на документах і доказах, отриманих французьким журналом Mediapart і німецьким Der Spiegel. В його аналізі взяли участь 15 ЗМІ під керівництвом EIC (European

Investigative Collaborations). Shomrim, через журналіста Даніеля Долева, був ізраїльським партнером у проекті. AmnestyTech, судово-медична лабораторія Amnesty International, допомогла в аналізі технічних знахідок.

Intellexa, компанія з розвідки та кіберзброї, створена колишніми ізраїльтянами, принаймні донедавна була зареєстрована в Греції та має пов’язані компанії в Ірландії та Північній Македонії. Він слугує «єдиним вікном» для потреб державного нагляду.

Масштабне розслідування також виявило, що колишній прем’єр-міністр Ізраїлю Ехуд Ольмерт працював консультантом фірми і, можливо, брав участь у допомозі продавати свої товари до Німеччини. Ольмерт підтвердив, що працює в Intellexa, але сказав, що їхні зв’язки припинилися кілька місяців тому.

У липні цього року Міністерство торгівлі США внесло в чорний список Intellexa та Cytrox, які належать різним громадянам Ізраїлю, серед яких колишній командир військової розвідки Таль Ділян, після того, як їх шпигунське програмне забезпечення було використано проти правозахисників, журналістів і політиків. І Intellexa, і Cytrox, які розробили Predator, опинилися в центрі масштабного політичного прослуховування телефонних розмов у Греції.

Ось ключові висновки з розслідування бомби.

Дуже ізраїльська єгипетська угода

Розслідування ґрунтується на документах і повідомленнях, пов'язаних з фірмою Nexa. Партнерство між Intellexa та Nexa було підписано в 2019 році та тривало принаймні до 2021 року. Nexa — це французька фірма, яка де-факто є ребрендингом старішої фірми масового стеження під назвою Amesys, першим відомим клієнтом якої був лівійський диктатор Муамар Каддафі. Поряд із Nexa, яка зареєстрована у Франції, у Дубаї була створена дочірня фірма під назвою Advanced Middle East Systems, або AMES, щоб допомогти на ринку різних технологій альянсу.

За даними розслідування, протягом багатьох років було кілька спроб просунути технологію в Єгипет, а після того, як Nexa та Intellexa об’єдналися, у 2020 році було принаймні дві спроби продати технології стеження режиму єгипетського президента Абдель-Фаттаха Аль. -Сіссі. У 2021 році було виявлено, що політик у вигнанні Айман Нур був заражений шпигунським програмним забезпеченням

Predator разом з іншою неназваною жертвою. Цього року стало відомо, що це був єгипетський законодавець Ахмед Алтантаві і що останніми місяцями робилися численні спроби зламати його телефон. Алтантаві оголосив, що балотується на майбутніх виборах у Єгипті.

Згідно з розслідуванням, у вересні 2020 року були розроблені плани проведення демонстраційної зустрічі в Каїрі. Щоб підготувати демонстрацію, була відкрита спільна група WhatsApp з високопоставленими представниками як французької, так і ізраїльської сторін, включаючи Оза Лів, одного із засновників групи, який сам був колишнім командиром старшого підрозділу розвідки. Це сталося незважаючи на минулі занепокоєння з приводу дотримання прав людини в країні та того, що технологія використовуватиметься для націлювання на членів ЛГБТК-спільноти, згідно з повідомленнями, надісланими офіційними особами.

Відповідно до повідомлень, ізраїльтяни та, можливо, навіть люди з Ізраїлю мали бути залучені до рекламної презентації, яка мала включати живу демонстрацію можливостей злому телефону. Групу також повідомили, що єгиптяни були налякані, що візит буде викритий - іншою єгипетською державною агенцією - через VIP-поставлення до посадових осіб Nexa та Intellexa в аеропорту.

Але демонстрація в Каїрі пройшла успішно: наприкінці 2020 року було підписано контракт. Про це французький гендиректор повідомив у групі Nexa-Intellexa WhatsApp, додавши три емодзі з пляшкою шампанського. «Дивовижно», — відповів віце-президент із продажів Intellexa, а Діліан додала: «Чудово! З Новим роком». Французький чиновник зазначив, що найближчим часом попросить показати підписану копію контракту: «З фараонами нічого не знаєш».

З невеликою допомогою Ольмерта

Розслідування також показало, що колишній прем'єр-міністр Ізраїлю Ехуд Ольмерт працював на Intellexa. Документи від 2022 року показують, що «колишній прем’єр-міністр Ізраїлю» мав бути залучений до рекламної пропозиції, яку фірма робила для BSI, федерального агентства з інформаційної безпеки Німеччини та органу, відповідального за кіберзахист Німеччини. Повідомлення показують, що BSI вагався; запропонована зустріч так і не відбулася, і BSI всі разом відмовилися.

В одному документі ім’я Ольмерта було відредаговано, але після того, як Шомрім зв’язався з колишнім прем’єр-міністром по телефону, він підтвердив, що працював на Intellexa. Ольмерт відмовився відповідати на запитання, зазначивши, що він у відпустці, але сказав, що консультаційна робота, яку він виконував для Intellexa, закінчилася кілька місяців тому.

За даними розслідування, протягом багатьох років було кілька спроб просунути технологію в Єгипет, а після того, як Nexa та Intellexa об’єдналися, у 2020 році було принаймні дві спроби продати технології стеження режиму єгипетського президента Абдель-Фаттаха Аль. -Сіссі. У 2021 році було виявлено, що політик у вигнанні Айман Нур був заражений шпигунським програмним забезпеченням Predator разом з іншою неназваною жертвою. Цього року стало відомо, що це був єгипетський законодавець Ахмед Алтантаві і що останніми місяцями робилися численні спроби зламати його телефон. Алтантаві оголосив, що балотується на майбутніх виборах у Єгипті…». ***(Omer Benjakob. Investigation: How Israeli Spyware Was Sold to Egypt and Pitched to Qatar and Saudi Arabia // Haaretz Daily Newspaper Ltd. (https://www.haaretz.com/israel-news/security-aviation/2023-10-05/ty-article/.premium/investigation-how-israeli-spyware-was-sold-to-egypt-and-pitched-to-qatar-and-saudi-arabia/0000018a-ff33-d037-a9ae-fffffdb00000?utm_source=flipboard&utm_content=Haaretz%2Fmagazine%2FIsrael+and+Middle+East+News). 05.10.2023).***

***

«Дослідники з компанії checkmarx виявили приховане шкідливе ПЗ (malware), націлене на користувачів месенджера Telegram та хмарних сервісів Amazon Web Services (AWS). Ця загроза є вкрай хитромудрим методом крадіжки даних, що робить її особливо небезпечною для широкого кола користувачів.

Фахівці з кібербезпеки відзначили, що шкідливе програмне забезпечення, відоме як «Агент Tesla», використовує складні механізми для обходу антивірусних систем та доставки шкідливого коду на пристрої жертв. Програмне забезпечення

здатне викрадати дані облікових записів та паролі, а також надсилати їх на віддалені сервери зловмисників.

Шкідливе програмне забезпечення поширюється через електронні листи з вкладеннями у вигляді інфікованих документів. Після відкриття вкладення на комп'ютері жертви активується шкідливий код, який, у свою чергу, починає збирати та надсилати персональні дані на сервери зловмисників.

Експерти наголошують, що основною метою атак є крадіжка облікових даних та паролів для доступу до акаунтів Telegram та AWS. Отже, рекомендується оновлювати антивірусні програми та уникати відкриття підозрілих вкладень в електронних листах.

Команда дослідників кібербезпеки продовжує роботу над виявленням та усуненням загрози. При цьому активно ведеться моніторинг мережі щодо нових атак і методів поширення шкідливого ПЗ. Особлива увага приділяється захисту даних користувача та підвищенню рівня безпеки сервісів Telegram і AWS». ***(Приховане шкідливе програмне забезпечення атакує користувачів Telegram // Internetua (https://internetua.com/prihovane-shkidlive-programne-zabezpecsennya-atakuye-koristuvacsiv-telegram). 14.10.2023).***

***

«Однією з найважливіших речей, які ви можете зробити для захисту своєї онлайн-безпеки, є встановлення одного з найкращих менеджерів паролів, але нещодавня кібератака доводить, що ви повинні бути обережними, навіть роблячи це. Завдяки прихованому зловмисному програмному забезпеченню, прихованому в Google Ads, ваш комп’ютер можуть заразити віруси.

Проблема стосується популярного менеджера паролів KeePass — точніше, він намагається видати себе за KeePass, використовуючи оманливу Google Ads. Вперше помічене Malwarebytes, мерзенне посилання з’являється у верхній частині результатів пошуку, тобто ви, швидше за все, побачите його перед законними веб-сайтами, які йдуть під ним.

Зазвичай це може не бути проблемою. Це тому, що Google Ads показує адресу цільового веб-сайту до того, як ви натиснете посилання, тому ви можете розпізнати його як підробку. Однак у цьому випадку імітатор KeePass використовує хитрий трюк, щоб замаскувати свою URL-адресу, роблячи її схожою на рекламне посилання на офіційний веб-сайт KeePass. Такий підступний обман міг би ввести в оману навіть найбільш уважного до безпеки користувача Інтернету.

Веб-сайт шкідливого ПЗ використовує Punycode, який може вставляти спеціальні символи в адреси веб-сайтів. У цьому випадку він замінює K у KeePass на K, який має майже нерозбірливий акцент під ним. При швидкому погляді ви можете навіть не помітити цього. Зрештою, це означає, що ви не відвідаєте справжній веб-сайт KeePass.

Коли ви клацаєте зловмисне посилання, вас швидко перенаправляють за різними URL-адресами, які використовуються для перевірки відвідувачів і їх фільтрації. Якщо веб-сайти визначать, що ви бот або використовуєте свій веб-браузер у заблокованому середовищі ізольованого програмного середовища, ви не досягнете кінцевого пункту призначення. Якщо вас вважають справжнім користувачем, ви потрапите на веб-сайт шкідливого програмного забезпечення.

Опинившись там, вам буде запропоновано завантажити вірус, який замаскований під менеджер паролів KeePass. Під час попереднього аналізу фірма безпеки Sophos виявила, що цей вірус пов’язаний із різними шкідливими програмами, які викрадають ваші паролі, дані кредитних карток тощо.

Як захиститися від такого роду шкідливих програм? Перша і найочевидніша відповідь – використовувати розширення для блокування реклами у веб-переглядачі. Це не дозволить цим шкідливим веб-сайтам дістатися до вас, незалежно від того, наскільки витонченими є їхні шахрайські прийоми.

Окрім цього, важливо встановити потужну антивірусну програму. Якщо ви не використовуєте блокувальник реклами, вам слід бути надзвичайно обережними, натискаючи будь-яке оголошення, яке з’являється в результатах пошуку. Якщо ні, ви можете стати жертвою зловмисного програмного забезпечення, навіть не усвідомлюючи цього». ***(Alex Blake. Hackers are using this incredibly sneaky trick to***

hide malware // Digital Trends Media Group (https://www.digitaltrends.com/computing/hackers-disguise-fake-keepass-website-google-ads/?utm_source=flipboard&utm_content=DigitalTrends%2Fmagazine%2FDigital+Trends%3A+Tech+for+the+Way+We+Live). 20.10.2023).

***

«За даними дослідження Barracuda Networks, яка спеціалізується на кібербезпеці, боти генерують близько 50% всього інтернет-трафіку у світі, а з них майже 30% — це так звані «погані» боти, які використовуються для різних злочинних цілей.

Це менше, ніж у 2021 році, коли їхня частка сягала 39%.

Автори дослідження пояснюють такий великий відсоток «поганих» ботів тим, що кіберзлочинці шукають нових способів обходити захист сайтів і створює більш складне та розумне програмне забезпечення.

Основною базою для запуску «поганих» ботів є Північна Америка, де переважають хмарні сервіси, такі як AWS або Microsoft Azure. Ці сервіси дозволяють швидко та легко реєструвати нові облікові записи та отримувати доступ до великої кількості IP-адрес.

Серед інших країн, які генерують шкідливий трафік ботів, виділяються ОАЕ (12%), Саудівська Аравія (6%), Катар (5%) та Індія (5%)». ***(Половина світового інтернет-трафіку припадає на ботів — дослідження // Internetua (https://internetua.com/polovina-svitovogo-internet-trafiku-pripadaye-na-botiv-doslidjennya). 20.10.2023).***

***

«Складна кросплатформна платформа зловмисного програмного забезпечення під назвою StripedFly п’ять років залишалася поза увагою дослідників кібербезпеки, заразивши за цей час понад мільйон систем Windows і Linux.

Касперський виявив справжню природу шкідливого фреймворку минулого року, знайшовши докази його активності, починаючи з 2017 року, причому шкідливе програмне забезпечення помилково класифікувалося лише як майнер криптовалюти Monero.

Аналітики описують StripedFly як не що інше, як вражаюче, що містить складні механізми приховування трафіку на основі TOR, автоматичне оновлення з надійних платформ, можливості розповсюдження, схожі на черв'яків, і спеціальний експлойт EternalBlue SMBv1, створений до публічного розкриття вади.

Хоча незрозуміло, чи використовувався цей фреймворк зловмисного програмного забезпечення для отримання прибутку чи кібершпигунства, Kaspersky каже, що його складність вказує на те, що це зловмисне програмне забезпечення APT (Advanced Persistent Threan).

Згідно з міткою часу компілятора для зловмисного програмного забезпечення, найраніша відома версія StripedFly з експлойтом EternalBlue датується квітнем 2016 року, тоді як публічний витік інформації групою Shadow Brokers стався в серпні 2016 року.

StripedFly у понад мільйонах систем

Фреймворк зловмисного програмного забезпечення StripedFly був вперше виявлений після того, як Касперський знайшов шелл-код платформи, впроваджений у процес WININIT.EXE, законний процес ОС Windows, який обробляє ініціалізацію різних підсистем.

Після дослідження впровадженого коду вони визначили, що він завантажує та виконує додаткові файли, наприклад сценарії PowerShell, із законних служб хостингу, таких як Bitbucket, GitHub і GitLab, включаючи сценарії PowerShell.

Подальше розслідування показало, що інфіковані пристрої, ймовірно, були вперше зламані за допомогою спеціального експлойта EternalBlue SMBv1, який був націлений на комп'ютери, піддані доступу до Інтернету.

Останнє корисне навантаження StripedFly (system.img) містить власний полегшений мережевий клієнт TOR для захисту мережевих комунікацій від

перехоплення, можливість відключення протоколу SMBv1 і поширення на інші пристрої Windows і Linux у мережі за допомогою SSH і EternalBlue.

Командно-контрольний сервер (C2) зловмисного програмного забезпечення знаходиться в мережі TOR, і зв'язок із ним включає часті повідомлення-маяки, що містять унікальний ідентифікатор жертви.

Для стабільності в системах Windows StripedFly коригує свою поведінку на основі рівня привілеїв, на яких він працює, і наявності PowerShell.

Без PowerShell він створює прихований файл у каталозі %APPDATA%. У випадках, коли PowerShell доступний, він виконує сценарії для створення запланованих завдань або зміни ключів реєстру Windows.

У Linux зловмисне програмне забезпечення приймає назву « sd-pam ». Він досягає стійкості за допомогою системних служб, файлу.desktop, що автоматично запускається, або змінюючи різні файли профілів і завантаження, такі як /etc/rc*, profile, bashrc або inittab. файли

Репозиторій Bitbucket, який доставляє корисне навантаження останнього етапу в системах Windows, вказує на те, що з квітня 2023 року по вересень 2023 року відбулося майже 60 000 заражень системи.

За оцінками, StripedFly заразив щонайменше 220 000 систем Windows з лютого 2022 року, але статистика за період до цієї дати недоступна, а репозиторій було створено в 2018 році.

Проте, за оцінками Касперського, понад 1 мільйон пристроїв були заражені фреймворком StripedFly.

Модулі шкідливих програм

Зловмисне програмне забезпечення працює як монолітний двійковий виконуваний файл із модулями, що підключаються, що надає йому операційну універсальність, яку часто асоціюють з операціями APT.

Ось підсумок модулів StripedFly зі звіту Касперського:

Зберігання конфігурації: зберігає зашифровану конфігурацію зловмисного програмного забезпечення.

Оновлення/видалення: керує оновленнями або видаленням на основі команд сервера C2.

Зворотний проксі: дозволяє віддалено виконувати дії в мережі жертви.

Обробник різних команд: виконує різноманітні команди, такі як захоплення знімка екрана та виконання командного коду.

Credential Harvester: сканує та збирає конфіденційні дані користувачів, такі як паролі та імена користувачів.

Повторювані завдання: виконує певні завдання за певних умов, наприклад, записування з мікрофона.

Модуль розвідки: надсилає детальну інформацію про систему на сервер C2.

Інфікатор SSH: використовує зібрані облікові дані SSH для проникнення в інші системи.

Інфектор SMBv1: черв'яки проникають в інші системи Windows за допомогою спеціального експлойта EternalBlue.

Модуль майнінгу Monero: майнить Monero, закамуфльований як процес "chrome.exe".

Присутність криптовалютного майнера Monero вважається спробою відтоку, причому основними цілями зловмисників є крадіжка даних і використання системи за допомогою інших модулів.

«Корисне навантаження зловмисного програмного забезпечення охоплює кілька модулів, що дозволяє актору працювати як APT, як майнер криптовалют і навіть як група програм-вимагачів», — йдеться у звіті Касперського.

«Примітно, що криптовалюта Monero, видобута за допомогою цього модуля, досягла свого піку в 542,33 доларів США 9 січня 2018 року, у порівнянні з її вартістю в 2017 році, яка становила близько 10 доларів США. Станом на 2023 рік вона підтримувала вартість приблизно в 150 доларів США».

«Фахівці Касперського підкреслюють, що модуль майнінгу є основним фактором, який дозволяє шкідливому ПЗ уникати виявлення протягом тривалого періоду».

Дослідники також виявили посилання на варіант програми-вимагача ThunderCrypt, який використовує той самий сервер C2 за адресою «ghtyqipha6mcwxiz[.]onion:1111».

«Модуль повторюваних завдань» також припускає, що невідомі зловмисники могли бути зацікавлені в отриманні прибутку для деяких жертв». ***(Bill Toulas. StripedFly malware framework infects 1 million Windows, Linux hosts // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/stripedfly-malware-framework-infects-1-million-windows-linux-hosts/?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology) . 26.10.2023).***

***

Програми-вимагачі

«Зловмисник злив повний вихідний код першої версії програми-вимагача HelloKitty на російськомовному форумі хакерів, стверджуючи, що розробляє новий, більш потужний шифрувальник.

Витік вперше виявив дослідник кібербезпеки 3xp0rt, який помітив загрозливого актора на ім’я 'kapuchin0', який випускав «першу гілку» шифрувальника HelloKitty.

Хоча вихідний код був оприлюднений кимось на ім’я 'kapuchin0', 3xp0rt повідомив BleepingComputer, що загроза також використовує псевдонім Gookee.

Зловмисник на ім’я Gookee раніше був пов’язаний із зловмисним програмним забезпеченням і хакерською діяльністю, намагаючись продати доступ до Sony Network Japan у 2020 році, пов’язаний з операцією Ransomware as a-Service під назвою «Gookee Ransomware», а також намагався продати вихідний код шкідливого програмного забезпечення. на форумі хакерів.

3xp0rt вважає, що kapuchin0/Gookee є розробником програми-вимагача HelloKitty, і тепер він каже: «Ми готуємо новий продукт, набагато цікавіший за Lockbit».

Випущений архів hellokitty.zip містить рішення Microsoft Visual Studio, яке створює шифрувальник і дешифратор HelloKitty і бібліотеку NTRUEncrypt, яку ця версія програми-вимагача використовує для шифрування файлів.

Експерт з програм-вимагачів Майкл Гіллеспі підтвердив BleepingComputer, що це законний вихідний код HelloKitty, який використовувався під час першого запуску операції з програмами-вимагачами у 2020 році.

Хоча випуск вихідного коду програми-вимагача може бути корисним для дослідження безпеки, публічна доступність цього коду має свої недоліки.

Як ми бачили, коли HiddenTear було випущено (з «освітніх міркувань») і вихідний код програми-вимагача Babuk опубліковано, зловмисники швидко використали цей код для запуску власних операцій здирництва.

До цього дня понад дев'ять програм-вимагачів продовжують використовувати вихідний код Babuk як основу для своїх власних шифрувальників.

Хто така HelloKitty?

HelloKity — це програма-вимагач, керована людьми, яка діє з листопада 2020 року, коли жертва написала повідомлення на форумі BleepingComputer, а ФБР пізніше оприлюднило PIN-код (приватне сповіщення галузі) для групи в січні 2021 року.

Банда відома зломом корпоративних мереж, крадіжкою даних і системами шифрування. Потім зашифровані файли та викрадені дані використовуються як важіль у машинах подвійного вимагання, де зловмисники погрожують витоком даних, якщо викуп не буде сплачено.

HelloKitty відома численними атаками та використовується в інших операціях з програмами-вимагачами, але найбільш розголошеною атакою стала атака на CD Projekt Red у лютому 2021 року.

Під час цієї атаки зловмисники стверджували, що вкрали вихідний код Cyberpunk 2077, Witcher 3, Gwent та інших ігор, які, як вони стверджували, були продані.

Влітку 2021 року група програм-вимагачів почала використовувати варіант Linux, націлений на платформу віртуальної машини VMware ESXi.

Програма-вимагач HelloKitty або її варіанти також використовувалися під іншими назвами, зокрема DeathRansom, Fivehands і, можливо, Abyss Locker.

ФБР поділилося великою колекцією індикаторів компрометації (IOC) у своїй пораді за 2021 рік, щоб допомогти фахівцям з кібербезпеки та системним адміністраторам захиститися від спроб атак, координованих групою програм-вимагачів HelloKitty.

Однак, оскільки шифрувальник змінювався з часом, ці IOC, ймовірно, застаріли». ***(Lawrence Abrams. HelloKitty ransomware source code leaked on hacking forum // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 09.10.2023).***

***

«…Програмне забезпечення-вимагач як послуга (RaaS), бізнес-модель на основі передплати існує вже багато років, але стала більш складною екосистемою з додаванням нових підмножин, таких як переговорники, аналітики аналізу загроз і спеціалісти зі зв'язків з громадськістю.

Атаки програм-вимагачів мають руйнівні наслідки для їхніх жертв, якими є невеликі компанії, великі корпорації та цілі країни. Критичні сектори, такі як енергетика, охорона здоров'я та транспорт, є сильними цілями, оскільки ці сектори перебувають під тиском, щоб відновити роботу своїх систем, і атаки на них можуть мати каскадні наслідки. Незважаючи на те, що більшість нападів здійснюються кримінальними елементами, національні держави-ізгої також здійснюють такі напади, щоб спричинити збурення в країнах, які вони вважають ворожими, або щоб приховати свою шпигунську діяльність. Дізнатися попередників зловмисників одразу після атаки нелегко, враховуючи можливості для спотворення інформації в кіберпросторі.

Атака програми-вимагача AIIMS у листопаді 2022 року є яскравим прикладом. П’ять серверів AIIMS, що містять 1,3 терабайта даних, були зашифровані, що призвело до повного збою онлайн-сервісів, включаючи реєстрацію пацієнтів, амбулаторні реєстрації та лабораторні послуги. За повідомленнями ЗМІ, також було зламано понад 4 мільйони записів пацієнтів. На повне відновлення служб знадобилося більше двох тижнів, оскільки понад 4000 комп’ютерів потрібно було очистити від шкідливого програмного забезпечення.

Індійська група реагування на комп’ютерні надзвичайні ситуації (CERT-IN), Об’єднання розвідувальних даних і стратегічні операції (IFSO) поліції Делі, Індійський координаційний центр боротьби з кіберзлочинністю (ICCC), Розвідувальне бюро (IB), Центральне бюро розслідувань (CBI), Національний університет судових наук, Національний центр захисту критичної інформаційної інфраструктури (NCIIPC) і Національне агентство розслідувань (NIA) були залучені для розслідування атаки.

IFSO звернулася до CBI з проханням написати до Інтерполу, щоб отримати подробиці про IP-адреси «ідентифікаторів електронної пошти з Хенані в Китаї та Гонконзі, які були використані для запуску кібератаки».3 Поліція Делі також порушила справу за розділом 66(F) Закону про внесення змін до IT 2008 року, який стосується кібертероризму.

Незважаючи на те, що присяжні ще не знають, хто відповідальний за атаку, цей епізод підкреслює необхідність посилення потенціалу в міру ускладнення нападів, необхідність обміну інформацією як усередині країни, так і за кордоном, а також правові рамки, які враховують з цих атак, які належать до категорії, відмінної від звичайних атак. За словами генерал-лейтенанта Раджеша Панта (у відставці), національного координатора з кібербезпеки на момент атаки, вона виявила кілька прогалин в існуючій національній системі кібербезпеки та механізмі реагування на інциденти. Він також закликав до створення вузлового міністерства для координації відповідей.

З точки зору міжнародного співробітництва, протягом короткого періоду здавалося, що загрозі програм-вимагачів було завдано нищівного удару, коли

Сполучені Штати разом з компаніями з кібербезпеки виступили з низкою ініціатив, щоб знищити інфраструктуру основних груп програм-вимагачів. Це сталося безпосередньо перед російсько-українською війною, і це також призвело до певної співпраці з боку російського уряду шляхом арештів. Однак згодом ці угруповання знову виникли та відновили свою інфраструктуру.

У 2021 році Сполучені Штати також очолили зусилля зі створення Міжнародної ініціативи з боротьби з програмами-вимагачами (ICRI), провівши віртуальну зустріч із 37 країнами. Переважна більшість учасників були з Європи та невелика частина з решти світу. Учасники пообіцяли «підвищити стійкість усіх партнерів CRI, перешкоджати кіберзлочинцям, протидіяти незаконному фінансуванню, створювати партнерства з приватним сектором і співпрацювати у всьому світі для вирішення цієї проблеми». Також було створено п'ять робочих груп у різних областях; стійкість (на чолі з Литвою та Індією), зрив (на чолі з Австралією), боротьба з незаконним фінансуванням (на чолі з Великою Британією та Сінгапуром), державно-приватне партнерство (на чолі з Іспанією) і дипломатія (на чолі з Німеччиною).

У 2022 році Білий дім скликав другий саміт із додаванням Бельгії. Серед ініціатив, оголошених після цієї зустрічі, було створення Міжнародної цільової групи з боротьби з програмами-вимагачами (ICRTF) на чолі з Австралією з мандатом «координувати стійкість, збої та протидію незаконній фінансовій діяльності», створення осередку злиття в Regional Cyber Центр захисту (RCDC) у Каунасі, Литва, для обміну технічною інформацією та створення інструментарію слідчого для допомоги правоохоронним органам. Країни-учасниці також зобов’язалися проводити навчання з боротьби з програмами-вимагачами кожні два роки.

Очікується, що третя ітерація саміту відбудеться наприкінці жовтня 2023 року зі значно розширеною когортою країн, що налічує близько сорока семи. Згідно з повідомленнями, очікується, що США закликатимуть країни публічно взяти на себе зобов’язання не платити викуп.6 Це набуває важливого значення, оскільки атаки на урядові мережі та системи зростають експоненціально. Лише минулого місяця Шрі-Ланка та Колумбія зіткнулися з перебоями через те, що їхні мережі були вражені

програмою-вимагачем. До цього уряд Коста-Ріки зупинився після атаки програм-вимагачів, націленої на майже 30 міністерств і державних установ. Незважаючи на те, що компанія не сплатила викупу, триваючі перебої в її послугах призвели до оціночних економічних збитків у 30 мільйонів доларів США на день і оголошення надзвичайного стану президентом.

Хоча великі та малі країни однаково вразливі до програм-вимагачів та інших кібератак, останні мають набагато менше ресурсів і можливостей, щоб протистояти виснажливим наслідкам цих атак, як це видно на прикладі Коста-Ріки, якій довелося попросити допомоги у США, Іспанія та Microsoft, щоб допомогти захиститися від цих атак. Згодом США надали 25 мільйонів доларів США для посилення кібербезпеки Коста-Ріки.

На національному рівні необхідно сформулювати стратегію програм-вимагачів, оскільки ця загроза кіберзлочинності впливає на уряди, підприємства та окремих осіб. Керуючись прислів'ям «якщо ви не можете виміряти, ви не можете цим керувати», поточна схема звітування про інциденти має надавати пріоритет повному звіту про атаки програм-вимагачів, включаючи дані про зловмисників, вжиті дії та рішення. Як показала реакція на атаку програм-вимагачів AIIMS, до розслідування мимоволі буде залучено кілька агенцій, і на основі даних, отриманих у результаті цього інциденту, може бути створена міжвідомча цільова група з досвідом роботи з програмами-вимагачами. Єдиний пункт для скарг також забезпечить швидшу реакцію та швидше пом'якшення та розгляд, особливо для малих і середніх підприємств, коли справа доходить до роботи з програмами-вимагачами.

Незважаючи на те, що зусилля ICRI заслуговують на похвалу, три роки тому, здається, він навряд чи вплинув на цунамі атак програм-вимагачів, які відбуваються по всьому світу, і майбутня зустріч має надати можливість для самоаналізу, чому саме так. Благочестиві обіцянки не платити викуп з боку країн не досягнуть багато чого, якщо вони не супроводжуватимуться більш енергійними зусиллями по боротьбі з лихом програм-вимагачів. Якщо ця модель співпраці спрацює, вона може стати шаблоном для цілеспрямованої відповіді на інші загрози в кіберсфері».

(Cherian Samuel. Synergizing International Cooperation And National Strategies To Combat Ransomware – Analysis // Eurasia Review (https://www.eurasiareview.com/21102023-synergizing-international-cooperation-and-national-strategies-to-combat-ransomware-analysis/?utm_source=flipboard&utm_content=EurasiaReview%2Fmagazine%2FEurasia+Review). 21.10.2023).

***

«Наприкінці вересня два підкомітети Палати представників Конгресу США провели спільні слухання щодо реагування на атаки програм-вимагачів. Слухання, проведені Підкомітетом з питань кібербезпеки, інформаційних технологій та державних інновацій і Підкомітетом з питань економічного зростання, енергетичної політики та питань регулювання, свідчать про велику зацікавленість політиків у запобіганні величезним збоям, які загрозливі суб'єкти можуть завдати як суспільству, так і приватні сектори. Ми повідомляємо про три теми, які повторюються протягом слухання.

Перша тема стосувалася ролі операційних бюджетів у підготовці до атак. Один експерт з кібербезпеки засвідчив, що організаціям може бути важко дозволити собі оптимальні інструменти для запобігання атакам і реагування на них, включаючи технічні засоби для шифрування даних і оновлення програмного забезпечення, стратегії управління ризиками та навчання співробітників. Члени комітету та свідки також обговорювали компроміс, коли «іноді інвестування в ресурс або інструмент кібербезпеки означає, що щось інше залишається нефінансованим». Наприклад, лікарні можуть витрачати менше на догляд за пацієнтами, щоб оплатити резервне копіювання системи та навчання лікарів заходам кібербезпеки. Органи місцевого самоврядування та уряди штатів також особливо вразливі до атак через обмежені бюджети, застарілі платформи та загальнонаціональну нестачу фахівців з кібербезпеки.

По-друге, незважаючи на бюджетні наслідки готовності до кібербезпеки, атаки програм-вимагачів продовжують спричиняти величезні витрати. Президент

медичної системи державного університету засвідчив, що витратив 65 мільйонів доларів у відповідь на атаку, навіть незважаючи на те, що викуп не було сплачено, а резервні копії були успішно використані. Свідки розповіли про витрати, які вони понесли на судово-медичну реакцію, відновлення систем і безперервність роботи, що дозволило співробітникам продовжувати роботу, поки системи залишалися в автономному режимі, що могло тривати тижнями або місяцями. Вони також посилалися на постійну репутаційну шкоду. Це свідчення підкреслює, що не існує недорогої панацеї від атак програм-вимагачів, навіть якщо їх успішно відбити.

Остання тема стосувалася типового профілю нападу. Члени комітету стикалися з тим, чи напади мають тенденцію бути невибірковими чи цілеспрямованими. Один експерт з кібербезпеки засвідчив, що атака програм-вимагачів зазвичай є «злочином з користі», але інший свідок зауважив, що навчальні заклади є найпоширенішими цілями певного шкідливого програмного забезпечення. Члени комітету обговорювали мотиви загрозливих суб'єктів, обговорюючи, чи були ці суб'єкти в першу чергу фінансовими, чи національними державами, які прагнули завдати шкоди критичній інфраструктурі. Деякі учасники сумнівалися, чи може штучний інтелект погіршити атаки програм-вимагачів, чи він може бути корисним для захисту від них. Свідки також надали протилежні докази щодо підтримки, яку вони отримували від уряду під час реагування на напад: один свідок вважав консультації з правоохоронними органами корисними, але досвід іншого показав, що «кавалерія не приходить».

Різні пропоновані перспективи можуть відображати час атак, про які йдеться, і швидко розвиваються практики суб'єктів загрози. Свідки слухань повідомляли про атаки у 2020 та 2021 роках. Так само члени підкомітету найчастіше згадували атаку на Colonial Pipeline у травні 2021 року, яка призвела до зупинки трубопроводу, дефіциту палива та оголошення надзвичайної ситуації для сімнадцяти штатів. Але тенденції програм-вимагачів швидко розвиваються. Наприклад, в одному звіті від квітня 2023 року зазначається, що, оскільки підприємства інвестують значні кошти в кібербезпеку, суб'єкти загроз, які мають менші шанси на успіх, все частіше націлюються на дорогі компанії та пред'являють вищі вимоги. Ця тенденція може

бути неочевидною з даних, зібраних з 2021 року». ***(Michael F. Buchanan and Sean Lau. House Subcommittees Hold Hearing on Combating Ransomware Attacks // Patterson Belknap Webb & Tyler LLP (https://www.pbwt.com/data-security-law-blog/house-subcommittees-hold-hearing-on-combating-ransomware-attacks#page=1). 23.10.2023).***

***

«…У звіті про програмне забезпечення-вимагач Arctic Wolf щодо реагування на інциденти компанія ділиться поточними даними про випадки реагування на інциденти (IR) зі своєї платформи Security Operations Platform та останніми даними про моніторинг темної мережі від Arctic Wolf Labs.

Моніторинг темної мережі показує різке збільшення атак програм-вимагачів

У темній павутині зловмисники підтримують так звані сайти витоку або ганьби. На цих сайтах вони погрожують своїм жертвам опублікуванням їхніх даних і таким чином тиснуть на них, щоб вони вимагали викупу. Хоча ці сайти не є точною документацією всіх глобальних кібератак, вони все одно є хорошим індикатором активності в темній мережі та дозволяють контекстуалізувати поточний ландшафт загроз. Arctic Wolf активно відстежує відомі місця витоку, щоб краще зрозуміти динаміку ландшафту загроз.

Значне збільшення кількості атак програм-вимагачів і активності в дарк-мережі в першій половині 2023 року (1-е півріччя) призвело до отримання найбільшого набору даних, який Arctic Wolf коли-небудь збирав у своєму моніторингу в темній мережі та даних про ІЧ-випадки. Експерт з питань безпеки спостерігав збільшення кількості інцидентів з програмами-вимагачами на 1% у першому півріччі 2023 року порівняно з другою половиною 43 року.

Провідні актори загрози

У першому півріччі 1 року Lockbit була групою загроз, яка публікувала найбільше публікацій на сайтах ганьби в дарк-ветері, причому кількість публікацій зросла більш ніж на 2023% порівняно з тим самим періодом минулого року. Однак

після піку активності в перші чотири місяці року кількість публікацій у дарк-мережі впала в травні та червні, посунувши групу з першої позиції.

MalasLocker з'явився в травні. У своїх перших публікаціях у дарк-мережі група опублікувала дані про велику кількість жертв, які базуються в Росії. Чи це випадковість, чи навмисне, не можна сказати з упевненістю. Однак географічне розташування жертв досить незвичне. Крім того, і сайт ганьби, і нотатки про викуп MalasLocker містять повідомлення, які вказують на мотивацію «хактивіста».

CI0p, група програм-вимагачів, яка вперше з’явилася в лютому 2019 року, була ідентифікована в червні як зловмисник за масштабними експлойтами MOVEit Transfer (CVE-2023-34362, CVE-2023-35036, CVE-2023-35708 і CVE-2023). - 36934) підтверджено. Arctic Wolf відстежував їх активність у місцях витоку з 14 червня по 14 липня 2023 року та спостерігав 169 випадків, у тому числі 120 у США, дев’ять у Великобританії та вісім у Німеччині.

Крім MalasLocker, який виглядає політично вмотивованим, Cl0p, Lockbit і переважна більшість атакуючих груп керуються фінансами. Незалежно від галузі компанії-жертви, доходу чи кількості співробітників, багато суб’єктів загрози запускають свої атаки, використовуючи зовнішні вразливості, такі як CI0p, або масово надсилаючи складні фішингові електронні листи організаціям по всьому світу.

Обробна промисловість, на яку спрямовані групи програм-вимагачів

Протягом першого півріччя 1 року виробничі компанії були найбільш частими жертвами атак програм-вимагачів. Незважаючи на велику кількість публікацій на веб-сайтах ганьби в темній мережі порівняно з іншими галузями, медіана* заяв про програмне забезпечення-вимагач від постраждалих у промисловості була нижчою за середню кількість заяв про зареєстровані випадки IP. Це показує, що, хоча обробна промисловість не є найприбутковішою для суб’єктів загрози, її легше використовувати через масштаб і складність її операцій.

Вимоги щодо викупу зростають у різних галузях: інфляція?

Середній запит на викуп за всі інциденти з програмами-вимагачами, на які Arctic Wolf відповів у першій половині року, становив 600.000 43 доларів США, що на XNUMX% більше, ніж за аналогічний період минулого року.

Чи інфляційний тиск також охопив кіберзлочинний бізнес? Швидше ні. Більш вірогідною є комбінація кількох факторів: з одного боку, групи програм-вимагачів намагаються компенсувати падіння продажів після того, як їм довелося придушити свою діяльність у 2022 році через російсько-агресійну війну. З іншого боку, за останній рік криптовалюти зросли в ціні. Ціна біткойна зросла з приблизно 25.000 30 доларів США 2022 червня 40.000 року до понад 30 2023 доларів США XNUMX червня XNUMX року.

Розглядаючи окремі галузі, можна побачити певні відмінності у вимогах щодо викупу в певних галузях порівняно з попереднім роком, при цьому середнє значення* вимог знову найвище в технологічному секторі та найнижче в будівництві. Ці застійні позиції відображають досвідченість учасників загроз і показують, що вони добре розуміють, скільки можуть платити які галузі. Це базується як на загальнодоступних фінансових даних компаній, так і на інформації, яку вони збирають під час атак на тисячі компаній щороку.

Підприємства малого та середнього бізнесу найбільше постраждали від програм-вимагачів

Малі та середні підприємства (МСП) особливо страждають від зростання кількості програм-вимагачів. У 82% жертв у першому півріччі 1 року було менше 2023 співробітників.

Хоча великі компанії та корпорації не застраховані від того, щоб стати жертвами, вони частіше мають більші бюджети безпеки. Таким чином, підприємства малого та середнього бізнесу часто стикаються з більшими труднощами щодо впровадження ефективної програми забезпечення безпеки через брак фінансових ресурсів і досвіду внутрішньої безпеки. Порівняно з великими компаніями з мільярдними доходами, малий і середній бізнес також менш здатний поглинати фінансові наслідки перерв у роботі в результаті кіберінциденту. Тому власники більш готові швидко заплатити викуп за відновлення роботи. Це робить їх

привабливою ціллю…» ***(Програми-вимагачі: зростає кількість, зростає вимога викупу // MedPressIT GbR (https://b2b-cyber-security.de/uk/%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC-%D0%B2%D0%B8%D0%BC%D0%B0%D0%B3%D0%B0%D1%87%D1%96%D0%B2-%D0%B7%D1%80%D0%BE%D1%81%D1%82%D0%B0%D1%94-%D0%BA%D1%96%D0%BB%D1%8C%D0%BA%D1%96%D1%81%D1%82%D1%8C-%D0%B7%D1%80%D0%BE%D1%81%D1%82%D0%B0%D1%8E%D1%87%D0%B8%D1%85-%D0%B2%D0%B8%D0%BC%D0%BE%D0%B3-%D0%B2%D0%B8%D0%BA%D1%83%D0%BF%D1%83/?related_post_from=11628). 11.10.2023).***

***

«Найкращий захист від атаки програм-вимагачів — припустити, що це станеться раніше. З 80% імовірністю цілями повторної атаки основними є малі та середні підприємства у сильно постраждалих галузях, включаючи охорону здоров'я та виробництво. Атаки програм-вимагачів піднялися до нового рекорду минулого місяця, збільшившись на 153% порівняно з вереснем минулого року.

Добре фінансовані групи організованої злочинності та Advanced Persistent Threat (APT) активно залучають фахівців зі штучного інтелекту та машинного навчання (ML) у центрі злочинної діяльності Telegram і в темній мережі, щоб шукати нові способи застосування нових технологій до старих поширених уразливостей і ризиків (CVE) і вразливості.

Використовуючи ШІ та ML, організована злочинність і зловмисники з національних держав випереджають найефективніші підприємства. У період з вересня 2022 по 2023 рік кількість груп програм-вимагачів, які подвійно здирували, зросла на 76%. З серпня по вересень кількість атак програм-вимагачів у сфері охорони здоров'я зросла на 86% порівняно з попереднім місяцем.

«Захист від програм-вимагачів — це не те, що ви робите, коли вас атакують», — Мерріт Баєр, польовий CISO компанії Lacework сказав VentureBeat. Захист від

програм-вимагачів дуже схожий на правильне забезпечення безпеки у вашому середовищі щодня — від керування ідентифікацією та секретами до надання інфраструктури до керування захистом даних і резервним копіюванням».

Збройні CVE ускладнюють зупинку програм-вимагачів

Керівники та засновники виробників середнього рівня, які зазнали численних атак програм-вимагачів, повідомили VentureBeat на умовах анонімності, що навіть після наймання консалтингових фірм з кібербезпеки зловмисники продовжують атакувати. Думка про те, що програми-вимагачі неминучі, приносить нову актуальність і зосередженість на покращенні керування виправленнями, безпеки даних, резервного копіювання, керування ідентифікацією та секретами та забезпечення більш безпечної інфраструктури.

Звіт Ivanti за 2023 рік показує, що зловмисники-вимагачі регулярно потрапляють під радари популярних сканерів, у тому числі сканерів відомих груп Nessus, Nexpose та Qualys. У звіті встановлено, що майстерність зловмисників стає настільки точною, що використання CVE у вигляді зброї, а потім ідентифікація слабких цілей на основі їхніх профілів стає нестримним у малих і середніх підприємствах.

Відповідно до звіту Іванті, групи програм-вимагачів зосереджуються на тому, щоб уникнути виявлення, одночасно використовуючи прогалини в даних і давні прогалини в застарілих CVE.

Срінівас Муккамала, директор із продуктів Ivanti «Актори загроз все частіше націлюються на недоліки в кібергігієні, включаючи застарілі процеси управління вразливістю», — сказав VentureBeat. «Сьогодні багатьом командам із безпеки та IT-технологій важко визначити реальні ризики, які становлять уразливості, і тому неналежним чином визначають пріоритети вразливостей для усунення. Наприклад, багато лише виправляють нові вразливості або ті, які були розкриті в національній базі даних уразливостей (NVD). Інші використовують лише Загальну систему оцінки вразливостей (CVSS), щоб оцінити та визначити пріоритетність вразливостей. «

Будьте готові, припустивши, що ваша компанія є ціллю програм-вимагачів

З огляду на безперервність бізнесу та фінансове здоров'я, програмне забезпечення-вимагач — це не лише рішення щодо кібербезпеки. Це бізнес-рішення. VentureBeat дізнався про те, що виробники платять викуп, щоб відновити працездатність, а потім знову потрапити під удар.

Підприємства середнього розміру з прибутком менше 100 мільйонів доларів часто не мають бюджету чи персоналу для безпеки, і зловмисники це знають.

«Дев'яносто відсотків усіх атак програм-вимагачів вражають компанії з доходом менше мільярда доларів», — повідомив Фуртадо у відеоінтерв'ю Gartner.

Фуртадо каже, що програмне забезпечення-вимагач є високоефективною стратегією кібератак, оскільки воно ставить будь-який бізнес у величезний тиск часу, щоб усунути злом, повернути свої дані та продовжити роботу.

«Програми-вимагачі повинні розуміти те, що, на відміну від будь-якого іншого виду інциденту безпеки, вони ставлять ваш бізнес на таймер зворотного відліку», — радить Фурадо.

У той час як правоохоронні органи рекомендують не платити викупи, майже третина постраждалих організацій зрештою платять, лише щоб виявити, що до 35% їхніх даних пошкоджені та не підлягають відновленню.

Опитування CrowdStrike показало, що 96% жертв, які заплатили викуп, також заплатили додаткові комісії за вимагання в середньому в розмірі 792 493 доларів США, лише для того, щоб виявити, що зловмисники також поділилися або продали свою інформацію в темній мережі через канали Telegram. Офіс контролю за іноземними активами також оштрафував компанії, які платили певним зловмисникам-вимагачам.

Підготовка до атак програм-вимагачів має бути перш за все діловим рішенням

Команди вищого керівництва, які вважають атаки програм-вимагачів неминучими, швидше визначать пріоритетність дій, спрямованих на зниження ризику атаки, і стримають її, коли вона станеться. Таке мислення перенаправляє обговорення на рівні правління кібербезпеки як операційних витрат на довгострокові інвестиції в управління ризиками.

CISO повинні брати участь у цьому обговоренні та мати місце в правлінні. З огляду на неминучість атак програм-вимагачів і ризиків для основної частини будь-якого бізнесу, CISO повинні направляти ради та надавати їм інформацію, щоб мінімізувати ризики. Чудовий спосіб для CISO отримати місце в правлінні — показати, як їхні команди отримують прибуток, забезпечуючи безперервну роботу та знижуючи ризики.

«Коли ваша правління захоче поговорити про програмне забезпечення-вимагач, нагадайте їм, що воно може приймати форму щоденних покращень — у вашій каденції виправлення, як ви керуєте ідентифікацією, як ви захищаєте середовища та створюєте інфраструктуру як код, як ви створюєте незмінні резервні копії тощо», — сказав Баєр VentureBeat.

Вона продовжила: «Програми-вимагачі — це одна з «витрат», яку ваше підприємство має врахувати, якщо воно не використовує необхідні методи безпеки та інновації».

CISO повинні мати місце в правлінні

Це велика зміна в тому, як ради директорів бачать і фінансують кібербезпеку, і чому CISO повинні мати місця в радах, щоб пояснити численні бізнес-вигоди від посилення безпеки підприємства.

«Я бачу все більше і більше CISO, які приєднуються до рад директорів», — сказав Джордж Курц, співзасновник і генеральний директор CrowdStrike, під час свого основного виступу на щорічному заході своєї компанії. «Я думаю, що це чудова можливість для кожного тут [у Fal.Con] зрозуміти, який вплив вони можуть мати на компанію. З точки зору кар’єри, це чудово бути частиною цієї зали засідань і допомагати їм у подорожі. Щоб бізнес був стійким і безпечним».

Він продовжив: «Додавання безпеки має сприяти розвитку бізнесу. Це має бути щось, що додає стійкості вашого бізнесу, і це має бути щось, що допомагає захистити підвищення продуктивності цифрової трансформації».

Наявність посібника з програмами-вимагачами — це велике значення

Керівники CISO розповідають VentureBeat, що наявність посібника допомогла їм відновитися після атак програм-вимагачів, оскільки це допомогло заощадити час під час атаки та стримати її.

Посібники також пояснюють вищому керівництву та правлінню, наскільки руйнівною може бути атака. Комунікаційний план під час атаки програм-вимагачів на публічну компанію є протверезним дзвінком, який змушує підтримку рухатися, кажуть CISO VentureBeat. Тепер, коли Комісія з цінних паперів і бірж (SEC) вимагає розкриття інформації, ще більша увага приділяється правильному використанню підручників.

Один із CISO великого публічного виробника споживчих товарів повідомив VentureBeat анонімно, що він зайшов настільки далеко, що опублікував письмовий прес-реліз із поясненням атаки програм-вимагачів. Правління відповіло, схваливши фінансування для більш багаторівневого підходу до захисту даних і резервного копіювання, регулярної перевірки резервних копій, покращеного керування виправленнями та захисту даних і робочих процесів аналізу та чітких планів виправлення.

У підручниках часто є розділи про обмеження, аналіз, виправлення та відновлення. Важливо розглядати посібник як документ, який потрібно регулярно переглядати та оновлювати SecOps, IT, юристами, PR та вищим керівництвом.

Для CISO зазвичай проводять моделювання інцидентів і настільні вправи, щоб перевірити свої платіжні книжки та переконатися, що вони регулярно оновлюються та переглядаються. Мета полягає в тому, щоб завжди шукати прогалини у відповідь і закривати їх до того, як відбудеться атака програм-вимагачів». ***(Louis Columbus. Surviving a ransomware attack begins by acknowledging it's inevitable // VentureBeat (https://venturebeat.com/security/surviving-a-ransomware-attack-begins-by-acknowledging-its-inevitable/). 26.10.2023).***

***

«Згідно з новим звітом, програми-вимагачі розширюються, урізноманітнюються та значно ускладнюють захист для компаній.

Останній звіт Elastic про глобальні загрози (GTR) проаналізував понад мільярд точок даних за останні 12 місяців, щоб краще зрозуміти ландшафт загроз програм-вимагачів, і виявив, що майже кожна атака на хмарну інфраструктуру починається з крадіжки облікових даних.

Це збігається з останніми новинами про те, що у вересні 2023 року активність програм-вимагачів досягла безпрецедентного рівня з понад 514 атаками, а загрози кібербезпеці підскочили на 40% за чотири роки.

Захист став «більш нудним» завданням

GTR Elastic спостерігав за сигнатурами зловмисних програм, поведінкою кінцевих точок і кампаніями противника. Він також розглянув прогнози загроз на наступний рік, прокоментувавши, що програми-вимагачі тепер є «набагато складнішим і нудним завданням», від якого потрібно захиститися.

У звіті встановлено, що більшість зловмисних програм становлять суміш стандартних інструментів і «дуже поширених» сімейств програм-вимагачів. Подібним чином, більше половини спостережуваних заражень зловмисним програмним забезпеченням були спрямовані на системи Linux, а близько 91% подій сигнатур зловмисного програмного забезпечення було зафіксовано на кінцевих точках Linux. Це на відміну від Windows, яка показала близько 6%, ймовірно, через те, що загрози залишаються на платформах з низькою видимістю.

У хмарі можуть бути проблеми

Згідно з GTR, компанії, які переходять з локальної IT-інфраструктури та програмного забезпечення на хмарні, піддаються особливому ризику.

Швидкість і кількість компаній, які переходять у хмару, можуть призвести до слабкого контролю доступу, незахищених облікових даних і різноманітних неправильних конфігурацій, які можуть зробити колись безпечне рішення тепер чутливим до атак. Зловмисники розпізнали ці недоліки та використовують їх для розгортання зловмисного програмного забезпечення.

Керівник відділу розвідки безпеки Elastic і директор з інженерних розробок Джейк Кінг пояснив: «Сьогоднішній ландшафт загроз дійсно безмежний, оскільки супротивники перетворюються на злочинні підприємства, зосереджені на

монетизації своїх стратегій атак. Відкритий вихідний код, зловмисне програмне забезпечення та використання штучного інтелекту знизили бар'єри для зловмисників, але ми також спостерігаємо зростання автоматизованих систем виявлення та реагування, які дозволяють усім інженерам краще захищати свою інфраструктуру. Це гра в кішки-мишки, і нашою найсильнішою зброєю є пильність і постійні інвестиції в нові оборонні технології та стратегії».

Наступний крок в еволюції програм-вимагачів

Лише рік тому операторам програм-вимагачів було потрібно в середньому чотири з половиною дні між початковим доступом і розгортанням шифрувальника. Тепер цей час скоротився до одного дня, а понад 50% заходів виконуються протягом 24 годин. У 10% випадків цей час розгортання може становити лише п'ять годин.

Причина такого збільшення швидкості, можливо, іронічна. Оскільки команди з кібербезпеки нарощують реакцію на загрози, хакери також еволюціонували, щоб працювати швидше. Тож у цьому немає жодних сумнівів, ми входимо до «наступного кроку в еволюції програм-вимагачів», але які відчутні кроки ви можете зробити, щоб краще захистити себе та бізнес?

Від встановлення програмного забезпечення для шифрування та використання VPN до обмеження доступу до критично важливих даних, є низка простих, але надзвичайно ефективних заходів кібербезпеки, які ви можете застосувати, щоб захиститися від атак програм-вимагачів і допомогти запобігти зростанню даних GTR». ***(Ellis Di Cataldo. Ransomware Is Getting Smarter and Harder to Defend Against // Marketing VF Ltd. (https://tech.co/news/ransomware-harder-defend-against?utm_source=flipboard&utm_content=other). 25.10.2023).***

***

Програми-трояни

«Хакери виявили, що оновлена версія трояна віддаленого доступу (RAT) RomCom під назвою PEAPOD націлена на військових і політичних лідерів Європейського Союзу (ЄС), які працюють над питаннями гендерної рівності.

За словами дослідників кібербезпеки з Trend Micro, хакерська група під назвою Void Rabisu (інша назва UNC2596) створила друкарську версію веб-сайту wplsummit — сайту, який рекламує саміт жінок-політичних лідерів (WPL), який відбувся в червні цього року. Цей шкідливий веб-сайт показав папку Microsoft OneDrive, яка містить виконуваний файл під назвою «Неопубліковані зображення 1-20230802T122531-002-sfx.exe».

Файл представлений як фотогалерея, і хоча він містить деякі фотографії з події (зібрані з соціальних мереж), він також містить PEAPOD.

Державна чи ні?

Сам PEAPOD — це зменшена версія RomCom RAT, яка містить 10 команд (у RomCom — 42). Ці команди включають виконання довільного коду, захоплення системної інформації та самознищення у разі компрометації. Дослідники вважають, що зловмисники скоротили непотрібний обсяг, щоб зробити RAT більш непомітним і його важче видалити.

Хоча методика, жертви та особи нападників відомі, мотиви досі залишаються загадкою. Hacker News повідомляє, що Void Rabisu є «незвичайною» групою, оскільки їх спостерігали як у фінансово мотивованих атаках, так і в шпигунських кампаніях.

«Void Rabisu є одним із найяскравіших прикладів, коли ми бачимо поєднання типових тактик, прийомів і процедур (TTP), що використовуються кіберзлочинними суб'єктами загрози, і TTP, які використовуються спонсорованими національними державами загрозливими суб'єктами, мотивованими головним чином шпигунськими цілями», – Trend. Мікро сказав.

«Хоч у нас немає доказів того, що Void Rabisu спонсорується національною державою, цілком можливо, що це один із фінансово вмотивованих загрозливих суб'єктів кримінального підпілля, які були втягнуті в кібершпигунство через надзвичайні геополітичні обставини, спричинені війною в Україні», - повідомили в Trend Micro.

За даними видання, атаки Void Rabisu часто мають бекдори, які виділяють Україну та країни, які підтримують її у війні проти Росії». ***(Sead Fadilpašić. Female***

political leaders and military bigwigs targeted by new cyberattack // Future US, Inc. (https://www.techradar.com/pro/security/female-political-leaders-and-military-bigwigs-targeted-by-new-cyberattack). 16.10.2023).

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«У рішучій співпраці проти кіберзлочинності правоохоронні органи трьох континентів демонтували інфраструктуру сумнозвісної операції з вимагачами Ragnar Locker.

Це видатне досягнення відбулося після самопроголошеної перемоги Українського кіберальянсу над програмою-вимагачем Trigona.

Фон

Ragnar Locker загрожував Інтернету з кінця грудня 2019 року, коли ФБР і CISA у березні 2022 року зробили суворе попередження про діяльність угруповання у спільному сповіщенні.

У попередженні пояснювалося: «Станом на січень 2022 року ФБР ідентифікувало щонайменше 52 організації в 10 критичних секторах інфраструктури, які постраждали від програми-вимагача RagnarLocker, включаючи організації в критично важливому виробництві, енергетиці, фінансових послугах, уряді та секторах інформаційних технологій». Крім того, було виявлено, що «учасники програм-вимагачів RagnarLocker працюють як частина сімейства програм-вимагачів, часто змінюючи методи обфускації, щоб уникнути виявлення та запобігання».

Зняття

Правоохоронні органи Чехії, Європи, Франції, Німеччини, Італії, Японії, Латвії, Нідерландів, Іспанії та США об’єднали зусилля, щоб знищити оперативну спроможність банди Рагнара Локера.

Ця спільна акція призвела до конфіскації угруповання Tor для переговорів і сайтів витоку даних у четвер. На постраждалих веб-сайтах тепер відображається повідомлення про їх вилучення в рамках цієї міжнародної правоохоронної дії проти групи Ragnar Locker.

На відміну від багатьох своїх мерзенних аналогів, Ragnar Locker діяв напівприватно, утримуючись від моделі Ransomware-as-a-Service, яка активно залучає сторонніх філій. Натомість вони співпрацювали із зовнішніми пентестерами, щоб проникати в мережі, зосереджуючись головним чином на корпоративних мережах, переміщаючись через них і викрадаючи дані перед шифруванням пристроїв.

Викрадені файли потім використовувалися в кампаніях подвійного вимагання, підступної тактики для максимізації фінансової вигоди шляхом стягнення плати з жертв двічі - один раз за розшифровку та відновлення, а потім для запобігання витоку публічних даних.

Захист від програм-вимагачів

Хоча великі підприємства часто стають основними цілями атак програм-вимагачів, ці загрози не оминають і окремих людей. Ось кілька порад щодо посилення вашої кібербезпеки:

Регулярні оновлення: оновлюйте свою операційну систему, програмне забезпечення та антивірусні програми, щоб виправляти вразливості системи безпеки.

Навчайтеся: будьте обізнані щодо шахрайства з фішингом і уникайте відкривання небажаних електронних листів або натискання підозрілих посилань.

Резервне копіювання даних: регулярно створюйте резервні копії своїх даних на зовнішній жорсткий диск або безпечну хмарну службу.

Використовуйте надійні паролі: використовуйте складні паролі та регулярно їх змінюйте. Розгляньте можливість використання менеджера паролів, щоб відстежувати їх.

Увімкніть багатофакторну автентифікацію: якщо можливо, використовуйте багатофакторну автентифікацію, щоб додати додатковий рівень безпеки.

Використовуйте спеціалізоване програмне забезпечення безпеки: такі рішення безпеки, як Bitdefender Ultimate Security, можуть допомогти запобігти атакам програм-вимагачів і захистити ваші дані від усіх цифрових загроз.

Припинення операції Ragnar Locker знаменує значну перемогу в боротьбі з кіберзлочинністю. Однак у міру розвитку цифрового ландшафту зростає і складність кіберзагроз. Бути поінформованим і застосовувати надійні методи кібербезпеки є вкрай важливими для захисту цифрової сфери». ***(Vlad CONSTANTINESCU. International Joint Operation Cripples Ragnar Locker Ransomware Ring // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/international-joint-operation-cripples-ragnar-locker-ransomware-ring/?utm_source=flipboard&utm_content=other%2F). 20.10.2023).***

***

«Фахівці кіберполіції спільно з іноземними колегами в межах багаторівневої міжнародної операції знешкодили хакерське угруповання, яке атакувало 168 компаній у країнах Європи, Азії та Америки.

«Оперативники Департаменту кіберполіції під процесуальним керівництвом Київської міської прокуратури, спільно із колегами з Європолу, Євроюсту, із залученням правоохоронців Франції, Чехії, Німеччини, Італії, Латвії, Нідерландів, Іспанії, Швеції, Японії та Канади провели масштабну міжнародну операцію зі знешкодження небезпечного хакерського угруповання», – йдеться у повідомленні.

Починаючи з 2020 року, зловмисники атакували вірусом-вимагачем 168 міжнародних компаній у країнах Європи та Америки. Зокрема вони заражали сервери шкідливим програмним забезпеченням та викрадали з них інформацію. У подальшому дані на комп’ютерах жертв зашифровувалися і робилися непридатними для використання.

За відновлення доступу члени угруповання вимагали від 5 до 70 мільйонів доларів у криптовалюті. У випадку несплати викупу або звернення до правоохоронців погрожували розповсюдити викрадені дані у даркнеті.

При цьому зауважується, що організатори чітко розподіляли обов'язки між учасниками групи. Окремі члени відповідали за збір інформації та пошук вразливих місць в архітектурі кібербезпеки жертв.

Зібрану інформацію вони передавали спільникам з навичками комп'ютерного програмування. Останні відповідали за створення та модифікування шкідливого програмного забезпечення з метою подальшого ураження конкретної компанії.

У межах міжнародного розслідування разом із правоохоронними органами ЄС та країн Азії українські правоохоронці провели масові обшуки в Києві у приміщеннях одного з учасників угруповання. Вилучено ноутбуки, мобільні телефони та електронні носії інформації.

У Франції затримали одного з розробників шкідливого програмного забезпечення. Днями проведено також обшуки у його спільників на території Іспанії, Латвії та Чехії.

Нині французькі компетентні органи розслідують кримінальне провадження за фактами несанкціонованого доступу та перебування в автоматизованих системах обробки даних, несанкціонованого вводу та підміни даних в автоматизовану систему обробки даних, перешкоди роботі системи автоматичної обробки даних, вимагання (здирство) в складі організованого кримінального угрупування, відмивання коштів (легалізація) в складі організованого кримінального угрупування, які передбачені рядом статей Кримінального кодексу Франції». ***(Кіберполіція сприяла викриттю міжнародної хакерської групи, яка атакувала 168 компаній // ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "МЕДІАКОМУНІКАЦІЇ" (https://bukvy.org/kiberpolicziya-spryyala-vykryttyu-mizhnarodnoyi-hakerskoyi-grupy-yaka-atakuvala-168-kompanij/). 24.10.2023).***

***

Технічні аспекти кібербезпеки

«Коли справа доходить до кібербезпеки, OSS часто може бути і причиною, і ліками від проблем нашого цифрового світу.

Код програмного забезпечення з відкритим вихідним кодом (OSS) певною мірою включений у більшість сучасних програмних програм. Частка коду OSS на відміну від пропрієтарного коду значно змінюється залежно від відповідного програмного забезпечення, і включення коду OSS може як підвищити безпеку програм, так і підірвати її, залежно від того, як воно розгортається.

Зловмисники шукають вразливості, щоб використати проломи в броні програмного забезпечення, яке організації використовують для розміщення та управління своїм цифровим існуванням. Оскільки ліцензування відкритого програмного забезпечення заохочує до співпраці та вдосконалення вже існуючого коду, це природно призводить до швидкого виявлення та виправлення помилок, зменшуючи вразливості, якими можуть скористатися зловмисники. Однак, оскільки OSS є вільно доступним для всіх, будь-хто, незалежно від своїх намірів, може отримати доступ, завантажити, модифікувати і повторно поширювати вихідний код OSS, і, залежно від процесу затвердження, може навіть мати можливість об'єднати свої модифікації з основною «офіційною» гілкою OSS. Рухи, що стоять за OSS, відрізняються своїми методами та впровадженням заходів безпеки та методів контролю якості, тому одні вміють виявляти потенційні ризики, тоді як інші можуть залишати їх поза увагою.

Поширення OSS є благословенням і прокляттям, оскільки навіть кваліфікованим і досвідченим розробникам програмного забезпечення важко визначити, які варіанти OSS є більш ризикованими з точки зору методу їх розробки та ймовірного впливу вразливостей. Справа ускладнюється тим, що компанії, особливо ті, які розробляють програми для власного використання, а не для перепродажу, часто не мають повного переліку OSS, розгорнутого в їх програмному забезпеченні, а це означає, що вони можуть не знати, яким уразливостям вони піддаються, і не стануть знати, коли виявлено відомі помилки та створено виправлення для їх усунення. Подібно до того, як конфіденційність за проектом і за замовчуванням є принципом, який звучить очевидно в теорії, але виявляється складним для реалізації на практиці, так само є включення заходів кібербезпеки на етапі розробки OSS і додатків, які включають їх.

Використання методів зниження ризиків у практиці кодування, а також розгортання безпечних (зашифрованих) каналів зв'язку для обміну та спільного вирішення занепокоєнь щодо можливих вразливостей може допомогти розробникам побудувати надійнішу OSS. Те, що код широко використовується, не означає, що він безпечний – розробники як OSS у його найчистішому розумінні, так і ті, хто адаптує та включає його у власні програми, повинні запроваджувати безпечний режим тестування. Це не лише належне управління, але й усе більш важливе пом'якшення юридичних ризиків, оскільки використання стороннього тестування навряд чи зменшить юридичну відповідальність у випадках, коли помилка, яку можна визначити та виправити, призводить до вразливості, яка сприяє порушенню безпеки.

Зусилля ЄС – ризик небажаних наслідків є великим

На рівні ЄС нещодавно були зроблені спроби врегулювати вплив OSS на кібербезпеку, але хоча ці законодавчі зусилля вітаються багатьма, також існує широке занепокоєння тим, що позиція однозначно неоднозначна, оскільки майбутнє законодавство не відображає реального розуміння того, як OSS працює та відіграє важливу роль у програмному забезпеченні багатьох типів, включаючи інструменти цифрової кібербезпеки. Критики побоюються, що це нерозуміння зрештою призведе до створення ненавмисного стримувального впливу на розвиток OSS.

NIS2

Директива NIS2 — це загальноєвропейське законодавство щодо кібербезпеки. Він набув чинності в 2023 році, оновивши попередній режим 2016 року, і передбачає правові заходи, спрямовані на підвищення загального рівня кібербезпеки в ЄС. Країни-члени мають перенести вимоги NIS2 до національного законодавства до жовтня 2024 року з наступними кінцевими термінами для держав-членів та організацій, яких це стосується.

NIS2 створює дві категорії для сутностей у сфері: важливі та важливі. Усі суб'єкти, які підпадають під дію, повинні відповідати ідентичним вимогам, але нагляд і правозастосування будуть більш надійними у випадку істотних суб'єктів. Збільшення відповідальності для організацій, що входять до сфери дослідження, супроводжуватиметься суворими зобов'язаннями звітності. Набагато більше

організацій підпадає під дію NIS2, ніж ті, які були охоплені старим режимом, і штрафи за недотримання можуть становити до 10 мільйонів євро або 2% світового доходу за серйозні збої. Ці штрафи можуть застосовуватися поряд із санкціями GDPR, якщо порушення також є порушенням даних і відповідальність виникає відповідно до режиму конфіденційності.

У зв'язку з великими труднощами, які мають вирішувати нещодавно включені суб'єкти, Декларація 52 NIS2 рекомендує інструменти OSS як силу для підвищення кібербезпеки назавжди:

«Інструменти та програми кібербезпеки з відкритим кодом можуть сприяти підвищенню відкритості та можуть мати позитивний вплив на ефективність промислових інновацій. Відкриті стандарти полегшують взаємодію між інструментами безпеки, сприяючи безпеці зацікавлених сторін промисловості. Інструменти кібербезпеки з відкритим кодом і Програми можуть використовувати ширшу спільноту розробників, уможливлюючи диверсифікацію постачальників. Відкритий вихідний код може призвести до більш прозорого процесу перевірки інструментів, пов'язаних з кібербезпекою, і керованого спільнотою процесу виявлення вразливостей. Тому держави-члени повинні мати можливість сприяти використанню відкритих вихідне програмне забезпечення та відкриті стандарти, дотримуючись політики щодо використання відкритих даних та відкритого вихідного коду як частини безпеки через прозорість Політика сприяння впровадження та сталого використання інструментів кібербезпеки з відкритим кодом є особливо важливою для малих та середніх підприємств зіткнутися зі значними витратами на впровадження, які можна було б мінімізувати, зменшивши потребу в певних програмах чи інструментах».

Закон про захист від кібернетичного середовища

Незважаючи на те, що NIS2 активно підтримує інструменти OSS, у проекті Регламенту ЄС про вимоги до кібербезпеки для продуктів із цифровими елементами, відомого як Закон про кібернетостійкість (CRA), можна визначити потенційно суперечливу думку. CRA прагне підвищити кіберстійкість цифрових продуктів, розміщених на єдиному ринку, встановлюючи суворі вимоги до постачальників, які

накладаються штрафами, навіть вищими, ніж ті, що передбачені NIS2, у розмірі до 15 мільйонів євро або 2,5% світового доходу – залежно від того, що більше.

Пам’ятаючи про необхідність захисту спільного підходу розробників OSS, CRA містить формулювання, призначені для захисту розробників OSS і співавторів від відповідальності за невиявлені або невиправлені помилки, відповідальність за які має бути в іншому місці. Однак критики поточного проекту CRA, запропонованого Комісією ЄС, вказали на низку сфер, де нерозуміння нюансів того, як на практиці працює розробка OSS, може перешкодити учасникам, які не схильні до ризику, пропонувати важливий внесок у розвиток через страх відповідальності за КРА.

Розробка OSS може передбачати внески окремих осіб, які діють особисто або спільно з фондом чи академічною групою. Якщо такі особи також працюють у компаніях, поточний текст CRA (Декларативна частина 10) включатиме внески таких осіб і, отже, проект у цілому в сферу дії CRA, оскільки проект не вважатиметься прийнятим «повністю децентралізована модель розвитку». У гіршому випадку проекти можуть забороняти робити внески особам, які працюють у компаніях, а компанії забороняють своїм працівникам робити внески в проекти OSS.

Ініціатива з відкритим кодом (OSI) підкреслила використання «некомерційного» як кваліфікатора серед інших груп як таке, що не має сенсу в контексті розробки програмного забезпечення, створюючи ризик того, що багато інших груп і учасників розробки OSS можуть бути піддані вимогам CRA згідно з цим визначенням, ніж передбачається. OSI рекомендує продовжити роботу над винятком із відкритим кодом для вимог CRA, щоб «виключити всі види діяльності до комерційного розгортання програмного забезпечення та чітко переконатися, що відповідальність за знаки CE не лежить на жодній стороні, яка не є прямим комерційним бенефіціаром розгортання». OSI стверджує, що залишення тексту в тому вигляді, в якому він є, може запобігти або навіть запобігти доступності OSS, яка підтримується глобально в ЄС.

Переглянута Директива про відповідальність за якість продукції

Окрім згаданого вище законодавства про кібербезпеку, питання відповідальності розробників програмного забезпечення за збитки, спричинені використанням уразливостей у їхньому програмному забезпеченні (OSS чи іншим чином), також є предметом поточних дебатів у контексті майбутньої переглянутої Директиви про відповідальність за продукт. (РПЛД). Цілком можливо, що RPLD значно збільшить зобов'язання щодо відповідності та витрати більшості розробників програмного забезпечення (особливо в OSS), а також відкриє для них нові вектори позовів.

Де це залишає OSS?

Хоча визнання важливості інструментів OSS у боротьбі з кіберзлочинністю в NIS2 може бути обнадійливим для тих, хто активно бере участь у розробці таких інструментів, поточний проект CRA може зробити розробку проектів OSS більш складною – і, звичайно, більш жорсткою регулюється всім потенційним використанням OSS у цифрових продуктах. Незалежно від того, чи буде внесено зміни до CRA для кращого відображення реалій розвитку OSS, очевидно, що організації (більшість із них), які впроваджують OSS у цифрові продукти, більше не можуть дозволити собі самовдоволення у своєму використанні OSS. Як мінімум, суб'єктам, які розміщують цифрові продукти на єдиному ринку, знадобиться принаймні ретельна документація про походження та тестування всього використовуваного коду, а для всіх проектів OSS можуть знадобитися набагато жорсткіші процеси розробки, щоб корпоративні учасники не випадково залучали децентралізовані проекти. сфера дії CRA». ***(Jo Joyce and Martijn Loth. Open Source Security vs Open Source Liability // Taylor Wessing (https://www.taylorwessing.com/en/interface/2023/open-source-software/open-source-security-vs-open-source-liability). 03.10.2023).***

***

«Незважаючи на повсюдне поширення в комп'ютерних мережах, протокол датаграм користувача вразливий до вразливостей системи безпеки та атак.

UDP є простим протоколом, оскільки він не потребує встановлення з'єднання чи обміну підтвердженнями для надсилання пакетів даних до місця призначення. Він просто передає пакет і не знає, чи досягають дані пункту призначення чи падають десь на шляху.

Програми, які потребують швидкого запиту та відповіді, як-от DNS, протокол динамічної конфігурації хоста (DHCP), аудіо та відео, зазвичай використовують UDP. Ці програми не можуть виявити, чи UDP отримує запит, але на них серйозно не впливають втрачені пакети – можливо, якийсь статичний звук або мерехтіння відео.

Але ця обмежена перевірка пакетів піддає UDP уразливості, які не впливають на інші мережеві протоколи, такі як TCP. Наприклад, TCP має пройти процес встановлення з'єднання, перш ніж відповідати на вхідні пакети даних з іншого кінця з'єднання. Він ігнорує вхідні пакети даних, які не надходять із з'єднання. Навпаки, програми UDP відповідають на будь-який отриманий запит, оскільки UDP не використовує встановлене з'єднання.

Поширені UDP-атаки

Зловмисники можуть використовувати атаки сканування портів, щоб оцінити служби UDP як потенційну ціль. Атака сканування портів надсилає пакети на хост і використовує його відповіді, щоб дізнатися про систему та знайти вразливі місця. Сервіси UDP також можуть бути вразливі до злому, якщо вони мають експлойт або помилку, яка дозволяє віддалений доступ і переповнення.

DoS- і DDoS- атаки можуть порушити роботу UDP та інших протоколів, як-от TCP. Зловмисники створюють DDoS-атаки, вставляючи в систему зловмисне програмне забезпечення — іноді тисячі. Зловмисники використовують вставлене програмне забезпечення на всіх заражених системах, щоб бомбардувати атакувану. Відповіді надходять до зараженої системи та відкидаються, але вхідний пакет став причиною DoS-атаки.

Зловмисники також можуть використовувати підробку IP- адреси, щоб вставити вигадану адресу джерела в пакети, які використовуються в атаці. Атакована система відповідає незалежно від того, чи належить адреса існуючій системі. Важко

захистити від IP-спуфінгу, оскільки зловмисник може використовувати багато підроблених адрес. Фільтр, який залежить від виявлення великого обсягу з певної адреси джерела, може не відфільтрувати підроблені адреси.

Як захиститися від UDP-атак

Однієї атаки може бути достатньо, щоб сповільнити корисну обробку. Обсяг законного трафіку та очікуваний обсяг атак можуть визначити тип захисту. Наприклад, деякі веб-сайти можуть залучати більшу кількість атак, а також атаки більш інтенсивні. Захист від розподіленої атаки вимагає певного типу зовнішньої фільтрації.

Для захисту від уразливостей UDP доступна низка варіантів, зокрема:

Підприємства можуть захистити цінну інформацію, налаштувавши VPN для законних джерел запитів.

Реалізуйте перевірку та фільтрацію вхідних пакетів у віртуальній машині, яка працює на тому самому сервері, що й віртуальна машина, що виконує програму. Сервер, що містить обидві віртуальні машини, має обмежену кількість можливостей обробки, і запуск аналізу пакетів і фільтрування у віртуальній машині все ще сповільнює роботу програми.

Постачальники брандмауерів включають фільтрацію пакетів для деяких типів атак, але часто включають інші типи фільтрації. У той час як брандмауер може зупинити атаки низького рівня, більш інтенсивні атаки, включно з розподіленими, можуть подолати брандмауер.

Використовуйте продукти виявлення та видалення вторгнень, щоб усунути певні вхідні атаки.

Програми можуть працювати в хмарних середовищах, які мають налаштовані служби захисту. Програми, які використовують SaaS, отримують певний тип захисту від хмарного постачальника.

Мережі доставки вмісту (CDN) також забезпечують захист територіально розподілених систем, які обслуговуються веб-сайтом. CDN використовуються веб-серверами, до яких часто звертаються, для прискорення роботи сайтів великого обсягу. Кожна система CDN має копію веб-сайту. Запит на один із цих сайтів

перенаправляє на найближчий CDN. DDoS-атаки також спрямовані на найближчий сервер CDN, тому кожен сервер CDN отримує частку атаки, що полегшує ефективніший захист.

Безсумнівно, атаки на UDP-сервіси триватимуть. У міру появи нових методів атак нові засоби захисту можуть допомогти захиститися від них. Навіть за наявних засобів захисту атаки вимагають від персоналу мережі пошуку вразливостей і впровадження відповідних засобів захисту». ***(David B. Jacobs. What to know about UDP vulnerabilities and security // TechTarget (https://www.techtarget.com/searchnetworking/answer/Are-there-any-inherent-security-problems-with-UDP?utm_source=flipboard&utm_content=other). 10.2023).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Злом платформи передачі файлів MOVEit, розробленої Progress Software і використовується компаніями будь-якого розміру, служить нагадуванням про можливі вразливості, з якими стикаються сторонні постачальники.

Під час злому в червні 2023 року зловмисники використали вразливість у програмному забезпеченні MOVEit. Завдяки ін’єкції структурованого запиту (SQL) шкідливого коду вони отримали несанкціонований доступ до платформи та викрали дані з кількох організацій.

І це не єдина резонансна атака, звинувачена в уразливостях стороннього програмного забезпечення. У грудні 2020 року злом SolarWinds, викликаний уразливістю програмного забезпечення SolarWinds Orion, дозволив зловмисникам проникнути в мережі кількох організацій.

Наслідки для бізнесу не можна недооцінювати. Такі вразливості створюють ризики не лише через порушення даних, але й через перерву в бізнесі, що може бути особливо небезпечним для виробничих компаній. Процес відновлення може тривати тижнями, що призведе до зупинки виробництва та втрати бізнесу. В інших галузях,

якщо система програмного забезпечення, надана постачальником, контролює критичну інфраструктуру, уразливість у цьому програмному забезпеченні може суттєво вплинути на його доступність.

Замість того, щоб зосереджуватися виключно на окремих вразливостях, для компаній вкрай важливо застосувати комплексний підхід до кіберпроцесів і керувати вразливими місцями на основі їх серйозності. Співпраця між індустрією кіберстрахування та клієнтами необхідна для посилення уваги до політики управління ризиками постачальників.

Така співпраця передбачає більш точне виявлення та оцінку ризиків, створених постачальниками, шляхом виходу за межі спрощених анкет постачальників до активного тестування та навчання обізнаності. Щоб забезпечити мінімальний стандарт, від постачальників можуть вимагати запровадити додаткові засоби контролю, щоб завоювати довіру клієнта та зрештою підписати угоду, щоб стати схваленим постачальником послуг. Обслуговування полісу кіберстрахування також може бути частиною вимог.

Реалізуючи ці кроки, компанії можуть зменшити свій вплив на вразливості, пов’язані з постачальниками. Крім того, обмін звітами, створеними постачальниками кібербезпеки на етапі оцінки, зі страховим ринком може допомогти отримати краще розуміння якості ризику та заощадити час клієнтів завдяки виключенню довгих анкет.

Важливо відзначити, що ландшафт ризиків постійно змінюється, і вразливості, пов’язані з постачальниками, також продовжуватимуть розвиватися. Прикладом деяких із цих тенденцій є: збільшення залежності від хмарного програмного забезпечення; зростання Інтернету речей (IoT), що підключає підприємства до більшої кількості пристроїв і систем поза їхнім прямим контролем; а також зростання штучного інтелекту (ШІ) і збільшення залежності від програмного забезпечення на основі ШІ для прийняття критичних рішень.

Щоб випереджати ці ризики, компанії повинні активно керувати ризиками третіх сторін. Ось дев’ять важливих кроків, які компанії повинні зробити, щоб захистити свій бізнес від ризиків, пов’язаних із постачальниками:

Вибір і контроль продавця. Замість того, щоб лише перевіряти постачальників під час процесу адаптації, слід запроваджувати постійний перегляд і аудит їхніх стандартів.

Інвентаризація обладнання та програмного забезпечення. Компанії повинні мати точне розуміння своєї мережевої інфраструктури. Необхідно створити мережеві схеми для оцінки мережевої сегрегації, ідентифікації серверів і програм і документування послуг, які вони надають.

Конфігурація та моніторинг хмарних сервісів. Хмарні служби за своєю суттю не є безпечними та потребують належної конфігурації та керування. Дуже важливо розуміти, як постачальники обробляють хмарні служби та безпеку з точки зору найкращих практик IT-безпеки.

Моніторинг діяльності третіх осіб. Важливо встановити та контролювати безпечний канал зв'язку між вашою компанією та постачальником. Надання їм окремого середовища з кількома рівнями безпеки, наприклад через інфраструктуру віртуального робочого столу (VDI) або інші безпечні системи, може допомогти зменшити ризики.

Керування виправленнями. Оперативне та ефективне керування виправленнями має важливе значення не лише для операційних систем, але й для програмного забезпечення сторонніх виробників. Патчі слід виконувати без затримки, щоб оперативно усунути будь-які відомі вразливості.

Шифрування даних. Шифрування має бути реалізовано як у стані спокою, так і під час передачі. Шифруючи дані, підприємства значно ускладнюють доступ кіберзлочинцям до цінної інформації та її неправомірне використання.

Кіберстрахування продавця. Розгляньте постачальників, які мають власні поліси кіберстрахування, включаючи страхування відповідальності та першої сторони. Це забезпечує додатковий рівень захисту та впевненості у випадку кіберінциденту за участю постачальника.

Аналіз впливу на бізнес і готовність. Впровадження та регулярне тестування безперервності бізнесу, аварійного відновлення та планів реагування на інциденти є

важливими. Визначте цілі часу відновлення та цілі точки відновлення, щоб забезпечити швидке та ефективне реагування.

Розвивайте знання безпеки. Розкажіть співробітникам і керівництву про типові вектори атак і важливість обережної поведінки. Підкресліть той факт, що атаки можуть початися з простого клацання в електронному листі. Пильність і увага до потенційних загроз можуть запобігти багатьом інцидентам кібербезпеки.

Оскільки кіберзагрози стають дедалі складнішими, а рівень складності кібератак зростає та становить значний ризик, компанії повинні діяти зараз. Ціна зламу може бути нищівною, що підкреслює необхідність для організацій, незалежно від їх розміру, приділяти пріоритет кібербезпеці. Інвестиції в передові технології виявлення та запобігання загрозам, використання регулярних програм навчання співробітників, впровадження надійних засобів контролю доступу та проведення регулярних перевірок безпеки є життєво важливими кроками, які необхідно вжити для захисту від нових кіберзагроз. Звичайно, кіберстрахування є важливим для того, щоб допомогти підприємствам зменшити ризики, якщо трапиться найгірше». ***(Mauro Marongiu. Key to Proactive Cyber Security Is Management of Third-Party Vendor Risks // Wells Media Group, Inc. (https://www.insurancejournal.com/news/international/2023/10/12/743926.htm). 12.10.2023).***

***

«Дослідники попереджають, що хакери скористалися невиправленою вразливістю нульового дня в мережевому програмному забезпеченні Cisco, щоб зламати десятки тисяч пристроїв.

У понеділок Cisco випустила попереджувальне попередження про те, що хакери активно використовують уразливість у IOS XE, програмному забезпеченні, яке підтримує низку мережевих пристроїв компанії. Cisco повідомила, що помилку було виявлено в інтерфейсі веб-адміністрування IOS XE, який можна використати, коли уражений пристрій підключається до Інтернету.

Список пристроїв, на яких працює програмне забезпечення Cisco IOS XE, включає корпоративні комутатори, бездротові контролери, точки доступу та промислові маршрутизатори, які корпорації та менші організації використовують для керування мережевою безпекою.

В окремій публікації в блозі підрозділ Cisco з аналізу загроз Talos повідомив, що ще невідомі хакери використовували цю помилку — відому як «нульовий день» — тип уразливості, який виявили зловмисники до того, як постачальник встиг її виправити — з принаймні 18 вересня. Cisco Talos заявила, що успішне використання надає зловмиснику «повний контроль над скомпрометованим пристроєм», що дозволяє «можливу подальшу несанкціоновану діяльність» у корпоративній мережі жертви.

Cisco поки не коментує масштаби експлуатації.

Однак Censys, пошукова система пристроїв і активів, підключених до Інтернету, повідомляє, що спостерігала майже 42 000 скомпрометованих пристроїв Cisco, відзначаючи «різке зростання» заражень порівняно з попереднім днем. станом на 18 жовтня.

У своєму аналізі недоліку Censys каже, що більшість скомпрометованих пристроїв розташовано в Сполучених Штатах, за ними йдуть Філіппіни та Мексика. У Censys заявили, що хакери націлені на телекомунікаційні компанії, які пропонують інтернет-послуги як домогосподарствам, так і підприємствам.

«Як наслідок, головними цілями цієї вразливості є не великі корпорації, а менші організації та особи, які є більш сприйнятливими», — заявили дослідники Censys.

Нульовий патч для нульового дня

Cisco ще не випустила патч для уразливості нульового дня, яка отримала максимальний рейтинг серйозності 10,0. Представник Cisco Алісса Мартін, яка представляє компанію через стороннє агентство, повідомила TechCrunch, що компанія «безупинно працює над виправленням програмного забезпечення», але відмовилася сказати, коли патч буде доступний.

Поки що невідомо, скільки пристроїв є потенційно вразливими, але Cisco зазначила у своєму повідомленні, що нульовий день вплинув як на фізичні, так і на віртуальні пристрої з програмним забезпеченням IOS XE, які мають функцію сервера HTTP або HTTPS. Замість виправлення Cisco «наполегливо» рекомендує клієнтам вимкнути функцію HTTP-сервера на всіх системах, що підключаються до Інтернету.

Також незрозуміло, хто використовує вразливість. Cisco Talos заявила, що після виявлення початкової експлуатації нульового дня у вересні вона спостерігала за діяльністю 12 жовтня, яку, за її оцінками, здійснював той самий актор. «Перший кластер, ймовірно, був початковою спробою актора та тестуванням коду, тоді як діяльність у жовтні, схоже, показує, що актор розширив свої операції, включивши встановлення постійного доступу за допомогою розгортання імплантату», — заявили в Cisco.

Cisco попередила, що поки що невідомі зловмисники також використали попередню вразливість CVE-2021-1435, яку Cisco виправила в 2021 році, щоб встановити імплантат після отримання доступу до пристрою.

«Ми також бачили пристрої, повністю підкріплені проти CVE-2021-1435, які успішно встановлювали імплантат за допомогою ще невідомого механізму», — сказали дослідники.

Окрім відключення функції HTTP-сервера, Cisco закликала адміністраторів потенційно зламаних пристроїв негайно шукати в їхніх мережах ознаки компрометації. CISA, урядове агентство з кібербезпеки США, також закликає федеральні агентства ввести заходи пом’якшення до 20 жовтня». ***(Carly Page. Hackers exploit zero-day to compromise tens of thousands of Cisco devices // Yahoo (https://techcrunch.com/2023/10/19/hackers-exploit-zero-day-to-compromise-tens-of-thousands-of-cisco-devices/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 19.10.2023).***

***

«Критична вразливість, яку хакери використовували з серпня, яка дозволяє їм обійти багатофакторну автентифікацію в мережевому обладнанні Citrix, отримала виправлення від виробника. На жаль, його застосування недостатньо для захисту уражених систем.

Уразливість, яка відстежується як CVE-2023-4966 і має рейтинг серйозності 9,8 з можливих 10, міститься в NetScaler Application Delivery Controller і NetScaler Gateway, які забезпечують балансування навантаження та єдиний вхід у корпоративних мережах відповідно. Уразливість розкриття інформації, яка випливає з недоліку в наразі невідомій функції, може бути використана, щоб хакери могли перехопити зашифрований зв'язок, що передається між пристроями. Цією вразливістю можна скористатися віддалено й без жодних дій людини, навіть якщо зловмисники не мають системних прав на вразливу систему.

компанія Citrix випустила патч для уразливості Минулого тижня разом із порадою, у якій міститься небагато деталей. У середу дослідники з охоронної фірми Mandiant заявили, що вразливість активно використовується з серпня, ймовірно, для шпигунства проти професійних служб, технологій і державних організацій. Mandiant попередив, що виправлення вразливості недостатньо для блокування уражених мереж, оскільки будь-які сеанси, захоплені до оновлення системи безпеки, залишатимуться й після цього.

Компанія написала:

«Успішне використання може призвести до можливості викрадення існуючих автентифікованих сеансів, отже, в обхід багатофакторної автентифікації або інших жорстких вимог автентифікації. Ці сеанси можуть тривати після розгортання оновлення для пом'якшення CVE-2023-4966. Крім того, ми спостерігали викрадення сеансу, коли дані сеансу були викрадені до розгортання виправлення та згодом використані загрозою.

Викрадення автентифікованого сеансу може призвести до подальшого доступу за низхідним потоком на основі дозволів і обсягу доступу, який було дозволено ідентифікатору або сеансу. Зловмисник може використовувати цей метод для збору

додаткових облікових даних, бокового повороту та отримання доступу до додаткових ресурсів у середовищі».

Mandiant надала вказівки щодо безпеки, які виходять за рамки порад, наданих Citrix. зокрема:

• Ізолювати пристрої NetScaler ADC і Gateway для тестування та підготовки до розгортання виправлень.

Примітка: якщо вразливі пристрої не можуть бути пріоритетними для виправлення, Mandiant рекомендує встановити для пристроїв обмеження вхідної IP-адреси, щоб обмежити вплив і поверхню атаки, доки не буде застосовано необхідні виправлення.

• Оновіть уразливі пристрої NetScaler ADC і Gateway до останніх версій мікропрограми, що пом’якшує вразливість.

• Після оновлення завершіть усі активні та постійні сеанси (для кожного пристрою).

– Підключіться до пристрою NetScaler за допомогою CLI.

• Щоб завершити всі активні сеанси, виконайте таку команду: kill aaa session -all

• Щоб очистити постійні сеанси балансувальників навантаження NetScaler, виконайте таку команду (де ім’я віртуального сервера/пристрою): clear lb persistentSessions

• Щоб очистити наявні сеанси ICA, виконайте таку команду: kill icaconnection -all

• Ротація облікових даних

– Через відсутність доступних записів журналу чи інших артефактів експлуатації, як запобіжний захід організаціям слід розглянути можливість заміни облікових даних для ідентифікаторів, які були надані для доступу до ресурсів через уразливий NetScaler ADC або пристрій Gateway.

– Якщо є докази підозрілої активності або бічного переміщення в середовищі, організаціям слід надати пріоритет ротації облікових даних для більшого обсягу

ідентифікацій, якщо віддалений доступ із однофакторною автентифікацією (SFA) дозволено для будь-яких ресурсів з Інтернету.

• Якщо на пристроях NetScaler виявлено веб-оболонки або бекдори, Mandiant рекомендує перебудувати пристрої за допомогою чистого вихідного образу, включаючи останню версію мікропрограми.

Примітка. Якщо потрібне відновлення пристрою за допомогою резервного образу, необхідно переглянути конфігурацію резервної копії, щоб переконатися, що немає доказів бекдорів.

• Якщо можливо, зменшіть зовнішній вплив і поверхню атаки пристроїв NetScaler, обмеживши вхідний доступ лише надійними або попередньо визначеними діапазонами IP-адрес джерела».

Ця порада виправдана, враховуючи послужний список попереднього використання критичних уразливостей Citrix. Наприклад, 18 липня Citrix розкрила та випустила патч для окремої вразливості 9.8. Через три дні, згідно з скануванням Інтернету організацією безпеки Shadowserver, понад 18 000 екземплярів ще не застосували критичне оновлення.

На той час, за даними Управління кібербезпеки та безпеки інфраструктури США, уразливість уже активно використовувалася. У наступні тижні Shadowserver і фірми безпеки F-Secure і IBM Security Intelligence відстежили тисячі випадків використання для крадіжки облікових даних.

Рекомендації Mandiant зводяться до наступного: якщо ваша організація використовує локальний NetScaler ADC або NetScaler Gateway, ви повинні припустити, що його зламано, і слідувати наданим інструкціям. І так, спершу це включає виправлення». ***(Dan Goodin. The latest high-severity Citrix vulnerability under attack isn't easy to fix // Condé Nast (https://arstechnica.com/security/2023/10/the-latest-high-severity-citrix-vulnerability-under-attack-isnt-easy-to-fix/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 20.10.2023).***

***

«Якщо ви використовуєте WinRAR, настав час оновити до останньої версії після виявлення серйозної вразливості безпеки, якою вже користуються зловмисники. Група аналізу загроз Google (TAG) виявила, що кілька підтримуваних державою хакерських груп використовували вразливість WinRAR з початку 2023 року.

«Зараз доступний патч, але здається, що багато користувачів все ще вразливі», — йдеться в дописі TAG у блозі, де детально описується експлойт WinRAR. «Компанія TAG спостерігала, як підтримувані урядом актори з низки країн використовують уразливість WinRAR у рамках своїх операцій».

WinRAR версії 6.24 і 6.23 включають виправлення діри в безпеці, але програма не оновлюється автоматично, тому вам доведеться вручну завантажити та встановити виправлення. Правильно, зараз 2023 рік, а одна з найпопулярніших програм для Windows досі не має функції автоматичного оновлення.

Уразливість WinRAR дозволяє зловмисникам виконувати довільний код, коли користувач Windows відкриває щось на зразок файлу PNG у архіві ZIP. TAG описує експлойт безпеки як «логічну вразливість у WinRAR, що спричиняє стороннє тимчасове розширення файлу під час обробки створених архівів, у поєднанні з примхою у реалізації Windows ShellExecute під час спроби відкрити файл із розширенням, що містить пробіли».

Експлойт також використовувався для націлювання на рахунки для торгівлі криптовалютою з квітня 2023 року. «Широке використання помилки WinRAR підкреслює, що експлойти для відомих уразливостей можуть бути дуже ефективними, незважаючи на наявність виправлення», — каже TAG. «Ці нещодавні кампанії, що використовують помилку WinRAR, підкреслюють важливість виправлення та те, що ще потрібно зробити, щоб полегшити користувачам підтримку безпеки та оновлення програмного забезпечення».

Це не перший випадок виявлення великої вразливості WinRAR. У 2019 році компанія з кібербезпеки Check Point Research виявила 19-річний експлойт виконання коду, який міг дати зловмисникам повний контроль над комп’ютером жертви…» ***(Tom Warren. PSA: it’s time to update WinRAR due to a big security vulnerability // Vox***

Media, LLC. (https://www.theverge.com/2023/10/18/23922075/winrar-security-vulnerability-exploit-patch-update). 18.10.2023).

***

«Хакери угруповання Sandworm, яке пов'язують із головним розвідувальним управлінням (ГРУ) Росії, а також китайські кіберзлочинці використовують уразливість популярного архіватора WinRAR для злому комп'ютерів, зокрема в Україні. Про цю загрозу кіберфахівці компанії Google попередили у своєму блозі.

Як показало дослідження, зловмисники використовують уразливість під назвою CVE-2023-3883, щоб таємно заражати й атакувати комп'ютери своїх жертв. Вони розсилають різним користувачам із України електронні листи з документом-приманкою у форматі PDF нібито з програмою навчання операторів дронів і ZIP-файлом, що містить вірус. Фахівці виявили у файлі «Навчальна-програма-Оператори.pdf/Навчальна-програма-Оператори.pdf_.bat» програму Rhadamanthys — це викрадач інформації, який, зокрема, здатний збирати облікові дані браузера й інформацію про дії користувача. Такий "інфокрад" поширюється хакерами за передплатою за 250$ на 30 днів.

У Google пишуть, що вразливість є в старих версій WinRAR, але в найсвіжішій версії 6.24 розробники її терміново виправили. Щоб уникнути ризику, користувачам слід оновити свій архіватор, завантаживши інсталятор на офіційному сайті розробника, а не з будь-яких інших джерел. У списку можна вибрати потрібну мову програми.

Нагадаємо, програма є умовно-безплатною. Нею можна користуватися вільно, але щоразу вам демонструватиметься віконце з пропозицією оплатити продукт, після закриття якого ви можете й далі користуватися WinRAR. Якщо вам подобається програма, то, звісно, варто підтримати розробника та купити довічну ліцензію.

Як зазначають кіберфахівці Google, хоча розробники вже усунули вразливість в архіваторі, проблема полягає в тому, що далеко не всі з 500 мільйонів користувачів програми її оновлюють після того, як її встановили колись на свій ПК. WinRAR не

вміє оновлюватися самостійно, а оскільки він справно виконує свою роботу роками, то люди просто забувають про те, що програми потрібно періодично оновлювати не тільки заради нових функцій, а й для усунення виявлених вразливостей.

Цю саму вразливість використовують і російські хакери з Fancy Bear, створивши фішингову (підроблену) сторінку, щоб обманом змусити українських користувачів завантажити ZIP-файл, який також може використовувати вразливість WinRAR. Документом-пасткою було запрошення на захід від аналітичного Центру Разумкова.

До речі, виявленою вразливістю користуються колеги російських хакерів із Китаю — угруповання APT40 запустило фішингову кампанію, націлену на користувачів у Папуа-Новій Гвінеї. "Фішингові електронні листи містили посилання Dropbox на ZIP-архів, що містить експлойт CVE-2023-38831, PDF-файл-приманку, захищений паролем, і файл LNK", — повідомляє Google. У результаті можна таємно завантажити бекдор (шкідлива програма для віддаленого доступу до комп'ютера) на ПК користувачів…» ***(Пилип Бойко. Терміново оновіть WinRAR: хакери ГРУ РФ зламують українців через популярний архіватор // Фокус (https://focus.ua/uk/digital/600182-terminovo-onovit-winrar-hakeri-gru-rf-zlamuyut-ukrayinciv-cherez-populyarnij-arhivator). 19.10.2023).***

***

«У новому звіті Cloudflare стверджується, що з моменту виявлення вразливості HTTP/2 Rapid Reset було проведено «тисячі» гіпероб'ємних атак розподіленої відмови в обслуговуванні (DDoS) HTTP, у яких 89 із них перевищили 100 мільйонів запитів в секунду (rps).

Завдяки цим атакам загальна кількість HTTP DDoS-атак за третій квартал року порівняно з другим кварталом зросла на 65%, додали в компанії. «Подібним чином DDoS-атаки L3/4 також зросли на 14%», — додається в документі.

У первинних цифрах у кварталі було 8,9 трильйона запитів HTTP DDoS-атаки, порівняно з 5,4 трильйона у другому кварталі та 4,7 трильйона в першому кварталі.

HTTP/2 Rapid Reset — це вразливість, яку було виявлено на початку цього місяця, коли дослідники безпеки з Google (та інші) помітили DDoS-атаки з небаченими раніше можливостями. У перший тиждень жовтня Google заявив, що заблокував атаку, яка в 7,5 разів перевищувала найбільший зареєстрований інцидент DDoS - 398 мільйонів обертів за секунду.

«Остання хвиля атак почалася наприкінці серпня і триває досі, спрямована на основних постачальників інфраструктури, включаючи сервіси Google, інфраструктуру Google Cloud і наших клієнтів», — зазначили тоді в Google.

Постачальник послуг хмарних обчислень Fastly також заявив, що заблокував атаку з частотою 250 мільйонів обертів за секунду.

«Бот-мережі, які використовують платформи хмарних обчислень і використовують HTTP/2, здатні генерувати до 5000 разів більше сили на вузол ботнету», — заявили в Cloudflare. «Це дозволило їм запускати гіпероб'ємні DDoS-атаки за допомогою невеликого ботнету з 5-20 тисяч вузлів».

Зловмисники, які стоять за цими кампаніями, зазвичай націлені на фірми в ігровій індустрії, IT, криптовалютах, комп'ютерному програмному забезпеченні та телекомунікаційних галузях. Зловмисники зазвичай знаходяться в США, Китаї, Бразилії, Німеччині та Індонезії, тоді як жертви проживають переважно в США, Сінгапурі, Китаї, В'єтнамі та Канаді.

«Другий квартал поспіль DDoS-атаки на основі DNS були найпоширенішими», — заявили в компанії. «Майже 47% усіх атак були засновані на DNS. Це на 44% більше, ніж у попередньому кварталі. SYN-затоки залишаються на другому місці, за ними йдуть RST-затоки, UDP-затоки та атаки Mirai». ***(Sead Fadilpašić. DDoS attacks are getting bigger and more powerful, and that's a really bad thing // Future US, Inc. (https://www.techradar.com/pro/security/ddos-attacks-are-getting-bigger-and-more-powerful-and-thats-a-really-bad-thing?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 29.10.2023).***

***

«Професори Університету Південної Австралії та Університету Чарльза Стерта розробили алгоритм для виявлення та перехоплення атак типу «людина посередині» (MitM) на безпілотних військових роботів.

Атаки MitM — це різновид кібератак, коли трафік даних між двома сторонами, у цьому випадку роботом і його законними контролерами, перехоплюється або для підслуховування, або для введення неправдивих даних у потік.

Такі зловмисні атаки мають на меті переривати роботу безпілотних транспортних засобів, змінювати передані інструкції, а в деяких випадках навіть перехоплювати контроль, інструктуючи роботів виконувати небезпечні дії.

«Операційна система робота (ROS) надзвичайно сприйнятлива до витоку даних і електронного викрадення, оскільки вона дуже мережева», — коментує професор Ентоні Фінн, який брав участь у дослідженні.

«Поява Industry 4, відзначена еволюцією в робототехніці, автоматизації та Інтернеті речей, вимагала, щоб роботи працювали спільно, коли датчики, виконавчі механізми та контролери повинні спілкуватися та обмінюватися інформацією один з одним через хмарні служби».

«Недоліком цього є те, що це робить їх дуже вразливими до кібератак».

Університетські дослідники розробили алгоритм, використовуючи методи машинного навчання, щоб виявити ці спроби та припинити їх за лічені секунди.

Алгоритм був протестований на копії GVR-BOT, який використовується армією США (TARDEC), і зафіксував успішне запобігання атакам у 99% випадків, при цьому помилкові спрацьовування відбувалися менш ніж у 2% перевірених випадків.

Розбірливі атаки MitM

Виявлення MitM, націленого на безпілотні транспортні засоби та роботів, є складним, оскільки ці системи працюють у відмовостійких режимах, тому відмінність між нормальними операціями та умовами несправності може бути туманною.

Крім того, робототехнічні системи можуть бути скомпрометовані на різних рівнях, від основної системи до її підсистем і підкомпонентів, що спричиняє проблеми з роботою, які можуть призвести до дисфункції робота.

Університетські дослідники розробили систему, яка аналізувала дані мережевого трафіку робота, щоб виявити спроби його скомпрометувати. Ця система використовує методи на основі вузлів, ретельно перевіряє дані пакетів і використовує систему на основі статистики потоку, яка зчитує метадані із заголовка пакета.

У докладному технічному документі, опублікованому дослідниками, розглядається специфіка моделі глибокого навчання CNN (згорточна нейронна мережа), яка була розроблена для цієї мети, що містить кілька рівнів і фільтрів, які підвищують надійність результату виявлення кібератак.

Реальні тести, проведені на копії бота з моделюванням кібератак на різні системи, дали чудові результати та високу точність ідентифікації навіть після 2-3 епох навчання моделі.

Оптимізовані версії цієї нової системи захисту можуть знайти застосування в аналогічних, але більш вимогливих роботах, таких як безпілотні літальні апарати.

«Ми також зацікавлені в дослідженні ефективності нашої системи виявлення вторгнень на різних роботизованих платформах, таких як безпілотні літальні апарати, чия динаміка є значно швидшою та складнішою порівняно з наземним роботом», — підсумовується в статті, опублікованій на порталі IEEE». ***(Bill Toulas. AI algorithm detects MitM attacks on unmanned military vehicles // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/ai-algorithm-detects-mitm-attacks-on-unmanned-military-vehicles/?utm_source=flipboard&utm_content=TomFalk2015%2Fmagazine%2FAi%2C+Deep+Learning+And+Neural+Networks). 14.10.2023).***

***

«Цифрова ера, час швидкого технологічного розвитку, змінила те, як ми взаємодіємо зі світом. Інтернет став невід'ємною частиною нашого життя – від

замовлення ранкової кави до робочих електронних листів. Однак цей віртуальний світ не позбавлений небезпек. У цю епоху зростання кіберзагроз Google активізувався, щоб забезпечити безпеку мільярдів своїх користувачів у всьому світі. Технологічний гігант нещодавно оголосив про серйозні оновлення свого широко використовуваного браузера Chrome, підвищуючи безпеку в Інтернеті за допомогою найсучасніших криптографічних алгоритмів.

Стрибок у шифруванні

В основі нових заходів безпеки Google лежить додавання криптографічного алгоритму під назвою X25519Kyber768. Цей алгоритм посилює протокол безпеки транспортного рівня (TLS), суть онлайн-шифрування. Ці оновлення, доступні в останній версії Chrome 116 і в базовій версії Chrome 115, служать для зміцнення системи шифрування, захищаючи дані користувачів від потенційних уразливостей.

Коли користувач вводить URL-адресу у веб-браузер, серія процесів відбувається протягом кількох секунд. Браузер надсилає HTTP-запит на сервер доменних імен (DNS), щоб отримати IP-адресу веб-сайту. Дані, що передаються із сервера, часто є відкритим текстом, що робить їх сприйнятливими до перехоплення. Однак за допомогою HTTPS, безпечного протоколу, ця інформація захищена від потенційних зловмисників, що гарантує конфіденційність і безпеку конфіденційних даних користувачів.

Посилення заходів безпеки

Нові оновлення Google також рекомендують користувачам отримати сертифікат SSL (Secure Sockets Layer), цифровий сертифікат, який забезпечує автентифікацію веб-сайту та забезпечує зашифроване з’єднання. Крім того, пропонується використовувати брандмауери для моніторингу та фільтрації вхідного та вихідного мережевого трафіку, запобігаючи несанкціонованому доступу до сервера.

Балансувальники навантаження відіграють вирішальну роль в управлінні вхідним мережевим трафіком. Вони розподіляють цей трафік між декількома серверами, щоб забезпечити швидшу роботу та запобігти перевантаженню серверів, забезпечуючи користувачам безперебійний та ефективний досвід перегляду.

Роль серверів

Веб-сервер, по суті, є серцем Інтернету. Він зберігає веб-сторінки та видає їх як HTTP-відповіді, коли отримує HTTP-запити від клієнтів. Сервер додатків, з іншого боку, виконує більш широкий спектр завдань. Він надає динамічний вміст, виконує специфічну для програми логіку, взаємодіє з базою даних для отримання запитуваних даних і надсилає їх назад клієнту для відображення.

Забезпечення майбутнього онлайн-перегляду

Оскільки кіберзагрози стають все більш складними, потреба в надійних заходах безпеки стає все більш критичною. Проактивний підхід Google до посилення безпеки свого браузера є свідченням постійних зусиль галузі для боротьби з цими новими загрозами. Нові оновлення спрямовані на вирішення критичних проблем безпеки та захист конфіденційності та даних користувачів, забезпечуючи більш безпечний і надійний досвід перегляду для користувачів у всьому світі». ***(Wojciech Zylm. Google's Strides in Cybersecurity: A Look at Chrome's Latest Updates // Microsoft (https://www.msn.com/en-xl/news/other/google-s-strides-in-cybersecurity-a-look-at-chrome-s-latest-updates/ar-AA1igdfW). 16.10.2023).***

***

«Хоча зараз усі знають про ізраїльський «Залізний купол» і його військову доблесть, ми мало що знали про його секретну зброю – «Кіберкупол».

У 1955 році Давид Бен-Гуріон, батько-засновник Ізраїлю, передбачив долю, що розгорнеться на просторах пустелі Негев, поблизу столиці Тель-Авіва. Він навіть не підозрював, що його пророцтво пізніше стане комплексом кібербезпеки площею 1800 акрів у Беер-Шеві, столиці Негева та центрі кібербезпеки Ізраїлю.

Ізраїль є повстанською силою в сучасній війні. Поки світ спостерігає, як традиційна битва перетворюється на цифровий театр, Ізраїль зібрав свої найкращі уми, щоб побудувати «Кібер-купол», призначений для ведення війни в кіберпросторі. Купол натхненний системою протиповітряної оборони «Залізний купол», який був розгорнуто в 2011 році.

Габі Портной, генеральний директор Ізраїльського національного кіберуправління (INCD), називає це «секретним соусом», зазначаючи, що X-фактор є генеративними платформами ШІ. Розробка цього технологічного купола розпалює криваву баню між Газою та Ізраїлем. Для Ізраїлю високі ставки, оскільки світ спостерігає за зміною концепції війни.

Кожні три роки нове покоління приєднується до кіберзахисту після завершення військової служби в Ізраїлі. Таким чином, простір між людиною та машиною розділено порівну в цих бойових кімнатах, зазначив Намрата Біджі Ахуджа з The Week, який нещодавно відвідав об’єкт посеред верблюжої землі.

Одна половина — молодь-ботанік, яка стежить за даними в реальному часі на кількох екранах. Інша половина повністю цифрова, працює на AI/ML — збирає, читає та інтерпретує дані. Розвідувальні служби використовують платформи, схожі на ChatGPT, щоб фільтрувати важливі загрози від необмеженого вмісту, що надходить у системи. Ці військові програми з підтримкою штучного інтелекту виконуються майже 14 000 технічного персоналу комплексу Беер-Шава, зазначила вона далі.

Міністерство оборони Ізраїлю було одним із перших у світі, хто використав ШІ для запобігання загрозам. У 2021 році країна Близького Сходу широко використовувала штучний інтелект під час операції для визначення цілей. Технологія використовувалася для визначення траєкторій ракет на основі радіолокаційної інформації, перехоплюючи ті, що прямували до густонаселених районів.

Маючи досвід на полі війни, держава тепер стикається з новим викликом – пануванням у ШІ. У поточній глобальній таблиці лідерів штучного інтелекту Ізраїль посідає четверте місце з прогнозованим розміром ринку в 1,54 мільярда доларів у 2023 році.

З квітня 2023 року кількість генеративних стартапів, пов’язаних зі штучним інтелектом, в Ізраїлі зросла більш ніж удвічі з 67 до 144. Загальна сума, зібрана цими стартапами, наразі досягла 2,3 мільярда доларів, що в 2,5 рази більше, ніж шість місяців тому. Наразі найбільший раунд у генеруючому просторі штучного інтелекту

в країні належить компанії природної мови AI21 Labs, яка залучила 155 мільйонів доларів Series C. Країна також є домом для Runway ML, яка була однією з перших компаній із інструментів редагування, яка інтегрувала машинне навчання в 2018 рік.

У розмові з майбутнім рятівником технологічної індустрії Ілоном Маском прем'єр-міністр Ізраїлю згадав про те, що найближчим часом країна буде висунута на третє місце у світі за рівнем штучного інтелекту. Інші урядовці також мали на меті використати технологічну майстерність Ізраїлю, щоб стати «наддержавою» ШІ.

Сили оборони також перемістили розвідувальні групи, включно з розвідувальним підрозділом 8200, до високотехнологічного кампусу Беер-Шева, який примикає до університету, який кілька років тому був безводним полем бруду та піску.

Незважаючи на інші розробки, цифрове відтворення Iron Dome виділяється. Чотири місяці тому Ронен Бар, голова ізраїльського агентства безпеки Shin Bet, говорив про те, що Тель-Авів разом із низкою країн розробляє систему «глобального кіберзалізного купола» на основі штучного інтелекту для виявлення та боротьби з загрозами.

Під час щорічної кіберконференції Бар заявив, що Ізраїль змирився з тим фактом, що «перемогти у цій війні палицями та камінням» просто неможливо». ***(Tasmia Ansari. Israel's GenAI-Backed End Game // Analytics India Magazine Pvt Ltd & AIM Media House LLC (https://analyticsindiamag.com/israels-genai-backed-end-game/?utm_source=flipboard&utm_content=aj7iohv%2Fmagazine%2FSUPERCARS+%26+JETS+%21+++++MIDDLE+EAST+WAR+%21+++++UKRAINE+WAR+%21++++WW%3F%3F%3F). 20.10.2023).***

***