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

№ 9 (вересень)

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.– №9 (вересень) . – 351 с.

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

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

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

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

ЗМІСТ

Стан кібербезпеки в Україні 4
Кібервійна проти України 4
Міжнародне співробітництво у галузі кібербезпеки 14
Світові тенденції в галузі кібербезпеки 15
Сполучені Штати Америки та Канада 85
Країни ЄС та Великобританія 113
Австралія та Нова Зеландія 131
Китай 134
Російська Федерація та країни ЄАЕС 137
Інші країни 138
Кібервійни та протидія зовнішній кібернетичній агресії 153
Кіберзахист критичної інфраструктури 177
Кіберзахист закладів охорони здоров'я 196
Захист персональних даних та соціальні мережі 199
Кібербезпека Інтернету речей. Штучний інтелект 221
Кіберзлочинність та кібертероризм 234
Діяльність хакерів та хакерські угруповування 267
Вірусне та інше шкідливе програмне забезпечення 279
Фішингові атаки 302
Операції правоохоронних органів та судові справи проти кіберзлочинців . 308
Технічні аспекти кібербезпеки 313
Виявлені вразливості технічних засобів та програмного забезпечення 317
Технічні та програмні рішення для протидії кібернетичним загрозам 333

Кібервійна проти України

«Російські кібероперації, можливо, не змогли завдати великого удару, якого боялися багато західних чиновників після вторгнення Москви в Україну в лютому 2022 року, але українські кіберчиновники попереджають, що Москва не припинила спроб.

Натомість головне контррозвідувальне відомство України попереджає, що Росія продовжує вдосконалювати свою тактику, намагаючись закріпити кібероперації як частину своєї доктрини ведення війни.

«Наша стійкість значно зросла», — заявив у четвер на кіберсаміті у Вашингтоні Ілля Вітюк, начальник відділу кібербезпеки Служби безпеки України (СБУ). «Але проблема в тому, що наш контрагент, Росія, наш ворог, також постійно розвивається і шукає нові шляхи [для нападу]».

Вітюк попередив, що Москва продовжує здійснювати від 10 до 15 серйозних кібератак на день, багато з яких демонструють ознаки того, що вони здійснюються в координації з ракетними ударами та іншими традиційними військовими маневрами.

«Це не якась геніальна молодь у пошуках легких грошей», — сказав Вітюк. «Це люди, які працюють день у день і мають наказ від свого військового командування знищити Україну».

Вітюк сказав, що цього року Росія здійснила 3000 кібератак проти України після того, як здійснила 4500 таких атак після свого вторгнення в 2022 році.

Крім того, він сказав, що російські чиновники націлюють на Україну близько 1000 кампаній дезінформації на місяць.

Минулого місяця, наприклад, СБУ викрила та заблокувала російську змову зловмисного програмного забезпечення, яке намагалося проникнути в критично важливі українські системи за допомогою мобільних пристроїв Android, захоплених у українських сил на полі бою.

Російські офіційні особи регулярно заперечують будь-яку причетність до кібератак, особливо тих, які спрямовані на цивільну інфраструктуру.

Але російські заперечення були сприйняті скептично на Заході, і в Сполучених Штатах, зокрема.

«Росіяни нарощують свої можливості та зусилля в кіберсфері», — сказав заступник директора ЦРУ Девід Коен, який виступав на тій же конференції у Вашингтоні.

«Це напружена битва щодня», — додав Коен, зазначивши, що боротьба в кіберпросторі далеко не одностороння.

«Росіяни стали жертвами чималої кількості кібератак, спрямованих на них з боку певного роду суб'єктів приватного сектору», – сказав він. «Були атаки на російський уряд, деякі хакерські атаки та атаки на витік інформації. Були атаки в інформаційному просторі на теле- та радіомовлення».

І Вашингтон, і Київ погоджуються, що кіберзахист України тримається, принаймні на даний момент.

Проте Вітюк висловив обережність.

«Ця війна — не спринт, це марафон», — сказав він. «Наш ворог розвивається, і [є] багато речей, які нам ще потрібно зробити, і багато речей, які нам ще потрібно прийняти, щоб ця перемога прийшла швидше».

Вітюк також попередив, що рішучість Росії не слід сприймати легковажно, вказавши на дані української розвідки, які показують, що Москва шукає способи розширити охоплення своїх кібероперацій проти Києва.

«Ми чітко бачимо, що є національна програма кібернаступу», – сказав Вітюк. «Тепер вони впроваджують у своїх вишах підконтрольні спецслужбам образливі [кібер] дисципліни».

«Вони починають вчити студентів, як атакувати державні системи, і це надзвичайно, надзвичайно небезпечно», – сказав він». ***(Jeff Seldin. Ukraine, US Intelligence Suggest Russia Cyber Efforts Evolving, Growing – Analysis // Eurasia Review (https://www.eurasiareview.com/09092023-ukraine-us-intelligence-suggest-russia-cyber-efforts-evolving-growing-***

analysis/?utm_source=flipboard&utm_content=EurasiaReview%2Fmagazine%2FEurasia+Review). 09.09.2023).

***

«Для підтримки свого вторгнення в Україну країна-агресорка продовжує використовувати кібернетичні можливості, зокрема і хакерські атаки та шкідливе програмне забезпечення, заявила розвідка Великої Британії.

Про це повідомляє Рубрика з посиланням на Міністерство оборони Великобританії у Twitter.

У відомстві нагадали, що 31 серпня Національний центр кібербезпеки Британії (NCSC) разом з міжнародними партнерами опублікував звіт про кампанію шкідливого програмного забезпечення, спрямовану на мобільні пристрої Android, які використовуються українськими військовими.

Шкідливе програмне забезпечення під назвою Infamous Chisel використовувалося російською групою кіберзагроз, відомою як Sandworm, яку пов'язують з Головним центром спецтехнологій Головного розвідувального управління Генштабу росії.

Infamous Chisel забезпечує постійний доступ до скомпрометованих Android-пристроїв, а також збір і вилучення даних з них. Програмне забезпечення націлене і на додатки, які використовують українські військові.

Британська розвідка зазначила:

«Дуже ймовірно, що Infamous Chisel використовувалося з метою крадіжки чутливої військової інформації. Ця діяльність демонструє, що Росія продовжує використовувати кібернетичні можливості для підтримки вторгнення в Україну».

Британська влада уже попереджала про ризики використання чатботів, керованих штучним інтелектом, стверджуючи, що їх можна обманом змусити виконувати шкідливі завдання.

У двох своїх публікаціях відомство зазначає, що експерти ще не розібралися з потенційними проблемами безпеки, пов'язаними з алгоритмами, які можуть

генерувати взаємодію, схожу на людську – так званими великими мовними моделями (LLM).

NCSC зазначає, що використання інструментів на основі штучного інтелекту, зокрема в роботі з обслуговування клієнтів та дзвінками з продажу, може нести ризики, особливо якщо такі моделі будуть підключені до інших елементів бізнес-процесів.

Науковці та дослідники неодноразово знаходили способи маніпулювати чатботами, даючи їм несанкціоновані команди або обманюючи їх, щоб вони обходили вбудовані в них захисні механізми.

Наприклад, чатбот на базі штучного інтелекту, який використовує банк, можна обманом змусити здійснити несанкціоновану транзакцію, якщо хакер правильно структурує свій запит.

Вплив штучного інтелекту на безпеку все ще перебуває в центрі уваги урядів країн по всьому світу. Зокрема, у США та Канаді вже фіксували використання технології LLM хакерами.

Нагадаємо, раніше Служба безпеки України повідомила, що українські кіберфахівці запобігли спробі російських спецслужб проникнути в електронну систему планування операцій ЗСУ.

У попередньому розвідувальному огляді Міноборони Британії йшлося, що росія з кінця червня звертається до громадян сусідніх країн та мігрантів з Центральної Азії, щоб завербувати їх для участі у бойових діях в Україні». ***(Британська розвідка: росія застосовує хакерські атаки проти військових ЗСУ // Рубрика (https://rubryka.com/2023/09/04/brytanska-rozvidka-rosiya-zastosovuye-hakerski-ataky-proty-vijskovyh-zsu/). 04.09.2023).***

***

Хакери, які працюють із зовнішніми, внутрішніми та військовими розвідками Росії, активізували кампанії цифрового вторгнення проти Генеральної прокуратури України та відділів, які документують військові злочини, повідомив голова Державної служби спеціального зв’язку та захисту

інформації України Юрій Щиголь (SSSCIP), який займається кіберзахистом у країні, яка охопила бойові дії.

«Відбулася зміна напрямку, від фокусу на енергетичних об'єктах до правоохоронних органів, які раніше не так часто ставали об'єктами нападів», – сказав Щиголь.

«Цей зсув у бік судів, прокуратури та правоохоронних органів свідчить про те, що хакери збирають докази про російські військові злочини в Україні», щоб слідкувати за розслідуваннями в Україні, додав він.

Шпигунська діяльність буде позначена в майбутньому звіті SSSCIP, який має бути опублікований у понеділок.

У звіті, з копією якого ознайомилося Reuters, йдеться, що хакери також намагалися зібрати розвідувальні дані про громадян Росії, заарештованих в Україні, з метою «допомогти цим особам уникнути судового переслідування та повернути їх назад до Росії».

«Групи, які ми ідентифікували як такі, що займаються цією діяльністю, є частиною ГРУ та ФСБ Росії», – сказав Щиголь.

Міністерство закордонних справ Росії та Федеральна служба безпеки (ФСБ) не відразу відповіли на письмові запити Reuters про коментарі. У ГРУ Росії не вдалося отримати коментар.

Щиголь відмовився назвати, які саме підрозділи стали мішенню хакерської кампанії, пославшись на міркування безпеки. За його словами, кількість інцидентів кібербезпеки, задокументованих SSSCIP, зросла на 123% за перші шість місяців цього року порівняно з другою половиною 2022 року.

Щиголь сказав, що російські хакери націлилися на державні органи та намагалися отримати доступ до їхніх серверів електронної пошти, не уточнюючи подробиць. Агентство Reuters не змогло незалежно перевірити жоден зі зломів, описаних Щиголем і звітом.

У вівторок Міжнародний кримінальний суд (ICC), що базується в Нідерландах, заявив, що наприкінці минулого тижня виявив «незвичайну

активність» у своїй комп’ютерній мережі. У п'ятницю ще не було зрозуміло, хто стоїть за зломом.

У березні суд потрапив у заголовки газет, коли видав ордер на арешт президента Росії Володимира Путіна за підозрою в незаконній депортації дітей з України. У Кремлі звинувачення та юрисдикцію суду відкидають.

ГІБРИДНА ВІЙНА

Напередодні вторгнення Росії в Україну в лютому 2022 року західні спецслужби попереджали про потенційні кібератаки, які можуть поширитися деінде та спричинити «поточну» шкоду глобальним комп’ютерним мережам.

Хоча на сьогодні мало доказів поширення, Росія регулярно використовує хакерські атаки разом із своїми військовими операціями.

Спроба російської спецслужби під назвою «Пісочний черв’як» здійснити деструктивну кібератаку на українську електромережу була зірвана у квітні 2022 року.

Щиголь сказав, що його відомство побачило докази того, що російські хакери отримували доступ до приватних камер відеоспостереження в Україні, щоб стежити за результатами ударів ракет дальньої дії та безпілотників.

«Ми задокументували кілька спроб отримати доступ до відеокамер поблизу об'єктів, які вони атакували, і до систем, які надають інформацію про стабільність енергетичної мережі», - сказав він.

Минулого року Росія атакувала українську енергетичну інфраструктуру зимовою повітряною кампанією, яка спричинила масштабні відключення електроенергії для мільйонів людей. Щиголь сказав, що енергетична інфраструктура також зазнавала кібератак і що він очікує, що ці атаки повторяться цієї зими.

«Потрібно розуміти, що кібервійна не закінчиться навіть після перемоги України на полі бою», – сказав Щиголь». ***(Tom Balmforth and James Pearson. Exclusive-Russian Hackers Seek War Crimes Evidence, Ukraine Cyber Chief Says // U.S. News & World Report L.P. (https://www.usnews.com/news/world/articles/2023-09-22/exclusive-russian-hackers-seek-war-crimes-evidence-ukraine-cyber-chief-***

says?utm_source=flipboard&utm_content=ARTJose%2Fmagazine%2FNEWS+%22THE+WORLD%22). 22.09.2023).

***

«Кіберзлочинність є серйозною загрозою для національної безпеки України. Лише протягом минулого року фахівці Держспецзв'язку зареєстрували в Україні понад 2 тисячі кіберінцидентів та ще більшу кількість кібератак на органи державної влади, фінансові установи, компанії у сфері критичної інфраструктури, логістики та енергетичного сектору тощо. Збитки від шахрайства в Інтернеті зросли на 96% порівняно з попереднім роком і досягли 1 мільярда гривень. При цьому російська агресія проти України супроводжується розгортанням все більш потужної війни в кіберпросторі. Ми вже маємо справу не з поодинокими атаками, а з масштабним наступом, який сплановано та підтримується на державному рівні.

Тому обговорення питань посилення боротьби зі злочинами в кіберпросторі та зміцнення кібербезпеки є надзвичайно важливими та актуальними. І я гордий тим, що Одеса в черговий раз продемонструвала своє лідерство в тих сферах, які є визначальними для нашої майбутньої перемоги. Йдеться про круглий стіл «Протидія кіберзлочинності в Україні: сучасний стан, особливості в умовах війни та прогнозування на післявоєнний період», який нещодавно відбувся на базі Одеського університету внутрішніх справ.

Цей захід став ефективною платформою для обговорення важливої проблематики із залученням наукової спільноти, фахівців з правоохоронних органів, а також – міжнародних експертів та представників громадського сектору. Зі свого боку запропонував учасникам круглого столу звернути увагу на кілька важливих моментів.

По-перше, протидія кіберзлочинності на різних рівнях локалізації проблеми повинна мати свою специфіку. Якщо на міжнародній арені це питання переважно до правників, то на рівні окремих регіонів – це скоріше справа для «технарів». Одеська обласна військова адміністрація, як і інші ОВА, приділяє значну увагу питанням посилення кіберзахисту, зокрема, систем державного управління та

об’єктів критичної інфраструктури. Тому впевнений, що конкретні напрацювання та пропозиції такого профілю будуть зустрінуті з помітною увагою та вдячністю.

По-друге, сьогодні точаться бурхливі дискусії навколо пошуку балансу у сфері перетинання інтересів держави, яка дбає про спільну безпеку, та особистості, яка намагається захистити власний простір. Далеко не завжди цей баланс знаходить своє відображення у відповідних нормах законодавства, і це подекуди призводить до зростання соціальної напруги. В Україні, яка в умовах війни потребує максимальної єдності, ці баланси мають бути бездоганними. Тому пропозиції щодо вдосконалення законодавчого поля, яке регулює питання кібербезпеки, є надзвичайно потрібними.

По-третє, технологічне оновлення дедалі більше прискорюється та вимагає створення гнучкої системи підготовки кадрів, які будуть здатними належним чином реагувати на виклики сучасності. Ми вже маємо відповідну мережу навчальних центрів Міністерства внутрішніх справ та Мінцифри. І ці центри досить успішно закривають потребу у технічній освіті та підвищенні кваліфікації фахівців, які працюють у галузі кібербезпеки. Але почивати на лаврах не на часі. Ми прагнемо перемоги, тому маємо бути на крок попереду від ворога. Отже, вдосконалення системи підготовки кадрів має тривати безперервно.

По-четверте, надійна система кібербезпеки передбачає належний рівень обізнаності населення про її специфіку та опанування навичками «кібергігієни». Для цього потрібна широка інформаційно-просвітницька кампанія, яка буде спрямована на роз’яснення населенню змісту сучасних кіберзагроз та способів захисту від них. Тому на часі більш інтенсивна та скоординована взаємодія відповідних державних органів, експертної спільноти та ЗМІ.

По-п’яте, Україна набуває унікального досвіду війни у кіберпросторі. Цей досвід є неоціненним та має послужити не лише нашій державі, а й нашим союзникам та партнерам. Як сказав наш президент: «Зараз ми є реципієнтом безпекової допомоги. Але Україна перемоги буде донором безпеки для нашого регіону, для всієї Європи, всього світу». Тому завдання акумуляції та узагальнення

цього досвід є серед першочергових. Він стане одним із наших внесків до систем колективної безпеки.

Впевнений, що спільно ми зможемо дати потужну відсіч ворогу та створити в Україні безпечний кіберпростір». ***(Олексій Леонов. Кібербезпека: актуальні завдання, що потребують ефективних рішень // USIONLINE.com (https://usionline.com/opinion/kiberbezpeka-aktualni-zavdannia-shcho-potrebuiut-efektyvnykh-rishen/). 28.09.2023).***

***

«Кібервійська України роблять дуже багато роботи щодо дестабілізації у цифровому середовищі Росії. Про це в ефірі телеканалу FREEДОМ заявив експерт у сфері кібербезпеки Сергій Денисенко.

При цьому він зазначив, що з метою безпеки публічно про конкретні успіхи українських кібервійськ не повідомляється.

За словами Денисенка, кібервійна складається з декількох елементів.

«Перше — в неї входить кіберрозвідка, а другий основний елемент — кіберзнищення. Наприклад, маючи доступ до якихось ресурсів, інформаційних баз даних, ніколи в житті жоден хакер не скаже, що він має туди доступ. І жодна компанія, яка виявить це втручання, не повідомить на весь світ, що її зламали і отримали якісь цінні дані. Це перше — кіберрозвідка. Друге — кібервійна, коли повністю знищуються ресурси, бази даних, у принципі, з новими технологіями бекапування, обсягами, які можуть зараз дозволити собі майже всі компанії, це не є проблемою, за великим рахунком. Єдине, щоб ця інформація нікуди не зникла. Це два основні аспекти», — пояснив експерт.

Він також висловив свою думку з приводу IT-коаліції, яка створюється Україною, Люксембургом і ще низкою європейських країн. Ще раніше Україна приєдналася до кіберцентру НАТО.

«Створення таких коаліцій і приєднання до кіберцентрів — дуже важливий шлях, тому що це все виходить на той рівень, що офіційно ми можемо передавати, обмінюватися інформацією щодо кіберінцидентів. Друге — що в цих коаліціях

буде куратор у плані менеджера, який організовуватиме. Третє — створюється команда, яка складається з розробників, ризик-менеджерів, технарів, які це все здійснюють технічно. І проведення валідації, верифікації обладнання, програмного забезпечення — це все буде більш централізовано, підконтрольно і має принести дуже велику користь нашим кібервійськам загалом», — розповів Сергій Денисенко». ***(Українські кібервійська роблять дуже багато роботи з дестабілізації цифрового середовища Росії // Internetua (https://internetua.com/ukrayinski-kiberviiska-roblyat-duje-bagato-roboti-z-destabilizaciyi-cifrovogo-seredovisxa-rosiyi). 24.09.2023).***

***

«Російські хакери збільшили кількість кібератак до 762 за півроку, однак вони перстали вражати критичні цілі. Це каже як про зміцнення українського захисту, так і про зниження амбіцій російських хакерів.

Видання Bloomberg зазначає, що початок російської війни в Україні включав деякі з наймасштабніших кібероперацій в історії, спрямованих на супутники та електростанції з метою шокувати населення та викликати у нього страх.

«Зараз, за словами українських чиновників, деякі з найвідоміших московських хакерів зосереджуються на таких кроках, як блокування веб-сторінки місцевого інформаційного агентства - більш скромний підхід, який спростовує твердження Володимира Путіна, що все йде за планом», - пише видання.

Нещодавно Служба кібербезпеки країни за підтримки Агентства США з міжнародного розвитку та Європейського Союзу опублікувала звіт, згідно з яким кількість російських кібератак по Україні зросла до 762 з січня по червень, що більш ніж вдвічі перевищує показники минулого року.

«Але кількість інцидентів, які вони назвали «критичними» за цей період, зменшилася на 81% до 27 - це свідчить про покращення захисту, а також про стриманіші амбіції Росії», - пише Bloomberg.

Тепер Росія атакує ЗМІ та телекомунікації, місцеві правоохоронні та урядові установи, які збирають докази військових злочинів, а також збирає дані про полонених росіян, що можуть постати перед судом за військові злочини.

Згідно зі звітом, пов'язані з державою хакери здебільшого уникали цілей, які могли бути використані для підтримки військових операцій. Натомість пов'язана з військовою розвідкою ГРУ група Sandworm, яка здійснювала одні з найагресивніших кібератак Росії по всьому світу, вдарила по українському державному інформаційному агентству в січні, намагаючись вивести з ладу його веб-сайт.

Незважаючи на зміни, українські експерти з кібербезпеки попереджають, що атаки на критичну інфраструктуру триватимуть. Приватна енергетична компанія ДТЕК повідомляла про неодноразові атаки на її IT-інфраструктуру як з боку хакерів, так і в результаті ракетних ударів. Російські хакери також намагалися зібрати інформацію про Запорізьку АЕС». ***(Російські хакери збільшили вдвічі кількість кібератак, але їх критичність знизилась, - ЗМІ // ХВИЛЯ (https://war.hvylya.net/uk/280126-rossiyskie-hakery-uvelichili-vdvoe-kolichestvo-kiberatak-no-ih-kritichnost-snizilas-smi). 29.09.2023).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Агенція США з міжнародного розвитку (USAID) виділила Україні грант на 500 тисяч доларів для впровадження інноваційних проєктів у сфері кібербезпеки.

Про це повідомляє Міністерство цифрової трансформації України.

Гранти отримають розробники, які запропонують найбільш ефективні інновації у сфері кіберзахисту. Один розробник може розраховувати на грант розміром близько 50 тисяч доларів.

У відомстві наголосили, що розробки українських фахівців не лише дадуть змогу захистити державні інформаційні ресурси, а й посилять світову кібербезпеку.

«Щодня рф здійснює атаки на урядові організації, органи влади, комерційний сектор. Ми ефективно захищаємося й даємо ворогу відповідь. Але нам потрібно більше інноваційних рішень і технологічних продуктів у сфері кіберу», — зазначив міністр цифрової трансформації Михайло Федоров.

Першими свої ідеї зможуть презентувати учасники конференції IT Arena, яка відбувається у Львові з 29 вересня по 1 жовтня, додали в Мінцифри.

Нагадаємо, у червні Сполучені Штати виділили Україні 37 мільйонів доларів на посилення стійкості до кібератак російських та інших хакерів.

Загалом з 2016 року Сполучені Штати надали 120 млн доларів на захист кіберпростору, з них 82 млн — за час повномасштабної війни. Це дозволяє вчасно виявляти кіберінциденти та загрози й реагувати на них, переконує Михайло Федоров.

А раніше у квітні Національна місія з кібербезпеки США відправила 43 своїх фахівців до України для боротьби з російськими кібератаками». ***(Ярослав Герасименко. Для захисту від російських кібератак Мінцифри та USAID запустили грантову програму на $500 тисяч // Громадське Телебачення (https://hromadske.ua/posts/dlya-zahistu-vid-rosijskih-kiberatak-mincifri-ta-usaid-zapustili-grantovu-programu-na-dollar500-tisyach). 29.09.2023).***

***

Світові тенденції в галузі кібербезпеки

«Cloudflare, Inc., компанія з безпеки, продуктивності та надійності, яка допомагає створювати кращий Інтернет, опублікувала нове дослідження, присвячене кібербезпеці в Азіатсько-Тихоокеанському регіоні. Згідно зі звітом, 83% індійських організацій стикалися з інцидентами кібербезпеки минулого року, а 48% виявили, що вони зазнали 10 і більше інцидентів. Інциденти здебільшого пов’язували з веб-атаками, фішингом і атаками на ланцюги поставок, причому респонденти вважали головною метою кіберзлочинців фінансову вигоду, а потім розповсюдження шпигунського програмного забезпечення та викрадання даних.

Звіт під назвою «Забезпечення майбутнього: опитування готовності кібербезпеки в Азіатсько-Тихоокеанському регіоні» також показав, що, незважаючи на частоту інцидентів кібербезпеки в Індії, лише 52% респондентів вважають себе високопідготовленими, а відсутність готовності коштує мільйони. 47% зазначили, що фінансові наслідки таких інцидентів перевищили 1 мільйон доларів США за останні 12 місяців, тоді як 27% зазнали фінансових невдач у розмірі не менше 2 мільйонів доларів.

«Готовність є ключовою, оскільки організації продовжують боротися з безпрецедентною складністю кібербезпеки. Враховуючи зростаючу цифрову майстерність Індії та постійну залежність бізнесу від технологій, для організацій вкрай важливо розвивати культуру безпеки, яка дає змогу їхнім керівникам підходити до кібербезпеки як до Це допоможе організаціям не тільки скоротити витрати, але й створити надійнішу та оптимізовану структуру кібербезпеки», — сказав Джонатон Діксон, віце-президент і керуючий директор Cloudflare у Азіатсько-Тихоокеанському регіоні, Японії та Китаї.

Наслідки інцидентів кібербезпеки поширюються на організаційні операції: 46% респондентів повідомили, що їхні організації скоротили або обмежили гібридну роботу, були змушені звільнити співробітників і відклали плани розширення, згідно зі звітом.

Крім того, звіт показав, що 57% керівників індійського бізнесу назвали нестачу кадрів найбільшою проблемою, з якою вони стикаються, коли йдеться про готовність до кібербезпеки, а 44% вказали, що брак фінансування перешкоджає їхній здатності захистити свій бізнес.

Компанія стверджувала, що це опитування було проведено компанією Sandpiper Communications від імені Cloudflare серед 4009 осіб, які приймають рішення та керівників у сфері кібербезпеки, від малих (від 150 до 999 співробітників), середніх (від 1000 до 2500 співробітників) і великих (понад 2500 співробітників) організацій». ***(Teena Jose. 83% of Indian Organizations Experienced a Cybersecurity Incident In the Past Year: Report // Entrepreneur Media, LLC (https://www.entrepreneur.com/en-in/news-and-trends/83-of-indian-organizations-***

experienced-a-cybersecurity/458587?utm_source=flipboard&utm_content=user%2Fentrepreneur). 06.09.2023).

***

«Майже половина керівників служби безпеки найбільших світових компаній очікують значного збільшення своїх бюджетів у наступному році, оскільки вони бачать, що економічні та соціальні заворушення спричиняють більше випадків крадіжок, шахрайства та витоку конфіденційної інформації.

Опитування 1775 керівників служби безпеки в 30 країнах показало, що їхні компанії втратили понад 1 трильйон доларів доходу в 2022 році в результаті інцидентів, не пов'язаних з кібербезпекою, подібно до грошового впливу кібератак високого рівня.

Опитування, проведене американською охоронною та кадровою компанією Allied Universal, показало, що компанії втрачають товари високого класу та інтелектуальну власність як всередині країни, так і за кордоном, причому Північна Америка сильно постраждала.

Опитування World Security Report, у якому Allied вперше зібрало та опублікувало думки такої кількості великих компаній, поставило під сумнів керівників, які спостерігали за загальним бюджетом безпеки у розмірі 660 мільярдів доларів США у 2022 році, або 3,3% їх світового доходу.

На запитання, що станеться з цими бюджетами наступного року, 46% відповіли, що вони «суттєво зростуть». Це призведе до зростання витрат, з якими борються компанії в усьому світі, починаючи від зарплат і закінчуючи енергією.

Головний виконавчий директор Allied Стів Джонс сказав Reuters, що хоча більшість шахрайства, підробки та втрати інтелектуальної власності були зумовлені фінансовою вигодою, деякі внутрішні витоки конфіденційної інформації були вмотивовані соціальними причинами.

«Існує такий соціальний вплив, або соціальна мотивація, або політична мотивація, за допомогою якої зловмисники присутні, щоб завдати шкоди компанії або вплинути на неї соціально та політично», — сказав він.

Звіт Allied, який володіє британською групою безпеки G4S (CSE: G4S), був розроблений, щоб оцінити вартість і масштаб порушень безпеки, а також чинники, які їх викликають.

У ньому перераховані економічні заворушення, спричинені високою інфляцією та погіршенням рівня життя, а також зміна клімату та соціальні заворушення як проблеми, які можуть призвести до порушень безпеки.

У Північній Америці 41% респондентів сказали, що стикалися з порушенням авторських прав з боку персоналу або підрядників, тоді як 32% втратили фізичну власність стороннім особам.

Приклади збитків включали крадіжки високоякісних товарів у технологічному та роздрібному секторах, тоді як фармацевтичний сектор боровся з підробками. Центри обробки даних також вважалися під загрозою через перебої з енергопостачанням або якщо порушення безпеки було пов'язано з кібератакою.

Відповідаючи на питання про майбутні витрати, 42% респондентів відповіли, що мають намір інвестувати в штучний інтелект (ШІ) і спостереження на основі ШІ, щоб швидше виявляти загрози». ***(Global companies to hike security spending as threats rise – survey // Fusion Media Limited. (https://www.investing.com/news/economy/global-companies-to-hike-security-spending-as-threats-rise--survey-3171319?utm_source=flipboard&utm_content=other). 11.09.2023).***

***

«У міру розвитку технологій розвиваються і стратегії та тактики, які використовують найхитріші кіберзлочинці. У цій безкінечній битві як організації, так і окремі особи повинні бути на крок попереду, щоб захистити свої дані та конфіденційність.

Але що все це означає для вас? Слідкуючи за майбутніми технологічними тенденціями, ви зможете перевірити свої заходи безпеки на майбутнє. Зрештою, модні технології формують майбутнє кібербезпеки кількома дивовижними способами.

Як нові технології змінюють кібербезпеку (і навпаки)

Постійний розвиток технологій діє як палка з двома кінцями. З одного боку, кіберзагрози стають все більш витонченими, використовуючи нові технології, такі як штучний інтелект (AI) та Інтернет речей (IoT), щоб проникнути в системи. З іншого боку, ті самі технологічні досягнення надають потужні інструменти для зміцнення кібербезпеки.

Коротше кажучи, у міру того, як змінюється ландшафт загроз, кібербезпека також повинна розвиватися. Швидке зростання 5G, роботизованої автоматизації процесів, генеративного штучного інтелекту тощо створює як проблеми, так і можливості. Широке впровадження 5G, наприклад, розширює зону атаки, пропонуючи більше точок входу для кіберзлочинців.

У той же час, оскільки люди діляться все більшою кількістю особистої інформації в Інтернеті, кіберзагрози, починаючи від крадіжки особистих даних і закінчуючи великомасштабними атаками, зростають. Абсурдна доступність особистих даних на платформах соціальних мереж робить людей серйозно вразливими до фішингових атак. Отже, настав час дізнатися більше про найбільші загрози безпеці, з якими ви можете зіткнутися сьогодні.

Після резонансних порушень у таких компаніях, як LinkedIn і Marriott International, корпорації почали впроваджувати надійні заходи кібербезпеки. Деякі з цих зусиль включають покращення виявлення вірусів, зменшення помилкових спрацьовувань і зміцнення захисту від нових загроз.

Взаємодія між технологіями та кібербезпекою — це складний танець, і йти в ногу з цим середовищем, що постійно змінюється, є ключовим для забезпечення нашого цифрового майбутнього.

1. Інтернет речей (IoT)

Інтернет речей (IoT) стає трансформаційною силою, з'єднуючи незліченну кількість пристроїв і революціонізуючи спосіб нашого життя та роботи. Зростання кількості пристроїв, що працюють на базі Інтернету речей, було не чим іншим, як вражаючим, покращуючи зв'язок і оптимізуючи складні бізнес-процеси в глобальному масштабі.

На жаль, це зростання кількості пристроїв Інтернету речей принесло з собою низку проблем кібербезпеки. Зараз ми спостерігаємо сплеск кібератак, націлених на пристрої Інтернету речей, що посилюється розширенням використання периферійних обчислювальних пристроїв і повсюдним впливом хмарних екосистем.

Найслабкіші місця в цій розгалуженій екосистемі включають незашифровані особисті дані, жорстко закодовані паролі, неперевірені оновлення програмного забезпечення, вразливість бездротового зв'язку тощо. До складності додає інтеграція мереж 5G з Інтернетом речей, посилюючи взаємозв'язок і розширюючи поверхню атаки.

У відповідь компанії активно працюють над передовими технологіями та рішеннями 5G для зміцнення захисту та боротьби з витоком даних.

2. Квантові обчислення

Квантові обчислення можуть змінити світ, використовуючи переваги дивних законів квантової механіки, таких як суперпозиція та заплутаність, для виконання обчислювальних завдань, які раніше були неможливо уявити. Його потенціал для вирішення складних проблем і обробки даних з багатьох джерел приголомшливий.

Однак із великою владою має бути й велика відповідальність. Квантові комп'ютери можуть зламати поточні методи шифрування, створюючи серйозну загрозу безпеці даних. Конфіденційні дані користувача, такі як інформація про здоров'я та фінанси, і навіть базова криптографія, що підтримує криптовалюти, можуть бути під загрозою.

Оскільки все більше і більше компаній продовжують інвестувати в цю захоплюючу, але складну технологічну тенденцію, кібербезпека має переосмислити себе, щоб йти в ногу з новими ризиками безпеки.

3. Штучний інтелект

Штучний інтелект (AI) і машинне навчання (ML) знаходяться в авангарді зміни кібербезпеки назавжди. Хоча існує сильне почуття оптимізму щодо їхнього потенціалу для покращення кібербезпеки, також зростає занепокоєння щодо ризиків, які вони становлять.

З іншого боку, штучний інтелект та машинне навчання сприяють інноваціям у кількох секторах, включаючи медицину, транспорт і, звичайно, кібербезпеку. Вони дають змогу фахівцям із кібербезпеки бути на випередженні, покращуючи виявлення загроз і реагування на них. Вони аналізують величезні масиви даних, виявляють аномалії та прогнозують потенційні порушення безпеки ще до того, як вони відбудуться.

Але той самий AI та ML також можуть використовуватися кіберзлочинцями для створення більш складних кіберзагроз. Ці технології дозволяють шкідливому програмному забезпеченню швидко розвиватися, що ускладнює виявлення та пом’якшення атак.

Оскільки штучний інтелект і машинне навчання продовжують розвиватися, наші засоби захисту також повинні захищатися від все більш витончених супротивників.

4. Технологія блокчейн

Спочатку розроблений для безпечних транзакцій у криптовалюті, децентралізований характер блокчейну та криптографічні принципи роблять його чудовим союзником у захисті даних, транзакцій та перевірки особи.

Основою внеску блокчейна в кібербезпеку є його незмінність. Після того, як дані записані в блок і додані до ланцюжка, змінити їх стає практично неможливо. Це гарантує, що конфіденційна інформація, наприклад записи транзакцій, залишається захищеною від підробки. У світі, де витоки даних і несанкціонований доступ широко поширені, ця незмінність стає потужним захисним механізмом.

Блокчейн, децентралізована мережа комп’ютерів, переосмислює парадигми кібербезпеки, усуваючи централізовані вразливості. Ця структура розподіляє дані між декількома вузлами, значно знижуючи вразливість до порушень. Крім того,

блокчейн може покращити перевірку особистості та захист конфіденційності, забезпечуючи уніфіковану безпечну платформу для підтвердження особи без розкриття конфіденційних даних. Тут користувачі зберігають контроль над своєю інформацією, зменшуючи ризики крадіжки особистих даних.

Однак необхідно подолати такі проблеми, як масштабованість, споживання енергії та регуляторні проблеми.

5. Модель безпеки без довіри

Модель нульової довіри діє за основним принципом, що довіру ніколи не можна презюмувати, незалежно від того, перебуває користувач чи пристрій у межах організації чи за її межами. На відміну від традиційного підходу, заснованого на периметрі, безпека з нульовою довірою вимагає безперервної перевірки довіри, покладаючись на такі фактори, як поведінка користувача, стан пристрою та оцінка ризику в реальному часі.

Відкинувши довіру за замовчуванням, надану користувачам і пристроям, компанії можуть знизити ризик внутрішніх загроз і підозрілих дій. Цей проактивний підхід гарантує, що привілеї доступу коригуються на основі поточної перевірки, зменшуючи вплив порушення. Основними компонентами принципів нульової довіри є передові методи автентифікації, цілодобовий моніторинг і надійне шифрування.

6. Хмарні обчислення та безпека

Із впровадженням хмарних обчислень динаміка зберігання та доступності даних змінилася. Багато хто приймає хмару за її масштабованість і економічну ефективність, але це також супроводжується критичними міркуваннями безпеки.

Керування ідентифікацією та доступом (IAM) відіграє важливу роль у безпеці хмари. Ці рішення дозволяють організаціям керувати ідентифікацією користувачів і контролювати доступ до хмарних ресурсів. Завдяки надійним механізмам автентифікації та авторизації IAM гарантує, що лише авторизований персонал може отримати доступ до конфіденційних даних.

Шифрування є ще одним наріжним каменем хмарної безпеки, оскільки воно гарантує, що навіть у разі несанкціонованого доступу інформація залишається нерозшифрованою.

У цю епоху віддаленої роботи хмарна безпека є більш важливою, ніж будь-коли. Оскільки співробітники отримують доступ до даних із різних місць і пристроїв, віртуальні приватні мережі (VPN) і рішення SASE (Sense) гарантують, що дані залишаються захищеними навіть за межами корпоративних мереж.

7. Технологія 5G

5G, п’яте покоління бездротових мереж, відкриває нову еру підключення з обіцянкою блискавичної швидкості Інтернету, меншої затримки та підтримки вражаючої кількості підключених пристроїв. Однак це також викликає занепокоєння щодо кібербезпеки.

По-перше, величезний обсяг підключених пристроїв може експоненціально збільшити поверхню атаки. Маючи більше точок входу в мережі та системи, кіберзлочинці знаходять середовище для використання вразливостей. Це вже не лише ноутбуки та смартфони – це пов’язані між собою міста, безпілотні транспортні засоби та критична інфраструктура.

Крім того, надвисока швидкість мереж 5G означає, що дані можуть бути перехоплені, змінені або викрадені за лічені мілісекунди. Крім того, поширення пристроїв IoT, які значною мірою залежать від підключення 5G, створює нові проблеми з безпекою.

8. Розквіт Метавсесвіту

Народження метавсесвіту породило складну мережу проблем. Одна з головних проблем зосереджена навколо захисту віртуальних активів. У метавсесвіті користувачі інвестують час і ресурси в придбання цифрових властивостей, починаючи від віртуальної нерухомості й закінчуючи внутрішньоігровими активами. Оскільки ці активи мають реальну цінність, це робить їх привабливими цілями для кіберзлочинців.

Оскільки користувачі Metaverse залучаються до захоплюючого цифрового досвіду, потенціал для шахрайства з особистими даними в ньому досягає даху.

Кіберзлочинці можуть використовувати вразливості в профілях користувачів, отримуючи несанкціонований доступ до особистої інформації або навіть видаючи себе за реальних користувачів. Отже, без надійних механізмів перевірки особи та інших подібних заходів метавсесвіт і надалі залишатиметься джерелом ризиків.

9. Поведінкова біометрія

Ця передова технологія кібербезпеки заглиблюється в тонкощі поведінки окремих користувачів, щоб посилити заходи автентифікації та безпеки.

На відміну від традиційних методів автентифікації (які зазвичай ґрунтуються на статичних облікових даних, таких як паролі, парольні фрази або PIN-коди), поведінкова біометрія аналізує динамічні, специфічні для користувача риси. Вони охоплюють цілу різноманітність поведінки, від ритму набору тексту та рухів миші до жестів на сенсорному екрані та того, як хтось тримає свій смартфон.

Хоча цей рівень персоналізації додає потужний рівень безпеки, він також має недоліки, зокрема проблеми з конфіденційністю та схильність до помилкових спрацьовувань/негативів, які є технічними проблемами з наслідками для кібербезпеки.

Адаптація до кіберзагроз, що постійно розвиваються

Оскільки наш цифровий домен постійно змінюється, випереджати загрози – це єдиний спосіб триматися над водою. Прийняття цих технологічних тенденцій має важливе значення для забезпечення нашого майбутнього онлайн у світі кібербезпеки, що постійно розвивається». ***(Sead Fadilpašić. The 9 Top Technology Trends That Are Shaping the Future of Cybersecurity // MUO (https://www.makeuseof.com/top-technology-trends-shaping-cybersecurity-future/?utm_source=flipboard&utm_content=Raster4%2Fmagazine%2FTech). 09.09.2023).***

***

«Зараз більшість менеджерів з інформаційних технологій болісно усвідомлюють наслідки атак на ланцюги поставок програмного забезпечення. Завдяки експлойтам, які впливають на ланцюги поставок SolarWinds, Log4Shell і

3CX, потужність і масштабна шкода, завдана цими атаками тисячам компаній, безумовно, добре відомі.

Щоб спробувати виправити ситуацію, цього літа запустили низку нових постачальників засобів безпеки ланцюга поставок. Серед них Ox Appsec Security Ltd., яка інтегрує ChatGPT для кращого захисту, а також Stacklock, який забезпечує кращий підпис криптографічного коду, і Sonatype Inc., яка створює переліки матеріалів з відкритим кодом. Вони доповнюють багатьох давніх постачальників програмного забезпечення безпеки, таких як Palo Alto Networks Inc. Prisma Cloud і Veracode Inc., які пропонують загальну безпеку програм протягом багатьох років.

Проблема з цими експлойтами ланцюга поставок полягає в тому, що вони мають кілька причин. По-перше, немає уніфікованої моделі управління, яка б охоплювала всіх зацікавлених сторін: розробників, кінцевих користувачів, клієнтів і корпоративних менеджерів. Часто ці різні групи мають суперечливі цілі та цілі або не знають, як оцінити безпеку своїх програмних компонентів, або навіть знають, які компоненти вони використовують.

Багато розробників покладаються на десятки, якщо не сотні проектів з відкритим вихідним кодом, будь-який з яких може бути скомпрометований і стати головним експлойтом завтрашнього дня. Окрім цих проблем, конвеєри розробки не можуть легко інтегруватися з існуючим програмним забезпеченням безпеки, що посилює пов’язані з цим ризики.

Незалежно від того, що спричинило збій у ланцюжку постачання, важливим є те, як IT може навчитися на цих поганих практиках і створити кращі хмарні програми. Саме тут на допомогу приходить Національний інститут стандартів і технологій. Він має нову колекцію в проекті документа під назвою «Стратегії інтеграції безпеки ланцюга поставок програмного забезпечення в конвеєри DevSecOps CI/CD», який було опубліковано наприкінці минулого місяця. Мета полягає в тому, щоб допомогти пришвидшити інтеграцію різноманітних заходів безпеки ланцюжка поставок програмного забезпечення в ці конвеєри та інфраструктури розробки.

Ці стратегії є частиною більшої серії NIST про найкращі практики DevSecOps і безпечних інфраструктур розробки програмного забезпечення разом з іншими зусиллями, які підтримує держава. Це на додаток до спільного набору рекомендацій Агентства національної безпеки та Агентства з кібербезпеки та безпеки інфраструктури, які були видані влітку, спрямовані на покращення безпеки трубопроводу розвитку. У вересні 2022 року обидві агенції також випустили набір рекомендацій для розробників.

Проект NIST намагається провести різницю між виявленням помилки програмного забезпечення, яка є ненавмисним дефектом, і дефектом, який використовує зловмисник у зловмисних цілях. Експлойт може бути влаштований групою хакерів, яка спеціально націлена на певний бізнес кінцевих користувачів, або це може бути результатом незадоволеного працівника, який прагне помститися.

Він також може запустити низку ін'єкцій у вихідний код певного проекту чи середовища тестування, або він може містити вкрадені облікові дані облікового запису за допомогою соціальної інженерії. Кожен із цих сценаріїв описується з точки зору потенційних наслідків для безпеки та кроків, необхідних для запобігання цьому.

IT-менеджери, знайомі з життєвим циклом розробки програмного забезпечення, ймовірно, вважатимуть проект елементарним, але для тих, хто не залучений у цю сферу, він надає загальну базу знань, яка допоможе просувати дискусії про безпеку ланцюга поставок програмного забезпечення.

У чернетці докладно описано, як виконати конкретні кроки, наприклад «визначити детальні повноваження для виконання різних завдань, таких як генерація та фіксація коду, створення збірок і пакетів, а також перевірка різних збірок і пакетів у сховищах коду та з них». Кожен із них описано далі з точки зору необхідних кроків безпеки.

Коментарі до чернетки NIST вітаються та мають бути надіслані до 13 жовтня. Їх можна надіслати електронною поштою на цю адресу». ***(David Strom. Software supply chain attacks are multiplying, but so are strategies to avoid them // (https://siliconangle.com/2023/09/07/software-supply-chain-attacks-multiplying-***

strategies-avoid/?utm_source=flipboard&utm_content=kuryakin%2Fmagazine%2FIn+Search+Of+The+Truth). 07.09.2023).

***

«З огляду на останні дані IBM, згідно з якими середня глобальна вартість витоку даних зросла на 2% до 4,45 млн доларів, можна подумати, що для багатьох із нас, особливо для тих, хто працює в індустрії кібербезпеки, діяти безпечно та безпечно буде мінімальним мінімумом. Я маю на увазі, це в назві: безпека.

Але чи спеціалісти з кібербезпеки роблять достатньо, щоб забезпечити свою роль у забезпеченні безпеки бізнесу? На жаль, факти викликають певне занепокоєння, оскільки більше половини (55%) фахівців з кібербезпеки визнали, що брали участь у ризикованій поведінці з кібербезпеки на роботі. Фахівці з безпеки є факелоносцями безпеки в організації, і на них дивляться як на людей, які повинні дотримуватися правил і процесів, запроваджених для забезпечення безпеки компанії. Пам’ятайте, що сучасні кіберзагрози націлені на всіх, тому ніхто не стоїть вище навчання з питань безпеки, особливо професіонали з безпеки.

Слід проводити регулярні тренінги з питань безпеки в масштабах усієї компанії, щоб усунути недостатню обізнаність щодо безпеки в організації. Проте це ж дослідження також показало, що половина фахівців з кібербезпеки визнали, що їхні організації проводять навчання лише раз на рік або раз на квартал. Якщо самі професіонали з безпеки демонструють ризиковану поведінку на роботі та не створюють належним чином рівень людського захисту у своїх організаціях, це малює похмуру картину, особливо в світлі нещодавніх порушень, спричинених людською помилкою.

Незалежно від того, приймаєте ви це чи ні, кожен співробітник розглядається як потенційна точка входу для хакерів і є найбільшим фактором ризику для безпеки організації; поширення атак соціальної інженерії є свідченням цього. Тому

навчання працівників найкращим практикам безпеки має першочергове значення, щоб утримати їх від ризикованої поведінки у сфері безпеки…

Розвиток сильної культури безпеки

Якщо співробітники, незалежно від їх ролі чи відділу, продовжуватимуть брати участь у такій ризикованій поведінці, кіберзагрози будуть постійно присутні. Щоб ефективно вирішити цю проблему та виправити ситуацію як у короткостроковій перспективі, так і за її межами, необхідно розвивати сильну культуру безпеки в організації.

Це включає в себе регулярне навчання з питань безпеки, яке має виходити за рамки простого інструктування персоналу щодо загроз. Це поширюється на те, щоб надати їм можливість ефективно реагувати та дозволити робочій силі вміло визначати оптимальні заходи профілактики.

Встановлення надійної культури безпеки є необхідною основою для зниження потенційного ризику кібератаки на організацію. Досягнення цього вимагає трансформації ставлення, поведінки, сприйняття відповідальності та загальних організаційних норм. По суті, мета полягає в тому, щоб бездоганно інтегрувати найкращі практики безпеки в усі можливі сценарії, процеси та операції, пристосовуючи їх до контексту кожного.

Щоб сприяти цьому, було знайдено новий технологічний підхід до створення сильної культури безпеки. Він зосереджений на виявленні та реагуванні на загрози, спричинені людською діяльністю (фішинг і загрози соціальної інженерії), і передбачає автоматизоване навчання в режимі реального часу. Це відрізняється від традиційного тренінгу з підвищення обізнаності з питань безпеки, який навчає працівників найкращим практикам безпеки в Інтернеті та зниження ризику стати жертвою поширених загроз кібербезпеці. У поєднанні обидва вони відіграватимуть вирішальну роль у покращенні поведінки всієї робочої сили.

У загальному плані кібербезпека повинна бути першочерговою турботою для кожного аспекту організації, кожного відділу та кожного співробітника. Успішне досягнення цієї мети призводить до підвищеної пильності серед користувачів, сприяючи формуванню мислення, яке визначає пріоритет відповідних реакцій на

потенційні загрози. Це допоможе організації в майбутньому». ***(Javvad Malik. How to Prevent Risky Cybersecurity Behaviors Creeping into Your Organization // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/blogs/prevent-risky-cyber-behaviors/). 13.09.2023).***

***

«Кібербезпека — це практика захисту мереж, даних (зокрема особистих і конфіденційних даних) і пристроїв від хакерів і кіберзлочинців шляхом вжиття запобіжних заходів.

Хоча кібербезпека може звучати як спеціалізована тема, якою займається IT-відділ, швидше за все, ваш бізнес використовує Інтернет у тій чи іншій формі для роботи. Кожен бізнес, який взагалі використовує Інтернет, великий чи малий, повинен практикувати кібербезпеку.

Є кілька способів підвищити кібербезпеку вашої мережі, пристроїв і даних. Ці методи варіюються від встановлення сканера вірусів на вашому пристрої до найму цілої команди консультантів з кібербезпеки. План дій щодо підвищення кібербезпеки для вашого малого бізнесу враховуватиме різні ризики, пов’язані з вашою компанією, і вживатиме необхідних запобіжних заходів…

Чому кібербезпека життєво важлива

Ризики кібератаки можуть бути руйнівними для бізнесу чи особи. Оскільки велика частина нашого особистого та робочого життя відбувається в Інтернеті, кібербезпека має бути життєво важливим компонентом використання Інтернету як для особистого використання, так і для бізнесу.

Кібербезпека у вашому бізнесі

Якщо ви власник бізнесу, важливо розглядати ризики свого бізнесу з точки зору кібербезпеки. Кожен бізнес буде різним, але незахищені мережі та пристрої, які зламано, можуть призвести до втрати грошей, часу та інформації вашого бізнесу. Серед ризиків: зловмисник може зламати деякі або всі ваші файли та викрасти конфіденційну інформацію.

Іншим наслідком хакерських дій у системі кібербезпеки є зниження довіри споживачів, що може мати руйнівний довгостроковий вплив на бізнес.

У сучасному світі штучний інтелект також є важливою проблемою не лише для корпорацій, а й для малого бізнесу. Малий і середній бізнес зараз використовує ChatGPT серед інших ШІ для багатьох функцій, але існує ризик того, що це може бути нестабільним, оскільки ШІ, можливо, створюють технологи, яким може бракувати розуміння того, як різноманітні закони, нормативні акти та договірні зобов'язання впливають на технологію.

Оскільки дуже багато компаній працюють або віддалено, або за допомогою гібридної моделі, важливо створити план кібербезпеки, який також враховує домашні мережі, і запровадити відповідні огорожі для таких інструментів, як ШІ, якщо це можливо.

Компанії можуть розглянути питання про навчання своїх співробітників щодо кібербезпеки, яке зазвичай включає інформування працівників про те, як виявляти/ідентифікувати підозрілі електронні листи та уникати завантаження зловмисного програмного забезпечення на пристрій.

Кібербезпека вдома

Заходи кібербезпеки однаково важливі для окремих користувачів, а ризики, з якими стикається окрема особа, однаково високі.

Нижче ми наведемо деякі поширені типи кіберзагроз і способи захисту.

Поширені типи кіберзагроз

Кібербезпека — це загальний термін, який стосується заходів безпеки проти низки кіберзагроз. Ось деякі з поширених.

Шкідливе програмне забезпечення

Шкідливе програмне забезпечення – це шкідливий файл або програма, яка завдає шкоди комп'ютеру. Зловмисне програмне забезпечення зазвичай заражає пристрій, спонукаючи користувача відкрити шахрайське вкладення, наприклад електронний лист або шкідливий веб-сайт. Наприклад, користувач може відкрити електронний лист із вкладенням, схожим на документ Word, але насправді є шкідливим програмним забезпеченням.

програми-вимагачі

Програми-вимагачі – це різновид зловмисного програмного забезпечення, розробленого для того, щоб за допомогою шифрування позбутися доступу користувача або компанії до файлів на їх комп'ютері. Причетні вимагатимуть викуп за доступ до ключа розшифровки для доступу до файлів, який може навіть не працювати, створюючи безпосередню загрозу існуванню бізнесу.

шпигунське програмне забезпечення

Шпигунське програмне забезпечення — це шкідливий файл або програма, призначена для збору інформації про користувача. Шпигунське програмне забезпечення – це тип шкідливого програмного забезпечення, яке збирає дані без відома користувача чи організації. Шпигунське програмне забезпечення працює у фоновому режимі пристрою, зазвичай залишаючись непоміченим для користувача, і може реєструвати натискання клавіш, історію веб-перегляду, особисті дані тощо.

Фішинг, смішинг і вішинг

Фішинг — це процес надсилання фальшивого електронного листа, який має на меті змусити користувача розкрити особисту інформацію про себе. Ці електронні листи часто містять заклик до дії або посилання, на яке одержувачі можуть натиснути. Вони можуть попросити банківську інформацію одержувача або іншу конфіденційну особисту інформацію. Наприклад, фішинговий електронний лист може повідомити одержувачу, що статус його облікового запису неповний і що йому потрібно оновити його (через шкідливе посилання).

Смішинг — це процес надсилання шахрайського SMS із тим самим зловмисним наміром. Vishing, практика телефонування або залишення голосових повідомлень з наміром отримати особисту інформацію для зловмисних цілей, є ще однією кібератакою. Незалежно від методу, основною метою цього типу атаки є отримання конфіденційної інформації або отримання негайного прибутку.

Компроміс корпоративної електронної пошти (BEC)

Компрометація бізнес-електронної пошти (BEC) — це різновид фішингової атаки, під час якої зловмисники видають себе за довірену особу та використовують

електронну пошту, щоб обманом змусити власника бізнесу чи високопоставленого керівника переказати кошти чи розкрити конфіденційну інформацію про компанію.

Соціальна інженерія

Зазвичай для кібератаки потрібні кілька конфіденційних відомостей про особу чи компанію. «Соціальна інженерія — це процес використання інформації, щоб отримати або витягнути з вас щось, що може мати додаткову цінність», — пояснив доктор Кріс Меттманн, головний спеціаліст з технологій та інновацій (CTIO) Лабораторії реактивного руху NASA.

Хакер може мати певні відомості про компанію та використати це, щоб завоювати довіру особи, яка потім може розкрити більш конфіденційну інформацію, яка надалі сприятиме атаці. Хакери використовують багато способів соціальної інженерії, зокрема через фішинг, соціальні мережі та телефонні дзвінки.

7 методів кібербезпеки, щоб захистити себе

1. Створіть надійні паролі та регулярно їх змінюйте. Згідно з даними Агентства з кібербезпеки та безпеки інфраструктури США, надійний пароль не є словом чи словосполучення, містить спеціальні символи та має 16 або більше символів.

Також важливо регулярно змінювати паролі. «Стандартна практика, якої корпорації та споживачі можуть дотримуватися, полягає в тому, щоб змінювати свій пароль кожні 60-90 днів у всіх своїх облікових записах», — порадив Меттманн.

Звичайно, коли ви регулярно змінюєте паролі, вам знадобиться спосіб запам’ятати їх усі. Для цього призначений менеджер паролів.

2. Використовуйте менеджер паролів

В Інтернеті доступно багато менеджерів паролів, які дозволять вам легко зберігати всю інформацію свого облікового запису. Деякі безкоштовні, а деякі платні. Google Chrome надає безкоштовний менеджер паролів, який також сповістить вас, якщо вашу інформацію для входу буде знайдено в темній мережі.

3. Налаштуйте двофакторну автентифікацію (2FA)

Двофакторна автентифікація або 2FA означає, що один із ваших пристроїв має бути у вашому фізичному володінні, щоб отримати доступ до вашого онлайн-облікового запису. Налаштування 2FA гарантує, що вам знадобляться як ваш комп'ютер, так і ваш телефон, наприклад, для доступу до облікового запису, тим самим запобігаючи зламам, отримуючи доступ лише до вашого імені користувача та пароля.

4. Налаштуйте брандмауер

Брандмауери захищають зовнішній доступ до вашої мережі від зловмисного трафіку. Брандмауери можуть бути як апаратними, так і програмними. Маршрутизатори можуть містити брандмауер, і багато операційних систем містять вбудований брандмауер, який користувачі можуть увімкнути.

5. Запустіть антивірусне сканування

Антивірусне сканування допоможе визначити, чи заражено ваш пристрій шкідливим програмним забезпеченням. «Антивірусне сканування виявить шкідливі та шпигунські програми, встановлені на вашому комп'ютері. Він активно скануватиме ваш комп'ютер на наявність таких речей. І він підтримує базу даних про те, як виглядають ці типи [вірусів], щоб він міг виявляти навіть те, що ми називаємо резидентними атаками, які чекали деякий час, але не були активовані», — пояснив Маттман.

Антивірусне сканування є стандартним для корпорацій, але Mattmann також рекомендує їх для окремих користувачів.

6. Активне сканування темної мережі

Активне сканування темної мережі шукатиме в темній мережі вашу особисту інформацію (PII). Ці інструменти доступні безкоштовно або за підпискою. Може бути корисно залучити служби, які спеціально обробляють ці сканування, і багато кредитних карток, таких як Capital One, тепер пропонують користувачам активний темний веб-моніторинг.

7. Регулярно оновлюйте програмне забезпечення

Один із найкращих способів захистити себе в Інтернеті – це регулярне оновлення програмного забезпечення. Зловмисники використовують відомі

вразливості програмного забезпечення, які виправлено в оновлених версіях програмного забезпечення. Операційні системи часто надають користувачам можливість автоматично оновлювати програмне забезпечення, що полегшує його відстеження.

8. Проведіть навчання з питань кібербезпеки для свого бізнесу

Якщо ви власник бізнесу, будь-який шкідливий електронний лист, який відкриває співробітник, ризикує заразити всю мережу всієї компанії. Це великий ризик. Компанії часто проводять інформаційні тренінги, щоб повідомити співробітникам про типи електронних листів, які є шахрайськими, і про те, на що слід звернути увагу.

Нижня лінія

Найкращі практики кібербезпеки важливі як для компаній, так і для окремих осіб. Реалізація плану кібербезпеки для компанії для особистого користування Інтернетом буде відрізнятися залежно від характеру бізнесу та того, як ви використовуєте Інтернет.

Важливо враховувати типи ризиків, з якими може зіткнутися ваш бізнес, і застосовувати способи його захисту. Те саме стосується особистого використання.

Однак передові практики, такі як регулярне оновлення програмного забезпечення та використання 2FA, легко застосувати, і вони підходять для будь-якої компанії та окремої особи…» ***(Leeron Hoory, Kiran Aditham. What Is Cybersecurity? Definition And Best Practices // Forbes (https://www.forbes.com/uk/advisor/business/software/what-is-cybersecurity/). 07.09.2023).***

***

«…Оборонні компанії, які працюють у секторі кібербезпеки, використовують останні патенти для стимулювання інновацій і підвищення безпеки операцій. Серед цих патентів «Система прямої передачі даних» сприяє безпечному обміну даними між схемами пам’яті, підвищуючи загальні можливості кібербезпеки. Водночас «Система керування доступом» ретельно перевіряє дані з

мобільних і підключених пристроїв для підтвердження запитів на доступ, забезпечуючи доступ до конфіденційної інформації лише авторизованим особам, таким чином посилюючи заходи кібербезпеки. Патент «Захищена від втручання система передачі даних» представляє захищену систему зв'язку між наземним і віддаленим модулями. Використовуючи різні методи модуляції та дублюючі сигнали, він запобігає фальсифікації та підвищує безпеку передачі даних. Цей патент пропонує оборонним компаніям надійне комунікаційне рішення для збереження конфіденційності та цілісності їхніх комунікацій.

Серед інших прикладів патентів, які оборонні компанії використовують для вдосконалення своїх технологій і програм кібербезпеки, можна назвати «Системи та методи безпечного моніторингу транспортного контейнера на предмет екологічної аномалії» та «Методи та системи автентифікації електричного літака для підзарядки». Впроваджуючи останні інновації, вони можуть покращити передачу даних, керування доступом, безпеку зв'язку, безпеку ланцюга постачання та системи автентифікації. Ці досягнення дозволять оборонним компаніям посилити свої заходи кібербезпеки та ефективно захистити свою конфіденційну інформацію та активи.

У другому кварталі 2023 року кількість заявок на патенти, пов'язані з кібербезпекою, знизилася на 7% порівняно з попереднім кварталом. Щорічно кількість заявок на патенти, пов'язані з кібербезпекою, в аерокосмічній, оборонній та безпековій промисловості впала на 6% порівняно з другим кварталом 2022 року.

Стратегічні тенденції угод у кібербезпеці в аерокосмічній, оборонній та безпековій галузях

Аерокосмічні, оборонні та безпекові компанії не лише зосереджуються на інноваціях, щоб розширити свої патентні портфоліо, але також здійснюють стратегічні інвестиції в кібербезпеку. Ці інвестиції спрямовані на забезпечення вигідних угод з партнерами та позиціонування в авангарді розвитку галузі. Деякі з нещодавніх угод підкреслюють важливість кібербезпеки в аерокосмічній, оборонній та охоронній галузях.

У другому кварталі 2023 року кількість угод, пов’язаних із кібербезпекою, в аерокосмічній, оборонній та безпековій галузях зросла на 100% порівняно з другим кварталом 2022 року. Щоквартально кількість угод у другому кварталі 2023 року зросла на 200% порівняно з попереднім кварталом...

Вплив на прийом на роботу

Що стосується нових вакансій, у другому кварталі 2023 року аерокосмічна галузь, галузь оборони та безпеки зазнала падіння на 4% порівняно з попереднім кварталом. У річному вимірі кількість оголошень про роботу також скоротилася на 7%. Зокрема, у другому кварталі 2023 року комп’ютерні та математичні професії з часткою 32% виявилися основними посадами, пов’язаними з кібербезпекою, в аерокосмічній, оборонній та безпековій галузях, а кількість нових оголошень про роботу впала на 7% у порівнянні з кварталом. Професії менеджменту зайняли друге місце з часткою 9% у другому кварталі 2023 року, а кількість нових оголошень про роботу зросла на 0,85% порівняно з попереднім кварталом. Інші відомі посади в сфері кібербезпеки включають професії в галузі архітектури та інженерії з часткою 7% у другому кварталі 2023 року, а також професії, пов’язані з бізнесом і фінансовими операціями з часткою нових оголошень про роботу в 5%.

RTX, Leidos, Rohde & Schwarz, Huntington Ingalls Industries і Northrop Grumman є одними з провідних компаній, які наймають працівників у сфері кібербезпеки в аерокосмічній, оборонній та безпековій галузях.

Країни, які сприяють запровадженню кібербезпеки в аерокосмічній, оборонній та безпековій галузях

США є лідером із запровадження кібербезпеки в аерокосмічній, оборонній та безпековій галузях, маючи найбільшу кількість патентів, вакансій і угод, пов’язаних із кібербезпекою. Тим часом Велика Британія, Греція, Німеччина та Японія також зберігають значні позиції щодо впровадження кібербезпеки в аерокосмічній, оборонній та безпековій галузях…

Підсумовуючи, аерокосмічна галузь, галузь оборони та безпеки використовує патенти для зміцнення кібербезпеки, покращення захисту даних, контролю доступу та безпеки зв’язку. Незважаючи на незначне зменшення

кількості патентних заявок, активізація угод і стратегічний найм відображають відданість галузі вдосконаленню заходів кібербезпеки...» ***(Cybersecurity in the aerospace, defense & security industry: analyzing innovation, investment and hiring trends // Verdict Media Limited (https://www.airforce-technology.com/data-insights/cybersecurity-in-ads/?cf-view). 12.09.2023).***

***

«Кібербезпека заслуговує на увагу, яку їй приділяють, але це не все, кінець усього, коли йдеться про те, що в кінцевому підсумку найважливіше для компаній: побудова та збереження довіри з існуючими та потенційними клієнтами. Тим не менш, спеціалісти з безпеки відіграють важливу роль у цьому головному пріоритеті розвитку цифрової довіри у своїх організаціях.

Давайте зробимо крок назад: цифрова довіра, за визначенням ISACA, — це «впевненість у цілісності відносин, взаємодії та транзакцій між постачальниками/постачальниками та клієнтами/споживачами в рамках пов'язаної цифрової екосистеми». У нашому сучасному бізнес-ландшафті цифрова довіра стала необхідною для виживання підприємств. Це те, що часто скеровує споживачів при виборі купувати в певних відомих компаніях, яким вони довіряють, а не в різних альтернативах, навіть якщо покупка коштує трохи дорожче або може бути не такою зручною. Якщо клієнти вам не довіряють, вони знайдуть когось іншого, щоб надати те, що вони шукають.

Цифрову довіру непросто досягти в епоху складних кіберзагроз, технологій, що швидко розвиваються, нормативно-правового ландшафту, що розширюється, і бізнес-моделей у всьому світі, зруйнованих пандемією та новими способами роботи. Безпека, безсумнівно, є ключовим компонентом цифрової довіри, але є й інші необхідні компоненти: якість, доступність, конфіденційність, етичність і чесність, прозорість і чесність, а також стабільність і стійкість. Таке багаторівневе розуміння цифрової довіри показує, що, незалежно від того, наскільки компетентні чи добре забезпечені, команди безпеки не можуть забезпечити цифрову довіру самостійно.

Концепція цифрової довіри починає резонувати у все більшій кількості залів засідань і офісів C-suite, але організаціям може бути важко позбутися замкнутого мислення, яке часто пускає коріння в різні бізнес-функції, включаючи безпеку. Практики безпеки мають чудову можливість кинути виклик цьому способу ведення бізнесу та почати конструктивний діалог у своїх організаціях про важливість міжфункціональних команд. А ще краще — добровільно очолити одну з цих команд: співпрацюйте зі своїми колегами у сферах ризиків, аудиту, конфіденційності, юридичних питань — навіть у тих сферах, про які часто не звертають уваги, як-от маркетинг і HR — і очоліть команду, яка буде прагнути до спільних підходів у досягненні цифрової довіри. Багатофункціональна команда не тільки принесе користь вашій організації, але й керівництво нею, ймовірно, окупиться вашим індивідуальним кар'єрним розвитком.

Крім прийняття міжфункціонального мислення, ще одним важливим способом, за допомогою якого групи безпеки можуть впливати на цифрову довіру, є ефективне реагування на інциденти. Уникнення серйозних інцидентів із безпекою — це, природно, план А, але в цьому небезпечному середовищі загроз іноді трапляються погані речі, незважаючи на всі наші зусилля. Хоча серйозний витік даних може завдати шкоди репутації компанії та підірвати довіру клієнтів, у команд безпеки все ще є можливість зміцнити цифрову довіру в довгостроковій перспективі, залежно від того, як вони впораються з наслідками.

Візьміть SolarWinds як приклад. У 2020 році розробник програмного забезпечення зіткнувся з наслідками великого злому ланцюжка постачання програмного забезпечення, але в кінцевому підсумку перетворив інцидент на можливість посилити свою безпеку та протоколи реагування на інциденти. Не менш важливо те, що компанія прийняла узгоджене рішення стати більш прозорою для клієнтів та інших зацікавлених сторін. «Спочатку ми ділилися інформацією з клієнтами, але не хотіли ділитися всіма деталями. Тепер ми будемо ділитися стільки, скільки вони захочуть, і набагато більше», — сказав Тім Браун, директор з корпоративних технологій SolarWinds. «Це змінило те, як усі наші клієнти оцінюють постачальників. Зараз вони вимагають більш детальної інформації, тому

що ми створили такий прецедент. Створивши цей прецедент, ми показали нашим клієнтам, що вони можуть нам довіряти. Більша прозорість у всьому ланцюжку поставок має вирішальне значення».

Звичайно, організації не повинні — і не повинні — чекати кризи, щоб повідомити про те, що вони роблять, щоб заслужити довіру клієнтів. Враховуючи, якою головною конкурентною перевагою може бути цифрова довіра, організації повинні голосно та з гордістю розповідати публічно історію своїх надійних практик цифрової довіри. Вони можуть вказувати на надійну політику компанії, що охоплює такі важливі теми, як генеративний штучний інтелект, управління даними та керування постачальниками, а також демонструвати відповідні рейтинги безпеки на видних місцях на веб-сайті компанії та в інших зовнішніх матеріалах. Цю прихильність до цифрової довіри також слід підкреслювати в розмовах з потенційними партнерами B2B та іншими важливими зацікавленими сторонами.

Цифрова довіра все частіше ставатиме необхідністю, а не розкішшю для компаній. Перш ніж будь-який клієнт прийме рішення про покупку, перед підписанням будь-якого контракту між діловими партнерами, повинні бути сформовані довірчі відносини. Наявність потужної системи безпеки є необхідним елементом для побудови такої довіри, але сучасний складний бізнес і технологічний ландшафт вимагають узгодженої роботи безпеки в усій організації, щоб створити міцну основу, необхідну підприємствам для успіху. Лідери підприємств завжди шукають те, що відрізняє їх від інших на ринку. Сильна цифрова довіра може стати відмінною рисою для сучасних підприємств, підсилена функціями безпеки, які визнають, як їхня робота підтримує ширшу цифрову екосистему, необхідну для процвітання бізнесу». ***(Pam Nigro. Security's important place in the broader digital trust ecosystem // BNP Media (https://www.securitymagazine.com/articles/99887-securitys-important-place-in-the-broader-digital-trust-ecosystem). 15.09.2023).***

***

«Кібербезпека часто не узгоджується з бізнес-цілями, згідно з дослідженням, проведеним компанією Forrester Consulting, яке виявило, що 97% організацій стикаються з проблемами, намагаючись узгодити пріоритети кібербезпеки з бізнес-результатами.

Понад дев'ять із десяти респондентів (93%) сказали, що їхнім організаціям важко оцінити показники своєї кібербезпеки по відношенню до бізнес-результатів.

Проблема поєднання кібербезпеки та бізнес-цілей була найбільш вираженою у фінансових послугах і страхуванні (47%), а також у медіа, індустрії розваг і дозвілля (також 47%), потім роздрібна та оптова торгівля (43%), комунальні послуги та телекомунікації (38%). вертикалі.

Піюш Панді, генеральний директор Pathlock, пояснив, що кібербезпека часто узгоджується з профілактичними заходами та вважається успішною, коли з компанією нічого не відбувається.

«Бізнес-результати зосереджені на тому, що відбувається — збільшення доходу, економія коштів, підвищення ефективності», — сказав він. Тому ці дві речі часто вважаються суперечливими».

Проте, за словами Панді, інвестиції в пріоритети кібербезпеки (часто через ініціативи CISO) призводять до того, що компанії ефективніше проходять аудит (економія витрат і репутації) або уникають порушень (економія матеріальних витрат і репутації).

«Узгодження пріоритетів кібербезпеки з бізнес-результатами — це питання переосмислення цінності, яку ми знаходимо в кібербезпеці, і показу керівництву керівництва, як це відповідає бізнес-цілям», — говорить він.

Джефф Хейдон, генеральний директор Ontinue, сказав, що справді ефективної комунікації між бізнесом і командами з кібербезпеки завжди було важко досягти, незважаючи на найкращі зусилля та наміри їхніх керівників, це «сумна реальність».

«Нещасним результатом є нездатність повністю узгодити ці пріоритети через брак розуміння», — пояснив він. «Часто цілі бізнес-сторони не втілюються чітко в дієві стратегії для команди з кібербезпеки, що призводить до неузгодженості.

Хейдон додав, що не всі організації мають такі проблеми з розбіжністю: організації, які визнають кібербезпеку як засіб для бізнесу, що дає змогу їхнім співробітникам працювати з будь-якого місця, або що це критично важливо для їхніх зусиль з цифрової трансформації, як правило, мають кращі результати.

Згідно з дослідженням, проблеми узгодження діляться на три основні категорії: суперечливі цілі, складність середовища та вимоги до конфіденційності.

«Дотримання вимог конфіденційності, очевидно, є складною проблемою для більшості компаній», — сказав Хейдон. «Вимоги конфіденційності часто накладають обмеження на те, як можна обробляти дані, що може суперечити бізнес-стратегіям, які вимагають більшого використання відкритих даних».

Він зазначив, що цей конфлікт змушує бізнес балансувати між дотриманням норм конфіденційності та проведенням агресивних бізнес-стратегій.

«Це складна та постійна робота, яку організації, ймовірно, завжди повинні тримати на пульсі», — сказав він.

З точки зору Pandey, лідери безпеки та бізнес-лідери повинні працювати разом, співпрацювати та забезпечувати прозорість, щоб узгодити ініціативи щодо кібербезпеки та відповідності бізнес-цілям.

«У сучасному складному цифровому ландшафті між найкращими практиками кібербезпеки та успішними бізнес-результатами існує як ніколи прямий зв’язок», — сказав він.

Наприклад, для ведення бізнесу на певних ринках багато галузей і уряди вимагають суворого дотримання нормативних вимог від організацій, від федерального уряду й оборони до фінансових послуг і критичної інфраструктури.

«Є багато найкращих практик, які організації повинні застосувати, щоб зруйнувати бар’єри між безпекою та бізнес-лідерами», – сказав він. «По-перше, кібербезпека повинна розглядатися як головний пріоритет для тих, хто приймає рішення на рівні правління».

Це означає, що CISO повинні бути присутніми на всіх засіданнях правління, а ініціативи з кібербезпеки слід активно обговорювати та розглядати на кожному засіданні правління.

По-друге, Панді сказав, що організації повинні визнати, що найкращі практики проактивної кібербезпеки та достатньо фінансовані команди/програми кібербезпеки недешеві і ніколи не будуть такими.

Гейдон зазначив, що компанії, які визнають кібербезпеку як фактор, що сприяє розвитку бізнесу, мають тенденцію до кращого міжфункціонального узгодження, і їхні бізнес-результати досягаються.

«Ефективне збалансування заходів безпеки з бізнес-потребами організації є життєво важливим для забезпечення безперервності бізнесу», — сказав він. «Тісна співпраця забезпечує взаємне розуміння цілей і обмежень, з якими стикається кожна команда».

Це сприяє створенню середовища для співпраці, де стратегії формулюються з урахуванням як бізнес-цілей, так і засобів захисту кібербезпеки, сприяючи більш гармонійній та ефективній операційній стратегії.

«Ставки просто занадто високі для більшого самовдоволення», - зазначив Хейдон. «Враховуючи зростаючу поширеність загроз кібербезпеці та швидку цифрову трансформацію, яку зазнають багато компаній, для організацій ніколи не було так важливо тісно узгодити свої бізнес-стратегії та стратегії кібербезпеки». ***(Nathan Eddy. Cybersecurity Goals Conflict With Business Aims // Techstrong Group (https://securityboulevard.com/2023/09/cybersecurity-goals-conflict-with-business-aims/amp/). 15.09.2023).***

***

«…Інтернет є домом для мільйонів веб-сторінок, баз даних і серверів. Цікаво, що сайти, які ми знаходимо в Google, Bing або Yahoo (тобто сайти, які проіндексовані), є лише верхівкою айсберга. Якщо бути точним, вони складають лише 5% від загального обсягу Інтернету, і це те, що ми називаємо «поверхневою мережею» або «відкритою мережею» – наприклад, вони «відкриті» для доступу для всіх.

Інша частина Інтернету включає приватні бази даних, наукові журнали та багато незаконного вмісту, який не проіндексований. Простіше кажучи, пошукові

системи не ідентифікують ці сторінки, і їх називають «глибоким Інтернетом». Незважаючи на те, що ми не проіндексовані, ми часто користуємося глибоким Інтернетом у нашому повсякденному житті, наприклад, у випадку сторінок, захищених паролем (на основі дозволу), згадайте про соціальні мережі та банківські сайти. Ці веб-сайти є домом для баз даних і вмісту, які, зрештою, формують підсумок послуг, якими ми регулярно користуємося.

Варто зазначити, що темна мережа по суті є частиною глибокої мережі – підмножиною – просто набагато небезпечнішою та обмеженішою. Незважаючи на те, що темна мережа є домом для багатьох законних дій, таких як конфіденційне спілкування між новинними організаціями та їхніми джерелами, вона переважно відома як привабливе місце для купівлі/продажу нелегальної зброї, наркотиків, шкідливого програмного забезпечення та даних. Це притулок для кіберзлочинців завдяки анонімності та зниженому ризику викриття, що забезпечується замаскованими IP-адресами.

Сайти в темній мережі використовують надійне шифрування, щоб завадити органам влади перехоплювати незаконні ринки. Отже, щоб запобігти надходженню та використанню даних у темній мережі, сканування темної мережі має стати регулярною практикою.

Що таке сканування темної мережі?

Темне веб-сканування — це послуга або інструмент, який допомагає вам дізнатися, чи була ваша особиста інформація незаконно опублікована в Інтернеті або, точніше, в темній мережі. Він проактивно шукає в базах даних ваші особисті дані, включаючи фінансові облікові дані та паролі, а також конфіденційні деталі, як-от зображення, відео тощо.

Коли сканування виявляє збіг, воно надсилає сповіщення. Ці сповіщення можуть включати інформацію про місцезнаходження даних, що дає змогу вжити відповідних заходів для посилення захисту, чи то відстеження чи зміна паролів.

Один із найпоширеніших способів потрапляння ваших даних у дарк-мережі – це хакерські атаки чи витоки даних, і якщо ви берете участь у цьому, ви можете навіть не знати, що ваші дані були розкриті. Крім того, з фішинговими атаками з

використанням підроблених веб-сайтів і оманливих електронних листів для отримання особистих даних є ймовірність, що ви можете знати про те, що стали жертвою.

Саме тут сканери темної мережі стають ще більш важливими, допомагаючи вам дізнатися, чи насправді ваші дані настільки безпечні, як ви думаєте.

Мета сканування темної мережі

Темна мережа недоступна через звичайні пошукові системи, тому отримати дані, які знаходяться в цій частині Інтернету, може бути досить складно. Сканування темної мережі — єдиний можливий спосіб зануритися в ці зашифровані бази даних.

Регулярне сканування темної мережі зменшує вікно можливостей для використання викраденої інформації, надаючи вам своєчасне попередження про будь-які дані в небезпеці. У результаті ви зможете швидко змінити свій пароль, скасувати свою кредитну картку або змінити розташування конфіденційних даних у вашій системі до того, як буде завдано будь-якої шкоди, і, сподіваємось, запобігти випадкам крадіжки особистих даних, крадіжки прав власності, кредитної картки шахрайство та торгівля даними.

Окрім підвищення безпеки шляхом виявлення вкрадених даних, сканування темної мережі також використовується правоохоронними органами для виявлення та боротьби з незаконними ринками в Інтернеті, включаючи терористичний контент, неліцензійний або незаконний продаж зброї та наркотиків та інші не менш жахливі речі.

Як працює темне веб-сканування?

Щоб провести сканування темної мережі, вам спочатку потрібно надати деякі дані компанії, яка виконуватиме сканування. Це може включати ваше повне ім’я, адресу електронної пошти, паролі, IP-адресу, дані кредитної картки, номер соціального страхування, інформацію в соціальних мережах тощо.

Потім компанія використовуватиме спеціалізоване програмне забезпечення або інструменти, щоб зіставити ваші дані з каталогами викрадених даних, зазвичай відомих як дампи даних. Якщо йому вдасться зібрати будь-яку інформацію, сканер

негайно надішле вам сповіщення, щоб ви могли вжити необхідних профілактичних заходів.

Тепер, оскільки ви будете ділитися своїми даними зі сканером темної мережі та компанією, яка ним володіє, важливо вибрати надійного та авторитетного постачальника, наприклад NordVPN, який використовує високоякісні та надійні засоби безпеки, зокрема Advanced Encryption Standard. (AES) із 256-бітними ключами, щоб ваші дані залишалися конфіденційними.

Крім того, коли справа доходить до конфіденційної інформації, ви повинні бути впевнені, що попередження про безпеку, які ви отримуєте, є своєчасними та точними, і що ви можете бути впевнені, що все добре, якщо ви не отримуєте жодних. Використання перевіреного та надійного бренду дає вам спокій.

Чи варто використовувати інструмент для сканування темної мережі?

Незважаючи на те, що сканування темної мережі чудово справляється із захистом ваших особистих даних, їм неможливо проглянути кожну пошукову систему на планеті чи всі куточки темної мережі. Це хороша новина для кіберзлочинців – у дарк-мережі продається близько 24 мільярдів імен користувачів і паролів.

Однак це ще не все сумно. Сканери темної мережі забезпечують охоплення ринків темної мережі з найбільшим трафіком, особливо тих, де відсутні додаткові гарантії конфіденційності, як-от сервери даних у популярних місцях темної мережі, включаючи веб-сайти, ринки та форуми.

Незалежно від того, чи йдеться про фізичну особу, компанію чи організацію, крадіжка даних може призвести до величезних збитків як доброї волі, так і грошей. Найгірше те, що ви можете навіть не знати про те, що ваші дані продаються підпільно, якщо, звичайно, ви не використовуєте інструмент сканування темної мережі.

Ще один невеликий недолік сканування темної мережі полягає в тому, що вони є інструментами детектива, а це означає, що ви самі можете вжити будь-яких профілактичних або виправних заходів.

Альтернативи темному веб-скануванню

На жаль, ви не можете дозволити собі розкіш вибирати з безлічі варіантів, коли справа доходить до виявлення витоку або викраденої інформації. Ви можете використовувати або сканування темної мережі, або моніторинг темної мережі – остання в основному є безперервною формою сканування темної мережі, і вона здатна проактивно шукати вкрадені дані, даючи вам трохи більше часу для реагування.

На додаток до них кілька інших інструментів, як-от сканування вразливостей і регулярне тестування на проникнення, забезпечують додатковий захист, виявляючи слабкі місця у вашій системі.

Ці процеси корисні, але найефективнішим заходом безпеки є дотримання гігієни кібербезпеки та оновлення програмного забезпечення. Ось кілька інших звичок, які вам не варто обговорювати:

Надійне керування паролями: ви, мабуть, чули це раніше, але регулярно міняйте свої паролі та намагайтеся використовувати унікальні паролі для всіх своїх основних облікових записів. Менеджер паролів може допомогти вам відстежувати всі ваші дані для входу та навіть створювати для вас надійні паролі.

Двофакторна автентифікація: увімкнення двофакторної автентифікації (2FA) значно покращує вашу цифрову безпеку. Навіть якщо ваша адреса електронної пошти та паролі потраплять у темну мережу, мало ймовірно, що будь-хто зможе ввійти у ваші облікові записи, якщо вони не зможуть зламати цей додатковий рівень безпеки, яким зазвичай є одноразовий пароль, надісланий через SMS-повідомлення. або інші автентифікатори TOTP, такі як Google Authenticator або Authy.

Слідкуйте за своїми фінансами: вам слід часто перевіряти виписки з банківського рахунку та кредитної картки, щоб переконатися, що в транзакціях немає аномалій. Якщо ви помітили транзакцію, яку не впізнаєте, зверніться до свого банку, щоб виконати необхідні подальші дії, наприклад заморозити свої кредитні картки.

Вибір служби сканування темної мережі

Як і в більшості речей, вибір правильного інструменту для роботи має велике значення – і те ж саме стосується сканування темної мережі. Вам краще вибрати відомого постачальника з добре задокументованою безпечною інфраструктурою.

Компанія також повинна мати надійну систему захисту даних і конфіденційності, щоб забезпечити надійне зберігання та захист від можливих вторгнень і витоків інформації, якою ви їй ділитеся.

Я пропоную ознайомитись із найкращими службами VPN, як-от NordVPN і Surfshark, а також Google One, якщо вам потрібен чудовий сервіс, який пропонує моніторинг і сканування в темній мережі разом із багатьма іншими інструментами для підвищення конфіденційності.

Хочете робити покупки самостійно? Не проблема – ось на що слід звернути увагу, вибираючи службу веб-сканування:

Всебічний охоплення: хоча сканувати всю темну мережу за один раз неможливо, найкращі постачальники пропонують максимальне охоплення підпільних ринків для отримання надійних результатів.

Нуль або незначна гарантія хибних спрацьовувань: останнє, що вам потрібно, це зв’язуватися з банківськими установами та блокувати ваші картки, коли ваших даних навіть немає в темній мережі. З цієї причини важливо переконатися, що обрана вами компанія не показує помилкових спрацьовувань.

Ключові показники для допомоги у виправленні ситуації: багато компаній надають вам ключові показники, як-от розташування будь-яких витоку даних, щоб спростити процес відновлення.

Нижня лінія

Темна мережа може бути небезпечним місцем – ніхто не хоче, щоб їхні дані опинилися там. Однак якщо це так, то можна виправити ситуацію до того, як буде завдано серйозної шкоди.

Чи потрібен вам сканер для темної мережі, залежатиме від ваших особистих обставин і ризиків, які ви піддаєте своїй повсякденній діяльності. Сканування може бути просто необхідним для людей із високим ризиком крадіжки особистих даних,

тоді як якщо ви не дуже багато в Інтернеті або тримаєтесь подалі від небезпечних сайтів, вам може не знадобитися регулярне сканування.

Однак, враховуючи, що навіть звичайні люди все частіше стають об'єктами онлайн-шахрайства та шахрайства, краще перестрахуватися, ніж шкодувати. У поєднанні зі здоровими звичками кібербезпеки сканування темної мережі забезпечить вам такий необхідний спокій». ***(Krishi Chowdhary. What is a dark web scan, and should I use one? // Future US, Inc. (https://www.tomsguide.com/features/what-is-a-dark-web-scan-and-should-i-use-one?utm_source=flipboard&utm_content=TomsGuide%2Fmagazine%2FTom%27s+Guide%3A+Full+Edition). 21.09.2023).***

***

«Зміна підходів до кібербезпеки призвела до повільного, але стабільного прогресу в обороні та захисті, але конкуруючі інтереси створюють дедалі більший виклик для тих, хто приймає рішення та практиків у сфері кібербезпеки, показує нове дослідження CompTIA, некомерційної асоціації технологічних працівників і промисловості.

Згідно зі звітом CompTIA «Стан кібербезпеки 2024», більшість професіоналів у сфері бізнесу та технологій вважають, що загальний стан кібербезпеки покращується як загалом, так і в їхніх організаціях. Вони також визнають, що ставки різко зросли, а кількість кіберзлочинців і загроз стрімко зросла. У той же час компанії збирають набагато більше даних, що створює нові наслідки для конфіденційності для клієнтів і операційний ризик для їхніх внутрішніх робочих процесів.

«Навіть невелике підвищення рівня задоволення вітається, але є багато можливостей для вдосконалення», — сказав Сет Робінсон, віце-президент із галузевих досліджень CompTIA. «Підприємства почали розглядати кібербезпеку як критичну функцію. Наступний етап вимагає багатогранного підходу до процесів, політики, людей і продуктів».

Організації реагують на кожен із цих фронтів. Генеративний штучний інтелект (AI) розглядається як інструмент, який може допомогти керувати зростаючою складністю кібербезпеки. Існує підвищена прихильність до навчання робочої сили, включаючи навчання для всього персоналу та підтримку сертифікації для технічних спеціалістів. Управління ризиками та практики нульової довіри набувають все більшого відбитку.

За словами Робінсона, проблема стає ще більшою, оскільки організації проходять через цифрову трансформацію та тісніше пов'язують технологічні ініціативи з успіхом бізнесу.

«Надмірні заходи кібербезпеки можуть перешкодити загальному прогресу, але якщо заходи занадто послаблені, це може призвести до серйозних інцидентів, що призведе до потенційно більших негативних наслідків», – пояснив він. «Це балансування — це робота на повний робочий день. Оскільки технологічні тенденції розвиваються та шаблони атак змінюються, справжньої рівноваги може бути неможливо досягти».

Основними загрозами для організацій є зловмисне програмне забезпечення, на яке вказали 40% респондентів у США, програмне забезпечення-вимагач (33%), злом прошивки (31%), атаки на основі Інтернету речей (31%), атаки на апаратному забезпеченні (31%) і фішинг (30). %). Потенційна шкода від нападу може бути катастрофічною. Серед респондентів у США інциденти кібербезпеки мали серйозний вплив на 22% організацій і помірний вплив на 43%.

CompTIA вважає, що є чотири важливі змінні, які необхідно враховувати, щоб збалансувати рівняння кібербезпеки. У звіті визначено тенденції, на які слід звернути увагу у 2024 році в цих сферах.

Продукт: протягом наступних двох-трьох років компанії бачать широкий спектр можливостей використання генеративного ШІ в кібербезпеці.

Моніторинг мережевого трафіку та виявлення шкідливих програм	53%
Аналіз моделей поведінки користувачів	50%
Автоматизація реагування на інциденти кібербезпеки	48%
Автоматизація конфігурації інфраструктури кібербезпеки	45%

Прогнозування областей, де можуть статися майбутні порушення	45%
Генерація тестів захисту кібербезпеки	45%

Люди: за невеликим відривом головна проблема, з якою стикаються організації, — це прогалина в навичках кібербезпеки. Щоб скоротити розрив, половина американських організацій використовує внутрішнє навчання для вдосконалення навичок кібербезпеки, а 43% допомагають співробітникам пройти сертифікацію для підтвердження своїх знань.

Політика. Управління ризиками стає основним методом оцінки зв'язку між зусиллями з кібербезпеки та бізнес-операціями. Трохи більше половини американських фірм використовують провідний підхід до виявлення та управління ризиками та пов'язаними з ними витратами. Майже 30% оцінюють ризики, але не використовують офіційну систему управління ризиками.

Процес: Побудова процесів кібербезпеки та інтеграція кібербезпеки в бізнес-процеси керує багатьма функціональними рішеннями, від оцінки нових технологій до управління, ризиків і відповідності, до навчання робочої сили. Загальна мета будь-якого процесу, прямого чи непрямого, полягає у відповідності принципам нульової довіри. Незважаючи на те, що лише 28% фірм вважають структуру нульової довіри частиною своєї стратегії, більше організацій дотримуються індивідуальних практик, які зазвичай включені в підхід нульової довіри». ***(Rick Smith. Cybersecurity tug-of-war intensifies but progress being made, new report says // WRAL TechWire (https://wraltechwire.com/2023/09/21/cybersecurity-tug-of-war-intensifies-but-progress-being-made-new-report-says/?amp=1). 21.09.2023).***

***

«…Кібербезпека – це сфера, яка має широкий спектр тем, від реагування на інциденти до етичного хакерства та від криптографії до безпеки мережі. Наявність різноманітності ускладнює кібербезпеку для новачків. Швидкий розвиток технологій змусив фахівців з кібербезпеки бути в курсі не тільки для того, щоб отримати прихильність цієї технології, але й для того, щоб усунути недоліки, які включають останні загрози та захист, пов'язані з процесом.

1.1 Технічні аспекти кібербезпеки

Технічний характер кібербезпеки змусив людей сприймати її як складне завдання. Такі поняття, як шифрування, брандмауери, виявлення вторгнень і системи безпеки, виявилися складними для багатьох новачків. Людина повинна добре та міцно розуміти комп'ютерну мову, протоколи безпеки комп'ютерних систем та комп'ютерні мережі.

1.2 Загрози, що розвиваються

Постійно мінливий ландшафт кіберзагроз додає ще один рівень проблем і складності. Ця сфера потребує постійної адаптації та навчання змінам, які регулярно відбуваються. Це динамічне середовище може налякати тих, хто тільки починає, через регулярну появу нових векторів атак і методів.

2. Ресурси для вивчення кібербезпеки

Наявність різноманітних ресурсів для онлайн-курсів відіграє вирішальну роль у визначенні легкості навчання та зменшенні тягаря ваших сумнівів під час вивчення кібербезпеки. На щастя, існує велика кількість навчальних матеріалів і курсів, призначених для новачків, а також для учнів усіх рівнів.

2.1 Онлайн-курси

Кілька онлайн-платформ пропонують курси з різних аспектів кібербезпеки. У нас є багато таких прикладів, як...

2.1.1Coursera

Coursera пропонує широкий вибір курсів з кібербезпеки від університетів і інституцій з усього світу. Курси охоплюють такі теми, як концепції кібербезпеки та нові технології, такі як етичне хакерство, мережева безпека та криптографія.

2.1.2 edX

edX надає доступ до курсів таких університетів, як Масачусецький технологічний інститут і Гарвард, з варіантами як для початківців, так і для досвідчених.

2.2 Сертифікати про навчання

Нам завжди потрібні підтвердження наших знань, а сертифікати є найціннішим способом підтвердження своїх знань і навичок у галузі кібербезпеки.

Деякі популярні та цінні сертифікати в цій галузі, які часто визнаються та поважаються роботодавцями, наведені нижче:

Безпека CompTIA+

Сертифікований спеціаліст з безпеки інформаційних систем (CISSP)

Сертифікований етичний хакер (CEH)

2.3 Книги та підручники

Знання для вивчення кібербезпеки доступні в будь-якому середовищі від електронних носіїв, таких як підручники та онлайн-класи, до друкованих носіїв, таких як книги. Існує величезний вибір книг і онлайн-підручників для самостійного навчання. деякі з них – «Хакерство: Мистецтво експлуатації» Джона Еріксона, «Основи мережевої безпеки» Вільямса Столлінгса та «Прикладна криптографія» Брюса Шнайера. Різноманітні блоги та канали YouTube, оскільки багато експертів у цій галузі ведуть блоги та канали, які пропонують різноманітні навчальні посібники, поради та інформацію, щоб детально вивчити кібербезпеку.

3. Крива навчання

Складність вивчення кібербезпеки також залежить від поточного рівня технічних знань і досвіду учня. Для тих, хто має міцну основу в IT або комп'ютерній інженерії чи науці, перехід до кібербезпеки може бути легким і гладким порівняно з новачками. З іншого боку, повному новачку може знадобитися витратити трохи часу на розуміння основ, перш ніж заглиблюватись у складні теми.

4. Практичні знання

Ми всі знаємо, що практичні знання мають вирішальне значення для незалежних експертів і дослідників з кібербезпеки, але практичний досвід також має таке ж значення в спільноті кібербезпеки. Доступні налаштування Labs, проведення експериментів і участь у CaptureThe Flag змаганнях (CTF). Це безцінні способи застосування вивченого в практичному контексті.

5. Менталітт учня з кібербезпеки

Настрій експерта з кібербезпеки, професіонала чи учня ніколи не повинен бути негативним, крім технічних навичок і знань, учень повинен культивувати певні настрої, як-от:

5.1 Цікавість

Допитливий розум необхідний не лише тим, хто вивчає кібербезпеку, але й тим, хто вивчає будь-яку галузь. Це спонукає людей досліджувати, запитувати та розуміти, як працює система та як її можна скомпрометувати.

5.2 Наполегливість

Кібербезпека – це сфера, яка відома невдачами та проблемами, які неминучі у повній кар'єрі чи кар'єрі в галузі кібербезпеки. У цій сфері необхідна стійкість, щоб подолати труднощі та продовжувати навчання.

5.3 Етична відповідальність

Найважливішим у курсі кібербезпеки чи курсах у будь-якій галузі є етика. Етичні міркування мають першорядне значення в кібербезпеці. Не тільки ті, хто навчається, але й у цій галузі повинні розуміти та дотримуватися етичних принципів хакерства, використовуючи свої знання для загального блага.

5.4 Безперервне навчання

Раніше вже згадувалося, що ландшафт кібербезпеки постійно розвивається та реформується. У цьому випадку хтось може втомитися від вивчення шаблону, що постійно змінюється, але він повинен взяти на себе зобов'язання постійного навчання. Це важливо для інженера з кібербезпеки, щоб випереджати нові загрози кібербезпеці.

6. Переваги вивчення кібербезпеки

Ми всі знаємо, що вивчення навичок кібербезпеки є важливим, але це також приносить певні переваги. Вивчення навичок кібербезпеки забезпечує практичні професійні та особисті переваги, які виходять далеко за рамки захисту ваших активів, це важливий набір навичок кібербезпеки в сучасному взаємопов'язаному світі, якому може навчитися будь-хто. Нижче наведено низку цінних переваг у цифровому світі. -

6.1 Захист особистої інформації

Розуміння кібербезпеки допоможе вам захистити вашу особисту інформацію, таку як фінансові дані, облікові записи в соціальних мережах і приватне спілкування, від кібернетичних впливів

6.2 Професійний розвиток

На поточному ринку праці існує високий попит на фахівців з кібербезпеки, які вивчають кібербезпеку, що може відкрити нові можливості для широкого кола компаній і організацій.

6.3 Запобігання крадіжці особистих даних

Знання безпеки дають вам змогу розпізнавати та запобігати крадіжці особистих даних, яка поширена в онлайн-світі.

6.4 Безпечні онлайн-трансакції

Це дозволяє вам проводити безпечні транзакції, не побоюючись фінансових втрат або шахрайства, що сьогодні викликає серйозне занепокоєння.

6.5 Захист ділових інтересів

Якщо ви хочете вести бізнес або працювати на когось, розуміння кібербезпеки має вирішальне значення для захисту конфіденційної інформації компанії, як-от даних клієнтів та інтелектуальної власності.

6.6 Управління репутацією

Як для окремих осіб, так і для компаній порушення кібербезпеки можуть призвести до погіршення репутації. Знання, як захистити цифрові активи, може запобігти таким інцидентам. Це допоможе розвивати ваш бізнес, а також зробить вас надійними.

6.7 Пом'якшення фінансових втрат

Знання кібербезпеки можуть допомогти вам не стати жертвою онлайн-шахраїв, фішингових атак, програм-вимагачів та інших кіберзагроз, які можуть призвести до фінансових втрат.

6.8 Відповідність і регулювання

У багатьох галузях промисловості існують особливі вимоги щодо захисту конфіденційної інформації. Знання кібербезпеки допомагає дотримуватися цих правил.

6.9 Тестування хакерства та федерації

Вивчення кібербезпеки може надати можливості для етичного хакерства та тестування на проникнення, де ви можете використовувати свої навички, щоб допомогти організаціям виявляти та виправляти вразливості.

6.10 Критичне мислення та вирішення проблем

Кібербезпека передбачає багато критичного мислення, вирішення проблем і увагу до деталей. Ці навички цінні не лише в кібербезпеці, але й у різних професійних та особистих контекстах.

6.11 Пропаганда кібербезпеки

Маючи знання про кібербезпеку, ви можете пропагувати та навчати інших безпечним онлайн-практикам, допомагаючи створити більш безпечне цифрове середовище для всіх, хто цього потребує.

6.12 Національна та громадська безпека

Кібербезпека відіграє вирішальну роль у національній та громадській безпеці. Розуміння кіберзагроз і способів захисту від них сприяє загальній безпеці суспільства.

6.13 Постійне навчання та адаптація

Сфера кібербезпеки є динамічною, у ній регулярно з’являються нові загрози та технології. Вивчення кібербезпеки заохочує мислення про постійне навчання та адаптацію.

6.14 Розширення особистих можливостей

Знання того, як захистити себе та свої цифрові активи, дає вам відчуття розширення можливостей в Інтернеті та робить вас більш видатним і впливовим.

6.15 Глобальний вплив

Кібербезпека не обмежена кордонами. Ваші знання та навички дізнаються, що індустрія кібербезпеки може мати глобальний вплив, сприяючи створенню більш безпечного цифрового середовища для людей у всьому світі.

7. Висновок

Отже, чи важко навчитися кібербезпеці? Що ж, відповідь має нюанси. Хоча ландшафтна сфера кібербезпеки постійно розвивається, загроза може бути страшною. Тим не менш, доступність таких ресурсів, як онлайн-курси, книги та

навчальні посібники з відданістю учнів, відіграє вирішальну роль у навчанні навичкам кібербезпеки. Інші не менш важливі фактори, як-от доступ до якісної освіти та прагнення до практичної практики, люди можуть отримати знання та навички, необхідні для ефективної навігації у світі кібербезпеки.

Не забувайте, що кібербезпека – це не просто ступінь технічного коледжу чи ступінь кібербезпеки; це мислення та відданість захисту цифрового світу. Цьому можна навчитися будь-яким засобом: формальна освіта, онлайн-курси, сертифікати чи самостійне навчання. Є широкі можливості для тих, хто бажає вчитися та вирушити в цю вирішальну подорож. Натисніть тут, щоб прочитати більше». ***(Risha. Is Cybersecurity Hard to Learn? 15 Perks of Learning Cybersecurity! // USA Tales (https://usatales.com/is-cybersecurity-hard-to-learn-15-perks-of-learning-cybersecurity/). 21.09.2023).***

***

«Протягом останніх років ви постійно зустрічаєте термін «технологія блокчейн», як правило, у контексті криптовалют, таких як біткойн. Насправді ви можете розмірковувати: «Що таке технологія блокчейн?» Схоже, що блокчейн — це звичайна фраза, але в теоретичному сенсі їй не вистачає легко зрозумілого визначення для середньої людини. Надзвичайно важливо з’ясувати, «що таке технологія блокчейн», охоплюючи використовувану технологію, її операційну механіку та те, як вона змінює правила гри для кібербезпеки.

Що таке технологія блокчейн?

Відповідно до IBM, блокчейн визначається як «колективна, незмінна книга, яка спрощує завдання документування транзакцій і нагляду за активами в корпоративній мережі».

Він функціонує як система для безпечного, відкритого та економічного відстеження будь-чого цінного.

Термін «блокчейн» походить від того, що кожна транзакція документується як «блок» даних. Блок може документувати кілька категорій даних, таких як кількість, вартість або позиція.

Коли актив переходить від власника до власника, ці блоки з'єднуються, утворюючи ланцюг. Ланцюжок охоплює деталі кожної транзакції, включаючи їх час і послідовність.

Блокчейн не має єдиної точки відмови. Кожен ланцюжок є незмінним, тому будь-який учасник не зможе розірвати посилання, щоб створити блок. Зміна одного з цих криптографічних ланцюжків майже немислима, оскільки взаємоприйнятий механізм консенсусу перевіряє правильність кожної транзакції в ланцюжку.

Кіберзагрози розвиваються з роками

Витрати на кібербезпеку, включно з Cyber Security Chicago, зазнали експоненціального зростання протягом останнього десятиліття, не демонструючи жодних ознак уповільнення. Згідно з галузевим звітом, організації по всьому світу мають намір виділити понад 1 трильйон доларів на захист від онлайн-загроз у період з 2017 по 2021 рік.

Незважаючи на ці вражаючі фінансові зобов'язання, зловмисники продовжують використовувати як добре відомі, так і нерозголошені вразливості, а також перехоплювати пристрої, програми та мережеві комунікації. CB Insights підрахувала, що приблизно 6 мільярдів конфіденційних файлів було вкрадено протягом періоду, що охоплює 2017-2018 роки. Інші галузеві дослідження показують зростання як кількості, так і вартості кібератак.

Ці хитромудрі атаки часто перевершують звичайні методи безпеки, включаючи автентифікацію, керування ключами, криптографію та проблеми конфіденційності. Оскільки через пандемію коронавірусу значна частина робочої сили зараз працює з дому, уразливі місця проявляються новими способами. Отже, замість того, щоб розробляти більш потужні інструменти, численні підприємства переоцінюють системи, які спочатку спричинили ці вразливості.

Як технологія блокчейн може революціонізувати кібербезпеку?

Коли лише близько 10 років тому блокчейн став основою для біткойнів, він став значною мірою взаємозамінним з криптовалютою в народній мові. Тим не менш, інші реалізації блокчейну, як-от Ethereum, стали основою для низки функцій, які виходять за рамки криптовалют. Серед них смарт-контракти, невзаємозамінні

токени (NFT), децентралізоване фінансування та розповсюджене програмне забезпечення тощо.

Децентралізована, керована консенсусом, ненадійна природа блокчейна за своєю суттю робить його стійким до атак. Для тих блокчейн-рішень, які використовують методи перевірки доказів роботи (наприклад, біткойни), зловмисники повинні захопити контроль над більшістю вузлів, щоб скомпрометувати транзакції реєстру — те, що навмисно потребує обчислень. Ці обчислювальні витрати можна застосувати до різних інших операцій безпеки, тим самим зменшуючи потребу в надійному центральному органі.

Численні атаки розподіленої відмови в обслуговуванні (DDoS) використовують сервери доменних імен Інтернету (DNS), які перетворюють IP-адреси на зручні для користувача імена веб-сайтів. Завдяки переміщенню DNS у блокчейн активи можна поширювати між численними вузлами, що робить неправдоподібним втручання зловмисників у базу даних.

Вплив блокчейну на кібербезпеку?

Блокчейн представляє альтернативний шлях до покращеної безпеки, менш відвідуваний і набагато менш привітний для кіберзлочинців. Цей метод зменшує вразливість, забезпечує надійне шифрування та ефективніше перевіряє право власності та цілісність даних. Це може навіть усунути необхідність певних паролів, які часто називають найслабшою ланкою кібербезпеки.

Децентралізація

Blockchain використовує децентралізовану систему розподіленого реєстру замість того, щоб покладатися на єдиний довірений центральний орган. Через технологію розподіленого реєстру (DLT) транзакції реєструються на кожному вузлі в мережі, створюючи суттєві перешкоди для кіберзлочинців, які намагаються спостерігати, викрасти або підробити дані. Його створено, щоб викликати довіру між учасниками в доменах, де довіра часто невловима.

Спільний консенсус

Алгоритм спільного консенсусу блокчейнів дозволяє безперервно відстежувати облікову книгу для виявлення незвичайної або зловмисної активності.

Надійні методи шифрування

Блокчейн-мережі вміло використовують шифрування та цифрові підписи, використовуючи інфраструктуру відкритих ключів для:

- Перевірка змін у конфігураціях
- Аутентифікаційні пристрої
- Охорона комунікацій

Інфраструктура, що містить асиметричні криптографічні ключі та цифрові підписи, часто є основою технології блокчейн, забезпечуючи перевірку права власності на дані та цілісність даних. У деяких випадках ці компоненти заперечують необхідність паролів, звичайного способу, за допомогою якого кіберзлочинці незаконно отримують доступ до облікових записів і мереж.

Незмінні записи

Блокчейн-реєстр залишається невразливим до змін. Якщо запис містить помилку, її можна виправити, ініціювавши іншу транзакцію, що призведе до збереження обох транзакцій.

Захист IoT

З розширенням спектру додатків у різних секторах пристрої Інтернету речей (IoT) часто стають жертвами кіберзлочинців через їх природні вразливості. Blockchain пропонує покращений захист для користувачів пристроїв IoT.

Запобігання DDoS-атакам

Атака розподіленої відмови в обслуговуванні (DNS) намагається заповнити сервер запитами, зазвичай націленими на фокусну точку, таку як IP-адреса або обмежена група IP-адрес.

Тим не менш, система доменних імен (DNS) на основі блокчейну може усунути цей єдиний фокус, ефективно нейтралізуючи цю кіберзагрозу.

Конфіденційність даних

Хоча прозорість блокчейну є основною перевагою, коли всі учасники можуть переглядати незмінні транзакції, дозволена мережа блокчейну дозволяє лише надійним мережам спостерігати за транзакціями або брати участь у них. Цього можна досягти за допомогою мінімального управління.

Більше того, блокчейну бракує звичайних цілей, до яких прагнуть кіберзлочинці, що ускладнює для них отримання несанкціонованого доступу через використання правил конфіденційності.

Безпека розумного контракту

Розумні контракти, які складаються з попередньо визначених правил, що зберігаються в блокчейні, запускають транзакції після виконання визначених умов. Цей автоматизований процес підвищує зручність платежів. Блокчейн залишається безпечним завдяки ретельному тестуванню його компонентів на автентифікацію, безпеку даних, контроль доступу та перевірку бізнес-логіки.

Висновок

Використовуючи інфраструктуру Blockchain, дуже легко запобігти крадіжкам даних і атакам на кібербезпеку в пристроях і мережах IoT. Крім того, Blockchain можна використовувати для захисту систем IoT, які часто схильні до витоку даних. Використовуючи цю структуру, ми можемо захистити хмарні обчислення/системи зберігання даних, які також є вразливими до зловмисних атак». ***(Rufaro Sithole. Blockchain Technology: A Game Changer for Cybersecurity? // Eyetro Digital (https://www.eyetrodigital.com/post/38/2023/9/blockchain-technology-a-game-changer-for-cybersecurity-2). 20.09.2023).***

***

«Згідно з нашим новим рецензованим дослідженням, працівники, які працюють віддалено, краще усвідомлюють загрози кібербезпеці, ніж ті, хто проводить більшу частину свого часу в звичайному офісі, і, швидше за все, вживуть заходів, щоб їх захистити.

Наші висновки ґрунтуються на даних опитування Amazon Mechanical Turk, зібраних від 203 учасників, які нещодавно перейшли на віддалену роботу на повний робочий день, а також від 147 офісних співробітників у багатьох організаціях у Сполучених Штатах. Ми не збирали дані про гібридних працівників.

Ми поставили співробітникам ту саму низку запитань про їхні робочі місця, а також про їхнє розуміння загроз кібербезпеці та дії, які вони вжили для захисту від них.

Щоб врахувати інші фактори, які можуть вплинути на те, як працівник реагує на передбачувані загрози та ризики кібербезпеці, ми врахували ключові характеристики учасників і різні фактори, зокрема вік, стать, тип галузі, розмір компанії, посаду та тривалість віддаленої роботи. Крім того, ми намагалися забезпечити надійність наших даних, консультуючись з іншими експертами та використовуючи різні статистичні методи.

Ми виявили, що віддалені працівники в середньому більше усвідомлювали загрози кібербезпеці та могли краще розпізнавати безпечні практики кібербезпеки та заходи захисту порівняно з офісними працівниками. Подібним чином наші дані показали, що віддалені працівники з більшою ймовірністю вживатимуть заходів обережності щодо кібербезпеки, ніж їхні колеги в офісі.

Чому це може бути так?

Коли співробітники працюють в офісі, вони, як правило, очікують, що їхня організація забезпечить і запровадить контрзаходи безпеки для боротьби з кіберзагрозами та ризиками. У результаті офісні працівники можуть стати самовдоволеними щодо обізнаності з кібербезпекою. Це може пояснити, що офісні працівники вживають менше кроків для зміцнення своєї кібербезпеки.

Навпаки, відсутність інституційної структури кібербезпеки змушує віддалених працівників бути більш уважними до ризиків, яким вони можуть наражатися.

Чому це важливо

Співробітники є першою лінією захисту від атак на кібербезпеку, кількість яких зростає. За даними Check Point Research, яка надає дані про кіберзагрози, кількість кібератак у всьому світі у 2022 році зросла на 38%.

І один із основних способів, якими хакерам вдається проникнути в корпоративні комп’ютерні мережі, – це через співробітників – наприклад, за допомогою фішингового електронного листа.

У перші дні пандемії COVID-19, коли більшість робочої сили було відправлено додому через карантини, кібербезпека викликала велике занепокоєння. На жаргоні кібербезпеки це збільшило «поверхню атаки» або сукупність усіх способів, у які мережа організації піддається потенційним ризикам безпеці. Компанії хвилювалися, чи будуть співробітники, які працюють віддалено, серйозно ставитися до кібербезпеки.

Оскільки віддалена робота все більше стає нормою для багатьох компаній, наше дослідження показує, що цей ризик не такий великий, як раніше побоювалися…

Що досі невідомо

Нам ще потрібно визначити, чи зменшиться підвищена обізнаність щодо кібербезпеки та запобіжна поведінка серед віддалених працівників з часом. Дослідження показують, що обізнаність щодо кібербезпеки, набута завдяки навчанню та програмам знань, має тенденцію з часом розсіюватися.

У зв'язку з тим, що віддалена робота стає все більш загальноприйнятою, чи настає безпека для цих працівників? Важливо знати, як довго підвищена обізнаність щодо кібербезпеки дозволить вживати заходів обережності та як віддалені працівники можуть відновити та підтримувати цю пильність». ***(Joseph K. Nwankpa, Pratim Milton Datta. Remote workers are more aware of cybersecurity risks than in-office employees: new study // The Conversation Media Group Ltd (https://theconversation.com/remote-workers-are-more-aware-of-cybersecurity-risks-than-in-office-employees-new-study-207801?utm_source=flip). 26.09.2023).***

***

«Елементарна гігієна безпеки є більш впливовою, ніж ви можете собі уявити. Хоча в галузевих заголовках часто домінують новітні технології та найновіші програмні чи апаратні рішення, гігієна базового рівня безпеки все ще захищає від 98% атак. Це включає такі заходи, як застосування принципів нульової довіри або підтримка систем в актуальному стані за допомогою останніх виправлень безпеки.

Однак, незважаючи на обіцянки цих основних гігієнічних заходів безпеки, багато організацій все ще не використовують їх належним чином. Якщо ми розглядаємо нульову довіру, то, наприклад, «Звіт Microsoft Digital Defense Report 2022» показує, що 93% заходів з відновлення програм-вимагачів виявили недостатній доступ до привілеїв і бічний контроль переміщення — це суперечить принципу нульової довіри щодо доступу з найменшими привілеями.

Проте хороша новина полягає в тому, що ніколи не пізно запровадити базову гігієну безпеки у власній організації. Продовжуйте читати про три головні елементи гігієни безпеки, які ви можете не помітити.

Стійкий до фішингу MFA

Якщо ввімкнути належним чином, багатофакторна автентифікація (MFA) є значним стримуючим фактором для кіберзлочинців. Часто зловмисники зосереджені на пошуку легкої мішені, тому MFA допомагає підвищити цей бар'єр для проникнення, вимагаючи від злочинців знати або зламати більше одного пароля чи методу підтвердження. Насправді MFA має можливість блокувати 99,9% атак компрометації облікового запису.

Однак, щоб бути ефективним, ваше рішення MFA має бути максимально простим для користувачів. Можливі варіанти MFA без тертя включають біометричні дані пристрою або сумісні з FIDO2 фактори, такі як ключі безпеки Feitan або Yubico.

MFA також слід застосовувати стратегічно, щоб захистити конфіденційні дані та критично важливі системи. Замість того, щоб покладатися на MFA для захисту кожної окремої взаємодії, організаціям слід вибрати політики умовного доступу, які запускають двоетапну перевірку на основі виявлення ризиків, а також наскрізну автентифікацію та єдиний вхід.

Сучасний засіб захисту від шкідливих програм

Інструменти розширеного виявлення та реагування (XDR) є критично важливими для виявлення та автоматичного блокування загроз, як-от атаки зловмисного програмного забезпечення. Це також допомагає надати своєчасну

інформацію групі безпеки, щоб вони могли бути більш гнучкими, реагуючи на загрози.

Ми рекомендуємо використовувати автоматизацію безпеки, впроваджуючи датчики, які автоматизують, співвідносять і пов'язують результати перед тим, як надсилати їх аналітику. Мета тут полягає в тому, щоб аналітик операцій із безпеки мав відповідну інформацію, необхідну для сортування та швидкого реагування на попередження. Організації також можуть зосередитися на автоматизації своїх систем визначення пріоритетів сповіщень, а також будь-яких загальних адміністративних процесів і робочих процесів операцій безпеки.

Захищайтеся від загроз у всіх робочих навантаженнях, використовуючи комплексні можливості запобігання, виявлення та реагування за допомогою інтегрованих XDR і керування інформацією та подіями безпеки (SIEM) можливостей. Важливо також знати про будь-які застарілі системи, якими ви зараз користуєтеся, оскільки в них можуть бути відсутні засоби контролю безпеки, наприклад антивірусні засоби та рішення для виявлення та реагування на кінцеві точки (EDR). Подібним чином слідкуйте за своїм середовищем, щоб зловмисники вимкнули безпеку. Відомо, що групи загроз очищають журнали подій безпеки та операційні журнали PowerShell як частину більшого ланцюга атак.

Захист даних

Нарешті, ви не можете запровадити достатній захист для своєї організації, якщо не знаєте, де розташовані ваші важливі дані та чи впроваджено правильні системи. Це особливо критично в сучасних гібридних робочих середовищах, які вимагають від користувачів доступу до даних із кількох пристроїв, програм, служб і географічних місць.

Глибокий підхід до захисту — це один із способів покращити безпеку ваших даних, щоб захистити від крадіжки чи витоку даних. Розробляючи цей підхід, переконайтеся, що у вас є повна видимість усіх ваших даних, включаючи будь-які локальні, гібридні чи багатохмарні розташування. Вам також потрібно буде правильно позначити та класифікувати свої дані, щоб зрозуміти, як до них здійснюється доступ, як вони зберігаються та надають спільний доступ.

Коли це буде зроблено, зосередьтеся на управлінні інсайдерським ризиком, досліджуючи контекст користувача навколо даних і те, як їх діяльність може призвести до потенційних інцидентів безпеки даних. Це також має включати впровадження належного контролю доступу, щоб запобігти неналежному зберіганню, зберіганню або друкуванню конфіденційних даних.

Нарешті, управління даними зміщується в бік бізнес-команд, які стають розпорядниками своїх власних даних. Це означає, що організаціям потрібен уніфікований підхід до управління даними для всього підприємства. Таке проактивне керування життєвим циклом може сприяти покращенню безпеки даних і демократизації.

Кібербезпека може бути постійною справою, але вона не завжди повинна бути складною. При належному застосуванні прості гігієнічні заходи безпеки можуть значно підвищити рівень безпеки». ***(Cyber Hygiene: A First Line of Defense Against Evolving Cyberattacks // Informa PLC (https://www.darkreading.com/microsoft/cyber-hygiene-a-first-line-of-defense-against-evolving-cyber-attacks?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 25.09.2023).***

***

«У цифрову еру спосіб оплати послуг і товарів зазнав глибоких змін. Зростання цифрових платіжних екосистем створило все більш взаємопов'язаний світ, де гроші та капітал безперебійно течуть усередині та через кордони. Це полегшило підприємствам і споживачам здійснення платежів, але також зробило їх більш уразливими до кіберзлочинності.

Кібербезпека відіграє вирішальну роль в успіху цієї екосистеми, тому компанії по всьому світу витрачають понад 70 мільярдів доларів на дослідження та розробки в галузі кібербезпеки. У всьому світі фінтех-компанії зазнали в 2,5 рази більше атак у першому кварталі 2022 року, ніж у тому ж кварталі попереднього

року. Ця цифра підкреслює необхідність захисту конфіденційних фінансових даних для запобігання шахрайству та забезпечення конфіденційності.

Усвідомлюючи загрозу, уряд Індії активізував свої зусилля з кібербезпеки. У лютому цього року для покращення інфраструктури кібербезпеки країни Міністерству електроніки та інформаційних технологій (MeitY) було виділено 625 крор рупій. Цей фонд також буде виділено на проекти з кібербезпеки та використовуватиметься групою реагування на кібербезпеку: Індійською групою реагування на надзвичайні ситуації з комп'ютерами (CERT-In). Виділена сума свідчить про прагнення Індії побудувати надійну інфраструктуру кібербезпеки.

За іронією долі, хоча загроза, яку створюють кіберзлочинці, реальна, для експертів з кібербезпеки вона дає можливість.

Можливість попереду

Розширення цифрової економіки створило ринкові можливості в 2 трильйони доларів для постачальників технологій і послуг кібербезпеки. Ця можливість виникає завдяки дедалі більшому впровадженню таких технологій, як шифрування, багатофакторна автентифікація, біометрія та штучний інтелект.

Відповідно до останнього прогнозу Canalys щодо кібербезпеки, інвестиції в кібербезпеку зростуть на 13% у 2023 році. У 2023 році малі та великі організації відчувають потребу розширити та поглибити захист кібербезпеки, розширити можливості виявлення та покращити реагування на інциденти для захисту від цифрових злочинів.

Для експертів з кібербезпеки в Індії ця спроба покращити кібербезпеку є можливістю. Кібербезпека також відіграватиме важливу роль у допомозі Індії зберегти свої позиції провідної цифрової економіки.

Кібербезпека: життєво важлива для індійських фінансових технологій і майбутнього

Кібербезпека має життєво важливе значення для фінтех-сектору Індії та майбутнього країни як цифрової держави. Економічне дослідження 2023 показало, що індійські споживачі швидко впроваджують фінтех-продукти. Цитуючи останній

Global FinTech Adoption Index, у звіті зазначено, що 87% індійців перейняли fintech, тоді як середній глобальний показник становить 64%.

Фінтех-компанії, які мають надійну структуру кібербезпеки та надійну платформу, можуть забезпечити величезні соціальні та економічні переваги, сприяти фінансовому охопленню та допомагати малому бізнесу розвиватися. Ці компанії використовують штучний інтелект і машинне навчання, щоб прискорити фінансову доступність шляхом автоматизації більшості процесів. Наприклад, фінтех-компанії, залучаючи малий бізнес до своїх платформ і дозволяючи ШІ аналізувати кредитоспроможність таких фірм, швидко видають кредити кредитоспроможним підприємствам. Залізна кібербезпека відіграє важливу роль у забезпеченні того, щоб такі виплати були вільними від шахрайства.

Такі технології, як штучний інтелект та машинне навчання, також допомагають швидко виявляти випадки дефолту та запобігають виплаті капіталу позначеним особам – і все це без втручання людини. Щоб переконатися, що такі рішення не є упередженими, вони підтримуються надійними та прозорими алгоритмами. Завдяки моніторингу за допомогою штучного інтелекту ті, хто використовує фінтех-платформи, насолоджуються безпроблемним досвідом, що призводить до більшої фінансової доступності в Індії.

Щоб Індія зберегла свою позицію ключового гравця в цифровій економіці, країна повинна приділяти більше уваги, ніж раніше, пом’якшенню загроз і виправленню вразливостей. Це забезпечить стійкість платіжних систем.

Незважаючи на досягнутий прогрес, потреба у зміцненні кібербезпеки ніколи не була такою великою.

Fintech має відповідати викликам кіберзлочинців

Звіт за 2019 рік показав, що майже 100% фінтех-компаній мали проблеми, пов’язані з конфіденційністю, безпекою та відповідністю через API, субдомени та залишені веб-додатки. У 2023 році ці загрози набагато складніші та небезпечніші для компанії. Нехтування заходами безпеки має негативний вплив на компанію, її персонал і клієнтів.

Останні дані Індійської групи реагування на комп'ютерні надзвичайні ситуації (CERT-In) підкреслюють, що в 2022 році в Індії сталося багато інцидентів кібербезпеки. У цьому році було зареєстровано 13,91 лакх випадків. Із збільшенням оцифровки зростатиме як кількість, так і складність таких атак.

Крім того, кіберзлочинність стає все більш складною. Загрозу кіберзлочинності посилює той факт, що до кінця 2023 року Індія зіткнеться з нестачею близько трьох мільйонів співробітників кібербезпеки. Ця нестача створює серйозну проблему для організацій. Підприємствам і компаніям буде важче ефективно керувати своєю кібербезпекою та оперативно реагувати на нові загрози.

Це вагомі причини для компаній захищати дані та мережі, а також використовувати шифрування, протоколи безпеки, ідентифікацію ризиків і управління ризиками, щоб уникнути витоку даних, крадіжки особистих даних, грошових втрат тощо». ***(Suresh Sharma. Fintechs must brace for rising cybersecurity challenges // HT Digital Streams Ltd (https://www.livemint.com/opinion/first-person/fintechs-must-brace-for-rising-cybersecurity-challenges-11695629860002.html?utm_source=flipboard&utm_content=other). 25.09.2023).***

***

«Історично IT (information technology) та OT (operational technology) працювали в різних світах, кожен з яких мав різні цілі та протоколи. IT, сформовані цифровою епохою, завжди наголошували на захисті цілісності даних і конфіденційності. У цьому просторі витік даних може призвести до значних наслідків, що робить надзвичайно важливим посилення цифрового захисту. З іншого боку, OT, спадщина промислової революції, спрямована на забезпечення безперебійної роботи машин і процесів. Будь-який простой машини може призвести до значних втрат виробництва, тому доступність і безпека системи є головним пріоритетом.

Ця різниця у фокусі створила помітний культурний розрив. IT-команди, які часто глибоко займаються управлінням даними, можуть не повністю усвідомити

реальний вплив зупинки виробничої лінії. Подібним чином команди OT, тісно пов'язані зі своїми машинами, можуть не помітити ширшого впливу витоку даних.

Технічні проблеми настільки ж значні. Системи OT складаються зі спеціалізованого обладнання, багато з яких було створено ще до того, як кібербезпека стала пріоритетом. Коли ці старі системи підключаються до сучасних IT-мереж, вони можуть стати слабкими місцями, відкритими для сучасних кіберзагроз. Цей ризик ще вищий, оскільки багато систем OT використовують унікальні протоколи та апаратне забезпечення. Ці системи, колись ізольовані, тепер є частиною більш розгалужених мереж, що робить їх доступними та вразливими через різні точки в мережі організації.

Крім того, звичайні IT-завдання, як-от оновлення програмного забезпечення, можуть бути складнішими в OT. Обладнання в OT часто має особливі вимоги від своїх виробників. Те, що є стандартом в IT, може стати складним завданням в OT через особливу природу його систем.

Поєднання IT та OT — це більше, ніж просто технічне завдання; це суттєва зміна в тому, як компанії бачать ризики та керують ними. Від фізичних ризиків під час промислової революції ми перейшли до часу, коли онлайн-загрози можуть мати реальні наслідки. Оскільки компанії стають частиною великих цифрових мереж і ланцюгів постачання, ризики зростають. Справжня проблема полягає в тому, як об'єднати стратегії безпеки IT і OT для ефективного управління кіберризиками.

Необхідність єдиних стратегій безпеки

Згідно з дослідженням Deloitte, приголомшливі 97% організацій пов'язують багато своїх проблем із безпекою зусиллями з конвергенції IT/OT. Це свідчить про те, що конвергенція IT та OT створює значні проблеми, підкреслюючи потребу в більш ефективних стратегіях безпеки, які об'єднують обидва домени.

Кроки для інтеграції безпеки IT і OT:

Визнайте розбіжності: Історичні траєкторії IT і OT були різними. IT стали стандартизованим фасилітатором бізнес-процесів, тоді як OT стабільно керує матеріальними активами, такими як виробничі механізми та системи опалення, вентиляції та кондиціонування. Таким чином, першим кроком до єдиного фронту є

визнання цих притаманних відмінностей і сприяння діалогу, який подолає розрив у розумінні між командами та керівниками IT та OT.

Розробіть уніфіковану систему безпеки:

Оптимізована архітектура: враховуючи чіткі принципи проектування OT, які традиційно віддають пріоритет ізольованим операціям, надзвичайно важливо розробити архітектуру, яка за своєю суттю захищає кожен компонент. Таким чином будь-яка вразливість в одній частині системи не загрожуватиме загальній стабільності та безпеці мережі.

Регулярні оцінки вразливості: обидва середовища повинні піддаватися періодичній оцінці для виявлення та усунення потенційних слабких ланок.

Багатофакторна автентифікація: для систем, які є ключовими для критичної інфраструктури, додавання рівнів автентифікації може підвищити безпеку.

Моніторинг у режимі реального часу та виявлення аномалій: розширені інструменти, які можуть ідентифікувати аномалії в шаблонах даних або функціях системи, є важливими. Такі аномалії часто вказують на можливі порушення.

Протоколи реагування на інциденти. Повинен бути розроблений чітко визначений, дієвий проект із детальним описом кроків, яких необхідно вжити у разі порушення безпеки.

Структуроване управління виправленнями: незважаючи на проблеми, з якими стикаються системи OT під час оновлення, систематичний підхід до розгортання виправлень, особливо для відомих уразливостей, є вирішальним.

Постійне навчання: кібернетичний ландшафт постійно розвивається, нові загрози з’являються щодня. Регулярні тренінги гарантують, що команди IT та OT готові долати ці виклики. Крім того, ініціативи з перехресного навчання можуть сприяти глибшому розумінню між командами, сприяючи спільному підходу до безпеки.

Впроваджуйте вдосконалені рішення безпеки: технічні відмінності між IT та OT вимагають рішень, які можуть ефективно подолати цей розрив. Інвестиції в сучасні інструменти безпеки, які пропонують такі функції, як моніторинг у реальному часі, виявлення аномалій і швидке реагування на загрози, можуть мати

ключове значення. Ці рішення мають бути достатньо гнучкими, щоб відповідати динамічній природі IT- та OT-середовищ, забезпечуючи нейтралізацію потенційних загроз до того, як вони можуть завдати шкоди.

Оцінка готовності до операційного ризику:

Кібербезпека – це командна робота. IT-команда має глибокі знання безпеки даних, тоді як команда OT має навички роботи з обладнанням і фізичними процесами. Для ефективного управління кіберзагрозами спеціалісти OT повинні розвинути сильніші навички кібербезпеки, а IT-спеціалісти повинні краще розуміти практичні виклики OT. Головний спеціаліст з інформаційної безпеки (CISO) повинен переконатися, що обидві команди мають потрібні інструменти, навчання та підтримку.

Фахівці з безпеки IT та OT повинні перевірити та оцінити:

- Відповідність їхніх стратегій реагування на інциденти основним IT та OT може вплинути на їхні операції та безпеку.
- Стійкість їхніх системних структур перед цими ризиками.
- Їхня майстерність у визначенні поведінки свідчить про ці ризики.
- Надійність їхніх протоколів віддаленого доступу для запобігання цим ризикам.
- Заходи, вжиті для усунення значних вразливостей у мережах IT та OT, пов’язаних із цими ризиками.

Висновок

Інтеграція стратегій безпеки IT і OT має першочергове значення в сучасну цифрову епоху. У міру розвитку кіберзагроз організації повинні прийняти цілісний підхід, використовуючи сильні сторони як IT, так і OT. Розвиваючи співпрацю, постійно оцінюючи ризики та впроваджуючи надійні заходи безпеки, організації можуть захистити свої операції та активи, забезпечуючи безпечне та стійке майбутнє». ***(Irfan Shakeel. Combining IT and OT security for enhanced cyber risk management // AT&T (https://cybersecurity.att.com/blogs/security-essentials/combining-it-and-ot-security-for-enhanced-cyber-risk-management). 27.09.2023).***

***

«Кібербезпека є одним із найвищих витрат, з якими стикаються підприємства, 12% IT-бюджету у середньому, і ці витрати стрімко зростають. У той час як компанія може звільнити персонал або скоротити витрати на маркетинг і дослідження та розробки в період нижчого зростання, підприємства не можуть йти на компроміс щодо кібербезпеки. Зростання кількості атак і підвищення складності атак означає, що ці витрати продовжуватимуть зростати, але ШІ та автоматизація можуть допомогти.

Згідно з журналом Cybercrime Magazine, якби кіберзлочинність була країною, вона була б третьою за величиною економікою світу, поступаючись США та Китаю. Очікується, що витрати, які підприємства спрямовують на кібербезпеку, зростуть з 8 трильйонів доларів до 10,5 трильйонів доларів до 2025 року. Statista погоджується з оцінками Cybercrime Magazine, заявляючи, що вартість кіберзлочинності досягне 10,3 трильйона доларів до 2025 року та 13,8 трильйона доларів до 2028 року.

…ШІ та автоматизація відіграють важливу роль у цій критично важливій, безкомпромісній галузі. Щодня виявляється 560 000 нових шкідливих програм, і програмні системи не встигають за цим. ШІ вже допомагає командам людей визначати, які загрози потребують додаткового аналізу, і в найближчій перспективі це суттєво знизить витрати на кібербезпеку. Також існує дефіцит кадрів у сфері кібербезпеки: опитування 2022 року стверджує, що 59% компаній мають дефіцит у цьому відділі та можуть бути не в змозі ефективно впоратися з атаками на кібербезпеку…

Як ШІ може покращити реагування на інциденти та виявлення загроз

Поєднання кібербезпеки з штучним інтелектом має природну спорідненість, оскільки кібератаки генеруються комп’ютером, і, у свою чергу, комп’ютери унікально здатні знаходити створені комп’ютером загрози. Автоматизація зменшує кількість помилкових спрацьовувань. Замість того, щоб отримувати кожну частину телеметрії, яку команда безпеки потребує для дослідження, рішення для виявлення

кінцевих точок і реагування за допомогою штучного інтелекту усувають шум, тому команда безпеки реагує лише на ті, які можуть бути критичними.

По суті, кібербезпека – це проблема даних. Платформи кібербезпеки завантажують, корелюють і запитують петабайти структурованих і неструктурованих даних із різних зовнішніх і внутрішніх джерел у режимі реального часу. Потім платформи кібербезпеки створюють насичений контекст і забезпечують кращу видимість, створюючи динамічне представлення даних у всій організації. Як наслідок, платформи кібербезпеки, керовані штучним інтелектом, часто дуже точно викликають відповідь.

Кількість кінцевих точок у корпоративній мережі експоненціально зростає: до 2025 року очікується підключення 27 мільярдів кінцевих точок. Були проведені приголомшливі дослідження, які показують, що 68% підприємств зазнали скомпрометованої кінцевої точки. Зламані облікові дані на комп'ютерах, ноутбуках і мобільних пристроях часто є найскладнішими точками доступу для захисту. Алгоритми можуть виявляти нові шкідливі програми на кінцевих точках на основі атрибутів відомих шкідливих програм. Несанкціонований доступ, витік даних і кіберзагрози з кінцевих точок також сприятимуть підвищенню попиту на периферійні децентралізовані рішення кібербезпеки ШІ.

Ринок мережевої безпеки є великим джерелом витрат на кібербезпеку. Алгоритми машинного навчання допомагають системам навчатися на досвіді, що допомагає ідентифікувати зловмисне програмне забезпечення в зашифрованому трафіку та знаходити внутрішні загрози. Алгоритмам машинного навчання не потрібно розшифровувати дані, вони можуть виявляти зловмисні шаблони та знаходити загрози, приховані за допомогою шифрування.

Хмарна безпека є сегментом кібербезпеки, який найшвидше розвивається. AI/ML може допомогти виявити підозрілі входи в хмарні програми, виявити аномалії на основі місцезнаходження та швидко визначити загрози за допомогою аналізу IP-репутації. Запобігання загрозам можливе шляхом використання хмарної телеметрії за допомогою систем штучного інтелекту, уникаючи необхідності експертної розробки правил. Симуляція шляху атаки також стала можливою за

допомогою штучного інтелекту, щоб допомогти змоделювати шлях зловмисника, щоб зменшити прогалини в охопленні. Вихідний веб-трафік можна відстежувати без необхідності налаштовувати віртуальні машини, зосереджуючись на обмеженні вихідного трафіку на основі джерела, ідентичності, призначення та типів запитів. Моделі машинного навчання також можуть виявляти нові загрози API на основі великих наборів навчальних даних. Це кілька прикладів того, як AI/ML покращує безпеку хмари.

Chat-GPT підвищує ризики безпеки, оскільки генеративний штучний інтелект здатний писати зловмисний код або діяти як помічник хакера-людини, який пише шкідливий код. Щоб вирівняти умови гри, найкращим захистом також будуть самонавчальні генеративні інструменти ШІ. Кількість завантажень для Chat-GPT значно зросла серед споживачів. Тим часом використання Chat-GPT серед хакерів зростає експоненційною кривою. Це допомагає проілюструвати, чому в середньостроковій перспективі крива впровадження ШІ може бути більш здоровою серед підприємств (а не споживачів).

За словами Маккензі Джексона, захисника розробників із GitGuardian, Chat-GPT, швидше за все, призведе до збільшення кількості хакерів. Це нове покоління називають «хакерами зі штучним інтелектом», тому що раніше вони не могли зламати самі, але тепер можуть зламувати за допомогою генеративного штучного інтелекту…

Що C-Suite говорить про ШІ та кібербезпеку

McKinsey опублікував нещодавній звіт, у якому 53 відсотки організацій вважають, що генеративний ШІ створює нові ризики для кібербезпеки. Штучний інтелект не тільки може допомогти підприємствам прискорити виявлення загроз, але й хакери можуть також прискорити життєвий цикл наскрізної атаки. В іншому опитуванні 38 відсотків підприємств заявили, що вони зменшують ризики кібербезпеки, пов’язані зі штучним інтелектом, порівняно з 32 відсотками, які зменшують неточності, що вказує на те, що кібербезпека є головним ризиком, пов’язаним зі штучним інтелектом.

За даними Forbes, 56% підприємств назвали питання управління, безпеки та можливості перевірки найпріоритетнішими для витрат на AI/ML. Це опитування було завершено у 2021 році, і, ймовірно, сьогодні ця цифра більша.

Що говорять керівники публічних компаній

Microsoft має один із найбільших у світі бізнесів у сфері кібербезпеки з 20 мільярдами доларів. Це більше, ніж шість найкращих компаній разом узятих. Компанія роками працювала над новою функцією автоматизації під назвою CoPilot, яка була оприлюднена цього місяця. Незважаючи на те, що він продається для Windows, Office 365 і браузерів Bing і Edge, він також стане компаньйоном ШІ для свого бізнесу з кібербезпеки. За словами генерального директора під час останнього звіту про прибутки: «наш Security Copilot, перший продукт, який використовує це наступне покоління штучного інтелекту для SecOps, буде доступний для клієнтів через платну програму раннього доступу цієї осені»…

Palo Alto Networks – це компанія, яка цього року досягла 78% прибутку за останнім звітом про прибутки. Зараз він торгується з приростом 66% з початку року. Під час останнього звіту про прибутки генеральний директор заявив: «Я думаю, що важливо розуміти, що протягом останніх п’яти років кібербезпека TAM продовжувала зростати. Він зріс приблизно на 14%, і він зріс вдвічі швидше, ніж зростав IT-ринок […] і, можливо, зараз, коли штучний інтелект став основною можливістю, кожен із нас намагається переконатися, що ми схопи це обома руками. Таким чином, ми й надалі спостерігатимемо, як темпи витрат на технології зростатимуть чи то вперед»…

Cloudflare — це акції, які з початку року зросли на 35% і цього року витісняють Nasdaq-100, що не мало, враховуючи ралі, яке спостерігає Big Tech. Генеральний директор нещодавно заявив, що його компанія спостерігає зростання бізнесу на своєму продукті R2: «І за нашими оцінками, Cloudflare є найбільш часто використовуваним хмарним провайдером серед провідних стартапів AI. Вони використовують R2, щоб допомогти отримати найнижчу вартість GPU для навчання своїх моделей».

висновок:

Використання штучного інтелекту для ідентифікації загроз, розпізнавання шаблонів і виявлення аномалій не є чимось новим. Швидше на ринок з'являються платформи з генеративним штучним інтелектом і автоматизацією, що самонавчається, тож загроза виявляється до її виникнення, а не після кібератаки. Замість виявлення загроз, кінцевою метою є запобігання загрозам.

Штучний інтелект найближчим часом не повністю замінить спеціалістів із безпеки, але він може сприяти ефективності шляхом автоматизації виявлення загроз, аналізу наборів даних і постійного навчання виявлення аномалій і нових атак до їх виникнення. Пропонуючи безагентні рішення, теоретично буде потрібно менше людей-агентів. Для нових технологій крива впровадження може бути складною (запитайте ентузіастів віртуальної реальності, як це відбувається). Але для галузей, де ШІ може запропонувати цінну пропозицію, яка може передбачувано знизити витрати за розумною ціною, сформується ринок. Ми вважаємо, що кібербезпека буде одним із наступних ринків, який буде зруйновано ШІ.

Якщо ви володієте акціями кібербезпеки або плануєте володіти акціями кібербезпеки, радимо вам відвідати наші щотижневі преміальні вебінари, які проводяться щочетверга о 17:00 за східним стандартним часом. Наступного тижня ми обговоримо акцію кібербезпеки, на яку нещодавно увійшли, і ту, на яку ми уважно стежимо, – які наші цілі, де ми плануємо купувати, а також де ми плануємо отримати прибутки». ***(Beth Kindig. The Next Market AI Will Disrupt Is Cybersecurity // Forbes (https://www.forbes.com/sites/bethkindig/2023/09/29/the-next-market-ai-will-disrupt-is-cybersecurity/?sh=31ca2db3f727). 29.09.2023).***

***

«Виявлення головних акторів національної держави може залежати від того, кого ви запитуєте, що підкреслює необхідність збору інформації про загрози з різноманітних джерел даних.

В умовах, коли геополітичні питання зараз можуть спонукати галузеві дискусії, організаціям буде краще, якщо вони сформулюють свою стратегію

кібербезпеки на основі інформації, яка відображає загрозливу діяльність у міжнародному масштабі.

Для деяких організацій ця вимога означає збір всебічної та, зокрема, різноманітної інформації про загрози.

«Більшість розвідувальних центрів наразі походять із Заходу або орієнтовані на Захід, і це може призвести до упередженості або спотвореного уявлення про загрози, зазначив Мінхан Лім, керівник відділу досліджень і розробок Ensign Labs. Сінгапурський постачальник кібербезпеки був створений через спільне підприємство між місцевою телекомпанією StarHub і державною інвестиційною компанією Temasek Holdings.

«Нам потрібно зберігати нейтралітет, тому ми обережні з тим, де ми малюємо канали даних», — сказав Лім в інтерв'ю ZDNET. «У нас є канали даних з усіх авторитетних джерел [розвідки про загрози], що важливо, щоб ми могли зрозуміти, що відбувається на глобальному рівні».

Ensign також має власні центри телеметрії та SOC (операційні центри безпеки), зокрема в Малайзії та Гонконзі, збираючи дані з датчиків, розміщених по всьому світу. Лім додав, що клієнтура постачальника складається з транснаціональних корпорацій (МНК), включаючи регіональні та китайські компанії, які мають офіси в США, Європі та Південній Африці.

Він зазначив, що загрозлива діяльність не обов'язково може бути мотивована геополітичними проблемами, оскільки деякі загрозливі дії походять з регіону, в якому базуються їхні цілі. Китайські клієнти постачальника, наприклад, зазнали кібератак, які походять з Азії.

Він додав, що більшість атак, як правило, мотивовані фінансово.

За словами Кендіда Вуста, віце-президента з досліджень кіберзахисту Acronis, коли задіяні суб'єкти загрози національних держав, першими трьома країнами, звідки походять атаки, є Китай, Росія та США.

Північна Корея та Іран завершують п'ятірку найпопулярніших місць, звідки відбуваються атаки на національних державах, і в країнах, які очолюють цю групу, змін мало, сказав Вуест, посилаючись на дані з мережі моніторингу Acronis.

Постачальник безпеки даних був заснований у Сінгапурі, а зараз його штаб-квартира знаходиться в Швейцарії. Його засновник Сергій Бєлоусов народився в Росії, але отримав громадянство Сінгапуру в 2001 році. У 2021 році він залишив посаду генерального директора і зараз працює головним науковим директором Acronis.

Повторюючи погляди Ліма, Вуест сказав ZDNET, що суб'єкти загрози національній державі США часто недостатньо представлені, оскільки більшість головних новинних організацій є західними і, як правило, не посилаються на цю конкретну групу акторів національної держави.

Він зазначив, що атаки, спонсоровані державою США, також є дуже цілеспрямованими, залучаючи одну-дві жертви, а не сотні, і часто залишаються непоміченими. Для порівняння, обсяг атак на національні держави з боку Китаю може здатися вищим, оскільки існує більше організацій, які шукають цю групу загрозливих осіб, сказав він.

Однак він додав, що напади з боку китайських національних державних акторів також були більшими за обсягом і частотою. Зокрема, збільшилася кількість атак, спрямованих на VPN і брандмауери, а також відомі вразливості в таких системах, як Microsoft Exchange Server.

Минулого місяця уряд США опублікував звіт, в якому висвітлюються найпоширеніші вразливості програмного забезпечення, які зазвичай використовувалися у 2022 році, вони включали кілька недоліків, які раніше висвітлювалися у 2021 році та використовувалися спонсорованими державою кіберакторами Китаю. Згідно із від 3 серпня заявою американських агенцій безпеки та їхньої п'ятірки Очі союзників, включаючи Австралію, Нову Зеландію, Канаду та Великобританію

Уряд Китаю, з іншого боку, звинуватив розвідувальні служби США на центр моніторингу землетрусів у Ухані в липні 2023 року в кібер-атаці, посилаючись на «дуже складне» шкідливе програмне забезпечення, яке використовувалося в інциденті. У Пекіні заявили, що атака, схоже, походить від підтримуваних урядом хакерів у США та спрямована на мережеве обладнання, яке збирає дані про

сейсмічні хвилі. Набори даних містили інформацію про національну безпеку, наприклад деталі військових оборонних споруд, які враховуються при визначенні сейсмічної інтенсивності.

Китайські чиновники припускають, що доступ до відповідних даних із центрів сейсмічного моніторингу може дозволити хакерам оцінити підземні споруди певної території та визначити, чи є це військовою базою. Ці дані стануть у пригоді іноземним військовим розвідкам, таким як Міністерство оборони США.

Американські постачальники технологій, однак, вважають, що китайські національні державні актори озброєні більш складними інструментами та тактиками.

«Китайське кібершпигунство пройшло довгий шлях від знайомої багатьом з нас тактики «знищи й захопи», — сказав Джон Хултквіст, головний аналітик Google Cloud Mandiant. «Вони змінили свої можливості з того, де домінували широкі, гучні кампанії, які було набагато легше виявити. Раніше вони були зухвалими, але тепер вони явно зосереджені на скритності».

«Результатом стає противник, який набагато важче відстежити та виявити. Реальність така, що ми стикаємося з більш досвідченим супротивником, ніж будь-коли, і нам доведеться працювати набагато наполегливіше, щоб не відставати від нього», — написав Хултквіст у коментарі до нещодавній злом безпеки Microsoft, який, як вважають, є роботою кібератакників із Китаю.

За даними Microsoft, ворожа група під кодовою назвою Storm-0558 отримала доступ до систем електронної пошти Microsoft для збору розвідувальних даних. Технологічний гігант заявив, що порушення вплинуло на 25 організацій, включаючи урядові установи США та облікові записи осіб, які, ймовірно, пов’язані з цими установами.

Китайська кібершпигунська діяльність дедалі більше використовує початковий доступ і стратегії після компрометації, спрямовані на мінімізацію виявлення, відзначається в публікації Google Cloud Mandiant у липні 2023 року. «Експлуатація китайськими групами загроз нульових днів у програмному забезпеченні безпеки, мереж і віртуалізації, а також націлювання на

маршрутизатори та інші методи для ретрансляції та маскування трафіку зловмисників як за межами, так і всередині мереж жертви», — сказав американський постачальник. «Ми з високою впевненістю вважаємо, що китайські групи кібершпигунства використовують ці методи, щоб уникнути виявлення та ускладнити атрибуцію».

В інтерв'ю ZDNET Халтквіст повторив підвищену складність атак з боку китайських національних державних акторів, які були помітно більш прихованими та їх важче виявити. Він вказав на складну атаку, спровоковану Storm-0558, як на ознаку того, що набори навичок значно покращилися.

Він назвав Китай, Росію, Північну Корею та Іран як провідних національних держав, з якими найчастіше стикаються клієнти Google Cloud Mandiant. Ці суб'єкти загрози також націлені на критично важливу інформаційну інфраструктуру та, у деяких випадках, співпрацюють з урядами або фінансованими державою ворожими групами та надають скомпрометовану інформацію розвідувальним службам.

Водночас Вуест вважав США найдосконалішими серед національних державних акторів, зазначивши, що група Equation, яка, як вважають, є частиною альянсу Five Eyes, який до сьогодні залишається непорушним, використовувала певний алгоритм шифрування в серії цілеспрямованих атак десять років тому.

Тоді він поставив атаки російських національних державних акторів на друге місце за рівнем витонченості, за ними йдуть їхні колеги в Китаї.

Китайські суб'єкти загрози часто обирають масштабність своїх атак, які зазвичай не є складними за своєю природою, сказав він, припускаючи, що така простота може бути пов'язана з тим, що немає причин для вдосконалення їх тактики, якщо ці атаки й надалі будуть ефективними. Наприклад, китайські зловмисники все ще використовують фішинг, який неважко здійснити, і він значною мірою залежить від людей як найслабшої ланки, сказав він.

І хоча Вуест визнав, що китайські атаки тепер є більш досконалими, він зауважив, що це було природним прогресом, оскільки більшість навичок зазвичай вдосконалювалися протягом двох десятиліть.

Опис китайських національних державних акторів як більш досвідчених може означати перебільшення ландшафту загроз і риторики, яку використовують західні уряди для підвищення загальної обізнаності організацій про необхідність мати якісний кіберзахист, сказав Вуест.

Він додав, що більшість кібератак сьогодні все ще спрямовані на старі вразливості, які організації залишили невиправленими.

Лім також зазначив, що зловмисники націлювалися на пристрої безпеки та намагалися уникнути виявлення. Він сказав, що актори тепер більш цільові та обізнані про прилади, які використовуються саме державними установами, і, отже, знають, на які пристрої орієнтуватися.

Зловмисники також постійно оновлюють свою тактику, використовуючи найсучасніші методи та націлюючись на популярні інструменти, такі як програми для відеоконференцій і VPN, додав він.

«Зростаюча загроза підкреслює потребу організацій у створенні основ і застосуванні найкращих практик», — сказав Вуест, який зазначив, що деякі компанії все ще не можуть виправити відомі вразливості. З огляду на стрімкий фішинг і 90% атак відбувається через електронну пошту, він також наголосив на важливості безпеки електронної пошти та інших заходів для боротьби з такими атаками.

Цей захист буде особливо критичним, оскільки все більше хакерів використовують генеративний штучний інтелект (ШІ), щоб створювати переконливіші фішингові повідомлення електронної пошти, збираючи особисту інформацію з облікових записів соціальних мереж для створення підроблених персонажів, сказав він.

Лім погодився, зазначивши, що його команда почала виявляти генеративний ШІ та інструменти машинного навчання, які використовуються для створення електронних листів, а також для обходу перевірки та контролю доступу.

Вуест додав, що кіберзлочинці можуть використовувати штучний інтелект, щоб збільшити масштаб і швидкість запуску атак, а також ускладнити перевірку та автентифікацію користувачів.

Він висловив стурбованість тим, що генеративний штучний інтелект призведе до руйнування багатьох галузей і суттєво змінить спосіб здійснення атак. Наприклад, якщо генеративний штучний інтелект використовується для запуску помилкових команд, ризик і потенційна загроза будуть значними, сказав він.

Халтквіст закликав лідерів галузі трансформувати свою практику разом із загрозливими супротивниками, інакше ризикує відстати. «Нам потрібно більше даних, краща техніка, кращі інструменти та кращі [оборонні] плани», — сказав він. «Технології постійно змінюються, як і супротивники. Нам потрібно наполегливо працювати, щоб залишатися на висоті». ***(Eileen Yu. Diverse threat intelligence key to cyberdefense against nation-state attacks // ZDNET (https://www.zdnet.com/article/diverse-threat-intelligence-key-to-cyberdefense-against-nation-state-attacks/). 29.09.2023).***

***

«У 2023 році ринок кібербезпеки процвітає, оскільки все більше підприємств впроваджують ініціативи цифрової трансформації, щоб підвищити свою продуктивність, ефективність і задоволеність клієнтів. На жаль, ці ініціативи також наражають бізнес на різні кіберзагрози, включаючи програми-вимагачі, фішинг і витоки даних. Як наслідок, кібербезпека має важливе значення для захисту інфраструктури, яка підтримує зусилля сучасних підприємств щодо цифрової трансформації. Це також призвело до зростання акцій кібербезпеки для продажу.

Однак не всі підприємства кібербезпеки будуть успішними на цьому висококонкурентному та динамічному ринку. Безліч компаній борються з відтоком клієнтів і залученням нових клієнтів у складному макроекономічному середовищі.

Без зайвих слів, нижче наведено список трьох компаній з кібербезпеки, яких інвесторам у публічні акції варто було б уникати.

Alarm.com (ALRM)

Alarm.com (NASDAQ: ALRM) не є компанією з кібербезпеки в традиційному розумінні. Скоріше, фірма є постачальником хмарних рішень безпеки та розумного

будинку для житлових і комерційних клієнтів. Охоронна фірма здобула велике визнання бренду завдяки встановленому обладнанню, яке забезпечує безпеку фізичних просторів та інфраструктури. Однак Alarm.com також використовує програмні засоби, щоб не лише забезпечити рівень аналітики даних, які збирає його апаратне забезпечення, але також використовує методи шифрування для безпечного зберігання даних клієнтів.

Незважаючи на те, що охоронна фірма здатна генерувати постійний прибуток, Alarm.com останніми роками намагався збільшити прибуток через відсутність попиту з боку клієнтів. Більшість клієнтів Alarm.com є мешканцями, і під час економічної нестабільності або спаду такі клієнти можуть або відтікати, або не мати стимулу платити за додаткові рішення. Наприклад, зростання доходу Alarm.com суттєво впало в 2022 році та продовжувало відбуватися в 2023 році. Згідно з останніми прогнозами, охоронна фірма отримає щонайменше 887,7 мільйонів доларів США доходу в 2023 році, що становить 22,2% падіння прибутку порівняно з минулим роком. фігура.

Крім того, форвардний мультиплікатор ціни до прибутку (P/E) Alarm.com також торгується високим рівнем 35x, що може свідчити про те, що від цього моменту багаторазове розширення невелике.

Окта (OKTA)

Okta (NASDAQ: OKTA) є провідною компанією з кібербезпеки, про яку я говорив у попередній статті, і моє переконання залишається переважно ведмежим. Фірма з кібербезпеки розробляє рішення для управління ідентифікацією та доступом (IAM) для хмарних програм і платформ. Іншими словами, Okta дозволяє своїм клієнтам безпечно керувати ідентифікаційними даними своїх співробітників, клієнтів і партнерів на різних пристроях і середовищах.

Незважаючи на те, що Okta займає міцні позиції на швидкозростаючому ринку IAM, який був зумовлений дедалі більшим впровадженням хмарних обчислень, мобільних пристроїв і віддаленої роботи, Okta також стикається з низкою серйозних проблем, які можуть перешкодити її майбутній продуктивності. через Зростання доходів у 2023 році знизилося те, що компанії стали більш

уважними до своїх витрат на технології, а Okta все ще в основному збиткова. Відставання у виручці та недостатня прибутковість є зв'язком, який інвестори в публічні акції ніколи не повинні бачити. Це робить його одним із тих акцій кібербезпеки, які можна продати.

Зрештою, оскільки трейдери стають все більш і більше втомленими від компаній з великою множинністю, може відбутися різкий розпродаж акцій Okta, що завдасть серйозної шкоди багатству багатьох інвесторів.

BlackBerry (BB)

BlackBerry (NYSE: BB), заснована ще в 1984 році, є колишнім піонером смартфонів, який значною мірою втратив своє попереднє домінування в мобільних телефонах таким компаніям, як Apple і Samsung. Що робило телефон BlackBerry особливим у ті часи, так це додатковий рівень безпеки. Незважаючи на те, що BlackBerry більше не продає нові смартфони, компанія вдосконалила ці функції безпеки у своєму центрі, щоб надавати програмне забезпечення та послуги для кібербезпеки, корпоративної мобільності та Інтернету речей (IoT).

Крім того, компанія змогла зібрати значну клієнтську базу в регульованих галузях, таких як уряд, охорона здоров'я та фінанси. Однак акції BlackBerry також можуть зіткнутися з величезними перешкодами в майбутньому, якщо її зусилля з повернення будуть зірвані. Давайте визнаємо, що компанія з кібербезпеки виходить на вже дуже конкурентний ринок із такими відомими конкурентами, як Microsoft (NASDAQ: MSFT), VMware (NYSE: VMW) і Symantec. Крім того, акції BlackBerry мають високу оцінку – компанія зазнала чистих збитків з часів пандемії, і зростання доходів також не різко зросло, залишаючи оцінки на підвищених рівнях.

Можливо, інвесторам було б краще переглянути інші акції кібербезпеки, перш ніж робити ще одну ставку на те, чи повернеться BlackBerry у форму». ***(Tyrik Torres. Ticking Time Bombs: 3 Cybersecurity Stocks to Dump Before the Damage Is Done // InvestorPlace Media, LLC. (https://investorplace.com/2023/09/ticking-time-bombs-3-cybersecurity-stocks-to-dump-before-the-damage-is-done/). 26.09.2023).***

***

«26 липня 2023 року Комісія з бірж цінних паперів (SEC) прийняла остаточне правило, призначене для розширення та стандартизації розкриття інформації щодо управління ризиками кібербезпеки, управління та звітування про інциденти. Нове правило встановлює додаткові вимоги щодо розкриття інформації для емітентів із США, які звітують, та іноземних приватних емітентів, включаючи всі компанії, акції яких торгуються на біржах США (публічні компанії). Ця публікація присвячена трьом ключовим діям, які публічні компанії повинні вжити згідно з новим правилом:

Інциденти. Розкривайте суттєві інциденти кібербезпеки у формі 8-K протягом чотирьох робочих днів після визначення інциденту як суттєвий, а також розкривайте будь-які суттєві оновлення на постійній основі.

Управління ризиками – Розкрийте процеси оцінки, ідентифікації та управління суттєвими ризиками від загроз кібербезпеці в річному звіті за формою 10-K.

Управління – Розкрийте інформацію про наглядову роль ради директорів і керівництво в оцінці та управлінні значними ризиками кібербезпеки в річному звіті за формою 10-K.

SEC прийняла аналогічні вимоги щодо розкриття інформації для іноземних приватних емітентів, які повинні розкриватися у формах 6-K і 20-F.

Дати відповідності

Усі емітенти звітності повинні будуть включити нове розкриття інформації в наступні річні звіти за фінансовий рік, який закінчується 15 грудня 2023 року або після цієї дати.

Починаючи з 18 грудня 2023 року необхідно дотримуватися правил звітування про кіберінциденти.

Меншим компаніям, які звітують, надається додаткові 180 днів до 15 червня 2024 року, щоб виконати вимоги щодо звітності про інциденти.

1. Розкриття суттєвих інцидентів кібербезпеки

Правило SEC встановлює новий пункт 1.05 до форми 8-K (або 6-K для іноземних приватних емітентів), який вимагатиме від публічної компанії розкривати суттєві кіберінциденти, які відбуваються в IT-системах компаній. У той час як державні компанії повинні були розкривати суттєві інциденти кібербезпеки згідно з попередніми правилами, нове правило передбачає конкретні терміни та формат для розкриття інформації.

Висновок щодо розкриття інформації про кіберінциденти: публічні компанії повинні забезпечити внутрішні процеси для визначення того, чи є інциденти кібербезпеки суттєвими, і повідомляти необхідні відомості про інцидент. Це включає початкове розкриття інциденту, а також будь-які суттєві оновлення. Через необхідний графік розкриття інформації компанії повинні бути готові виконувати ці оцінки та розкривати інформацію, навіть якщо інцидент кібербезпеки триває. Команди з питань безпеки, юридичних питань і корпоративних комунікацій державних компаній повинні співпрацювати, щоб налаштувати плани реагування на кіберінциденти та процеси фінансової звітності відповідно до цих зобов'язань.

а) Час розкриття кіберінцидентів

Останнє правило вимагає, щоб публічні компанії розкривали інформацію про суттєві інциденти кібербезпеки в новому пункті 1.05 форми 8-K протягом чотирьох робочих днів після визначення того, що інцидент є суттєвим або призведе до суттєвих змін для інвесторів. Якщо публічна компанія розкриває інформацію про кіберінцидент, остаточне правило також вимагає, щоб компанії надали оновлення цієї інформації у зміненій формі 8-K без невиправданої затримки або протягом чотирьох робочих днів після того, як інформація стане доступною. Невчасне подання розкриття інформації за пунктом 1.05 не призведе до втрати права на отримання форми S-3.

Згідно з правилом, компанії повинні без необґрунтованої затримки визначити, чи є інцидент кібербезпеки суттєвим. Інформація є суттєвою, якщо «існує значна ймовірність того, що розумна особа вважатиме її важливою» під час прийняття інвестиційного рішення. SEC заявляє, що компаніям слід враховувати як кількісні, так і якісні фактори, такі як фінансові витрати, втрата інтелектуальної

власності, «шкода репутації компанії, відносинам із клієнтами чи постачальниками чи конкурентоспроможності, [і] можливість судового розгляду чи регуляторних розслідувань чи дій».

На відміну від інших нормативних актів щодо звітування про кіберінциденти, майже всі з яких зберігають звіти про інциденти конфіденційними, документи за формою 8-K стають загальнодоступними через систему EDGAR SEC. Це може призвести до того, що компанії будуть змушені публічно розкривати серйозні кіберінциденти до того, як інцидент буде локалізовано або пом'якшено, що може ускладнити зусилля компаній з відновлення та координацію з іншими федеральними відомствами.

Крім того, правило SEC дозволяє компаніям відкладати розкриття інформації на термін до 30 днів, якщо Генеральний прокурор США повідомить SEC, що розкриття інциденту може становити значний ризик для національної або громадської безпеки. У «надзвичайних обставинах» розкриття може бути відкладено на термін до 60 днів. Однак ці винятки, ймовірно, будуть застосовуватися лише в окремих випадках.

b) Формат розкриття кіберінцидентів

Точний зміст розкриття може відрізнятися від одного інциденту до іншого. Правило SEC вимагає, щоб розкриття інформації про інциденти кібербезпеки зосереджувалося на матеріальному впливі інциденту, а не на деталях самого інциденту. Зокрема, пункт 1.05 форми 8-K вимагатиме від публічних компаній розкривати «суттєві аспекти характеру, обсягу та часу інциденту, а також суттєвий вплив або ймовірний суттєвий вплив інциденту на реєстранта, включаючи його фінансовий стан і результати діяльності».

Правило SEC також роз'яснює, що компанії не зобов'язані розкривати технічну інформацію в таких подробицях, щоб це заважало процесу реагування на інциденти компаній. Це включає конкретну інформацію про план реагування, захисні заходи, відповідні системи або потенційні вразливості. Однак, як і у випадку з іншими розкриттями інформації, розкриття інформації про кібербезпеку

є предметом відповідальності відповідно до розділу 18 Закону про біржі за суттєві викривлення чи упущення.

Після первинного розкриття, якщо з'явиться додаткова інформація, яка мала бути розкрита під час первинного розкриття, публічні компанії повинні подати змінену форму 8-K. Компаніям не потрібно оновлювати всю інформацію; має бути надано лише інформацію, яка вимагалася б у початковому розкритті відповідно до пункту 1.05(a).

2. Управління ризиками кібербезпеки та розкриття стратегії

Останнє правило додає пункт 106(b) до Регламенту SK, що вимагає розкриття інформації про процеси управління ризиками кібербезпеки публічних компаній у річних звітах. Це включає в себе опис процесів шляхом «оцінки, ідентифікації та управління суттєвими ризиками від загроз кібербезпеці з достатньою деталізацією, щоб розумний інвестор міг зрозуміти ці процеси». Правило передбачає наступний невичерпний перелік потенційних елементів розкриття:

Чи були і як описані процеси інтегровані в загальну систему управління ризиками компанії;

Ступінь, в якому компанія залучає консультантів, аудиторів або інших сторонніх постачальників послуг у зв'язку з процесами управління ризиками кібербезпеки;

Чи є в компанії процеси для нагляду за значними ризиками кібербезпеки, пов'язаними з використанням сторонніх постачальників послуг;

Будь-які ризики, пов'язані з загрозами кібербезпеці або попередніми інцидентами, які суттєво вплинули на компанію або мають обґрунтовану ймовірність суттєво вплинути на компанію, зокрема через бізнес-стратегію, операції чи фінансовий стан; і

Будь-яка інша суттєва інформація.

Правило SEC також містить вказівки щодо типів ризиків, які публічні компанії можуть враховувати в цьому контексті. Серед інших ризиків це включає ризик зриву бізнес-операцій, викрадення інтелектуальної власності, заподіяння шкоди працівникам або клієнтам, репутаційний ризик, судові та юридичні ризики.

Висновок щодо розкриття інформації про управління кіберризиками: багато компаній мають внутрішню програму управління ризиками кібербезпеки, включаючи процеси оцінки ризиків. Команди з питань права, безпеки та корпоративних комунікацій повинні розглянути можливість співпраці над шаблоном опису цих програм для щорічного розкриття інформації для інвесторів. Компанії захочуть подумати про те, як забезпечити точність і відповідність розкритої інформації, використовуючи мову, прийнятну для поточних і потенційних інвесторів. Опис слід переглядати та оновлювати, коли відбуваються суттєві зміни в організаційній системі управління ризиками або ландшафті кіберзагроз.

3. Розкриття інформації про управління кібербезпекою

Остаточне правило також додало два положення до пункту 106(c) Регламенту SK, які вимагають від публічних компаній розкривати інформацію, пов'язану з річними звітами про управління кібербезпекою. Це включає окремі описи ролей правління та керівництва в нагляді за ризиками кібербезпеки.

Згідно з правилом, щорічні звіти публічних компаній повинні описувати нагляд правління за ризиками від загроз кібербезпеці. У звіті також має бути вказано комітет правління (якщо такий є), який відповідає за нагляд за ризиками кібербезпеки, і описано, як рада чи комітет інформуються про ризики.

Крім того, останнє правило вимагає, щоб річні звіти публічних компаній описували роль керівництва в оцінці та управлінні значними ризиками кібербезпеки, а також відповідний досвід керівництва. Правило зазначає, що компаніям слід розглянути можливість оприлюднення такого невичерпного списку:

Чи займаються керівні посади чи комітети оцінкою суттєвих ризиків кібербезпеки та керують ними, а також повний опис характеру їхнього відповідного досвіду;

Процеси, за допомогою яких такі особи або комітети інформуються про запобігання, виявлення та пом'якшення інцидентів у сфері кібербезпеки та контролюють їх; і

Чи повідомляють такі особи або комітети інформацію про значні ризики кібербезпеки раді директорів.

Висновки щодо розкриття інформації про управління кіберризиками: державним компаніям слід розглянути можливість перегляду кадрової структури відділу кібербезпеки, щоб забезпечити інформування вищого керівництва та правління про інциденти кібербезпеки та зусилля з управління ризиками. Компанії повинні перевірити, як управління ризиками кібербезпеки розподіляється на рівні правління, і переконатися, що комітети правління мають достатні повноваження щодо цих обов'язків. Компанія може розглянути можливість створення підкомітету з кібербезпеки, особливо якщо аудиторській комісії компанії потрібні додаткові ресурси для ефективного нагляду за цими питаннями. Нарешті, компаніям слід розглянути можливість розробки нормативних описів цих процесів управління для щорічної звітності та підготуватися до оновлення описів за потреби.

Дійте швидко, щоб адаптуватися до правил кібербезпеки SEC

Хоча ключові вимоги щодо розкриття інформації набудуть чинності лише наприкінці 2023 року, публічні компанії мають підготуватися до прозорості, якої вимагає правило. Загалом остаточні правила мають спонукати публічні компанії переглянути свої інвестиції в управління кіберризиками, управління та нагляд. Ефективне управління ризиками кібербезпеки залежить від співпраці співробітників із різних відділів у всьому бізнесі. Компанії повинні переконатися, що групи безпеки, юристів і комунікацій є частиною процесу на ранньому етапі, щоб співпрацювати над найефективнішим процесом для виконання вимог SEC щодо розкриття інформації.

Ми рекомендуємо публічним компаніям негайно переглянути та, якщо необхідно, змінити свої процедури розкриття інформації щодо кібербезпеки, щоб забезпечити своєчасне подання звітів відповідному персоналу. Це може включати перегляд планів реагування на інциденти, щоб переконатися, що члени команди зациклені на відповідному етапі для належного аналізу інцидентів на суттєвість. Оскільки розкриття інцидентів за формою 8-K, яких вимагає остаточне правило, стає загальнодоступною інформацією, групи реагування на інциденти повинні бути

готові до того, що розголошення інциденту, який не був пом'якшеним, може ненавмисно наражати компанію на додаткові спроби вторгнення, і повинні забезпечити належний захист. відповідати.

Компанії також можуть розглянути можливість розробки таблиці регулятивних повідомлень, щоб відстежувати різні зобов'язання щодо звітування про інциденти. Багато компаній підпадають під дію кількох нормативних актів щодо інцидентів кібербезпеки в усьому світі з різними часовими рамками сповіщень, і розробка діаграми може допомогти забезпечити належне своєчасне розкриття інформації під час реагування на кіберінцидент.

Ці міркування мають на меті підкреслити деякі ключові кроки, які компанії можуть зробити зараз, щоб підготуватися до остаточних правил SEC. Вони не є вичерпним переліком, і кожна публічна компанія повинна оцінити процеси та процедури, які можуть бути необхідними та відповідними в контексті її діяльності, бізнесу та нормативного середовища». ***(Harley L. Geiger. Key Actions for Public Companies under the SEC's New Cybersecurity Rules // Venable LLP (https://www.venable.com/insights/publications/2023/08/key-actions-for-public-companies-under-the-sec). 05.09.2023).***

***

«У березні уряд США випустив нову стратегію кібербезпеки, автором якої є Офіс національного кібердиректора.

Поділена на п'ять основ і 27 стратегічних цілей, стратегія викладає сміливе бачення захисту критичної інфраструктури, ліквідації загроз, формування ринкових сил для забезпечення безпеки, інвестування в стійке майбутнє та налагодження міжнародних партнерств. Якщо ця стратегія буде повністю реалізована, ця стратегія поставить перед бізнесом у контрактній сфері завдання посиленого контролю та вищих стандартів безпеки, а також можливість конкурувати за замовлення та гранти, спрямовані на зміцнення критично важливої цифрової інфраструктури країни.

Стратегія включає кілька сфер, що представляють інтерес для державних підрядників, з потенціалом збільшення фінансування для різних проектів, а також можливістю додаткового регулювання та примусового виконання.

В одному розділі, наприклад, обговорюється використання федеральних грантових програм для стимулювання створення критичної цифрової інфраструктури. Інший описує способи, якими уряд міг би «використовувати федеральні закупівлі для покращення підзвітності», але також закликає посилити вимоги безпеки для постачальників, які продають федеральному уряду. Нарешті, одне положення окреслює плани щодо «пожвавлення федеральних досліджень і розробок для кібербезпеки» за допомогою різноманітних центрів досліджень і розробок, що фінансуються з федерального бюджету.

Уразливості «нульового дня».

Найбільш суперечливий розділ закликає притягнути до відповідальності компаній-розробників програмного забезпечення за створення небезпечного коду. Незважаючи на те, що використання вразливостей «нульового дня» за останні роки досягло найвищого рівня за весь час, що призвело до масштабних наслідків для промисловості та уряду, ідея притягнення компаній до відповідальності за створення небезпечного коду є серйозним відхиленням від попередніх норм. Дехто ставив під сумнів, чи містить стратегія достатньо деталей для належного впровадження, тоді як інші зазначали, що ця мета може змінити спосіб закупівлі програмного забезпечення всім урядом.

Щоб підкреслити цю зміну в мисленні, Агентство кібербезпеки та безпеки інфраструктури разом із кількома міжнародними партнерами опублікували принципи безпеки за проектом і за замовчуванням у квітні. Ці вказівки мали на меті змінити культуру ставлення технологічної спільноти до вразливого програмного забезпечення та перекласти тягар безпеки на виробників технологій.

У рамках розгортання цього нового способу мислення директор CISA Джен Істерлі зазначила у своїй промові в Університеті Карнегі-Меллона, що концепція Secure-by-Design і -Default має на меті перекласти тягар із споживачів і малого бізнесу та великих технологічних компаній. Це означає, що в разі повного

впровадження такі великі технологічні компанії, як Microsoft і Google, нестимуть більший ступінь відповідальності, ніж середній державний підрядник, особливо компанії, які класифікуються як малий бізнес.

Перенесення тягаря відповідальності є суперечливим, оскільки до цього моменту великі компанії-розробники програмного забезпечення припускали, що якщо вони продовжуватимуть виявляти та виправляти вразливості, вони будуть захищені від більшості негативних наслідків. Насправді Microsoft інституціоналізувала ідею регулярного випуску оновлень і виправлень свого програмного забезпечення до того, що «вівторок виправлення» став основним продуктом галузі з 2003 року.

Однак, оскільки зловмисники продовжують використовувати вразливості нульового дня як ніколи раніше, потреба в безпечному програмному забезпеченні ніколи не була такою великою. У 2021 році була використана найбільша кількість нульових днів в історії, причому лідирували спонсоровані державою актори. У 2023 році злочинні групи програм-вимагачів використовували критичні вразливості, що призвело до сплати викупу на сотні мільйонів доларів.

У липні 2023 року ONCD опублікував План реалізації національної стратегії кібербезпеки, у якому вказано терміни, відповідальні установи та конкретні вказівки щодо багатьох цілей, викладених у стратегії. План, наприклад, поклав на Управління та бюджет відповідати за впровадження змін Федерального положення про закупівлі, які вимагаються відповідно до виконавчого наказу 14028 до першого кварталу 24 фінансового року, і закликав Управління науково-технічної політики працювати з різними грантами - змусити агентства визначати пріоритетність інвестицій у «мови програмування, безпечні для пам’яті».

«Безпека за проектом»

Жодне з цих положень не передбачало свіжого фінансування для впровадження. Вражаюче те, що положення «Безпека за проектом» мало один із найслабших планів впровадження в усьому документі, закликаючи ONCD провести юридичний симпозіум до другого кварталу 24 фінансового року, щоб «вивчити різні підходи до системи відповідальності за програмне забезпечення».

Зрештою, те, як розподілятимуться федеральні долари протягом наступних кількох фінансових років, визначатиме справжній вплив нової стратегії та плану впровадження. Хоча здається, що такі офіси, як ONCD і CISA, наполягають на різких змінах у сфері кібербезпеки, відсутність у них регуляторних та бюджетних повноважень може перешкодити реалізації цих планів.

У разі повного впровадження ця стратегія матиме чистий позитивний вплив на простір державних контрактів шляхом збільшення федеральних інвестицій у розробку безпечних технологій і зменшення вразливостей у основному програмному забезпеченні, яке використовують усі державні підрядники. Поки рано говорити, чи справді це сміливе бачення майбутнього стане реальністю». ***(Noah Rivers. What new federal cybersecurity policy means for government contractors // Yahoo (https://news.yahoo.com/federal-cybersecurity-policy-means-government-175959798.html?fr=sycsrp_catchall). 11.09.2023).***

***

«Міністерство внутрішньої безпеки (DHS) рекомендує федеральним чиновникам змінити спосіб, у який жертви розкривають кібератаки, створивши єдиний портал для повідомлень, а не поточний процес, який передбачає кілька різних відомств, які діють як основні контактні точки.

Ці та інші зміни в процесі звітування про кіберінциденти були детально описані Конгресу в новому звіті робочої групи DHS.

Міністр внутрішньої безпеки Алехандро Майоркас сказав, що рекомендації його команди спрямовані на те, щоб допомогти уряду зрозуміти цифрові атаки та допомогти жертвам.

«У критичний період відразу після кібератаки нашим партнерам з приватного сектору потрібні чіткі, узгоджені вказівки щодо обміну інформацією, щоб допомогти нам швидко пом’якшити несприятливі наслідки», — сказав пан Майоркас у заяві.

Відповідно до звіту, процес звітування на єдиному порталі та інші зміни необхідні, щоб запобігти подальшій шкоді федеральної бюрократії тим, хто

постраждав від небезпечних хакерів». ***(Ryan Lovelace. DHS wants to streamline victim reporting of cyberattacks, warns bureaucracy is getting in the way // The Washington Times, LLC (https://www.washingtontimes.com/news/2023/sep/21/dhs-wants-streamline-victim-reporting-cyberattacks/?utm_source=flipboard&utm_content=TheWashTimes%2Fmagazine%2FNews+From+The+Washington+Times). 21.09.2023).***

***

«Нестача фахівців з кібербезпеки в Сполучених Штатах (750 000+ відкритих вакансій станом на лютий) викликає серйозне занепокоєння з далекосяжними наслідками для національної безпеки.

Оскільки технології продовжують розвиватися, а кіберзагрози стають все більш складними та витонченими, нація стикається з гострою нестачею кваліфікованих людей, здатних захистити її фізичну та цифрову інфраструктуру.

Чим більше зв'язків ми стаємо як суспільство, тим більшою стає площа атаки для противників.

Рецепт катастрофи

Дефіцит посилюється багаторічними процесами державних закупівель, які потім продовжуються нескінченними протестами після укладання контракту. Це ставить програми національної безпеки США принаймні на одне-два покоління позаду векторів атак противника. Їх швидке впровадження та застосування пов'язаних зі штучним інтелектом технологій для автоматизації операцій лише збільшить ці прогалини.

Додайте все це до дефіциту кіберпрофесіоналів у США, і ми маємо рецепт катастрофи. Дефіцит кіберпрофесіоналів глибоко впливає на здатність Америки захищати конфіденційні дані, критичну інфраструктуру та державні системи.

Нещодавні кібератаки – Solar Winds, Oldsmar Beach, Colonial Pipeline, Pipe Dreams та інші – виявили вразливі місця старої інфраструктури та перевантажених спеціалістів із безпеки. Наразі майже кожна робота в IT у США має кіберкомпонент.

Вразливі місця від дому до батьківщини

Надмірна залежність від інструментів виявлення, які попереджають вас про інцидент, маскує більшу проблему. Як суспільство, ми все більше залежимо від понад 31 мільярда переважно незахищених пристроїв Інтернету речей, які розгортаються по всьому світу в наших будинках, транспортних засобах, комунікаційних пристроях, об'єктах для виробництва та розподілу електроенергії та води тощо.

Це неприйнятний ризик, з яким ми несвідомо, але постійно стикаємося. За останнє десятиліття ніхто не вирішив впровадити ці вразливості в наше повсякденне життя, але ми стали жабою в повільно киплячому цифровому казані.

Крім того, органи національної безпеки та військові операції значною мірою залежать від кіберспроможності. Від збору розвідданих до захисту від шпигунства, агенціям США потрібні висококваліфіковані кіберпрофесіонали для захисту від загроз з боку конкуруючих країн і недержавних організацій.

Дефіцит таких експертів підриває здатність нації створити ефективний кіберзахист, залишаючи США відкритими для зовнішніх ворогів.

Усі шукають один і той самий дефіцитний талант

Поширення кіберзагроз збільшило попит на фахівців з кібербезпеки в усіх секторах. Оскільки організації приватного та державного секторів намагаються захистити свої фізичні та цифрові активи, вони змагаються за обмежену кількість кваліфікованих кандидатів, що підвищує зарплати та вартість послуг кібербезпеки.

Малі та середні підприємства, які можуть не мати ресурсів, щоб залучити та утримати ці дорогі таланти, часто виявляються особливо вразливими.

Усі описи посад на пошукових дошках мають однакові бажання – 4-річний ступінь плюс ступінь магістра або доктора філософії, плюс 2-3 роки роботи в Центрі безпеки. Все для роботи початкової та середньої ланки!

Більше того, з приблизно 180 000 дипломів аспірантів і докторів філософії, які щорічно присуджуються в США, за оцінками, понад 50 відсотків не є громадянами США. Багато з них повернуться на батьківщину; деякі можуть навіть застосувати свої кібернавички для наших ворогів.

На жаль, існує тенденція переоцінювати «академічні» повноваження над досвідом на цих посадах. Не варто скидати з рахунків тих, хто має дипломи – їх просто не вистачає. Посадові інструкції з кібербезпеки часто завищують складність, порівнюючи їх із знаннями, необхідними для медичної професії.

Значний відсоток цих вакансій можуть бути зайняті людьми, які проходять навчальні табори тривалістю 16 тижнів або менше або програми отримання мікросертифікатів. є співробітники США, Насправді на передовій кібернетики які не мають ступеня доктора філософії, магістра чи навіть бакалавра.

Змусити промислові та державні комісії з найму комфортно приймати нетрадиційні та досвідчені таланти на кіберпосади є культурною, а не технічною перешкодою.

Навіть відповідність мінімальним академічним вимогам після 6–9 років навчання та навчання може залишити кандидатів із обмеженим практичним досвідом роботи з клавіатурою. Вони також часто мають заборгованість у коледжі, а державні посади платять значно менше, ніж Google, Meta чи Microsoft.

Вирішення проблеми можна почати зараз

Вирішення цих проблем вимагає багатогранного підходу. Освіті та навчанню слід віддавати пріоритет від початкової освіти до університетських і нетрадиційних програм сертифікації. Заохочення студентів до кар’єри в галузі кібербезпеки, інформатики та суміжних галузях може допомогти створити конвеєр кваліфікованих експертів.

Крім того, програми перепідготовки та підвищення кваліфікації можуть допомогти фахівцям із суміжних дисциплін перейти на посади з кібербезпеки. Учнівство та мікросертифікати, які можна передавати, також допоможуть.

Державно-приватне партнерство має вирішальне значення. Співпраця між державними установами, науковими установами та приватним сектором може сприяти обміну знаннями, досвідом і ресурсами. Пропонування таких стимулів, як стипендії, стажування та гранти, залучить більше людей. Різноманітні та інклюзивні практики найму можуть розширити коло потенційних кандидатів, забезпечуючи ширший спектр перспектив.

Якщо не впоратися з гострою нестачею кіберперсоналу, США можуть стати жертвою кібератак із далекосяжними наслідками, що вплине на критичну інфраструктуру, економічну стабільність і загальну безпеку. Для створення наступного покоління кіберпрофесіоналів не потрібно і не повинно знадобитися від 7 до 9 років.

Зусилля, спрямовані на інвестування в освіту, навчання та співпрацю між секторами, мають важливе значення для створення сильної та спроможної робочої сили з кібербезпеки, яка зможе захистити цифровий ландшафт країни. Створення можливостей для людей, які не мають диплому, вийти на сферу діяльності та/або перекваліфікувати людей, які хочуть повернутися до робочої сили, є єдиним життєздатним варіантом задоволення попиту». ***(Paul Maguire. How to Fix the Dearth of US Cyber Professionals Impacting National Security // The Defense Post (https://www.thedefensepost.com/2023/09/22/us-cyber-professionals-national-security/). 22.09.2023).***

***

«Останніми тижнями спостерігався сплеск новин про діяльність, пов'язану з кібернетичною діяльністю False Claims Act (FCA). Наприклад, 1 вересня 2023 року суд розпечатав позов qui tam проти Університету штату Пенсільванія щодо звинувачень у недотриманні зобов'язань Міністерства оборони («DoD») щодо кібербезпеки. Крім того, 5 вересня 2023 року Міністерство юстиції (DOJ) оголосило про багатомільйонну угоду FCA з Verizon у рамках своєї Ініціативи цивільного кібершахрайства (яка зосереджена на залученні FCA для переслідування шахрайства, пов'язаного з кібербезпекою, державними підрядниками та одержувачі грантів, як ми вже обговорювали тут). Ці та інші випадки свідчать, як багато хто припускав, що кількість правоохоронних заходів і розголосу, пов'язаних із раніше закритими справами qui tam, продовжуватимуть збільшуватися. Вони також сигналізують, що підрядники та університети повинні підготуватися до додаткової перевірки та потенційних претензій інформаторів у цій сфері.

Звинувачення інформаторів щодо відповідності DFARS кібербезпеці

1 вересня 2023 року Окружний суд США для Східного округу Пенсільванії розпечатав позов qui tam FCA (спочатку поданий 5 жовтня 2022 року), який стверджував, що Університет штату Пенсільванія не забезпечив «адекватну безпеку» закритої інформації захисту (CDI), відповідно до договірних вимог пункту DFARS 252.204-7012. Згідно з цим пунктом, «адекватна безпека» визначається як (принаймні) впровадження всіх 110 елементів керування, викладених у NIST SP 800-171. Крім того, федеральні правила вимагають, щоб підрядники Міністерства оборони проводили самооцінку дотримання цих 110 заходів контролю та повідомляли про оцінку відповідності (зі 110) у Системі ризиків ефективності постачальників Міністерства оборони (SPRS).

Серед іншого, у позові стверджується, що Penn State сфальсифікував щонайменше 20 документів, пов'язаних із його самооцінкою NIST SP 800-171 та іншими самоатестаціями. Зокрема, у позові стверджується, що незважаючи на те, що «ніколи не досяг відповідності DFARS», університет «неправдиво засвідчував відповідність з 1 січня 2018 року». У позові також стверджується, що конфіденційна інформація опинилася під загрозою, коли університет переніс частину своїх даних у комерційну хмарну службу зберігання.

У 2015 році співрозмовник у цій справі працював тимчасовим керівником інформаційної служби в Лабораторії прикладних досліджень Пенсильванського штату та був частиною групи, призначеної для оцінки відповідності Університету штату Пенсільванія на початку 2022 року. Міністерство юстиції поки що не втрутилося та має повідомити Суд до 29 вересня 2023 року, якщо має намір вступити у справу.

Цей позов інформатора FCA є значущим принаймні з двох причин. По-перше, це підтверджує те, що підрядники та субпідрядники Міністерства оборони є легкою мішенню для викривачів, особливо коли вони мають надзвичайно довгі списки дій, як-от 110 заходів контролю, які вони регулярно підтверджують. Таким чином, надзвичайно важливо вжити заходів для забезпечення того, щоб самоатестації та заяви були точними, а також щоб вони сприяли культурі співпраці,

прозорості та підзвітності, коли йдеться про кібербезпеку, щоб знизити ймовірність того, що працівник стане інформатором. По-друге, університети та інститути вищої освіти з державними контрактами не захищені від претензій FCA, пов'язаних з кібернетичною інформацією, і повинні переконатися, що вони розуміють і дотримуються державних норм кібербезпеки.

Міністерство юстиції України щодо врегулювання ініціативи щодо цивільного кібершахрайства

5 вересня 2023 року Міністерство юстиції оголосило про своє останнє врегулювання справи про кібершахрайство в рамках Ініціативи цивільного кібершахрайства. Згідно з мировою угодою Verizon Business Network Services, LLC («Verizon») погодилася виплатити 4 091 317 доларів США за розв'язання звинувачень Закону про неправдиві претензії щодо того, що вона не повністю задовольнила певні засоби контролю кібербезпеки у зв'язку з послугою інформаційних технологій, наданою федеральним агентствам. Зокрема, угода стосується керованої довіреної служби Інтернет-протоколу Verizon (MTIPS), яка призначена для надання федеральним агентствам безпечного підключення до публічного Інтернету та інших зовнішніх мереж. Міністерство юстиції стверджувало, що рішення MTIPS від Verizon не повністю задовольняє три обов'язкові параметри контролю кібербезпеки для довірених підключень до Інтернету щодо контрактів з адміністрацією загального обслуговування («GSA») з 2017 по 2021 рік.

Вирішуючи звинувачення, Міністерство юстиції пояснило, що Verizon отримала значну заслугу, оскільки Verizon самостійно розкрила проблему, ініціювала незалежне розслідування та перевірку відповідності проблем, а також надала додаткові письмові розкриття інформації. Verizon також співпрацювала з урядовим розслідуванням і вжила оперативних і істотних заходів для виправлення ситуації. У мировій угоді пояснюється, що 2,7 мільйона доларів із суми мирової угоди є реституцією, що означає, що приблизно 1,3 мільйона доларів припадає на застосування урядом множника (згідно з FCA, уряд може вимагати відшкодування збитків у потрійному розмірі, а також певні передбачені законом штрафи). Тут

загальна сума компенсації приблизно в 1,5 рази перевищує суму відшкодування. Це досить поширене явище у випадках, коли підрядники самостійно виявляють невідповідність вимогам, як це зробив Verizon.

Це рішення Міністерства юстиції підкреслює важливість надійних систем відповідності підрядників і культури, яка сприяє внутрішнім перевіркам для виявлення проблем, самовиявленню, внутрішнім розслідуванням і співпраці з урядом.

Основні висновки для федеральних підрядників і університетів

(Повторний) перегляд і підтвердження розуміння зобов'язань і практики кібербезпеки. Зараз гарний час для підрядників та університетів переглянути свою позицію щодо кібербезпеки та переконатися, що зусилля з дотримання нормативних вимог належним чином ведуться, а будь-які самоатестації та заяви є точними та обґрунтованими. Зобов'язання державного підрядника щодо кібербезпеки є складними та можуть заплутати – переконайтеся, що ваша команда добре розуміє вимоги, а якщо ні, заручіться допомогою для навчання та інструктажів.

Створіть потужну функцію контролю відповідності та аудиту/моніторингу. Підрядники та університети повинні розуміти зобов'язання щодо кібербезпеки, дотримуватися необхідних стандартів і впроваджувати сувору політику, процедури та засоби контролю. Постійні/постійні внутрішні перевірки мають вирішальне значення для виявлення та вирішення будь-яких потенційних прогалин у дотриманні.

Оперативно розслідуйте внутрішні скарги. Внутрішні скарги можуть бути складними, особливо враховуючи, що система відповідності вимогам кібербезпеки є складною та швидко змінюється в реальному часі. Внутрішні скарги цілком можуть бути законними. Але також можливо, що працівники можуть не повністю розуміти справжні зобов'язання компанії щодо відповідності. Компанії повинні серйозно ставитися до всіх внутрішніх скарг, а також розглянути питання про наймання адвоката та/або незалежних консультантів, щоб забезпечити належне розслідування скарг щодо фактичних зобов'язань компанії щодо відповідності та

внесення виправлень, якщо це необхідно. Крім того, як нещодавно багато писав наш колега Девід Дуглас, повага до занепокоєнь працівників, розуміння занепокоєнь і тримання співробітників у курсі подій під час внутрішніх розслідувань призводить до зміцнення організації.

Нещодавнє правозастосування – це лише початок. Увага до цієї сфери не зникне найближчим часом. Таким чином, ми очікуємо значного збільшення примусових дій (як з ініціативи уряду, так і з ініціативи інформаторів). Якщо відповідність кібербезпеці не була на першому місці у вашому списку, настав час (і, ймовірно, минулий час) перемістити його вгору». ***(Townsend L. Bourne, Nikole Snyder. Recent Cyber-Related False Claims Act Activity Signals Contractors and Universities Should Examine Their Cybersecurity Practices and Brace for an Uptick in Enforcement // Sheppard Mullin (https://www.organizationalintegrity.com/2023/09/recent-cyber-related-false-claims-act-activity-signals-contractors-and-universities-should-examine-their-cybersecurity-practices-and-brace-for-an-uptick-in-enforcement/#page=1). 12.09.2023).***

***

«Управління кіберризиками є фундаментальним питанням для університетів, державних органів та інших організацій. Генеральний аудитор Британської Колумбії нещодавно опублікував аудиторський звіт, у якому виявилося, що рада керівників університету не забезпечила належного нагляду за практикою управління ризиками кібербезпеки в університеті. Звіт містить корисні рекомендації для рад університетів та інших державних рад директорів у Британській Колумбії та по всій Канаді.

Фон

Кіберризики – ризики втрат і витрат/зобов’язань, які зазнає або несе організація в результаті інциденту, який негативно впливає на системи інформаційних технологій організації або на конфіденційність, цілісність або доступність даних організації – є критичним організаційним ризиком. Канадського центру кібербезпеки Національна оцінка кіберзагроз на 2023-2024 роки

попереджає, що програми-вимагачі є постійною загрозою для канадських організацій.

Кібербезпека має бути пріоритетом для всіх канадських університетів. Численні канадські університети зазнали резонансних атак програм-вимагачів, що призвело до збоїв у роботі, втрати конфіденційних даних (включаючи особисту інформацію) та завдало шкоди репутації. Їх роль у проведенні досліджень також робить університети мішенями для шпигунства та крадіжки інтелектуальної власності, в тому числі суб'єктами, які фінансуються державою. Ця загроза пов'язана з унікальною проблемою: мережі університетських інформаційних технологій дуже розподілені, що ускладнює їх захист, а колегіальне управління та культурні норми в університетах можуть перешкоджати впровадженню надійних практик кібербезпеки.

Рада керуючих університету зазвичай несе загальну відповідальність за управління, адміністрування та контроль над майном університету, доходами, бізнесом і справами, що вимагає від ради ефективного нагляду за рішеннями та діяльністю керівництва університету. Отже, рада керуючих університету повинна бути залучена та брати активну роль у діяльності університету з управління кіберризиками та переконатися, що керівництво університету ефективно впровадило відповідну політику та практику для управління кіберризиками та реагування на інциденти кібербезпеки.

Звіт Генерального аудитора

Генеральний аудитор Британської Колумбії є незалежною посадовою особою Законодавчого органу Британської Колумбії, який відповідає за проведення перевірок державних установ з метою інформування людей Британської Колумбії та їх обраних представників про те, як уряд керує своїми обов'язками та ресурсами. У серпні 2023 року Генеральний аудитор оприлюднив звіт про перевірку практики нагляду за кібербезпекою ради керуючих Університету острова Ванкувер (VIU), державного університету відповідно до Закону про університет Британської Колумбії з головним кампусом у Нанаймо, де навчаються 12 200 і рада керуючих із

15 членів. У звіті пояснюється, що VIU був обраний для перевірки, «оскільки він має такий самий розмір, як багато інших університетів Британської Колумбії».

У відео на YouTube, яке оголошує звіт, Генеральний аудитор пояснює, що кількість атак на кібербезпеку зростає, а рада керівників кожного університету відіграє «важливу роль у нагляді за управлінням ризиками кібербезпеки». Вони переглядають стратегії захисту IT-систем і особистих даних і притягують керівництво університету до відповідальності за ці стратегії». У звіті Генерального аудитора додатково пояснюється роль керівництва VIU та ради керуючих. Керівництво несе відповідальність за проведення оцінки ризиків, впровадження та функціонування процесів зменшення ризиків, а також звітування правлінню про статус програм управління ризиками. Очікується, що рада контролюватиме управління ризиками кібербезпеки, оцінюючи, чи керівництво: (1) має чинні політики та процедури кібербезпеки; (2) регулярно оцінює та контролює ризики кібербезпеки; і (3) отримує регулярні звіти про стан кібербезпеки установи.

Генеральний аудитор виявив, що рада керуючих VIU визначила ролі та обов'язки щодо нагляду за управлінням ризиками та встановила очікування щодо покращення управління ризиками підприємства, включаючи кібербезпеку. Однак генеральний аудитор дійшов висновку, що рада не забезпечила належного нагляду за методами VIU щодо управління ризиками кібербезпеки. У звіті пояснюються такі висновки:

1. Рада встановила наглядові ролі та обов'язки, але політики були застарілими, а відгуки не були задокументовані.

Генеральний аудитор сподівався, що VIU матиме задокументовані ролі та відповідальність за нагляд правління за управлінням ризиками кібербезпеки за допомогою політики управління та управління ризиками, включаючи оцінку правлінням того, чи відповідає президент очікуванням щодо управління ризиками кібербезпеки.

Генеральний аудитор виявив, що політика управління ризиками застаріла. Правління востаннє переглядало та схвалювало цю політику в 2012 році,

незважаючи на запланований перегляд у 2017 році. Рада перевіряла, але офіційно не затверджувала оновлену політику в 2023 році.

Генеральний аудитор також виявив, що рада встановила президентські цілі, пов'язані з кібербезпекою, і розглянула показники президента щодо цілей через щоквартальні оновлення, але рада не задокументувала свій зворотний зв'язок з президентом.

2. Рада не мала відповідної підготовки/навчання для нагляду за управлінням ризиками кібербезпеки.

Генеральний аудитор сподівався, що VIU матиме орієнтаційну програму для правління, яка б конкретно стосувалася обов'язків ради з нагляду за управлінням ризиками кібербезпеки, а також щорічну програму розвитку (навчання) для членів правління, щоб допомогти підвищити їхні предметні знання в сферах ризику, включаючи ризики кібербезпеки., щоб допомогти їм у виконанні їхніх наглядових обов'язків або розглянути зміни в наглядовій ролі правління.

Генеральний аудитор виявив, що VIU не відповідає обом вимогам. Орієнтаційна програма правління, хоч і стосується управління ризиками та згадує кібербезпеку, не містить інформації про наглядові обов'язки ради щодо управління ризиками кібербезпеки. Крім того, у правління не було щорічної програми розвитку для оновлення сфер значного ризику, таких як управління ризиками кібербезпеки, хоча політика управління VIU вимагала програми.

3. VIU мала задокументовану структуру управління ризиками, але правління не вчасно переглядало стратегії зменшення ризиків керівництва.

Генеральний аудитор сподівався, щоб рада регулярно переглядала оцінки керівництвом ризиків кібербезпеки, включно з тим, як керівництво оцінювало та зменшувало ризики кібербезпеки, визначало пріоритетні сфери ризиків, а також задокументовані дії та результати пом'якшення. Генеральний аудитор також звернувся до правління, щоб підтвердити, що керівництво оцінило дотримання правових і нормативних вимог.

Генеральний аудитор виявив, що рада перевірила систему управління ризиками кібербезпеки VIU і підтвердила, що система та політика були доведені до

відома персоналу, студентів та інших ключових груп. Однак Генеральний аудитор також виявив, що рада занадто повільно виконує свої наглядові обов'язки через затримку між визначенням керівництвом кібербезпеки як пріоритетного ризику в червні 2022 року та переглядом правлінням у березні 2023 року задокументованої оцінки ризиків і плану пом'якшення. У звіті пояснюється: «Правління зобов'язане просити керівництво надати [стратегії зменшення ризиків кібербезпеки] протягом року, щоб допомогти забезпечити постійну оцінку реакції керівництва на ризики кібербезпеки».

У звіті підсумовуються чотири рекомендації Генерального аудитора:

Переконайтеся, що керівні та політичні документи, що визначають ролі та відповідальність за управління ризиками кібербезпеки, переглядаються та затверджуються за графіком.

Створіть річну програму розвитку та переконайтеся, що члени правління проходять щорічне навчання з управління ризиками кібербезпеки, щоб підтримати їх у виконанні наглядових функцій.

Оновіть програму ознайомлення з правлінням, щоб включити інформацію про ролі та обов'язки щодо нагляду за управлінням ризиками кібербезпеки.

Щороку переглядайте стратегії зменшення ризиків кібербезпеки.

Звіт підтверджує, що VIU прийняв усі рекомендації.

Інші корисні вказівки

Звіт Генерального аудитора є частиною зростаючої кількості вказівок, виданих урядовими установами, регуляторами та авторитетними організаціями, щоб допомогти радам виконувати свої обов'язки щодо управління кіберризиками. Нижче наведено приклади нещодавно опублікованих або оновлених інструкцій.

У жовтні 2022 року Австралійський інститут директорів компаній і Австралійський спільний дослідницький центр кібербезпеки опублікували вказівки під назвою «Принципи управління кібербезпекою», щоб допомогти директорам, фахівцям з управління та їхнім організаціям активно наглядати за кіберризиками та керувати ними. Посібник призначений для організацій усіх видів і розмірів, включаючи малі та середні підприємства та неприбуткові організації. У посібнику

пояснюється, що кібербезпека має бути вбудованою в існуючу практику управління ризиками (включно з регулярним звітуванням і оцінкою засобів контролю кіберризиків), які відображають кіберапетити організації, схвалені радою директорів.

Сполученого Королівства У березні 2023 року Національний центр кібербезпеки анонсував оновлену версію свого набору інструментів кібербезпеки для правлінь, щоб допомогти радам забезпечити, щоб кіберстійкість і управління ризиками були вбудовані в їхні організації. Інструментарій пояснює важливі аспекти кібербезпеки, рекомендує дії для окремих директорів та їхніх організацій, а також містить запитання та відповіді, щоб допомогти директорам приймати обґрунтовані рішення щодо управління кіберризиками. Подібно до звіту Генерального аудитора щодо VIU, Інструментарій пояснює, що управління ризиками кібербезпеки має бути «безперервним ітеративним процесом», а розгляд кіберризиків має бути інтегрованим у загальноорганізаційні процеси управління ризиками та прийняття рішень.

У березні 2023 року Національна асоціація корпоративних директорів і Альянс безпеки в Інтернеті опублікували четверте видання Посібника директора з нагляду за кіберризиками, щоб надати корпоративним директорам оновлені вказівки, які відображають зміни в ландшафті кіберзагроз. Посібник зосереджений на шести ключових принципах покращення нагляду за кіберризиками для організацій усіх типів і розмірів. Принципи узгоджуються з практиками, рекомендованими у звіті Генерального аудитора щодо VIU. Наприклад, ради повинні вимагати від керівництва ідентифікувати та кількісно оцінювати кіберризики, обумовлювати, які ризики слід приймати, пом’якшувати чи передавати, а також документувати плани управління ризиками.

Коментарі

Управління ризиками кібербезпеки вимагає від правління організації та вищого керівництва приймати бізнес-рішення на основі оцінки ризиків, які відповідають толерантності організації до ризику. Щоб ці рішення були обґрунтованими та обґрунтованими, вони повинні бути поінформованими (тобто

базуватися на своєчасній, повній та достовірній інформації) і прийматися чесно та добросовісно за допомогою відповідних порад незалежних та кваліфікованих бізнес-, юридичних та технічних експертів...

Управління ризиками кібербезпеки передбачає дотримання законів про конфіденційність/захист особистої інформації, законодавства про працю/зайнятість і прав людини, і часто вимагає особливої уваги під час переговорів та адміністрування контрактів із постачальниками послуг/постачальниками та клієнтами. Своєчасна юридична консультація може допомогти організації керувати ризиками кібербезпеки відповідно до нормативних вказівок і найкращих практик, дотримуючись вимог законодавства. Крім того, юридичний радник, який регулярно виступає в якості інструктора з інцидентів у сфері кібербезпеки, може надати унікальне уявлення про поточне середовище загроз і переважну практику реагування на інциденти. З цих причин у Посібнику директора NACD/ISA з нагляду за кіберризиками пояснюється, що ради «повинні розуміти правові наслідки кіберризиків, оскільки вони стосуються конкретних обставин [організації]», і рекомендує, щоб ради проводили «регулярні засідання з юридичних питань»., регулятивні чи договірні тенденції» та залучити зовнішніх консультантів, щоб надати «багатоклієнтську та галузеву точку зору на тенденції кіберризиків». ***(Daniel J. Michaluk, Bradley Freedman. The Vancouver Island University audit report – board oversight of cybersecurity risk management // Borden Ladner Gervais LLP (https://www.blg.com/en/insights/2023/09/vancouver-island-university-audit-report-board-oversight-of-cybersecurity-risk-management). 13.09.2023).***

***

«Національна стратегія кібербезпеки (NCS) — це план уряду США зі створення безпечної та захищеної цифрової екосистеми шляхом захисту критично важливої інфраструктури (наприклад, лікарень і об’єктів чистої енергетики) від кіберзагроз, розширення державних/приватних партнерств і співпраці з міжнародними коаліціями, а також зміцнення його технологічне

управління. Мета полягає в тому, щоб цифрову інфраструктуру легше захистити, ніж атакувати, і зробити її безпечною та доступною для всіх американців. Ключовою частиною NCS є підтримка зусиль щодо конфіденційності шляхом підвищення відповідальності технологічних компаній та інших підприємств, які працюють з даними людей. У цьому посібнику висвітлюється те, що компанії повинні знати про план.

Чому США потрібна національна стратегія кібербезпеки?

Ризик, який становлять загрози кібербезпеці, величезний, а наслідки цілеспрямованих атак ще більші. На індивідуальному рівні порушення даних можуть спричинити крадіжку особистих даних і втрату доходу; на корпоративному рівні вони можуть порушити безперервність бізнесу, завдати шкоди репутації та викрасти інтелектуальну власність; а на урядовому рівні вони можуть завдати шкоди установам, вимкнути електромережі та комунікаційні мережі.

Останніми роками спостерігається збільшення кількості спонсорованих державою кібератак — згідно з урядовими даними, з 2000 по 2022 рік вони зросли на 300 відсотків. Для підприємств середня фінансова вартість атаки програм-вимагачів уже перевищує 4,5 мільйона доларів США, і ці атаки стають лише складнішими.

Національна стратегія кібербезпеки – це зусилля уряду, спрямоване на розширення державно-приватного партнерства, зміцнення захисту та альянсів у сфері кібербезпеки, захист мереж, систем, функцій і даних, продовжуючи просувати технологічні інновації. Деякі з цілей плану включають наступне:

Спрощення звітування про загрози

Створення реакції першого дотику на кібератаки

Розробка термінів і методів виконання

Розподіл ресурсів і визначення відповідальних державних органів

Стимулювання кібергігієни

Удосконалення державно-приватного партнерства

Що таке Національна стратегія кібербезпеки?

NCS — це план дій із п’яти компонентів, спрямований на посилення зусиль із кібербезпеки та об’єднання всіх зацікавлених сторін для досягнення успіху. Надійна національна політика кібербезпеки має важливе значення для того, щоб розвивати перспективи нових технологій і одночасно мінімізувати ризики, які вони несуть.

Стовп перший: захист критично важливої інфраструктури

Захист критичної інфраструктури, включаючи системи та активи, життєво важливий для національної безпеки, громадської безпеки та економічного процвітання. NCS стандартизує стандарти кібербезпеки для критичної інфраструктури, наприклад, обов’язкові тести на проникнення та формальне сканування вразливостей, і спростить повідомлення про інциденти та порушення кібербезпеки.

Він прагне позначити постачальників інфраструктури як послуги (IaaS) як «критичну інфраструктуру», поклавши на них більше обов’язків щодо забезпечення безпеки та захисту даних і використовуючи юридичну відповідальність для усунення небезпечних програмних продуктів і невиправлених уразливостей. Він також запровадить модель кібербезпеки з нульовою довірою для федеральних мереж.

Стовп другий: знищення та демонтаж суб’єктів загрози

Після того як національна інфраструктура буде захищена та забезпечена, NCS активізує зусилля з нейтралізації загроз, які можуть поставити під загрозу кіберекономіку. Ці зусилля покладатимуться на глобальну співпрацю та обмін розвідувальними даними для боротьби з нестримними кампаніями з кібербезпеки та надання підтримки підприємствам шляхом використання національних ресурсів для тактичного знищення супротивників.

Компоненти цього стовпа включають підвищення обізнаності про суб’єктів загрози, програми-вимагачі, крадіжки IP-адреси та інші зловмисні атаки, а також створення Ради з перевірки кібербезпеки (CSRB) для перегляду катастрофічних інцидентів і розробки стратегії на основі повторюваних моделей атак. Він також запровадить нові вказівки для галузей промисловості, які вже постраждали,

наприклад, виробництво, енергетика, охорона здоров'я та державний сектор, а також нові стандарти опису матеріалів для програмного забезпечення, щоб знизити ризики ланцюжка поставок.

Стовп третій: формування ринкових сил для забезпечення безпеки та стійкості

Будучи найбільшою економікою світу, США мають достатньо ресурсів, щоб очолити кібербезпеку, що розрахована на майбутнє, і підвищити впевненість і стійкість у секторі програмного забезпечення. Мета полягає в тому, щоб дати можливість приватним компаніям довіряти екосистемі, створювати інноваційні системи, забезпечувати мінімальний збиток і забезпечувати стабільність ринку під час катастрофічних подій.

Пріоритетний план на цьому етапі включає зусилля щодо захисту конфіденційності та безпеки особистих даних шляхом створення федеральних грантів для заохочення інвестицій у безпечну інфраструктуру та інвестування в ініціативи кіберстрахування, щоб допомогти приватним компаніям відновитися від масштабних атак. Він також запровадить програму маркування безпеки Інтернету речей (IoT), щоб підвищити обізнаність споживачів про ризики пристроїв IoT.

Стовп четвертий: інвестуйте в стійке майбутнє

Щоб агресивно поєднувати інновації з безпекою та створювати неприступний щит проти зростаючої кількості кіберзлочинів, уряд виділив кошти для захисту технологій наступного покоління, одночасно забезпечуючи необхідну передачу технологій і поширення інформації між приватним і державним секторами. NCS зробить особливий поштовх для виявлення даних, архітектури захисту та шифрування в усіх зв'язках уряду та бізнесу.

Цей компонент також включає стажування з кібербезпеки та Національний альянс кіберкриміналістики та навчання для навчання робочої сили та підвищення рівня кіберграмотності, а також розгортання унікальної цифрової автентифікації для запобігання фішинговим атакам і створення надійної системи цифрової ідентифікації (TDIF).

П’ятий компонент: налагодження міжнародних партнерств для досягнення спільних цілей

Глобальні лідери дізнаються, що кібердипломатія є найбільш перспективною стратегією для перетворення ворогів на союзників. Завдяки п’ятому компоненту уряд візьме на себе зобов’язання продовжувати глобальні ініціативи проти цифрової війни та створювати надлишок довіри серед союзників.

Серед способів, якими вона сподівається досягти цього, є створення централізованого трекера для координації ініціатив із розподілу витрат, створення безпечних і надійних глобальних ланцюгів постачання та зміцнення потенціалу країн-партнерів для захисту від кіберзагроз. Він також створить інфраструктуру розвідки про загрози для співпраці з союзниками та глобальними агентствами.

Що підприємствам потрібно знати про NCS?

Підприємствам доведеться дещо змінити своє мислення щодо кібербезпеки в рамках NCS. У ньому наголошується, що добровільного прогресу в напрямку кращої кібербезпеки та практик конфіденційності даних уже недостатньо, а, можливо, взагалі не працює. Більше того, уряд запровадить нові стандарти та регуляторні рамки та перекладе відповідальність на підприємства, які не виконають свою роль. Це також стимулюватиме найкращі практики кібербезпеки.

Нижче наведено три основні дії, до яких NCS змушуватиме підприємства:

Виявляйте та мінімізуйте вразливості, вживаючи профілактичних заходів для тестування та захисту свого середовища загроз, а також холдингових партнерів і сторонніх постачальників за аналогічними стандартами кібербезпеки.

Усувайте вразливості ланцюга постачання, обмінюючись інформацією через нові державно-приватні партнерства, виправляючи відомі вразливості, забезпечуючи навчання працівників кібербезпеці та розробляючи плани реагування на критичні інциденти.

Розробляючи програмне забезпечення, процеси, продукти та мережі, щоб захистити конфіденційність і дані, приділяйте увагу питанням кібербезпеки. NCS чітко дає зрозуміти, що очікує від компаній більшої відповідальності та намагатиметься її дотримуватись.

Підсумок: корпоративні зміни в NCS

Національна стратегія кібербезпеки є першою ініціативою уряду США з кібербезпеки за 15 років. Таким чином, це живий документ, план, який постійно розвивається, щоб створити кіберстійкість і захистити США та їхніх союзників від загроз. Більше ніж просто заповнення прогалин, він амбітно прагне прокласти шлях до міцного, справедливого та інклюзивного кібермайбутнього. Підприємства будь-якого розміру повинні будуть зіграти певну роль у його розгортанні та матимуть важливе значення для його успіху, але він націлений особливо на підприємства: ставки вищі, ресурсів більше, а їхні відповіді можуть служити основою та найкращим практики для малих підприємств». ***(Avya Chaudhary. National Cybersecurity Strategy: What Businesses Need to Know // TechnologyAdvice (https://www.datamation.com/security/national-cybersecurity-strategy-what-businesses-need-to-know/). 25.09.2023).***

***

Країни ЄС та Великобританія

«У серпні 2023 року уряд Великої Британії опублікував свій Національний реєстр ризиків за 2023 рік («Реєстр ризиків») із переліком 89 основних публічно визнаних ризиків, з якими стикається Велика Британія.

Кібератаки на газову інфраструктуру, інфраструктуру електроенергетики, цивільну ядерну інфраструктуру, інфраструктуру постачання палива, систему охорони здоров’я та соціального забезпечення, транспортний сектор, телекомунікаційні системи та один або декілька роздрібних банків Великобританії названі ключовими ризиками у звіті.

Таким чином, ризики, пов’язані з кібернетичною діяльністю, займають важливе місце, і враховуючи кількість кібератак на критично важливу національну інфраструктуру в усьому світі, уряд Великобританії підтвердив свій намір переглянути зобов’язання щодо кібербезпеки, які містяться в Регламенті мережевих та інформаційних систем («NIS») 2018 року. Однак через відсутність проекту британського еквівалента Директиви ЄС «NIS2» організації наразі мають лише ті

матеріали, які компетентні органи NIS опублікували (та оновили), щоб вказати, які організації критичної національної інфраструктури (CNI) повинен зробити.

Велика увага приділяється енергетичній безпеці

Одним із ключових висновків у Реєстрі ризиків було те, що саме енергетична безпека є «ризиком, що зростає», і, зокрема, класифікація трьох основних ризиків, включаючи «перебої в постачанні енергії», які раніше були виключені зі звіту, тепер була зроблена. громадськість.

Ця підвищена прозорість стала результатом попередньої критики «неприйнятного та непотрібного рівня секретності» спеціальним комітетом Палати лордів з оцінки ризиків і планування ризиків. Деякі ризики все ще не згадуються в документі з міркувань національної безпеки, але ймовірно, що деякі з них також будуть пов'язані з кібернетичною природою.

Виконання зобов'язань щодо перегляду Правил UK NIS 2018

Після консультацій, які почалися в січні 2022 року, уряд Великої Британії оголосив про свій намір оновити правила NIS 2018, щоб покращити кіберстійкість Великобританії.

Вихід Сполученого Королівства з ЄС означає, що тиск щодо забезпечення гармонізації заходів між державами-членами ЄС не застосовується однаково, і тим часом уряд має вирішити інші гострі політичні та законодавчі проблеми.

Хоча Сполучене Королівство не відразу пішло по стопах ЄС NIS2, збільшення кіберризику, як зазначено в Національному реєстрі ризиків 2023 року, уряд Великобританії все ж залишив цю тему в законодавчому порядку денному; про що свідчать відповіді на подальші запитання після консультацій, надані в Палаті громад на початку 2023 року та в Палаті лордів у березні та червні 2023 року.

Дії компетентного органу

У той час як уряд Великобританії буде основним рушієм змін, компетентні органи NIS також прагнули реагувати на підвищення рівня загрози у відповідних секторах. Кілька останніх прикладів:

Ofgem

Як призначений співкомпетентний орган разом з Департаментом енергетичної безпеки та Net Zero (раніше BEIS) для газового та електричного секторів у Великій Британії, Ofgem також продемонстрував серйозність, з якою вони підходять до теми кібернетики, призначивши Стюарта. 16 червня 2023 року Окін став членом команди вищого керівництва.

Приєднавшись до Ofgem у 2019 році та отримавши завдання налагодити функцію кіберрегуляції, Один наглядав за впровадженням рамок відповідності перехідних, газових та електричних мереж та інформаційних систем (NIS), а також технічним керівництвом для інвестицій RIIO Price Control.

У квітні 2022 року Ofgem опублікував вичерпні рекомендації NIS для операторів низьких потоків газу та електроенергії, що надають основні послуги у Великій Британії з метою допомогти OES у виконанні їхніх регулятивних обов’язків і в постійному управлінні безпекою та стійкістю відповідних мереж та інформаційних систем. Рекомендації щодо правозастосування та штрафної політики стали доступними в грудні 2022 року. Ofgem продовжує консультуватися з OES на цю тему, звернувшись до NIS Reporting у лютому 2023 року, зокрема щодо переглянутих версій шаблонів звітності для покращення звітності. Після цього 17 травня 2023 року було опубліковано рішення прийняти переглянуті версії шаблонів звітності.

Ofcom

Подібним чином у травні 2023 року Ofcom, як компетентний орган для компаній у підсекторі цифрової інфраструктури, опублікував своє рішення переглянути свої вказівки щодо OES у підсекторі цифрової інфраструктури.

Це включало зниження порогових значень для звітування про інциденти: вплив на споживачів, необхідний для звітування про інцидент, тепер нижчий. Це рішення було прийнято у відповідь на наслідки коронавірусу та додаткову важливість цифрових провайдерів після опублікування останньої версії в 2018 році.

Ядерний

Зобов'язання щодо ядерної кібербезпеки окремо виокремлені з Регламенту NIS 2018 року, і ще невідомо, чи вирішить Велика Британія оновити Регламент безпеки ядерної промисловості 2013 року, щоб виконати Стратегію цивільної ядерної кібербезпеки 2022 року. На сьогоднішній день жодного оголошення чи процесу консультацій не матеріалізовано.

На винос

Відповідно, хоча на сьогоднішній день не було накладено жодних штрафів відповідно до Регламенту NIS 2018, організації, які є OES, і їх відповідальна посадова особа NIS (NRO), зокрема, повинні приділяти пильну увагу як діям уряду Великобританії, так і діям відповідних компетентних органів. орган (або органи). Організації повинні вжити заходів для підвищення своєї стійкості, покращити планування реагування на інциденти, щоб вони могли діяти швидко та належним чином у разі інциденту, щоб зменшити шкоду, і переконатися, що вони можуть пояснити свій вибір щодо управління ризиками у разі збою». ***(Ridvan Canbilen and Jessica Matheret. Cyber risk in Critical National Infrastructure features prominently in UK 2023 National Risk Register // Herbert Smith Freehills (https://hsfnotes.com/cybersecurity/2023/09/05/cyber-risk-in-critical-national-infrastructure-features-prominently-in-uk-2023-national-risk-register/#page=1). 05.09.2023).***

***

«Команда DACB Cyber and Data Risk надає короткий виклад шостого щорічного звіту про активний кіберзахист Національного центру кібербезпеки.

З 2017 року Національний центр кібербезпеки («NCSC») запустив програму під назвою «Активний кіберзахист» («ACD»), намагаючись захистити бізнес-спільноту Великобританії від значної кількості кібератак на товари. Метою програми ACD є «Захистити більшість людей у Великій Британії від більшості шкоди, спричиненої більшістю кібератак у більшості випадків».

4 липня 2023 року NCSC опублікувала свій шостий щорічний звіт про програму ACD, у якому, зокрема, виявилося, що фішинг залишається найпоширенішим типом кібератак у Великобританії з понад 77 000 інцидентів. У світлі цього цікаво відзначити, що у звіті зазначено, що фішингові кампанії на тематику уряду Великобританії зменшилися на 17%, тоді як служба звітування про підозрілу електронну пошту NCSC до кінця 2022 року отримала майже сім мільйонів повідомлень, що призвело до видалення понад 40 000 шахрайств і понад 72 000 шкідливих URL-адрес. У середньому NCSC знадобилося менше 6 годин, щоб видалити шкідливі URL-адреси з Інтернету.

У звіті також зроблено такі ключові висновки:

- кількість видалень шкідливих сайтів впала за минулий рік, що можна пояснити зменшенням поштових серверів здирництва та шахрайства з інвестиціями в криптовалюту;
- На 39% більше організацій підписалися на безкоштовні послуги ACD « Перевірка безпеки електронної пошти » та «Перевірте свою кібербезпеку», які дають змогу нетехнічним користувачам і, відповідно, компаніям, які мають знання з кібербезпеки щодо захисту від спуфінгу, шифрування електронної пошти та виявлення вразливостей для захисту своїх системи;
- криза в Україні була послідовним приводом для шахрайства з криптовалютою протягом 2022 року; і,
- Служба захисту доменних імен (PDNS) ACD, яка надає захисні механізми для запобігання доступу організацій до шкідливих сайтів, які містять зловмисне програмне забезпечення, фішингові атаки тощо, заблокувала 11 мільярдів DNS-запитів для 420 000 доменів у 2022 році.

У цьому звіті висвітлюються постійні виклики кібербезпеці, головною загрозою яких є фішингові атаки. Це ще раз підкреслює важливість того, щоб усі організації мали спеціальні знання, системи та інструменти для захисту своїх систем від кібератак. З огляду на те, що малий бізнес стикається з додатковими перешкодами, включаючи фінансовий тиск і управління суперечливими пріоритетами, багатообіцяючим є те, що NSDC запровадив програми, щоб

допомогти малому бізнесу з відповідними знаннями щодо кіберризиків для розробки надійних систем кібербезпеки». ***(Patrick Hill and Sonali Malhotra. Cyber Criminals Continue Phishing for Trouble // DAC Beachcroft LLP. (https://www.dacbeachcroft.com/en/gb/articles/2023/august/cyber-criminals-continue-phishing-for-trouble/). 04.09.2023).***

***

«Відповідно до звіту, опублікованого сьогодні Savanti, однією з провідних британських консалтингових компаній з кібербезпеки, компанії Великобританії дедалі частіше піддаються ризику кібератак, оскільки відсутність ефективних заходів кібербезпеки призводить до значної фінансової та репутаційної шкоди.

У звіті під назвою «Ефективне управління кібербезпекою: джерело конкурентної переваги» пропонується суворе попередження організаціям Великобританії, зазначаючи, що більшість директорів вважають свої ради неефективними в розумінні кіберризиків.

У 2022 році глобальні кібератаки зросли на 38% порівняно з попереднім роком. Це тривожне зростання є очевидним у Великобританії, де за останні 12 місяців було зареєстровано 2,4 мільйона випадків кіберзлочинності.

Прогнози Cybersecurity Ventures показують, що до 2025 року глобальна вартість кіберзлочинності може сягнути астрономічних 8,4 трильйона фунтів стерлінгів на рік. Якби кіберзлочинність була країною, вона мала б третю за величиною економіку світу, поступаючись лише США та Китаю.

У звіті також розглядаються значні витрати, пов’язані з кібератаками, висвітлюються останні резонансні інциденти. Серед них атаки на виборчу комісію, яка розкривала особисті дані виборців протягом 14 місяців, а також порушення за участю відомих компаній, таких як British Airways і Boots. У цих випадках банківські реквізити та контактна інформація співробітників були скомпрометовані, що призвело до серйозних юридичних наслідків для організацій і втрати довіри громадськості.

Серйозне занепокоєння полягає в тому, що хоча ради директорів віддають пріоритет кібербезпеці, 59% директорів визнали, що їм бракує розуміння її впливу. Річард Брінсон, генеральний директор Savanti, прокоментував: «Багато інвесторів сприймають кіберпростор як канарку у вугільній шахті для здоров'я та стійкості бізнесу. Хоча прогрес був досягнутий, багатьом радам все ще важко ефективно розподіляти свої обов'язки».

Навпаки, у звіті підкреслюється, що компанії з «кіберзалученими» дошками мають значні переваги. До них належать збільшення доходів, вищі показники успіху в залученні клієнтів і підвищена довіра інвесторів.

Брінсон вважає, що ради директорів можуть вжити дієвих заходів для покращення свого кіберуправління. Рекомендації включають наявність принаймні одного члена правління з безпосереднім досвідом роботи з кібербезпекою, регулярне включення кіберпитань до порядку денного щоквартальних засідань правління та підготовку до часу, який може знадобитися для відновлення після великого кіберінциденту, наприклад атаки програм-вимагачів.

Брінсон також застеріг британські компанії бути проактивними щодо майбутніх правил кібербезпеки. «Тепер у США від компаній вимагається розкривати порушення кібербезпеки, що впливають на їхні прибутки, протягом чотирьох днів. Дуже ймовірно, що подібне законодавство незабаром буде прийнято у Великій Британії та Європі, яке замінить поточні правила звітності GDPR. Підприємства повинні випередити ці неминучі нормативні зміни». ***(Ryan Fowler. More UK companies failing to tackle cyber security, reveals new report // The Intermediary (https://theintermediary.co.uk/2023/09/more-uk-companies-failing-to-tackle-cyber-security-reveals-new-report/). 11.09.2023).***

***

«…Брак експертів з кібербезпеки в уряді Великої Британії має викликати серйозне занепокоєння, згідно з новим звітом Комітету з питань публічних рахунків (PAC). Обмеження в оплаті праці означають, що урядові департаменти не можуть повною мірою конкурувати з приватним сектором на

важкодоступних посадах із браком експертів з кібербезпеки, чиї навички є особливою проблемою.

Проте деякі нестачі цифрових навичок спричинені контрпродуктивним скороченням персоналу на тлі боротьби за наймання та утримання необхідних кваліфікованих людей у цифровій робочій силі державної служби, стверджується у звіті.

Експертів з кібербезпеки важко набрати, вони вимагають премії

У Великій Британії спостерігається серйозний дефіцит цифрових навичок, і кваліфіковані цифрові професіонали мають перевагу на ринку, що ускладнює наймання департаментами. Прочитайте звіт «Цифрова в уряді: вирішення проблем, які перешкоджають ефективності» трансформація. За оцінками уряду, кількість фахівців у сфері цифрових технологій, даних і технологій на державній службі становить приблизно 4,5%, менше половини необхідної кількості порівняно з еквівалентним середнім показником по галузі від 8% до 12%, тому кількість буде потрібно подвоїтися. «Департаменти стикаються з особливою нестачею таких посад, як архітектори даних і експерти з кібербезпеки, яких важко найняти, і де навички мають перевагу на ринку».

Незважаючи на важливість цифрових технологій для сучасної державної служби, вимога до вищих керівників широкого профілю краще розуміти цифровий бізнес не була формалізована, стверджується у звіті PAC. PAC рекомендував, щоб цифрові обов’язки, такі як покращення цифрових послуг і вирішення проблем із застарілими системами з найвищим ризиком, були включені в листи про призначення на найвищих рівнях у всіх департаментах.

Цифрове не можна розглядати як побічну проблему

Однією з характерних рис цифрової революції є швидкі та прискорені зміни, прокоментувала член парламенту Мег Хілліер, голова PAC. «Наше розслідування виявило, що цифрові послуги Уайтхолла, далекі від того, щоб трансформуватися з потрібною швидкістю, здатні лише на поетапні та поступові зміни. Здібності департаментів у майбутньому перешкоджають нестачі персоналу, а також

відсутності підтримки, підзвітності та уваги з боку нагору. Зокрема, відсутність експертів з кібербезпеки має викликати холод у спині уряду».

Уряд говорить про свої амбіції щодо цифрової трансформації та ефективності, водночас активно скорочуючи ті самі ролі, які могли б допомогти їх досягти, додала вона. «Наше розслідування не переконало нас, що ці цілі будуть досягнуті в умовах конкуруючого тиску та пріоритетів». До цифрових технологій не слід ставитися лише як до іншої сторони, вони повинні бути основою того, як уряд думає про надання послуг. «Без швидкої та суттєвої модернізації можливості для покращення послуг для населення й надалі будуть втрачені». ***(Michael Hill. Lack of cybersecurity experts in UK government should "send chill" down its spine // CSO (https://www.csoonline.com/article/652186/lack-of-cybersecurity-experts-in-uk-government-should-send-chill-down-its-spine.html). 13.09.2023).***

***

«Кабінет міністрів Литви в середу затвердив національну програму розвитку кібербезпеки Міністерства оборони на 2023-2030 роки.

У документі вказується, що поточна модель кібербезпеки є неадекватною для зростаючої сфери кібербезпеки.

Крім того, програма також охоплює поліцію та пов'язані з нею установи, сказав Людас Алішаускас, керівник Національного центру кібербезпеки, на засіданні уряду в середу.

«В рамках однієї програми ми маємо на меті мати лабораторію та готувати спеціалістів та експертів. У рамках іншої програми ми оновлюємо архітектуру кіберзахисту, щоб створити єдину платформу для надання послуг суб'єктам кібербезпеки», – додав він.

Документ передбачає кардинальний перегляд існуючої системи формування та впровадження національної політики кібербезпеки шляхом залучення більшої кількості інституцій до управління та забезпечення безпеки.

Також планується удосконалити систему управління кібербезпекою та організаційно-технічні вимоги до кібербезпеки, запровадити нові технічні та

організаційні засоби, вирішити питання підготовки фахівців та навчання персоналу державних установ і населення.

Загальний бюджет нової програми становить 52,3 млн євро.

Зусилля спрямовані на збільшення частки розслідуваних критичних кіберінцидентів з 50 до 100 відсотків протягом наступних семи років, а також на підвищення частки людей, які перевіряють безпеку веб-сайтів, з 23,3 до 40 відсотків». ***(Lithuanian government approves €52m plan to beef up cyber security // Lithuanian Radio and Television (LRT) (https://www.lrt.lt/en/news-in-english/19/2081523/lithuanian-government-approves-eur52m-plan-to-beef-up-cyber-security). 20.09.2023).***

***

«Законопроект Великобританії про безпеку в Інтернеті (OSB), який довго обговорювався, був схвалений Палатою лордів, відкриваючи йому шлях для того, щоб стати законом. Але це зіштовхнуло уряд, який запропонував законопроект, проти технологічних компаній, які надають послуги безпечного обміну повідомленнями. Критики кажуть, що це дозволить владі Великобританії змусити постачальників послуг зламувати шифрування користувачів.

У липні 68 науковців з кібербезпеки опублікували відкритий лист, у якому виклали свою стурбованість OSB. У ньому вони стверджують, що законопроект підриває безпеку та конфіденційність користувачів в Інтернеті.

OSB також зустрів значний опір з боку промисловості. Apple випустила заяву, в якій пояснює, що шифрування «допомагає звичайним громадянам захистити себе від стеження, крадіжки особистих даних, шахрайства та витоку даних. OSB становить серйозну загрозу для цього захисту».

У квітні кілька постачальників безпечних повідомлень, таких як Whatsapp, Element, Session і Signal, підписали ще один відкритий лист із закликом до уряду Великобританії переглянути законопроект.

Проте зараз законопроект має стати законом. На високому рівні OSB покладає обов’язки обережності на постачальників так званих інтернет-послуг «від

користувача до користувача», які дозволяють користувачам завантажувати або ділитися вмістом, який можуть бачити інші користувачі. Це стосується таких дій, як завантаження фотографій в Instagram або надсилання повідомлень через WhatsApp.

Це відрізняє соціальні медіа та служби онлайн-повідомлень від таких інтернет-сервісів, як онлайн-банкінг, у яких лише постачальник бачить вміст, завантажений кінцевим користувачем. Ці обов'язки спрямовані на те, щоб запобігти передачі користувачами незаконного вмісту, наприклад матеріалів сексуального насильства над дітьми.

Чому шифрування важливо?

Оскільки OSB стосується додатків для обміну повідомленнями, експерти з кібербезпеки висловили занепокоєння щодо потенціалу законопроекту для підриву так званого наскрізного шифрування. Для програм обміну повідомленнями, таких як WhatsApp і Signal, наскрізне шифрування гарантує, що лише відправник даного повідомлення та їхні одержувачі можуть прочитати вміст повідомлення. Навіть постачальник послуг не може прочитати повідомлення.

Це стало предметом суперечок для урядів і розвідувальних служб у всьому світі, оскільки це означає, що вони більше не можуть переконати технологічні компанії дозволити їм доступ до повідомлень користувачів.

Прихильники наскрізного шифрування, такі як група активістів цифрових прав Electronic Frontier Foundation, стверджують, що конфіденційність спілкування є фундаментальним правом, яке захищає вразливі групи, такі як дисиденти в авторитарних режимах. Вони стверджують, що шифрування допомагає забезпечити цю конфіденційність.

Однак такі критики, як розвідка та правоохоронні органи, стверджують, що широке використання цієї форми шифрування перешкоджає їхній здатності виявляти злочинну діяльність, таку як тероризм або сексуальна експлуатація дітей.

Чи є єдиним законодавством щодо ОСБ, яке дозволяє це зробити?

OSB — не перший законодавчий акт, який зазнав критики через його потенціал підривати безпеку та конфіденційність наскрізного шифрування. У 2018

році австралійський уряд прийняв Закон Тола, який також містив заходи, які зобов'язують технологічні компанії співпрацювати з владою. Політики стверджували, що необхідно боротися з тероризмом. Але була сильна негативна реакція з боку критиків, які сказали, що це може підірвати шифрування.

Нещодавня пропозиція Європейської комісії передбачає аналогічні вимоги до постачальників послуг, створених користувачами, у країнах ЄС і викликала власний відкритий лист від дослідників безпеки та конфіденційності, стурбованих потенційною шкодою для безпечного цифрового суспільства.

Чи може OSB допомогти підірвати шифрування?

Законопроект конкретно вимагає від британського регулятора комунікацій Ofcom видавати «кодекс практики» для постачальників послуг між користувачами. Кодекси створюють підставу для Ofcom отримувати інформацію від цих провайдерів і штрафувати їх за невиконання.

Ці кодекси також вимагають, щоб усі постачальники послуг між користувачами «повинні вживати або використовувати пропорційні заходи, щоб запобігти потраплянню осіб через незаконний контент за допомогою послуги».

Депутат від Консервативної партії Деміан Коллінз, який – як міністр технологій і цифрової економіки з липня по жовтень 2022 року – допомагав розробити OSB, заявив під час нещодавніх дебатів, що компанії повинні «докласти всіх зусиль, щоб виявляти, проактивно виявляти, контент, пов'язаний із сексуальними проявами дітей. експлуатації». Але він також додав: «Ми не будемо вимагати від компаній зламати шифрування».

У відкритому листі 68 вчених вказується на фундаментальний недолік цього аргументу: «Не існує технологічного вирішення протиріччя, притаманного як збереженню конфіденційної інформації від третіх сторін, так і обміну цією ж інформацією з третіми сторонами».

Президент додатка для обміну повідомленнями Signal Мередіт Віттакер каже, що в законопроекті немає засобів захисту від злому шифрування.

Дійсно, мова OSB дозволяє Ofcom видавати «повідомлення», які можуть бути використані, щоб змусити програми обміну повідомленнями підірвати

шифрування. Вони вимагатимуть від постачальника послуг «використовувати акредитовану технологію для ідентифікації незаконного контенту, оприлюдненого публічно чи приватно за допомогою сервісу, і швидко видаляти цей контент».

Оскільки наскрізне шифрування принципово перешкоджає постачальнику послуг читати надісланий користувачем вміст, це вимагає зламати шифрування для ідентифікації цього вмісту.

Який результат ми можемо побачити?

Дивлячись на мову OSB, занепокоєння експертів з кібербезпеки, здається, мають певну основу, незважаючи на заперечення Деміана Коллінза та Міністерства внутрішніх справ. OSB надає механізми для уряду, щоб змусити програми обміну повідомленнями підірвати власні заходи безпеки для досягнення своїх цілей.

Вилучити ці положення було б просто. Видалення фрази «або приватно» з законопроекту дозволило б OSB залишитися майже недоторканим, одночасно вирішуючи проблеми провайдерів, які використовують наскрізне шифрування.

Тому дуже іронічно, що оскільки і Signal, і WhatsApp зазначили, що вони покинуть Великобританію, а не підривають шифрування, поточне формулювання британського законопроекту про безпеку в Інтернеті потенційно зробить користувачів у Великій Британії наскрізного шифрування менш безпечними в Інтернеті». ***(Benjamin Dowling. The UK just passed an online safety law that could make people less safe // The Conversation Media Group Ltd (https://theconversation.com/the-uk-just-passed-an-online-safety-law-that-could-make-people-less-safe-213595?utm_source=flipboard&utm_content=Mothership2018%2Fmagazine%2FTECHIE+STUFF). 25.09.2023).***

***

«Генеральний директор Ради кібербезпеки Великої Британії, професор Саймон Хепберн, в інтерв'ю телекомпанії ITN розповів про ключові досягнення за останні 12 місяців. Хепберн оцінив роботу Ради щодо професійних

стандартів кібербезпеки, кар'єри та навчання, а також охоплення та різноманітності.

У рік, який він назвав «дуже напруженим», рада — орган саморегулювання сектору кібербезпеки Великої Британії — працювала як на місцевому, так і на міжнародному рівнях для розвитку екосистеми кібербезпеки у Великобританії.

Чотири нові стандарти кібербезпеки Ради кібербезпеки Великобританії

«Ми розробили чотири професійні стандарти кібербезпеки в різних сферах», — сказав Хепберн. Це управління кібербезпекою та управління ризиками, архітектура та дизайн безпечної системи, тестування безпеки та аудит і гарантія.

«Коли ми працювали з організаціями над розробкою цих стандартів, ми багато працювали над підвищенням рівня кібербезпеки як професії, яка є дуже, дуже важливою та є одним із наших ключових пріоритетів».

Рада співпрацює з кількома організаціями, які є фахівцями в певних областях кібербезпеки, щоб розробити стандарти, додала Хепберн. Серед них міжнародна професійна асоціація ISACA та галузеві організації (ISC)? та Чартерний інститут інформаційної безпеки (CIISec).

Стандарти є ключовою основою роботи ради щодо створення загальновизнаного професійного стандарту для сектору кібербезпеки Великобританії, щоб надати фахівцям можливість отримати дипломований статус за 16 спеціалізаціями.

«Ми провели людей через цей процес, і нам дуже приємно, що у нас є багато успішних кандидатів, а також деякі не дуже успішні, але це весь процес навчання. Ми використовуємо це навчання як частину наступний розвиток подій.

За словами Хепберн, Рада також розробила свою Технічну консультативну групу, до складу якої входять експерти з безпеки в державних департаментах і різних організаціях/установах, які переглядатимуть і оцінюватимуть критерії того, що вона розробила.

Робота Ради кібербезпеки Великої Британії над вирішенням проблеми з дефіцитом навичок, покращення різноманітності

Хепберн запитали про поточну нестачу талантів у сфері кібербезпеки у Великій Британії, як зазначено в нещодавньому звіті Департаменту науки, інновацій та технологій (DSIT), який показав, що приблизно 50% британських компаній мають прогалину в базових навичках кібербезпеки. «Це викликає занепокоєння, але ми завжди знали, що це існує», - сказав він. «Це довготривала гра — це марафон, а не спринт».

Перше ключове, що Рада зробила, щоб допомогти вирішити проблему нестачі навичок, — це підвищити популярність кібербезпеки як професії, співпрацюючи зі школами для підвищення обізнаності молодих людей, а також для зміни кар'єри, сказала Хепберн. «Наша роль — справді демістифікувати коріння професії кібербезпеки, використовуючи такі речі, як наш онлайн-інструмент кар'єри, щоб показати, як кваліфікація та досвід узгоджуються з конкретними можливостями».

За словами Хепберн, Рада також працює над покращенням представництва у сфері кібербезпеки Великобританії. Це включає в себе публікацію документу про процес різноманітності, в якому досліджуються бар'єри, з якими кольорові люди та представники етнічних меншин стикаються, коли роблять кар'єру в сфері кібербезпеки. «Збільшення кількості етнічних меншин у кібернетичному просторі, а також піднесення жінок у кібернетичному просторі. Крім того, ми займаємося інтелектуальним лідерством, розглядаємо такі проблеми, як нейрорізноманіття. Для нас це справді соціальна мобільність; це стосується профілювання можливостей і забезпечення того, щоб усі усвідомлювали, що вони Ласкаво просимо до цієї професії». ***(Michael Hill. UK Cyber Security Council CEO reflects on a year of progress // CSO (https://www.csoonline.com/article/653755/uk-cyber-security-council-ceo-reflects-on-a-year-of-progress.html). 27.09.2023).***

***

«Згідно з новим звітом, сектор кібербезпеки в Ірландії потребує додатково 1000 працівників щорічно.

У звіті, оприлюдненому на Cinc23, щорічній конференції Cyber Ireland, виявилося, що в 2022 році в Ірландії було 6707 унікальних оголошень про роботу

для фахівців з кібербезпеки, що втричі перевищує попит у 2019 році. За оцінками, до 2030 року в цьому секторі може працювати 17 000 людей. в Ірландії.

Згідно з дослідженням, середня зарплата в галузі кібербезпеки становить 75 000 євро, що майже вдвічі перевищує середню зарплату в Ірландії.

Еойн Бірн, кластерний менеджер Cyber Ireland, сказав: «Цей звіт надає чіткі докази зростання попиту на таланти з кібербезпеки в Ірландії, показуючи, як у 2022 році було втричі більше оголошень про роботу порівняно з 2019 роком.

«Це демонструє переваги підтримки зростання цього сектору, включаючи зростання регіональної зайнятості, високоцінні робочі місця та можливість позиціонувати Ірландію як лідера кібербезпеки на міжнародному рівні».

За даними Cyber Security Ireland — кластерної мережі фірм із кібербезпеки — Ірландія є домом для п’ятірки провідних світових компаній із забезпечення безпеки.

За даними групи, у зростаючому секторі кібербезпеки Ірландії працює близько 500 фірм, у яких працює понад 7300 професіоналів, а у 2022 році галузь внесла в економіку Ірландії приблизно 1,1 мільярда євро.

Cyber Security Ireland прогнозує, що 83 відсотки підприємств очікують, що їх команда з кібербезпеки зросте протягом наступних дванадцяти місяців, і більше половини очікують, що це зростання відбуватиметься на рівні 25 відсотків або вище.

«Згідно з поточними оцінками зростання, Ірландія може позиціонувати себе як світового лідера в галузі кібербезпеки, збільшивши кількість робочої сили до понад 17 000 до 2030 року та підтримуючи до 2,5 мільярдів євро річної валової доданої вартості в економіку на рік, за умови відповідного бізнес-середовища,» - повідомили в організації.

Звіт суперечить дослідженню IDA, опублікованому в червні, яке показало, що загальне наймання сповільнилося на 40 відсотків, причому багатонаціональні та технологічні сектори сповільнюють набір або скорочують кадри з кінця пандемії». ***(Emmet Ryan. Demand for cyber security staff trebled since 2019 // Business Post***

(https://www.businesspost.ie/news/demand-for-cyber-security-staff-trebled-since-2019/). 27.09.2023).

***

«Керівників пенсійних схем закликають пам'ятати про ризики кібербезпеки після того, як дослідження RPC виявило збільшення на 4000 відсотків повідомлень про порушення даних до Управління уповноваженого з інформації (ICO) за рік до червня 2023 року.

Дослідження показало, що британські фінансові фірми повідомили про 640 порушень кібербезпеки до ICO за рік до 30 червня 2023 року, що майже втричі більше, ніж 187 порушень кібербезпеки за попередній період.

Пенсійні схеми Великої Британії повідомили про найбільше зростання кількості порушень кібербезпеки, згідно з дослідженням, з шести у 2021/22 році до 246 у 2022/23 році.

Дійсно, RPC припустив, що пенсійні схеми можуть бути особливою мішенню для хакерів, оскільки вони зберігають величезну кількість цінних, конфіденційних фінансових даних, а також пенсійні схеми для безперебійної виплати пенсіонерам, що робить їх потенційно вразливими до вимог викупу.

Враховуючи це, партнер RPC і голова кібер- і технологічного страхування Річард Брівінгтон стверджував, що кібербезпека є «основоположною для юридичних обов'язків довірених осіб пенсійної схеми», попереджаючи, що довірені особи пенсійної схеми можуть нести відповідальність за нездатність належним чином керувати кіберризиками.

Фірма також зазначила, що відповідно до вказівок Пенсійного регулятора з кібербезпеки довірені особи залишаються відповідальними за безпеку інформації та активів схем, навіть якщо щоденні функції передані аутсорсингу.

У світлі цього RPC запропонував будь-якому бізнесу, який хоче захистити себе від наслідків кібератаки, щоб інвестувати в розуміння свого кіберсліду та ризиків, які він створює, і мати правильні політики/процедури.

На додаток до цього було рекомендовано організаціям розглянути можливість кіберстрахування для забезпечення покриття збитків у результаті кіберінциденту, а також доступу до юридичної, технічної криміналістики та PR-підтримки.

Брівінгтон заявив: «Це викликає занепокоєння те, що так багато компаній, що надають фінансові послуги, особливо пенсійні схеми, зазнали певної форми кібератак, що призвело до витоку даних.

«Іноді можна припустити, що великі компанії, що надають фінансові послуги, мають надійний кіберзахист, тому вони є непроникними – це, звичайно, не зупинило хакерів продовжувати спроби».

Питання кібербезпеки були ключовим напрямком для пенсійних схем на тлі зростання занепокоєння щодо ризиків кібератак, оскільки постачальники послуг і пенсійні схеми прагнуть захистити інформацію та переваги учасників.

Ці занепокоєння посилилися після того, як на початку цього року кіберінцидент Capita вплинув на низку пенсійних схем із доказами «обмеженого вилучення даних із невеликої частини постраждалого майна обслуговування, яке може включати деякі дані клієнтів, постачальників або колег».

Пенсійний регулятор також нещодавно підкреслив цей інцидент як нагадування про важливість бути уважним до кіберризиків, підкресливши необхідність для всіх керівних органів вжити заходів для захисту членів і активів від кіберризиків.

Однак галузеві експерти також стверджують, що Пенсійний регулятор повинен надати більш чіткі вказівки щодо кіберризиків, включаючи приклади найкращої практики та практичні кроки для довірених осіб і менеджерів схем». ***(Sophie Smith. UK pension schemes reveal 4,000% rise in cyber security breaches // Pensions Age (https://www.pensionsage.com/pa/UK-pension-schemes-record-4000-pc-rise-in-cyber-security-breaches.php). 25.09.2023).***

***

«Недавнє дослідження, проведене спільно Австралазійською асоціацією управління юридичною практикою (ALPMA) і AUCloud, пролило світло на тривожний стан кіберзагроз, з якими стикаються юридичні фірми в Австралії та Новій Зеландії. Висновки однозначні: ландшафт кіберзагроз величезний.

Серед найбільш тривожних відкриттів дослідження кібербезпеки юридичної фірми, яке опитало 85 юридичних фірм, є те, що понад 50 відсотків респондентів відчувають себе погано підготовленими до вирішення кіберінциденту.

Ще 19 відсотків компаній визнали, що не вживають достатніх заходів для захисту своєї діяльності в поточному середовищі загроз. Викликає занепокоєння те, що 14 відсотків опитаних фірм заявили, що вони вже ставали жертвами спроб кібератак.

Цікаво, що незважаючи на цю тривожну статистику, 47 відсотків опитаних юридичних фірм стверджували, що мають у своєму штаті спеціалістів із кібербезпеки.

Однак значна кількість фірм вказали на відсутність «обізнаності та навчання працівників» як на головну перешкоду їхнім зусиллям у сфері кібербезпеки. Питання готовності стає серйозним: 34 відсотки фірм не мають письмового плану реагування, а серед тих, що мали його, 31 відсоток мали лише неповний план.

Юридичні фірми опинилися в облозі широкого спектру кіберзагроз, включаючи спроби фішингу, вторгнення зловмисного програмного забезпечення, розподілені атаки типу «відмова в обслуговуванні» (DDoS) і навіть внутрішні загрози.

Пітер Мелоні, генеральний директор AUCloud, визнаючи відставання в готовності, похвалив фірми за їхню зростаючу обізнаність про кіберзагрозу.

«Кіберзлочинність, на жаль, є найбільшою загрозою для австралійського бізнесу та є однією з наших галузей, що найшвидше розвиваються в усьому світі, і це не завдає шкоди», — сказав він.

85 відсотків опитаних фірм шукають зовнішню IT-підтримку для посилення своїх заходів кібербезпеки. Він підкреслив, що значне економічне становище

Австралії, стратегічний геополітичний статус і розвинена технологічна інфраструктура роблять її основною мішенню для кібератак.

Емма Елліотт, генеральний директор ALPMA, вважає результати дослідження тривожним сигналом для юридичної галузі.

Вона зазначила, що учасники ALPMA відрізняються за розміром і готовністю до кібербезпеки: деякі мають надійну інфраструктуру, а інші покладаються на зовнішню підтримку для захисту своїх операцій і даних клієнтів. Елліотт підсумував: «Кібербезпека є постійною та дуже реальною загрозою для наших учасників та їхніх компаній».

Перед обличчям цієї ескалації загрози очевидно, що юридичні фірми повинні залишатися пильними та продовжувати посилювати свої заходи кібербезпеки, щоб захистити своїх клієнтів і свою власну діяльність». ***(Law Firm Cybersecurity Threat Risk Is 'Formidable' Says Australasian Survey // LawFuel (https://www.lawfuel.com/law-firm-cybersecurity-threat-risk/). 13.09.2023).***

***

«Уряд Австралії розробляє свою стратегію кібербезпеки, яка передбачатиме формування шести кіберщитів.

Про це заявила міністр внутрішніх справ Клер О'Ніл під час кіберсаміту AFR 18 вересня, а більше подробиць з'явиться пізніше цього року.

За словами О'Ніла, ці щити допоможуть захистити підприємства, організації та громадян, створюючи «згуртовану та сплановану національну відповідь».

Перший щит спрямований на створення сильних громадян і компаній, які розумітимуть, що вони мають силу захистити себе.

«До 2030 року ми хочемо, щоб громадяни та компанії розуміли кіберзагрози, розуміли, які дії вони можуть вжити, щоб захистити себе, і мали належну підтримку, щоб, коли вони стали жертвою кібератаки, вони могли повернутися вгору, — сказала О'Ніл.

Другий щит буде зосереджений на безпечних технологіях через наявність чітких глобальних стандартів цифрової безпеки в продуктах, які сприятимуть розвитку безпеки в продуктах від самого початку, пояснив О'Ніл.

Третій кіберщит передбачає обмін загрозами та блокування, обмін розвідданими в регіоні між приватним і державним секторами.

«Це одна з найцікавіших частин стратегії. Таким чином, до 2030 року ми передбачаємо світ, у якому уряд і бізнес зможуть обмінюватися даними про загрози в режимі реального часу, а потім блокувати загрози, перш ніж вони завдадуть шкоди населенню Австралії», — сказала вона.

«Є багато надихаючої, цікавої роботи, яку потрібно зробити, і багато речей, які ми можемо зробити за короткий термін».

Четвертий кіберщит передбачає захист доступу до критичної інфраструктури.

«Ми володіємо критично важливою інфраструктурою, ми надаємо основні послуги, і ми, звичайно, зберігаємо багато дуже конфіденційних і приватних даних про австралійців. Ось чому частина цього року буде присвячена посиленню урядом власного кіберзахисту, щоб переконатися, що ми захищаємо нашу країну», – сказала вона.

П’ятим кіберщитом буде суверенний потенціал, де, за словами О’Ніл, вона очікує, що до 2030 року в Австралії буде процвітаюча кіберекосистема з необхідними навичками.

Останній щит передбачає вжиття скоординованих глобальних дій і сприяння створенню більш стійкого регіону.

О'Ніл пояснила, що її план передбачає створення щитів дворічними блоками, причому перший «горизонт» з 2022 по 2025 рік зосереджений на створенні міцної основи.

«У міру зміни форми кіберпроблеми ми підводимо підсумки та кожні два роки розроблятимемо наступний етап цього плану, який зрештою призведе до того, що країна буде оточена цими шістьма міцними щитами захисту, які допоможуть захистити наших громадян», — сказала вона.

«У нас є справді спільний чіткий національний імператив побудувати кібербезпечну Австралію». ***(Julia Talevski. Government creates cyber shields to beef up security measures // IDG Communications, Inc. (https://www.arnnet.com.au/article/708823/government-creates-cyber-shields-to-beef-up-security-measures/?fp=2&fpid=1). 20.09.2023).***

***

Китай

«Оскільки Китай намагається посилити безпеку своїх внутрішніх даних, правоохоронні органи розширюють зусилля щодо стежити за відповідністю по всій країні – від великих технологічних фірм до менших вуличних підприємств. Тепер компанії, починаючи від ресторанів і закінчуючи масажними кабінетами, отримують попередження про покарання, які їм загрожують за недотримання нових правил кібербезпеки в країні.

Минулого місяця поліція міста Чженьцзян у східній провінції Цзянсу провела перевірку безпеки на місцевих підприємствах, видаючи попередження тим, хто пропонує Wi-Fi без реєстрації справжнього імені, повідомили місцеві ЗМІ в понеділок.

Посилаючись на Закон країни про кібербезпеку, попередження наказували компаніям «виправити» свої послуги, які не «впроваджували заходи захисту технічної безпеки», як того вимагає закон, згідно зі звітом.

Коли поліцейські перевірки почали набирати хвилю, поліція в Хуайані, іншому місті Цзянсу, почала роздавати подібні попередження місцевому бутіку масажу ніг, посилаючись на закон країни про безпеку даних.

Компанію попередили після того, як поліція заявила, що вона зберігала інформацію про клієнтів, таку як імена та ідентифікаційні номери, які вважаються конфіденційні дані, не встановивши достатніх заходів безпеки для захисту даних.

Перевірки безпеки проливають нове світло на зростаючу увагу Китаю до того, як компанії обробляють персональні дані, оскільки влада продовжує посилювати контроль за кібербезпекою. Пекін також працює над зміцненням

законодавчої бази захисту даних, яка вважається ключовою опорою національної безпеки.

Нові положення про захист даних включає вимоги до проведення регулярних перевірок усіх компаній, які обробляють персональні дані. Ці правила з'явилися в той момент, коли Пекін цього року посилює свої зусилля по боротьбі зі шпигунством, попереджаючи про несанкціоноване отримання «документів, даних, матеріалів і предметів, пов'язаних з національною безпекою та інтересами».

У 2016 році Китай прийняв закон про кібербезпеку, наголошуючи на необхідності підтримувати контроль над суверенним кіберпростором країни та національною безпекою. Спираючись на цю основу, у вересні 2021 року було впроваджено Закон про безпеку даних, щоб обмежити способи обробки даних. Закон також наголошує на необхідності захисту національної безпеки та інтересів, роблячи захист безпеки даних пріоритетом національної безпеки.

Алекс Робертс, шанхайський радник з технологій, медіа та телекомунікацій юридичної фірми Linklaters, сказав, що нещодавні примусові заходи є чітким сигналом від Влада Китаю повідомляє, що будь-який неофіційний пільговий період закінчився, і підприємства – незалежно від їх розміру – повинні вжити заходів для дотримання законів країни про конфіденційність і безпеку даних.

«Хоча примусовий захід служить нагадуванням компаніям про їхні зобов'язання щодо безпеки та захисту даних, він також викликав дискусію серед учасників галузі щодо його справедливості щодо малих підприємств, які можуть бути не в змозі дозволити собі вживати інколи дорогі заходи відповідності», Робертс сказав.

Закон Китаю про захист особистої інформації, який набув чинності в 2021 році, натякнув, що майбутнє законодавство може бути введено для вирішення цієї проблеми, сказав Робертс, оскільки він вимагає розробки спеціальних «спеціальних правил і стандартів захисту особистої інформації» для малих підприємств, які обробляють особисті дані.

Однак, додав Робертс, галузь ще не побачила ці правила впровадження або графік їх публікації.

Анджела Чжан, ад'юнкт-професор права в Університеті Гонконгу, сказала, що останні випадки, очевидно, відображають зміщення уваги місцевих органів влади щодо дотримання правил безпеки даних для малих і середніх фірм і організацій.

«Це чітко вказує на тенденцію, коли китайська влада посилює правила безпеки даних. На відміну від великих корпорацій, малі та середні підприємства часто не мають надійних механізмів відповідності. Це могло пояснити недавній сплеск примусових дій проти них», – сказала вона.

«Однак штрафи, що стягуються згідно з цим законом, як правило, є відносно невеликими, а об'єктами примусових заходів, як правило, є не відомі корпоративні актори. Це свідчить про те, що правозастосування може не мати такого впливу на великі корпорації», – додала вона.

Гао Фупін, професор права Східно-Китайського університету політичних наук і права в Шанхаї, сказав, що для підвищення обізнаності всіх підприємств необхідні більш комплексні заходи правопорядку, тоді як малі підприємства, які обробляють дані, частіше піддаються ризику незаконного продажу та обміну інформацією. даних.

«Я вважаю, що всі підприємства повинні відповідати основним вимогам безпеки зберігання даних… для персональних даних. У разі витоку це стосується не лише особистої конфіденційності, а більше соціальної безпеки. Тому на підприємства слід чинити [комплаєнс] тиск», — сказав Гао.

За словами Гао, оскільки безпека даних тепер має більший пріоритет, дотримання таких вимог може спричинити додаткові витрати та незручності з боку компаній.

Оскільки влада посилює правозастосування відповідно до положень Закону про безпеку даних, штрафи накладаються на різні компанії, які не дотримувалися правил кібербезпеки та були визнані такими, що ризикують витоком даних.

У статті, опублікованій в обліковому записі WeChat у середу, Бюро безпеки мережі Міністерства громадської безпеки навело випадки, пов'язані з даними, за останні два роки, 336 з яких було розглянуто в Цзянсу.

У статті попереджено про можливі витоки даних в галузі охорони здоров'я, фінансах і нерухомості, попередивши, що такі витоки можуть завдати «значної шкоди суспільним інтересам, економічним операціям, правам та інтересам особи, а також можуть вплинути на національну безпеку та соціальну стабільність». ***(Vanessa Cai. As China steps up cybersecurity enforcement, smaller businesses are feeling the heat // South China Morning Post Publishers Ltd. (https://www.scmp.com/news/china/politics/article/3233931/china-steps-cybersecurity-enforcement-smaller-businesses-are-feeling-heat?utm_source=flipboard&utm_content=SCMPNews%2Fmagazine%2FSCMP). 10.09.2023).***

***

Російська Федерація та країни ЄАЕС

«Киргизстан покращив свій рейтинг у Національному індексі кібербезпеки (NCSI).

Киргизстан займає 91 місце з 37,66 балами. Країна піднялася зі 112 позиції наприкінці 2022 та на початку 2023 років.

Серед держав Центральної Азії Киргизстан займає хороші місця за такими показниками:

- Розробка політики кібербезпеки (1 місце в Центральній Азії),
- Кризове управління в кібербезпеці (1 місце в Центральній Азії)
- Електронна ідентифікація та довірчі послуги (2 місце після Казахстану)
- Освіта та професійна підготовка (2 місце в Центральній Азії після Казахстану)
- Захист цифрових сервісів (на одному рівні з Казахстаном та Узбекистаном)
- Захист персональних даних (на одному рівні з Казахстаном і Узбекистаном)
- Казахстан посідає 78 місце в NCSI, Узбекистан займає 94 місце, Таджикистан займає 153 місце, Туркменістан займає 164 місце@. ***(Kyrgyzstan***

improves rankings in National Cyber Security Index // AKIpress News Agency (https://akipress.com/news:728735:Kyrgyzstan_improves_rankings_in_National_Cyber_Security_Index/). 01.09.2023).

***

«Російські проксі-сервери в окупованому Криму 22 вересня заявили про кібератаку «безпрецедентного» масштабу.

Олег Крючков, російський представник на окупованому півострові, заявив у Telegram про збої в роботі інтернет-сервісів у Криму. Наразі невідомо, чи триває кібератака, і Київ її поки не коментує.

Атака сталася після того, як Міноборони Росії повідомило про те, що українська ракета вразила штаб Чорноморського флоту РФ у Севастополі напередодні 22 вересня…». ***(Nate Ostiller. Large-scale cyberattack reported in occupied Crimea // The Kyiv Independent (https://kyivindependent.com/large-scale-cyber-attack-reported-in-occupied-crimea/?utm_source=flipboard&utm_content=Varlin26%2Fmagazine%2FTWILIGHT%3A+2000+%3D+TWILIGHT%3A+2023+%28IYKYK%29+-+THE+RUSSIAN+INVASION+OF+DEMOCRATIC+UKRAINE+AND+THE+RETURN+OF+EVIL+EMPIRES). 22.09.2023).***

***

Інші країни

«Дослідження показало, що 73% опитаних сінгапурських компаній сказали, що їхній бюджет на кібербезпеку зріс для впровадження можливостей безпеки наступного покоління, захисту талантів і збільшення онлайн-комерції.

У своїй заяві світовий лідер у сфері безпеки Palo Alto Networks зазначив, що 85% місцевих компаній у Сінгапурі погоджуються, що кібербезпека є головним пріоритетом, оскільки вона обговорюється на рівні правління.

Щоб усунути прогалини в кіберзагрозах, компанії в Сінгапурі впроваджують хмарну безпеку (45%), захищають IoT і OT (41%) і захист кінцевих точок (39%).

У регіоні АСЕАН інтеграція Al є найкращою технологією, яку впроваджують підприємства АСЕАН, особливо ті, що працюють у галузях телекомунікацій/техніки/комунікацій.

«Це відображає підхід організацій у Сінгапурі, де 41% розглядають можливість інтеграції Al (включно з машинним навчанням, прогнозною аналітикою, розпізнаванням голосу та аналітикою настроїв) у найближчі один-два роки», — йдеться в заяві.

У квітні 2023 року онлайн-опитування включало 500 корпоративних IT-керівників і бізнес-лідерів у п'яти ключових галузях SEA: послуги (банківські, фінансові), державний/державний сектор/основні послуги, телекомунікаційні/технічні/комунікації, роздрібна торгівля/готель/їжа та напої, транспорт і логістика, і виробництво. З 500 по 100 були з Сінгапуру, Малайзії, Індонезії, Філіппін і Таїланду». ***(The majority of businesses increased cybersecurity budget // Microsoft (https://www.msn.com/en-sg/news/other/the-majority-of-businesses-increased-cybersecurity-budget/ar-AA1gE35n). 13.09.2023).***

***

«У той час як малі та середні підприємства знаходяться в авангарді інновацій та економічного зростання, Корпорація цифрової економіки Малайзії (Mdec) повідомила, що у 2019 році 84% із них стикалися з кіберзагрозами, а 76% стикалися з ними більше одного разу.

Дослідження, проведене минулого року Асоціацією малого та середнього бізнесу Малайзії, показало, що лише 26% малих і середніх підприємств вирішили оцифрувати свою діяльність або використовувати платформи електронної комерції у 2021 році, а решта 57% ще не зробили цього.

Розмовляючи з theSun, генеральний директор компанії Novem CS з кібербезпеки Муругасон Тангаратнам сказав, що малим і середнім підприємствам рекомендується встановлювати системи кібербезпеки для захисту від хакерів.

«Малі та середні підприємства втричі частіше стають мішенями кіберзлочинців. Вони особливо вразливі до атак програм-вимагачів, оскільки навіть невеликі суми викупу можуть вплинути на них через невелику норму прибутку».

Муругасон сказав, що всі МСП повинні провести «перевірку стану здоров'я», щоб виявити ризики для безпеки.

Коли це буде зроблено, їхні вимоги будуть визначені, і вони зможуть приступити до планування своїх інвестицій у кібербезпеку.

«Є багато професійних фірм з кібербезпеки, які проводять перевірку стану здоров'я, і це може не коштувати малим і середнім підприємствам великих грошей. Деякі рішення можуть просто включати вдосконалення внутрішніх процесів і підвищення обізнаності про кібергігієну», – сказав він.

Хоча існує багато методів, які використовуються кіберзлочинцями для злому компаній, «фішинг» залишається найпопулярнішим методом отримання доступу до конфіденційної інформації, оскільки він передбачає соціальну інженерію.

Інші ознаки включають раптове збільшення мережевого трафіку, аномалії входу та доступ у нестандартні години або з незвичних місць, численні невдалі спроби входу, повільні комп'ютерні системи або мережеві операції та нерозпізнані запити входу.

Муругасон сказав, що деякі з найбільших загроз кібербезпеці для МСП походять від поведінки та звичок працівників.

«Ці загрози варіюються від підозрілого посилання, яке перенаправляє користувача на підроблений веб-сайт, або кіберзлочинця, який видає себе за зацікавленого клієнта, щоб обманом змусити персонал надати конфіденційну інформацію».

За словами Муругасона, інвестуючи в навчання з питань кібербезпеки, МСП можуть показати своїм клієнтам і партнерам, що вони серйозно ставляться до захисту даних і вживають профілактичних заходів для запобігання кібератакам.

«Працівники повинні виявляти розсудливість, щоб забезпечити безпеку свого підприємства. Обов'язковим є навчання працівників проти шахрайства та методів

обману, щоб вони дотримувалися кібергігієни та ніколи не наражали бізнес на небезпеку».

Що стосується витоку даних, він сказав, що різні набори даних надають різну інформацію власникам і кібер-зловмисникам.

«Доступна інформація залежить від характеру бізнесу, його важливості в ланцюжку постачання та того, що кіберзлочинці вважають найціннішими активами підприємства.

«Однак кіберзлочинці зазвичай націлюються на великі облікові записи для захоплення. Ті, якими зазвичай керує генеральний директор організації або головний фінансовий директор, мають вдвічі більше шансів бути прийнятими, ніж середні працівники», – сказав він.

У Малайзії є урядові організації, які можуть надати допомогу корпораціям, які зазнали кібератак, наприклад Малайзійська команда реагування на надзвичайні ситуації з комп'ютерами (MyCERT).

Cyber999 MyCERT, центр реагування на інциденти кібербезпеки, показав, що в третьому кварталі 2022 року він отримав 2240 інцидентів кібератак, що на 13% більше, ніж у другому кварталі того ж року». ***(Qalif Zuhair. SMEs advised to install cyber security systems // Sun Media Corporation Sdn. Bhd. (https://www.thesundaily.my/local/smes-advised-to-install-cyber-security-systems-PM11489886). 14.09.2023).***

***

«13 вересня 2023 року парламент Бангладеш прийняв новий Закон про кібербезпеку 2023 року (CSA), який спрямований на запобігання кіберзлочинам і поширенню неправдивої інформації. Трохи більше ніж за місяць до цього, 7 серпня, кабінет уряду Бангладеш вирішив скасувати суперечливий Закон про цифрову безпеку 2018 року (DSA) і замінити його запропонованим CSA.

Правозахисні групи, які зосереджені на правах людини та цифрових правах, стверджують, що новий закон є, по суті, ребрендинговою версією свого

попередника, DSA. Новий закон містить багато спірних положень, які несуть ризик використання та зловживання, потенційно націленими на правозахисників, журналістів, опозиційних діячів та осіб, які висловлюють незгоду чи критикують уряд. Закон про кібербезпеку 2023 року був поспішно прийнятий під час 24-ї сесії парламенту Бангладеш 11-го скликання, яка завершилася 14 вересня 2023 року. Були припущення, що ця сесія може стати останньою перед майбутніми парламентськими виборами в січні 2024 року…

Драконівський закон про цифрову безпеку 2018 року

Закон про цифрову безпеку 2018 року став законом 8 жовтня 2018 року, всього за кілька місяців до парламентських виборів 2018 року. Його основною метою було запобігання поширенню тероризму, пропаганди та ненависті, спрямованих проти релігійних або етнічних меншин через соціальні мережі чи інші електронні медіаплатформи. До цього свобода вираження поглядів у Бангладеш була підірвана Законом про інформаційно-комунікаційні технології (ІКТ) (2006), який містив драконівський розділ 57, який надавав поліції повноваження арештовувати осіб за розміщення в Інтернеті контенту, який вважався «фальшивий», «непристойний» або «наклепницький».

Однак DSA виявився більш драконівським, що викликало протести з боку правозахисників, журналістів, юридичних експертів та окремих осіб, які висловлювали занепокоєння щодо його неоднозначної мови та тенденції криміналізувати законне вираження думок і думок. Згідно з цим актом, органи влади отримали широкі повноваження — наприклад, повноваження арештовувати людей і обшукувати приміщення без ордера за підозрою в скоєнні або плануванні злочину в Інтернеті. За даними уряду, з жовтня 2018 року було порушено понад 7000 справ відповідно до Закону про цифрову безпеку, і приблизно 86 відсотків із них все ще очікують слухань. DSA Tracker, зусилля Центру урядових досліджень у Бангладеш, відстежив 1321 справу станом на 31 травня 2013 року, в яких обвинуваченими є 4121 особа, з яких 1454 були заарештовані.

Закон про кібербезпеку (2023): перейменована версія DSA

За словами міністра юстиції Анісула Хука, DSA 2018 не було скасовано, а трансформовано та модернізовано після внесення змін до деяких розділів, а потім перейменовано на Закон про кібербезпеку. Новий закон передбачав деяке пом'якшення покарань, наприклад, для розділу 21 DSA, який спочатку передбачав 10-річний термін ув'язнення за поширення «пропаганди», пов'язаної з Визвольною війною Бангладеш; у CSA це покарання зменшено до 7 років.

Міністр юстиції зазначив, що були враховані думки зацікавлених сторін. Однак широкій громадськості було надано короткий термін, з 10 серпня по 22 серпня 2023 року, щоб подати свої пропозиції та занепокоєння електронною поштою. Посольство США в Дакці опублікувало заяву, в якій стверджувалося, що уряд не дав зацікавленим сторонам достатньо часу або можливостей переглянути та внести свій внесок, щоб забезпечити відповідність закону міжнародним стандартам. Згідно із заявою, CSA зберігає численні елементи з DSA, які все ще становлять загрозу свободі слова. Крім того, було зазначено, що CSA містить положення про відмову в звільненні під заставу за правопорушення згідно з певними розділами, а деякі визначення є надто широкими і можуть бути використані зловживанням, щоб залякати та змусити замовкнути критиків…

ЗМІ та захисники цифрових прав постійно підкреслюють, що новий закон суперечить різним положенням Конституції Бангладеш і суперечить міжнародним стандартам прав людини. Крім того, розділ 42 CSA, подібний до розділу 43 DSA, надає органам влади повноваження проводити рейди, обшуки або арешти на підставі підозри в скоєнні злочину чи його неминучості, або наявності доказів. буде знищено. Однак міністр юстиції стверджував, що згідно з новим CSA немає можливості для арешту без ордера, а розділ 42 містить юридичну вимогу.

Правозахисник Саад Хаммаді критикує претензії уряду:

Підвищення штрафу та скасування тюремного ув'язнення за наклеп не є й близьким до виправлення DSA.

Громадськість з нетерпінням чекає офіційної версії закону, щоб зрозуміти, які зміни внесено на основі коментарів зацікавлених сторін та пропозицій постійної

комісії Верховної Ради з питань пошти, телекомунікацій та інформаційних технологій до проекту, оприлюдненого в мережі понад місяць тому». ***(Rezwan. The government of Bangladesh quietly passed the new Cyber Security Act 2023 // Global Voices (https://globalvoices.org/2023/09/19/the-government-of-bangladesh-quietly-passed-the-new-cyber-security-act-2023/). 19.09.2023).***

***

«ОАЕ розробляють бачення кібербезпеки, яке посилить боротьбу з цифровою злочинністю протягом наступних 50 років, сказав високопоставлений чиновник.

Цей крок забезпечить країні «найвищий рівень стійкості», підвищивши її здатність «вирішувати зростаючі цифрові виклики», заявив у середу доктор Мохаммед Аль Кувейті, голова Ради кібербезпеки ОАЕ, цільової групи онлайн-безпеки Еміратів.

«Оскільки ОАЕ з нетерпінням чекають свого сторіччя у 2071 році, у нас була можливість зупинитися, вивчити, як може розвиватися світ і як ми можемо використовувати технології для оптимізації результатів для людства», — сказав він.

Доктор Аль Кувейті виступав під час заходу, організованого Радою з кібербезпеки ОАЕ та KPMG Lower Gulf.

Рада з кібербезпеки була створена Кабміном у листопаді 2020 року на тлі сплеску загрози та атаки на комп’ютери та Інтернет у всьому світі.

Рада відповідає за законодавство щодо зміцнення кібербезпеки, яке підлягає затвердженню Кабінетом міністрів.

ОАЕ зафіксовано 77-відсоткове збільшення кількості електронних листів, які містили фішингові загрози, у другому кварталі цього року. У звіті, опублікованому в серпні охоронною компанією Kaspersky, в

За його словами, тактика стає все більш витонченою.

Відповідно до звіту, опублікованого Радою з кібербезпеки та KPMG, розвиток захоплюючої віртуальної реальності «розмиє реальне життя та вигадку, коли бізнес буде процвітати у віртуальному світі, а дані стануть новими грошима».

«Роботи бездоганно інтегруються в наше життя, від засобів особистої гігієни до військових систем, тоді як штучний інтелект зможе передбачати та формувати майбутнє», — The Cyber Next 50. йдеться у звіті

Машини також можуть розвинути здатність читати людські думки та маніпулювати ДНК.

До 2071 року якість життя та щастя все більше визначатиметься безпечним і захищеним гібридом фізичного та цифрового світу.

Відповідно до звіту, ОАЕ потрібно буде адаптувати своє законодавство з кібербезпеки, щоб підготуватися до наступних 50 років.

Очікується, що до 2050 року населення планети досягне 9,7 мільярдів.

Зміна клімату вже впливає на продовольчу безпеку та спричиняє переміщення населення, а також деградацію екосистем, йдеться у звіті.

З огляду на те, що глобальне споживання енергії зросте на 50 відсотків до 2050 року, важливість відновлюваної та ефективної енергії також зростає.

Доктор Аль Кувейті сказав, що ці виклики вимагають «наполегливої роботи, щоб протистояти їхнім наслідкам і пом’якшити їх».

Незважаючи на ці ризики, технології дають надію на краще майбутнє, сказав він.

За його словами, технологічні інновації включають штучний інтелект, гіперзв’язок, біоінженерію, квантові обчислення, космічні технології, робототехніку, розумне виробництво, доповнену реальність і ядерний синтез». ***(Sunil Singh. UAE plans cybersecurity vision for next 50 years // The National (https://www.thenationalnews.com/business/technology/2023/09/20/uae-plans-cybersecurity-vision-for-next-50-years/). 20.09.2023).***

***

«У березні був створений Азербайджанський центр кібербезпеки 2023 за підтримки PASHA Holding Group та Інституту Техніон в Ізраїлі. За наступні 3 роки в центрі підготують понад 1000 осіб у сфері кібербезпеки. 15 тренерів з Ізраїлю надасть знання та навички з новітніх кібербезпеки загрози, тенденції та найкращі практики.

Центр обладнаний аудиторіями, навчальними кабінетами, симуляційні кімнати та лабораторії з новітніми технологіями та обладнання. Начальник Державної безпеки генерал-полковник Алі Нагієв Сервіс Рашад Набієв, Міністр цифрового розвитку та Транспорт, Габі Ашкеназі, колишній міністр закордонних справ Ізраїлю, Боаз Голані, виконавчий віце-президент і генеральний директор Technion, на відкритті були присутні представники посольства Ізраїлю церемонія Центр.

Азербайджан постійно вживає заходів щодо запобігання кібер загрози та загрози, пов'язані з інформаційною безпекою. У 2021 році Азербайджан посів 40 місце серед 194 країн світу Індекс кібербезпеки.

Сектор кібербезпеки входить до складу Азербайджану стратегії розвитку до 2030 року. Раніше Азербайджан затвердив а стратегія інформаційної безпеки та кібербезпеки для 2023-2027 роки.

Відповідно до цієї стратегії Азербайджан створить вимоги кібербезпеки для національного цифрового повітряного простору, визначати податкові пільги та інші обов'язкові платежі у зв'язку з цим з розвитком технологій захисту інформації, удосконал захисту персональних даних, створення консультаційних платформ на інформаційної безпеки та кібербезпеки, вжити заходів щодо підготовки національних ресурсів у сфері криптографічного захисту та розробити план організаційної структури для створення кіберорганізації.

Крім того, буде розроблено план створення організаційна структура, оцінка ризиків і план управління захищати та керувати критичною інформаційною інфраструктурою в надзвичайних ситуацій і війни та електронної інформаційної системи Сформується «кіберзлочинність».

Критерії та показники для виявлення та вимірювання інцидентів також будуть визначені критичні випадки та інформація буде підтримуватися реєстр ризиків безпеки.

Мінцифри та транспорту, Держ Служба спеціального зв'язку та захисту інформації та Центральний банк Азербайджану працює над розвитком і захист державних цифрових систем та веб-ресурсів.

Центральний банк Азербайджану також працює над а стратегія кібербезпеки для банків Азербайджану, яка запланована для реалізації цього року. Уряд також працює над створення урядової хмари (G-cloud) в Азербайджані та надання хмарних послуг державним, приватним та іноземним сутності.

Асоціація організацій кібербезпеки Азербайджану також була створена для об'єднання на одній платформі компаній, організацій, та фахівців, які працюють у сфері інформ технології та кібербезпека в країні.

Critical Infrastructure Defense Challenge 2023 (CIDC-2023)

Захід відбудеться в Бакинському конгрес-центрі 26-27 Жовтень 2023 року, організований спільно Держспецзв’язку і Служба безпеки інформації Азербайджанської Республіки (SCSID) і Службою державної безпеки Азербайджану.

CIDC-2023 об’єднає вітчизняні та іноземні компанії, державного та приватного секторів, студентів та експертів у цій галузі.

Подія включатиме перші змагання з кібервійни в Азербайджан розвиває здатність захищати критичну інформацію системи від кібератак і управління інформаційними системами в умовах кризи ситуації. Команди-учасниці повинні будуть забезпечити віртуальну інформаційних систем у конкурсі, який проводитиме в моделювання кібератак.

Потрібна правова база для кібербезпеки в Азербайджані посилено, оскільки кіберзброя в різних формах (наприклад, Stuxnet вірус) вже намагалися порушити роботу держави кіберінфраструктура. Існує нагальна потреба побудувати сильний і, щоб запобігти ризикам кібератак на країну цифрова інфраструктура, потужна та добре захищена кібермережа необхідно. Крім того, просування та вдосконалення

кіберзаконодавства і створення кібер-армії стало життєво необхідною умовою Азербайджан посилить національну кібербезпеку держави.

19 вересня під час проведення локальної антитерористичної операції проведені Азербайджаном на його території в Карабахській економічній області для роззброєння сепаратистського режиму і після його капітуляції, урядові установи зазнали кібератак з боку терористичний режим.

Велика Британія готова підтримати Азербайджан у сфері кібернетики безпеки. Про це написав на своїй сторінці посол Великобританії в Азербайджані Фергюс Олд Сторінка в соціальних мережах після інциденту.

«Азербайджан знаходиться в складному і особливому районі слід звернути увагу на небезпеки, які можуть становити кібератаки і найкращі способи їх запобігання. Британські компанії завжди готовий підтримати Азербайджан у цій сфері», - сказав Фергюс.

Раніше піддалися ряд державних органів Азербайджану кібератаки під час антитерористичних заходів у Карабаху.

«Було понад чотири мільйони DDoS-атак на секунду зареєстровані лише на офіційному сайті президента. спеціалісти нашої служби продовжують працювати в цьому напрямку в посиленому режимі режимі», – сказав глава держдепартаменту Турал Мамедов Служба спеціального зв'язку та захисту інформації.

«Штучний інтелект у новому поколінні економіка:

Виклики та можливості в рамках конференції «Застосування технологій четвертої промислової революції в народного господарства» в рамках «Соц.-екон Стратегія розвитку Азербайджанської Республіки для 2022-2026».

Близько 9 великих проектів, що охоплюють державні, приватні та цивільні секторів, а також 69 напрямів діяльності, призначених для реалізації ці проекти сприятимуть економічному зростанню Азербайджану 2030, підвищення конкурентоспроможності галузей, сприяння доступу громадян до послуг, а також покращення надання громадських послуг послуг, сказав заступник міністра економіки Азербайджану Сахіб Алекперов.

Азербайджан передбачає часте використання штучного інтелект

Найближчим часом Азербайджан планує запровадити штучне розвідник вільно володіє азербайджанською мовою та післяазербайджанською вміст. Метою ініціативи є захист Азербайджану культурне багатство та розширення використання ШІ в Баку та його регіонах, що допоможе збільшити економічне зростання та стимулювати роботу та створення промисловості.

«У майбутньому широке використання технологій AI буде вимагають підвищеної уваги до цієї сфери, підготовки спеціалістів з новим мисленням і визначенням етичних норм. Стрімкий розвиток технологій і поява передових моделей GPT створити велику потребу у створенні стандартів закупівель", – сказав заступник міністра економіки.

Щоб краще організувати процес закупівель на підприємстві, керівництво має визначити єдиний план штучного стратегія розвитку інтелекту. За статистикою, У 2022 році ринок штучного інтелекту оцінювався в 136 мільярдів доларів і очікується, що річний темп зростання буде 37,3 відсотків з 2023 по 2030 рік.

Азербайджан проводитиме всі державні закупівлі за допомогою цифрові платформи

З введенням в дію нового закону «Про публічні закупівлі» в Азербайджані з 1 січня наступного року планується організувати і проводити 100% державних закупівель з використанням цифрових платформ, Mammad Аббасбейлі, голова Державної служби антимонопольного контролю та Нагляд за ринком споживачів при Мінекономіки Азербайджан, сказав.

«Законопроект підготовлено відповідно до міжнар практика і на сьогоднішній день усі процеси та негативні аспекти пройшли оцінюється на основі висновків, отриманих від державних організацій та Ринок. Таким чином, з 1 січня всі державні закупівлі в Азербайджан буде проводитися з використанням цифрових платформ. Переваги цього буде величезним. Ми підходимо до цього з точки зору погляд на підтримку розвитку підприємництва»

«Після запровадження цих платформ вся діяльність послуги буде оцифровано», - підсумував М.Аббасбейлі…». ***(Abbas Ganbay. Cyber security thrives***

in Azerbaijan due to strong measures // AzerNewsAz (https://www.azernews.az/analysis/215252.html). 27.09.2023).

***

«Навігація у складному світі кібербезпеки в Єгипті стала важливою для бізнесу. У цій статті розглядається система кібербезпеки Єгипту, підкреслюється важливість законодавства та нормативних актів. Зі стрімким цифровим розширенням юридичні фірми з кібербезпеки в Єгипті та юристи з кібербезпеки відіграють ключову роль у керуванні підприємствами в Республіці.

Структура кібербезпеки в Єгипті

В основі ефективних заходів кібербезпеки лежить надійна та динамічна структура. Низка єгипетського законодавства регулює цю сферу, надаючи як загальні, так і нюансовані вказівки.

Відповідне законодавство

Закон Єгипту про боротьбу з кіберзлочинами та інформаційними технологіями (№ 175 від 2018 року): цей закон є основою законодавства про кіберзлочини в Єгипті. У ньому описано покарання за несанкціонований доступ, порушення конфіденційності даних та інші форми кіберзловживань.

Закон 151/2020 про захист персональних даних: цей закон спрямований на захист особистої інформації осіб, встановлюючи новий стандарт захисту даних і суттєво впливаючи на кібербезпеку в Єгипті.

Закон про регулювання телекомунікацій (№ 10 від 2003 року): цей закон встановлює правила, що стосуються цифрового зв’язку, який також містить вказівки щодо безпечної передачі даних.

Наслідки законодавства

Дотримання цих законів має першочергове значення, враховуючи зростаючу складність кіберзагроз як у Єгипті, так і в усьому світі. Компанії з кібербезпеки в Єгипті відіграють ключову роль у забезпеченні надійного захисту та відповідності бізнесу існуючим законам.

Взаємодія між законом про кібербезпеку та корпоративним правом в Єгипті

Одним із найбільш забутих, але важливих аспектів ведення бізнесу в Єгипті є розуміння взаємодії між законом про кібербезпеку та корпоративним правом. Цифровізація бізнес-операцій зробила кібербезпеку невід'ємною частиною корпоративного управління, створивши низку викликів і можливостей.

Правові рамки збігаються

Закон Єгипту про боротьбу з кіберзлочинами та інформаційними технологіями розроблений для захисту цифрових просторів, але він також має прямі наслідки для корпоративного управління. Тепер компанії зобов'язані прийняти суворі протоколи керування даними та кібербезпеки, щоб уникнути штрафних санкцій. З іншого боку, Закон Єгипту про компанії (№ 159 від 1981 року) та Закон про інвестиції (№ 72 від 2017 року) встановлюють правову основу для ділових операцій, включаючи аспекти, пов'язані з управлінням даними, інтелектуальною власністю та поведінкою в Інтернеті.

Наслідки для корпоративної відповідальності

Поєднання законодавства про кібербезпеку та корпоративного права в Єгипті потенційно може призвести до збільшення корпоративної відповідальності. Наприклад, якщо компанія не захистить дані клієнтів і зазнає порушення, вона не тільки несе відповідальність згідно із законодавством про кібербезпеку, але й може зіткнутися з наслідками відповідно до ширшого корпоративного законодавства. Це вимагає надійної правової стратегії, яка відповідає як нормам кібербезпеки, так і протоколам корпоративного управління.

Роль відповідальних осіб

Враховуючи взаємопов'язаний характер законодавства про корпоративну та кібербезпеку, компанії часто наймають спеціалістів з комплаєнсу або звертаються за допомогою до фірм з кібербезпеки в Єгипті. Ці професіонали гарантують, що бізнес не лише дотримується вказівок щодо кібербезпеки, але й дотримується корпоративного законодавства, таким чином уникаючи потенційних правових конфліктів.

Потреба в інтегрованих правових стратегіях

Кібербезпека більше не є окремою IT-проблемою, а комплексним юридичним викликом. Компанії повинні прийняти інтегровані стратегії, які задовольняють вимоги як корпоративного законодавства, так і законодавства про кібербезпеку. Це часто передбачає комплексну оцінку ризиків, перевірку відповідності та постійні юридичні консультації – це послуги з кібербезпеки, які пропонує Andersen Egypt.

Розуміння конвергенції законодавства про кібербезпеку та корпоративного права має важливе значення для компаній, які прагнуть процвітати в динамічному бізнес-середовищі Єгипту. Оскільки нормативні документи постійно розвиваються, активність, а не реагування на зміни, може надати компаніям конкурентну перевагу. Тут досвід Andersen Egypt як фірми з кібербезпеки в Єгипті може забезпечити необхідну перевагу в навігації в цьому складному ландшафті.

Тенденції кібербезпеки в Єгипті

Важливо бути в курсі постійних змін ландшафту загроз, які впливають на кібербезпеку в Єгипті. Розуміння цих тенденцій допомагає організаціям підготуватися до майбутнього та краще захистити свої активи.

Збільшення уваги до хмарної безпеки

З прискоренням переходу до хмарних обчислень кібербезпека в Єгипті тепер також передбачає захист хмарних активів. Безпечна міграція та зберігання даних у хмарі – це послуги, які пропонують різні технологічні компанії в Єгипті, що підкреслює еволюцію кібербезпеки в Республіці.

Підсумок: подорож крізь складний ландшафт кібербезпеки в Єгипті

Світ кібербезпеки в Єгипті складний, але з ним можна подолати за наявності належного досвіду та вказівок. Зважаючи на зростання онлайн-загроз і швидку зміну законодавства, компанії, які працюють в Єгипті, повинні надавати пріоритет кібербезпеці. Розуміння наслідків різноманітних законів і нормативних актів і тримати руку на пульсі нових кіберзагроз має вирішальне значення для захисту активів і підтримки відповідності.

Andersen Egypt пропонує неоціненну послугу в цьому відношенні, допомагаючи підприємствам орієнтуватися в цьому складному ландшафті. Ми

пропонуємо спеціалізований досвід у зменшенні ризиків, відповідності та випередженні нових кіберзагроз. Враховуючи це складне середовище, компанії повинні зробити кібербезпеку пріоритетом не лише для захисту своїх поточних операцій, але й для забезпечення довгострокової стійкості та успіху.

У цьому швидко мінливому ландшафті, де кібербезпека може бути різницею між успіхом і невдачею бізнесу, всебічне розуміння та профілактичні заходи є вашими найціннішими активами. У цій подорожі відділ кібербезпеки Andersen Egypt виступає в якості найважливішого союзника, надаючи досвід і послуги, необхідні для успішної навігації у сфері кібербезпеки». ***(Cybersecurity in Egypt: Navigating the Legal and Technological Landscape // Andersen in Egypt (https://eg.andersen.com/cybersecurity-in-egypt/). 26.09.2023).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Експерт попередив, що кібератаки ворогів Великої Британії стають «безжальними», оскільки ми вступаємо в «нову еру» глобального конфлікту.

Це сталося після того, як російські хакери нібито отримали надсекретну інформацію про безпеку деяких із найбільш конфіденційних військових об’єктів країни, включаючи базу атомних підводних човнів HMNB Clyde на західному узбережжі Шотландії та лабораторію хімічної зброї Портон-Даун.

«Потенційно дуже шкідлива» атака минулого місяця, здійснена хакерською групою LockBit, яка, як відомо, має зв’язки з російськими громадянами, призвела до витоку тисяч сторінок даних у темну мережу після нападу на приватну охоронну фірму Zaun, повідомила газета Sunday Mirror.

Компанія, яка забезпечує захист сайтів, пов’язаних з Міністерством оборони, заявила, що стала жертвою «складної кібератаки».

Відповідаючи на цю новину, Кевін Керран, професор кібербезпеки Ольстерського університету, сказав інформаційному агентству Пенсільванії, що

атака LockBit була «серйозною», оскільки ми наближаємося до потенційної «Третьої світової війни» після вторгнення Росії в Україну.

Він сказав, що рейд «ймовірно» спонсорувала російська держава, враховуючи характер його мети, і що кібератаки ворогів Британії стали «безжальними».

Професор Керран попередив, що ми не готові до цієї нової ери, оскільки сторонні компанії, які зберігають дані про нашу військову інфраструктуру, не регулюються належним чином.

Він сказав: «Ви не можете просто очікувати від сторонніх постачальників дотримання ваших правил.

«Завжди існує ризик, коли у вас є сторонні постачальники, і вам цікаво, чи дотримуються вони найкращих галузевих практик.

Це викликає занепокоєння, тому що зараз все онлайн – кіберзлочинність є найбільшим злочином у світі.

З огляду на нову еру, в яку ми вступаємо, а саме на межі Третьої світової війни, все серйозно.

Вони невпинні з цими атаками. Їхній найкращий шлях у нашу країну — через нашу кібербезпеку. Це нація в зоні ризику.

У цьому випадку, враховуючи ціль, мої гроші підуть на те, що це буде спонсоровано державою».

Едвард Лукас, фахівець із безпеки та оборони, сказав: «Проблема в тому, що ми не живемо в мильній бульбашці – ми приносимо речі із зовнішнього світу. Ось де вразливі місця.

«(Ця інформація) дає їм уявлення про фізичне місцезнаходження та речі, які входять і виходять із цього місця – це як лілія. Ви повинні стрибати з одного на інший, щоб дістатися туди, куди ви хочете».

Ці коментарі з’явилися після того, як депутат від Лейбористської партії Кеван Джонс, який входить до спеціального комітету з питань оборони Палати громад, закликав уряд пояснити, чому комп’ютерні системи Зауна були «настільки вразливими», попередивши: «Це потенційно дуже шкодить безпеці деяких із наших найбільш чутливих систем. сайти».

«Будь-яка інформація, яка надає механізми безпеки потенційним ворогам, викликає величезне занепокоєння», – додав він.

Уряд поки що відмовився відповідати на занепокоєння, а речник сказав: «Ми не коментуємо питання безпеки».

У заяві на своєму веб-сайті, опублікованій у п'ятницю, Zaun заявив, що вжив «усіх розумних заходів для пом'якшення будь-яких атак на наші системи», і пояснив, що вони передали справу до Національного центру кібербезпеки (NCSC).

У ньому пояснили, що злом стався через «підроблений комп'ютер з Windows 7», на якому було запущено програмне забезпечення для однієї з їхніх виробничих машин, але мережа була «в іншому випадку оновлена».

У ньому сказано: «На момент атаки ми вважали, що наше програмне забезпечення кібербезпеки перешкоджає будь-якій передачі даних.

Однак тепер ми можемо підтвердити, що під час атаки LockBit вдалося завантажити деякі дані, можливо, обмежені вразливим ПК, але з ризиком доступу до деяких даних на сервері.

Вважається, що це 10 ГБ даних, 0,74% наших збережених даних.

Загальновідомо, що Zaun є фахівцем у високонадійному огородженні периметра та постачав огородження для багатьох відомих об'єктів.

Місця, де використовуються наші продукти, включають в'язниці, військові бази та комунальні служби»…» ***(Russian cyberattacks 'relentless' as threat of WW3 grows, expert warns // National World Publishing Ltd. (https://www.newschainonline.com/news/russian-cyberattacks-relentless-as-threat-of-ww3-grows-expert-warns-356805?utm_source=flipboard&utm_content=newschain%2Fmagazine%2FNewsChain). 04.09.2023).***

***

«Національні держави-ізгої «безперечно» використовують генеративний фейковий контент для зламу урядів і компаній у всьому світі, заявив колишній кіберкомандир підрозділу 8200 ЦАХАЛ полковник (рез.) і керівник

ідей Team8 Боббі Гілбурд у своєму першому всебічному інтерв'ю англійською мовою після відходу з IDF менше року тому.

«Зараз у світі складніше з точки зору блокування хакерів, незалежно від того, чи є вони національними державами чи кіберзлочинцями. Де є гроші, там знаходять можливості. «Кіберзлочинці знаходяться на високому рівні», — сказав старший чиновник однієї з провідних ізраїльських фірм із кіберзахисту.

Відповідаючи на запитання про серію кібератак на Ізраїль, яку приписують Ірану, колишній високопосадовець підрозділу 8200 ЦАХАЛу (АНБ Ізраїлю) сказав: «Іноді вони [хакери] стирають межу між урядовими хакерствами та кіберзлочинністю, і ця межа стає сірою. Було опубліковано, що Іран, Росія, Китай і Північна Корея іноді використовують кіберзлочинність, що іноді є лише прикриттям».

Нещодавня резонансна кібератака в Ізраїлі на «Медичний центр Мааней Ієшуа» може бути кіберзлочинністю, вона має такі характеристики – і іноді кіберзлочинці атакуватимуть державний орган, наприклад лікарню. Вони також не завжди [обережно] спрямовують цілеспрямовану атаку, але можуть розпорошувати всюди і намагатися вразити одну з 5000 цілей».

«Згідно з загальнодоступною інформацією, близько 10-15% компаній-жертв хакерів платять викуп», якщо їх зламали за допомогою програм-вимагачів, тоді як «деякі відмовляються від даних, а деякі повертають дані за допомогою резервних копій».

Гілбурд додав: «Нападники дуже розумні. Вони як тюремники [даних], які знають, як просити, і знають, скільки просити. Вони займаються бізнесом і хочуть заробити гроші. Частина грошей потім йде на дослідження та розробки для створення сильніших атак на майбутнє».

Далі він запитав: «Чому почастішали напади? Програми-вимагачі майже завжди починаються з людського фактору. Ви отримуєте фішинговий електронний лист, який виглядає дуже надійним. Ви відкриваєте посилання, і вони надсилають програму-вимагач. Фішинг став набагато персоналізованішим».

«Він містить правильне ім’я людини та посаду за допомогою автоматично створеного інструменту для фішингу, GPT та інших інструментів. Раніше ви могли позначати помилки на івриті, але тепер переклад, який є загальнодоступним для всіх мов, чудовий», – попередив він.

Проблеми, представлені за допомогою ШІ

Ще одна проблема з використанням генеративного ШІ (штучного інтелекту), який використовується для злому, полягає в тому, що «визначити [кібер-зловмисника] стає ще складніше. У минулому це могло бути несправність або помилка. Можливо, хтось пише щось російською», що підказує слідчим особу хакера або, можливо, іншомовне слово підкрадається помилково або щоб ввести слідчих в оману.

Іншими підказками для приписування були години роботи хакерів відносно часових поясів певних країн, певний зв’язок із певними святами та використання слів, але все це не є на 100% надійним.

Крім того, «Іноді у зловмисному програмному забезпеченні ви можете побачити схожий код або тактику, які раніше приписувалися певній особі. Це завжди було мистецтвом, з криміналістикою, деякі уряди мають більше можливостей для цього, але врешті-решт, все ще є припущення, і це не відповідає рівню доказів для суду», — сказав Гілбурд.

Але за допомогою генеративного штучного інтелекту навіть багато з цих попередніх «дірок» криміналістичного сліду заповнюються, що ще більше ускладнює визначення того, хто був зловмисником.

Ідеал кіберрозвідки все ще полягає в тому, щоб запобігти злому за допомогою сигналів попереднього попередження, але реально кажучи Гілбурд сказав: «Жодна організація не може повністю уникнути атаки. У якийсь момент ви будете проникнуті».

У цьому дусі Team8 зараз випускає звіт, який вперше побачив Post, в якому міститься опитування близько 150 CISO (керівників інформаційної безпеки) з компаній зі списку Fortune 500, які заявили, що безпека ШІ перетворилася з однієї з багатьох проблем на одна з трьох головних проблем.

Далі у звіті говориться, що значного очікуваного скорочення фінансування кіберзахисту не відбулося.

Гілбурд пояснив, що «завжди важко побачити переваги інвестування в кібербезпеку, поки на вас не нападуть. Потім ми побачили, що сповільнилося [фінансування кіберзахисту] як частина ширшого світового економічного спаду. Деякі країни починають розвиватися, але деякі навіть досі називають це повною рецесією. Тому ми очікували зниження інвестицій у кібербезпеку».

«Ми були здивовані організаціями, з якими ми працюємо в останньому опитуванні нашого села з 350 CISO, прийшло 140 CISO, і хоча ми очікували зниження фінансування кіберзахисту, фінансування в основному залишилося на тому ж місці або трохи зросло. Навіть у невеликій кількості випадків, коли було падіння фінансування, воно було меншим, ніж очікувалося», – сказав він.

Крім того, Гілбурд обговорив нову загрозу штучного інтелекту в соціальних мережах.

«Тепер з’явилися нові загрози бренду компанії, тож існують засоби захисту бренду. Це [узгоджена] кампанія атаки впливу на соціальні медіа, це новий тип атаки», — попередив він.

Колишній співробітник підрозділу 8200 ЦАХАЛу сказав: «Усі кібератаки та засоби захисту стають кращими завдяки ШІ. Не буде остаточного переможця, як немає переможця в битві вірусів і антивірусів».

Деякі люди попереджають, що «ШІ — це кінець, і тепер ми ніколи не дізнаємося, що правда. Деякі кажуть, що захист GPT AI — це «кінець фейкових новин — ні те, ні інше не є правдою», оскільки обидві сторони продовжуватимуть мчати вперед.

У цьому ключі новий захист AI для захисту бренду «може автоматично виловлювати, ідентифікувати та видаляти публікації», які зловмисно атакують ваш бренд. Частина процесу, за його словами, включає доведення того, що зловмисник порушує політику платформи соціальних мереж, будь то Twitter, Facebook чи інше, або використовує підроблену особу.

Він сказав, що Team8 шукає нові способи використання автоматизації для процесу ідентифікації та видалення помилкових зловмисних публікацій за допомогою генеративного штучного інтелекту. Автоматизований процес може навіть надсилати листи до Twitter, щоб видалити публікацію та зрозуміти відповідь Twitter.

Гілбурд сказав, що третя і четверта версії GPT вже «до такої міри озброєні, що я вважаю, що майбутні п'ята і шоста версії GPT будуть відрізані від широкого загалу».

Це пояснюється тим, що GPT може створювати фальшиві голоси високого рівня та виконувати тисячі розмов із банками та службою обслуговування клієнтів, щоб викрасти інформацію чи навіть кошти.

«Це гра в кішки-мишки», яка змагається за використання ШІ для нападу та захисту. «Раніше ми могли бачити сигнатури шкідливих програм, тепер ми можемо виявляти їх евристично. Зараз усі компанії використовують штучний інтелект на захист для ідентифікації контенту за допомогою спеціальної пошукової системи, яку професори також використовують для запобігання плагіату».

Метод евристики оцінює всі матеріали за стандартним набором правил. Якщо предмет отримує оцінку вище певного рівня, він негайно визначається як підробка.

Звіт також показав, що CISO занепокоєні вразливістю третіх сторін – коли постачальника для компанії зі слабкішим кіберзахистом зазнають злому, що призводить до злому цієї компанії, навіть якщо вона сама має кращий захист. Нарешті, у звіті говориться, що керівники CISO продовжують хвилюватися через те, що співробітники недостатньо остерігаються цифрових спроб використовувати їх для проникнення в компанію.

Що стосується атак на державний сектор, Гілбурд висловив вотум довіри Національному кіберуправлінню Ізраїлю (INCD.)

«INCD чудово працює та має можливість залучати людей із великим кібердосвідом. Багато людей, які служили зі мною в частині 8200, вирішили продовжити роботу в державному секторі. Багато з них були залучені до сектору кібератак, тому вони це розуміють і тепер переносять це розуміння на захист. Це

чудово для Ізраїлю і не тривіально». ***(YONAH JEREMY BOB. Rogue states using fake GPT content to hack governments - ex-IDF cyber chief // Jpost Inc. (https://www.jpost.com/israel-news/article-757758?utm_source=flipboard&utm_content=JerusalemPost%2Fmagazine%2FIsrael+News). 06.09.2023).***

***

«Оскільки Інтернет пронизує майже кожен аспект нашого життя, кібервійна стала важливим інструментом для багатьох країн-ізгоїв. Хоча правозахисники зазвичай не сприймають це так само серйозно, як фізичні воєнні злочини, ця позиція потенційно може змінитися в майбутньому, як свідчить нещодавня заява головного прокурора Міжнародного кримінального суду (МКС).

За словами Каріма Хана, головного юриста МКС, Гаага готова розпочати розслідування та переслідування, пов'язані з кіберзлочинами, які порушують міжнародне право. Незважаючи на те, що багато лідерів і експертів з безпеки вже давно виступають за спеціалізовані закони для боротьби з кібервійною, Хан вважає, що існуючі міжнародні закони достатні для притягнення кіберзлочинців до відповідальності.

У недавній статті у Foreign Policy Analytics (через Wired) Карім стверджував, що кібервійна може мати серйозний руйнівний вплив на життя людей і може бути використана для сприяння військовим злочинам, злочинам проти людства та геноциду. Крім того, це може служити засобом для підтримки фізичних нападів на суверенні національні держави, підкреслюючи необхідність міжнародного кримінального правосуддя протистояти цій зростаючій загрозі.

Карім зазначив, що хоча в Римському статуті немає жодного конкретного положення, присвяченого кіберзлочинам, він також підкреслив, що Міжнародний комітет Червоного Хреста однозначно заявив, що кібератаки мають бути спрямовані виключно на військові цілі, а не на цивільні об'єкти, такі як електромережі та лікарні.

Для тих, хто не знайомий, Римський статут – це угода, прийнята МКС у 1998 році для розгляду чотирьох основних міжнародних злочинів, включаючи геноцид, злочини проти людства, військові злочини та злочин агресії.

Карім пояснив, що його погляд на серйозність кіберзлочинів випливає з того факту, що межі між фізичними та цифровими фронтами війни давно розмиті. Цифрова сфера може завдати «збитків і страждань, які можна порівняти з тими, яким прагнули запобігти засновники ICC». Для боротьби з кіберзлочинами, які завдають шкоди цивільному населенню, Карім підтвердив, що його офіс «збиратиме та переглядатиме» докази, пов'язані з незаконною кібердіяльністю національних держав.

Після публікації статті МКС офіційно оголосив, що буде переслідувати справи про шахрайські кібероперації, які суперечать Римському статуту.

У заяві, наданій Wired, речник ICC уточнив, що ці справи розглядатимуться лише за «відповідних обставин» і коли «серйозність є достатньо серйозною». Однак ні Хан, ні речник не надали подробиць про те, як цю нову політику можна застосувати, щоб притягнути Росію до відповідальності за її триваючі кібератаки на цивільну інфраструктуру в Україні». ***(Kishalaya Kundu. The International Criminal Court will start prosecuting cyber war crimes // TechSpot, Inc. (https://www.techspot.com/news/100090-international-criminal-court-start-prosecuting-cyber-war-crimes.html?utm_source=flipboard&utm_content=user%2FTechSpot). 08.09.2023).***

***

«Відповідно до стратегії Пентагону, оприлюдненої цього тижня, Китай і Росія готові здійснити серію кібератак на критично важливу інфраструктуру та захисні мережі США, якщо почнеться війна.

Така тактика, яка має на меті посіяти хаос, відволікти дорогоцінні ресурси та паралізувати військову мобілізацію, спостерігалася у Східній Європі під час вторгнення Росії в сусідню Україну, конфлікту, який забарвлює нову

Кіберстратегію Пентагону до 2023 року. 12 вересня було оприлюднено незасекречене резюме документа.

«Сполучені Штати кидають виклик зловмисникам у кіберпросторі, які прагнуть використати наші технологічні вразливості та підірвати конкурентоспроможність нашої армії», — йдеться у вступі. «Вони націлені на нашу критичну інфраструктуру та ставлять під загрозу американський народ. Захист і подолання цих кіберзагроз є обов'язковим завданням Міністерства оборони».

Представники оборонного відомства вже давно вважають Китай і Росію загрозою національній безпеці. У той час як Китай становить найсерйознішу та довгострокову загрозу, вони кажуть, що Росія викликає більш безпосередні занепокоєння. Обидві країни володіють серйозними кібер-арсеналами. У звіті Міжнародного інституту стратегічних досліджень у 2021 році Китай і Росія були поміщені на другу сходинку рейтингу кібернетичних компаній. США засіли першими.

Стратегія, яка замінює версію 2018 року, описує Китай як «широку та всеосяжну» загрозу кібершпигунству, здатну переховуватися з комерційними секретами оборони та стежити за громадянами США. Крім того, він називає Росію онлайн-маніпулятором і переслідувачем критичної інфраструктури, такої як трубопроводи, лікарні та транспорт.

«Кіберпроблеми скрізь — у критичній інфраструктурі, всередині країни та за кордоном — це те, що є головним у голові наших ключових керівників вищої ланки», — сказав 11 вересня Грегорі Тухілл, бригадний генерал ВПС у відставці та колишній федеральний головний офіцер з інформаційної безпеки. на конференції в Національній Гавані в Меріленді. Його коментарі прозвучали перед публікацією резюме стратегії.

«Ми продовжуємо розглядати критичну інфраструктуру як мішень для кібератак, включаючи такі речі, як відмова в обслуговуванні, шкідливе програмне забезпечення, програми-вимагачі, крадіжка інтелектуальної власності», — додав він. «Ми дуже стурбовані цим».

Стратегія Пентагону збігається з планами цифрового захисту Білого дому, які були оприлюднені в березні. У них адміністрація Байдена пообіцяла використовувати «всі інструменти національної влади», щоб перешкодити та знищити зловмисних кіберакторів поблизу та далеко.

Для цього знадобиться значне співробітництво з іноземними урядами, лідерами галузі тощо.

«Сузір'я національних дипломатичних і оборонних відносин є фундаментальною стратегічною перевагою», – йдеться в стратегії Пентагону. «У кіберпросторі можливості союзників і партнерів поєднуються з можливостями Сполучених Штатів, щоб забезпечити своєчасний обмін інформацією та взаємодію, а також зробити внесок у нашу колективну безпеку». ***(Colin Demarest. China, Russia will use cyber to sow chaos if war starts, Pentagon says // Yahoo (https://news.yahoo.com/china-russia-cyber-sow-chaos-180404260.html?fr=sycsrp_catchall). 12.09.2023).***

***

«Проросійським хакерським групам вдалося отримати доступ до трьох поштових скриньок Міністерства внутрішніх справ Латвії.

Про це порталу Delfi розповіли представники латвійського відомства, повідомляє «Європейська правда».

За даними порталу, у понеділок на різних хакерських Telegram-каналах було опубліковано кілька внутрішніх документів МВС Латвії, а також окремі листування електронною поштою.

У відомстві наголосили, що інцидент розслідують, також застосовують додаткові методи підвищення рівня безпеки.

«Ми можемо підтвердити, що в електронній системі МВС спостерігають активність, пов'язану зі спробами несанкціонованого доступу», – зазначили у латвійському МВС.

Також у міністерстві зазначили, що в рамках розслідування інциденту не було виявлено жодних доказів, які б свідчили про несанкціонований доступ до

державних інформаційних систем, які перебувають у віданні інформаційного центру МВС, або про їхню несправність…». ***(Проросійські хакери отримали доступ до поштових скриньок МВС Латвії // Європейська правда (https://www.eurointegration.com.ua/news/2023/09/6/7168910/). 06.09.2023).***

***

«Іранська кібератака, націлена на ізраїльських шукачів роботи, була виявлена Національним кіберуправлінням у четвер, причому управління попередило, що хакери зливали особисту інформацію людей, які були ціллю.

Атака була здійснена шляхом надсилання підроблених повідомлень користувачам сайту пошуку роботи під виглядом офіційних повідомлень із сайтів. Повідомлення включають шкідливе посилання, яке відкриває вкладку браузера, що містить код, який намагається ввімкнути камеру пристрою, і підроблену сторінку входу, яка записує дані для входу цільового користувача.

У Національному кіберуправлінні відзначили, що повідомлення містять помилки, а посилання дещо відрізняється від URL-адреси офіційного веб-сайту, використовуючи «.com» замість «.co.il».

Особиста інформація, виточена хакерами, включає фотографії посвідчень особи та файли резюме, серед іншого.

Директорат надав відповідним веб-сайтам інформацію, необхідну для перевірки їхніх комп’ютерних систем, щоб виявити, чи кібератака була спрямована саме на них.

Управління із захисту конфіденційності Ізраїлю закликало користувачів веб-сайтів пошуку роботи бути обережними, отримуючи повідомлення від незнайомих їм контактів, і негайно змінити пароль, який вони використовують для таких веб-сайтів.

«Важливо бути уважним до спроб подальших атак через фішинг у текстових повідомленнях (WhatsApp, SMS тощо) та електронній пошті», — сказали в Управлінні. «Як запобіжний захід завжди рекомендується вводити потрібну послугу, ввівши URL-адресу самостійно, а не використовуючи посилання».

Наприкінці липня Shin Bet оголосила, що виявила спробу Ірану зібрати інформацію від ізраїльських дослідників і державних службовців за допомогою фішингової кампанії з підробленими профілями LinkedIn». ***(TZVI JOFFRE. Iranian cyberattack targets Israelis, leaking personal information // Jpost Inc. (https://www.jpost.com/israel-news/article-760037?utm_source=flipboard&utm_content=JerusalemPost%2Fmagazine%2FIsrael+News). 21.09.2023).***

***

«Китай звинуватив США у проникненні на сервери Huawei Technologies Co., починаючи з 2009 року, у рамках широкомасштабної спроби викрадення даних, кульмінацією якої стали десятки тисяч кібератак на китайські цілі минулого року.

Міністерство державної безпеки Китаю в пості Підрозділ Tailored Access Operations Агентства національної безпеки здійснив атаки в 2009 році, який потім постійно стежив за серверами, повідомило на своєму офіційному акаунті WeChat у середу. Він не надає подробиць про напади з 2009 року.

Кібератаки є точкою напруженості між Вашингтоном і Пекіном, який звинуватив свого політичного суперника в організації атак на китайські цілі з тих пір, як Едвард Сноуден зробив вибухові звинувачення в шпигунстві США. Вашингтон і дослідники з кібербезпеки заявили, що ця азіатська країна спонсорувала атаки на Захід.

Звинувачення міністерства з'явилися в той час, коли дві країни борються за технологічну перевагу. Huawei, зокрема, викликала тривогу у Вашингтоні, оскільки лідер телекомунікаційних технологій представила смартфон на основі вдосконаленого чіпа, розробленого ним Semiconductor Manufacturing International Corp. Це незважаючи на багаторічні санкції США, спрямовані на те, щоб відрізати Huawei від американських технологій. йому потрібно розробляти складні чіпи та телефони.

Сполучені Штати «перебільшують» концепцію національної безпеки, пригнічуючи китайські підприємства, заявила прес-секретар Міністерства закордонних справ Мао Нін журналістам на регулярному прес-брифінгу в Пекіні в середу.

«Ми хочемо сказати США, що придушення та стримування Китаю не зупинить розвиток Китаю. Це тільки зробить нас більш рішучими в нашому розвитку», – сказав Мао.

У вівторок міністр торгівлі США Джина Раймондо сказала, що вона була «засмучена», коли Huawei випустила Mate 60 Pro під час її візиту до Китаю минулого місяця, але зазначила, що США не мають доказів того, що азіатська країна може виробляти передові напівпровідники, які живлять телефон, «у масштабі». ***(Debby Wu. China Accuses US of Hacking Huawei Servers as Far Back as 2009 // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2023-09-20/china-accuses-us-of-hacking-huawei-servers-as-far-back-as-2009?utm_source=flipboard&utm_content=bloomberg%2Fmagazine%2FBloomberg). 20.09.2023).***

***

«…в четвер, португальська компанія VisionWare виявила 961 кібератаку проросійських хакерів проти західних країн і організацій у період з жовтня 2022 року по березень 2023 року.

Звіт під назвою «Дії проросійських кіберугруповань проти держав-членів НАТО» зосереджується на кіберзлочинній діяльності, яку здійснюють хакерські групи KillNet і NoName057(16) і підтверджено португальською компанією VisionWare.

Розмовляючи з Lusa, Бруно Кастро, засновник і генеральний директор VisionWare, визнав, що немає жодних підтверджень того, що проросійський хактивізм спонсорується державою, і що можлива причетність Кремля «незрозуміла».

«Немає жодних матеріалів, щоб зробити висновок, що угруповання пов'язані з Кремлем (або ГРУ — Головне розвідувальне управління чи ФСБ — Федеральна служба безпеки Російської Федерації). Але є дуже злагоджена наступальна стратегія, яка відповідає інтересам російського уряду», – підкреслив він.

Центр створює геополітичні звіти про досліджувані загрози, відстежує суб'єктів ризику, сповіщає в режимі реального часу, коли дані інституцій скомпрометовані, виробляє звіти про аналіз і дослідження основних загроз та суб'єктів, розділених за часом і сектором ризику.

Згідно зі звітом, у Telegram було проаналізовано 8347 повідомлень: 6805 посилаються на Killnet і 1542 посилаються на NoName057(16).

Протягом аналізованого періоду групи найбільше націлювалися на сектори, пов'язані з «урядом, банками та обороною», з 371 нападом. Січень 2023 року став місяцем із найбільшою частотою атак — 333, або близько 35% від загальної кількості.

Португалія стала жертвою двох атак KillNet, які вразили портали національного органу охорони здоров'я (DGS) і факультет фармації.

У двох проаналізованих кварталах 41% атак Killnet припадало на Сполучені Штати. Однак Естонія, Латвія та Литва, на які припало 33,9% атак, здійснених цією групою, та Польща виділяються серед країн, на які найбільше нападає NoName057(16).

У аналізований період дві хакерські групи зосереджувалися на Польщі, зокрема, оскільки на неї було скоєно 123 атаки.

Відповідаючи на запитання про те, що чекає попереду проросійські хакерські групи, Кастро сказав, що вони продовжуватимуть реагувати на поточні події, спостерігаючи за відносинами Росії з третіми країнами.

«Це дослідження, засноване на детальному аналізі щоденних явищ, які ми спостерігаємо за допомогою цих груп, припускає, що цілі будуть виходити за межі України. Наприклад, KillNet взяла на себе відповідальність за широкомасштабні атаки Distributed Denial-of-Service (DDoS) на великі аеропорти США в жовтні 2022

року. Ці атаки не вплинули на рейси, але порушили або затримали послуги аеропорту», — сказав він.

«Усі ці DDoS-атаки завдають репутаційної та фінансової шкоди, багато з яких є більшою, ніж ми уявляємо. У звіті, який ми представляємо, висвітлюється розвиток можливостей, ресурсів і руйнівної сили цих груп для нападу на держави та сприяння дестабілізації суспільств», – додав Кастро». ***(José Sousa Dias. Portuguese company detects 961 pro-Russian cyber attacks in Western Europe // EURACTIV MEDIA NETWORK BV. (https://www.euractiv.com/section/politics/news/portuguese-company-detects-961-pro-russian-cyber-attacks-in-western-europe/?utm_source=flipboard&utm_content=EURACTIV%2Fmagazine%2FEURACTIV). 09.2023).***

***

«У світі, де битви все частіше ведуться за допомогою кодів і клацань, а не гармат і калібру, безшумний фронт кібервійни продовжує зростати. Цього місяця нахабна цифрова атака з боку Ісламської Республіки Іран оголила особисті дані незліченної кількості ізраїльтян, кинувши тінь на ключові дипломатичні переговори та роботу Генеральної Асамблеї ООН. У міру того, як технології все більше впроваджуються в наше життя, лінії традиційної геополітики стираються, породжуючи нові, невидимі поля битв.

Навігація складним геополітичним ландшафтом Близького Сходу часто веде крізь лабіринт ракетних ударів, регіональних проксі-війн і ескалації ядерних амбіцій. Однак, оскільки технології рухають нас вперед, увага має бути перенаправлена на нову таємну сферу: цифрову сферу. Поєднання складних кіберможливостей Ірану та його непохитної позиції проти Ізраїлю окреслює тривожний план, спрямований на більшу мету – дестабілізацію самих стовпів демократії.

Для будь-якого проникливого аналітика кібератаки Ірану на Ізраїль набагато вагоміші, ніж прості спалахи у віртуальному ландшафті. Як помітила Сюзанна

Мелоні, старший науковий співробітник Інституту Брукінгса, у своєму дослідженні, конфронтаційна позиція Ірану щодо Ізраїлю не обмежується звичайними полями битв. Це глибоко переплетене з ідеологічною боротьбою, яка виходить за межі політичних суперечок, заглиблюючись у антисіонізм і навіть антисемітизм. Ворожнеча Ірану по відношенню до Ізраїлю завжди була не просто геополітикою: вона також ідеологічна та екзистенціальна.

Розраховані зусилля Ірану знищити Ізраїль зсередини

Цифрові стратегії Ірану — це не просто символічні демонстрації влади, а продумані кроки, спрямовані на руйнування ізраїльської суспільної тканини зсередини. Як повідомляє Центр стратегічних і міжнародних досліджень (CSIS), ці кіберініціативи мають на меті «порушити повсякденне життя Ізраїлю, деморалізувати ізраїльське громадянство та підірвати довіру до здатності ізраїльського уряду захистити свій народ».

Онлайн-агресія Ірану є лише одним з аспектів набагато ширшої та комплексної стратегії. Кеннет Поллак, відомий дослідник Близького Сходу, підкреслює, що войовнича риторика Ірану також служить подвійній меті. Поллак припускає, що «Іран використовує свою запальну риторику щодо Ізраїлю як внутрішній центр об’єднання та як засіб регіонального впливу».

Хоча Ізраїль протягом тривалого часу обирався улюбленою та головною мішенню іранського режиму – ворогом, якого потрібно знищити, ненависть Тегерана також відображає його ворожнечу до того, що представляє єврейська держава. Як проникливо зазначив доктор Майкл Рубін з Американського інституту підприємництва, «дії Ірану відображають ширшу ідеологічну конфронтацію з наріжними каменями демократичних суспільств: незалежністю, демократією та свободою».

Коли Іран завдає удару по Ізраїлю, професор Емі Зегарт зі Стенфордського університету підкреслює, що «це не просто політичний крок проти національної держави; це пряма образа основ демократичних принципів».

Оскільки Ізраїль демонструє стійкість перед лицем цих викликів, професор Ієн Бреммер з Євразійської групи застерігає західні демократії: «Стало Ізраїлю —

це канарка у вугільній шахті. Вразливі місця, з якими він стикається сьогодні, можуть бути такими, з якими Захід зіткнеться завтра».

У світлі цього для демократичних країн вкрай важливо визнати свою спільну участь у цих кібернападах і відповідно зміцнити свій захист.

Історично так склалося, що набіги Ірану на кібервійну можна простежити разом із хронологією важливих геополітичних подій, виявляючи помітну модель агресивної цифрової поведінки, яка часто супроводжується великими міжнародними подіями або у відповідь на них.

У 2010 році світ став свідком нищівних можливостей хробака Stuxnet, кіберзброї, яка, як вважають, була спільно розроблена США та Ізраїлем для саботування ядерної програми Ірану. Ця безпрецедентна атака ознаменувала нову еру в кібервійні, і Іран звернув увагу на це (див. книгу Кіма Зеттера «Зворотний відлік до нульового дня» 2014 року).

Тоді, після виходу США з JCPOA у 2018 році, Іран був пов'язаний із запуском Shamoon, зловмисного програмного забезпечення для видалення даних, яке раніше було націлено на Saudi Aramco у 2012 році, здавалося, як негайний і зухвалий цифровий контрудар.

У 2019 році на тлі напруженості навколо атак на нафтові танкери в Оманській затоці з'явилися повідомлення про те, що іранські хакери атакували урядовців США в рамках фішингової кампанії, ще раз підтверджуючи синхронізацію цифрових злочинів із гарячими політичними подіями (Міністерство юстиції США, 2020 р.).).

З 2021 по 2022 роки зухвалі кібероперації призвели до розкриття персональних даних незліченної кількості громадян Ізраїлю. Ці дії відбулися на тлі застопорених дипломатичних переговорів і напередодні важливої сесії Генеральної Асамблеї ООН, сигналізуючи про знайому модель, коли Іран зміцнює свою позицію на переговорах за допомогою агресивних цифрових дій.

УЗЯТИ РАЗОМ ці випадки малюють картину еволюції ідеологічної траєкторії Ірану. Вони не є поодинокими інцидентами, а підкреслюють, як Тегеран постійно використовує кібероперації і як заходи у відповідь, і як стратегічні

інструменти, щоб збігатися з важливими дипломатичними подіями та потенційно впливати на них.

Схема викликає тривогу. Націливши свою кіберзброю на рівень хлору в ізраїльській воді, медичні установи та навіть бази даних шукачів роботи, Тегеран демонструє свій намір використовувати будь-які вразливості. Це означає, що західні демократії з їх постійно зростаючою цифровою інфраструктурою однаково ризикують.

Більше того, як свідчить нещодавня риторика Ірану, ця кібервійна виходить за межі простих технологічних протистоянь. Заяви таких лідерів, як аятола Алі Хаменеї, які передбачають неіснування Ізраїлю протягом 25 років, або тривіальна тривіалізація Голокосту через суперечливі конкурси карикатур, означають явну та небезпечну ідеологічну схильність. Такі настрої не тільки кидають виклик легітимності Ізраїлю, але й віддзеркалюють глибший антисемітський підтекст.

Якщо їх не зупинити, ці подвійні загрози – цифрові та ідеологічні – можуть об'єднатися в грізний виклик опорам демократії. Для Сполучених Штатів, які вже відчули на собі руйнівну силу кібератак, розуміння багатогранного підходу Ірану має вирішальне значення. Політики США повинні забезпечити цілісний підхід, який пом'якшує загрози в кіберсфері, водночас кидаючи виклик суперечливим і шкідливим наративам Ірану.

У світі, де цифрова війна може суттєво впливати на геополітику, важливо пам'ятати, що в її основі це більше, ніж просто одиниці та нулі. Це ідеологічна битва, яка кидає виклик принципам демократії та свободи.

Оскільки ми обережно вступаємо в цю цифрову епоху, США разом зі своїми союзниками повинні рішуче протистояти тим, хто прагне підірвати ці заповітні цінності». ***(CATHERINE PEREZ-SHAKDAM. Iran's cyberattacks on Israel target the pillars of democracy – opinion // Jpost Inc. (https://www.jpost.com/opinion/article-760572?utm_source=flipboard&utm_content=beebrah%2Fmagazine%2FIran). 27.09.2023).***

***

«Хакери з Індії, які називають себе Індійськими кіберсилами, погрожували атакувати канадські веб-сайти у відповідь на заяви про те, що уряд Індії зіграв роль у вбивстві канадського громадянина, який просував незалежну сикхську державу. Група поділилася повідомленням на платформі обміну повідомленнями X, в якому йдеться про те, що кібератаки в Канаді почнуться протягом трьох днів. Веб-сторінка канадської стоматологічної клініки вже постраждала від вандалізму з повідомленням «Зламано індійськими кіберсилами».

Канадська влада та експерти з кібербезпеки перебувають у стані підвищеної готовності, уважно стежать і зміцнюють захист, щоб захистити інші потенційні цілі від подібних атак. Тим часом уряд Індії поки не виступив з офіційною заявою щодо погроз або їхньої ймовірної причетності до смерті громадянина Канади.

Королівська банда програм-вимагачів залишається непоміченою в Далласі протягом місяця

У відповідних новинах про кібербезпеку Королівська банда програм-вимагачів, яка атакувала Даллас, штат Техас, на початку цього року, залишалася непоміченою в IT-інфраструктурі міста майже місяць, викравши особисту інформацію понад 30 000 людей. Місто виділило 8,5 мільйона доларів США на відновлення та відновлення систем, які постраждали від атаки. Спочатку банда отримувала доступ до IT-системи через обліковий запис служби.

Цей інцидент підкреслює важливість регулярного моніторингу та оновлення заходів безпеки в IT-інфраструктурі організації, щоб запобігти значним порушенням даних. Крім того, міська влада закликає інші муніципалітети інвестувати в оновлення своїх протоколів кібербезпеки, щоб зменшити ризики майбутніх атак програм-вимагачів і захистити конфіденційні дані.

Округ Хайндс бореться з постійними атаками програм-вимагачів

Округ Хайндс у штаті Міссісіпі цього місяця все ще має справу з атакою програм-вимагачів, що не дозволяє жителям сплачувати податки на нерухомість, завершувати операції з нерухомістю або купувати автомобільні бирки з 7 вересня. Офіційні особи округу старанно співпрацюють з експертами з кібербезпеки, щоб

вирішити цю проблему та якнайшвидше відновити нормальну роботу. Тим часом жителів закликають залишатися терплячими та пильними, оскільки влада шукає альтернативні рішення для надання цих основних послуг.

Банда програм-вимагачів AlphV зламує виробника автомобільного обладнання Clairon

Група програм-вимагачів AlphV взяла на себе відповідальність за злом компанії Clairon, виробника аудіо-, відео- та навігаційного обладнання для автомобілів від великих виробників. В якості доказів він опублікував скріншоти вкрадених документів. Група кіберзлочинців стверджує, що мала доступ до конфіденційних даних, включаючи фінансові записи, інформацію про співробітників і конфіденційні ділові документи. Clairon співпрацює з експертами з кібербезпеки та правоохоронними органами, щоб пом'якшити вплив злому та запобігти подальшому несанкціонованому доступу до даних.

Уразливість MOVEit від Progress Software вражає більше організацій

Кількість організацій, які постраждали від уразливості в програмному забезпеченні для передачі файлів MOVEit від Progress Software, продовжує зростати, тепер це стосується Національної розрахункової палати США та Корпорації фінансових установ через чотири місяці після початкового виявлення. Ці організації приєднуються до зростаючого списку постраждалих сторін, підкреслюючи далекосяжні наслідки вразливості для різних секторів економіки. Оскільки все більше компаній виявляють вплив цього впливу на їхні системи та дані, це підкреслює важливість своєчасного усунення вразливостей програмного забезпечення, щоб запобігти потенційним широкомасштабним порушенням.

Компанія Kannact Inc. бореться з витоком даних, що зачіпає тисячі людей

Kannact Inc., компанія з підтримки охорони здоров'я, розташована в Орегоні, сповіщає близько 118 000 осіб про витік даних у результаті злому її програмного забезпечення для передачі файлів. Компанія оголосила про порушення в червні, але все ще працює над визначенням точної кількості жертв. Окрім потенційно скомпрометованої особистої інформації, порушення могло призвести до розкриття конфіденційних медичних даних постраждалих осіб. У відповідь Kannact активно

впроваджує подальші заходи безпеки та тісно співпрацює з правоохоронними органами, щоб розслідувати інцидент і мінімізувати будь-які потенційні збитки.

Фізична особа з Нігерії засуджена за шахрайство з комерційною електронною поштою

Нарешті, у листопаді суд США засудив нігерійця за звинуваченнями в змові, пов'язаній із шахрайством із діловою електронною поштою. Оманливі електронні листи змусили жертв переказати гроші. Крім того, ці шахрайські електронні листи часто видають себе за високопоставлених керівників, змушуючи нічого не підозрюючих працівників повірити, що вони переказують кошти для законних цілей компанії. Для боротьби з цією зростаючою проблемою компанії впроваджують суворіші заходи безпеки та підвищують обізнаність співробітників щодо ризиків шахрайства в бізнес-електронній пошті…» ***(Deanna Ritchie. Indian Cyber Force Targeting Canadian Sites, and Other Cybercrimes // ReadWrite, INC (https://readwrite.com/indian-cyber-force-targeting-canadian-sites-and-other-cybercrimes/?utm_source=flipboard&utm_content=ReadWrite%2Fmagazine%2FAll+Stories). 26.09.2023).***

***

«В епоху, коли цифрова сфера перетворилася на театр стратегічного значення, 22 вересня 2023 року високопоставлені чиновники оборони США та Китаю зібралися в Пентагоні на важливий саміт з кібербезпеки.

Це гібридне зібрання, яке бездоганно інтегрувало особисте та віртуальне відвідування, стало гострим нагадуванням про постійний вплив глобальної пандемії COVID-19 на міжнародні взаємодії. Однак, окрім логістичних складнощів, ця дипломатична увертюра мала важливу мету: ознайомити китайську делегацію з нещодавно оприлюдненим Резюме кіберстратегії на 2023 рік від Міністерства оборони США.

Тлом, на якому відбулася ця історична зустріч, став Меморандум про взаєморозуміння між США та КНР щодо сповіщення про механізм заходів зміцнення довіри щодо основних військових дій, основоположна угода, підписана в

2014 році. Ця угода, про яку часто не помічають, але має глибоке значення, відіграє ключову роль у запобіганні непорозуміння та помилкові припущення між двома військовими силами. Його сфера охоплює широкий спектр предметів, охоплюючи повітряний простір і морську взаємодію, протоколи кризового зв'язку та сприяння військовим академічним обмінам. Асамблея Пентагону послужила відчутним доказом непохитної прихильності обох країн цьому механізму, сигналізуючи про спільне прагнення намітити нову структуру військової співпраці між Сполученими Штатами та Китаєм.

У центрі цього дипломатичного тет-а-тет всеосяжний документ лежав нещодавно оновлений Резюме кіберстратегії на 2023 рік, наданий Міністерством оборони США. Цей стратегічний проект є наріжним каменем для втілення цілей, сформульованих у Стратегії національної безпеки до 2022 року, Стратегії національної оборони до 2022 року та Національній стратегії кібербезпеки до 2023 року, у дієві плани. Його резонансне послання: Пентагон рішуче налаштований на зміцнення своїх кібермереж та інфраструктури, гарантуючи, що вони залишатимуться неприступними, доступними, надійними та стійкими перед лицем нових загроз.

Особливістю цієї зустрічі є те, що вона вийшла за рамки одностороннього брифінгу. Натомість він перетворився на предметний форум, де дискусії охоплювали широкий спектр питань, пов’язаних з кібернетичною інформацією. Розмови охоплювали обговорення встановлення норм і пом’якшення загроз у сфері кіберпростору до складніших діалогів щодо стратегій стримування, спільних ініціатив і реалізації заходів зміцнення довіри. Виник одностайний консенсус: взаємна повага та довіра мають бути основою цієї важливої сфери, де дії можуть відбиватися на глобальному цифровому ландшафті.

Важкість цієї зустрічі неможливо переоцінити. У світі, де кіберпростір став незламною опорою національної безпеки та глобальної стабільності, діалог між великими державами, такими як Сполучені Штати та Китай, має першочергове значення. Ці зустрічі виходять далеко за межі символічних жестів; вони є глибоко

прагматичними, спрямовані на відчутні ризики, що зростають, у тому числі ймовірність неправильного спілкування та ненавмисної ескалації в цифровій сфері.

Результати цього дипломатичного обміну слід сприймати як важливий крок до створення міцної основи довіри в кіберпросторі. Хоча грізні виклики залишаються, а різноманітні кіберстратегії тривають, залучення такого характеру є багатообіцяючим. Вони означають спільне визнання неодмінної потреби в системі правил і норм у кіберпросторі, що віддзеркалює структури управління, які регулюють традиційну військову діяльність.

Міжнародне співтовариство має прислухатися до цієї важливої події. Це є гострим нагадуванням про те, що співпраця та дипломатія мають відігравати ключову роль у подоланні складних викликів цифрової епохи, які постійно розвиваються. Просуваючись вперед, Сполучені Штати та Китай у співпраці з іншими країнами повинні підтримувати ці конструктивні діалоги, постійно розширювати спільну мову та досліджувати нові шляхи співпраці в експансивній сфері кіберпростору. Ця зустріч символізує важливий крок до безпечнішого та надійнішого цифрового кордону, де довіра та співпраця мають першочергове значення для захисту взаємопов'язаного світу, у якому ми рухаємося. Перед обличчям кіберландшафту, що динамічно розвивається, де загрози змінюються, а технології прогресують, уроки, отримані в результаті цієї дипломатичної спроби, знайдуть резонанс у всьому світі, підкреслюючи незмінну роль дипломатії в забезпеченні того, щоб цифровий домен залишався простором, де мир і стабільність перемагають конфлікти і розбрат». ***(Noureen Akhtar. Bridging The Digital Chasm: A Deep Dive Into US-China Cybersecurity Talks – OpEd // Eurasia Review (https://www.eurasiareview.com/25092023-bridging-the-digital-chasm-a-deep-dive-into-us-china-cybersecurity-talks-oped/?utm_source=flipboard&utm_content=EurasiaReview%2Fmagazine%2FEurasia+Review). 25.09.2023).***

***

«Цього тижня ізраїльська компанія Cyber 2.0 збирається впровадити своє рішення кібербезпеки в міжнародному аеропорту Цинциннаті/Північний Кентуккі (CVG).

У світі, де швидкий технологічний прогрес значно покращив авіацію, вони також запровадили нові кіберзагрози, які можуть поставити під загрозу глобальні авіаперевезення. Це актуальне питання стало головним пріоритетом як для країн, авіакомпаній, постачальників технологій, так і для широкої громадськості.

Зараз бортові системи значною мірою покладаються на передову технологічну інфраструктуру, що робить двигуни, навігаційні системи, протоколи безпеки та комунікації вразливими цілями для кібератак. Порушення таких систем могло призвести до втрати контролю над літаком у польоті.

Крім того, порушення кібербезпеки можуть порушити роботу різних аспектів авіації, зокрема обслуговування пасажирів, і потенційно скомпрометувати особисту інформацію пасажирів. Інфраструктура аеропортових компаній також є потенційними цілями для кібератак, здатних вплинути на розгортання та обслуговування критичних авіаційних технологій.

Ефективне реагування на кіберзагрози в авіаційному секторі вимагає широкого співробітництва між країнами, авіакомпаніями, технологічними компаніями та дослідницькими установами. Ця співпраця необхідна для забезпечення безпечних і безперебійних авіаперельотів.

Провівши масштабні дослідження та розробки, Cyber 2.0, провідна компанія з кібербезпеки, оприлюднила новаторську концепцію, яка включає відображення всіх ризиків кібербезпеки в аеропортах по всьому світу. Крім того, система аналізує аномальні дії, що відбуваються в цифровій інфраструктурі аеропортів. Ця інноваційна система не тільки визначає потенційні ризики, але й запобігає кібератакам на ці інфраструктури в реальному часі.

«З моменту, коли ми представили можливості нашої системи персоналу аеропорту в Кентуккі та продемонстрували унікальну морську систему кібербезпеки, розроблену відповідно до потреб порту Ашдод, ми почали працювати

над розробкою спеціального рішення для аеропортів у всьому світі», — сказав Шенір Розенфельд., генеральний директор Cyber 2.0. «Ми вважаємо, що потенціал у цій галузі величезний, і ми працюємо над тим, щоб позиціонувати Cyber 2.0 як найкраще рішення для запобігання кібератакам в аеропортах і морських портах по всьому світу».

Cyber 2.0 нещодавно був обраний Bird Foundation для співпраці з аеропортом CVG у Кентуккі щодо впровадження їхнього рішення кібербезпеки в усіх системах аеропорту. 18-місячний проект має на меті надати це передове рішення для аеропортів у всьому світі після завершення.

Оскільки авіаційна галузь продовжує розвиватися, партнерство між Cyber 2.0, CVG і Bird Foundation знаменує собою значний крок у напрямку забезпечення кібербезпеки систем аеропортів у всьому світі, створюючи прецедент важливості глобальної співпраці в протидії новим кіберзагрозам у секторах критичної інфраструктури». ***(Israeli company to implement cybersecurity system at Kentucky airport // Jpost Inc. (https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-757532?utm_source=flipboard&utm_content=Kobifeller%2Fmagazine%2FIsrael+startup+nation+). 04.09.2023).***

***

«Компанії, що надають послуги критичної інфраструктури на Тайвані, у майбутньому повинні будуть призначити керівника відділу кібербезпеки, а аудиторські повноваження уряду будуть розширені після перегляду законодавства про кібербезпеку.

В інтерв'ю, опублікованому в понеділок (4 вересня), заступник міністра цифрових питань Нін Є (葉寧) сказав, що заплановані зміни до Закону про управління кібербезпекою вимагатимуть від «спеціальних неурядових установ» призначити керівника служби кібербезпеки. «Спеціальні неурядові установи» визначаються як ті, які забезпечують критичну інфраструктуру, належать уряду або фінансуються державою.

Йех сказав, що приклади компаній, які будуть зобов'язані виконувати функції нагляду за кібербезпекою, включають Chunghwa Telecom, Far EastTone, корпорацію міжнародного аеропорту Таоюань та інші. Іншим прикладом є державний постачальник електроенергії Taipower, а також фінансовані державою організації, такі як Науково-дослідний інститут промислових технологій, більш відомий як ITRI.

Ревізії також розширять сферу цих перевірок, а органи місцевого самоврядування отримають повноваження їх проводити, сказав він. Міністерство співпрацює з місцевими органами влади для проведення перевірок установ на рівні міст або районів, сказав Є.

Єх також сказав, що зміни розширять поліцейські повноваження та дозволять розширити міжміністерську та міжвідомчу співпрацю. На практиці це дозволить урядовим установам розгортати ресурси з різних міністерств там, де вони найбільше потрібні, сказав він.

Поправки будуть подані до законодавчого органу для розгляду після його наступного засідання, сказав Йе, яке, як очікується, відбудеться не раніше 15 вересня.

Йех додав, що міністерство опублікує вказівки щодо забезпечення того, як обробка даних служить суспільному благу та підвищує конфіденційність даних. Очікується, що обидва набори інструкцій будуть опубліковані в середині вересня, сказав він». ***(Jono Thomson. Taiwan toughens cyber security regulations for infrastructure providers // Taiwan News (https://www.taiwannews.com.tw/en/news/4990283). 05.09.2023).***

***

«Нові, більш жорсткі правила кібербезпеки для літаків з електронним підтримкою вражають авіакомпанії по всьому світу, і такі перевізники, як Southwest Airlines, тепер стикаються з «величезним завданням, але ми сприймаємо його серйозно», - зазначає представник авіакомпанії.

Проблеми підтримки кібербезпеки постійно зростають, оскільки цифрова революція продовжує розвиватися. За даними Infosecurity Magazine, корпорація середнього розміру підприємства зараз використовує майже 80 продуктів кібербезпеки. Авіакомпанії повинні особливо піклуватися про кіберзахист, оскільки на кону життя, а також гроші. Урядова агенція Eurocontrol повідомила про збільшення кількості кібератак на авіакомпанії у 2020 році на 61%.

Нові літаки з електронною підтримкою мають набагато більше цифрових можливостей. Застарілі літаки використовували архітектуру для передачі даних через дроти, яка дозволяла лише передавачам надсилати дані до приймачів, а не навпаки. Літаки нового покоління, такі як Boeing 737 MAX, 787 і Airbus A350, використовують мережу передачі даних Ethernet для критично важливих додатків, що дозволяє пристроям обмінюватися даними один з одним.

Нова технологія видаляє дроти, зменшує вагу та збільшує можливості, але вона також відкриває кіберуразливості. Це важливо, тому що сьогодні багато модифікацій кабіни є в основному оновленням програмного забезпечення, а не заміною обладнання.

У США авіакомпанії, які здійснюють польоти на нових літаках Boeing, керуються декількома нормативними документами, зокрема консультативним циркуляром FAA 119; Керівництво оператора з безпеки авіаційної мережі (ANSOG) компанії Boeing, яке було переглянуто у 2021 році; і, за посиланням, RTCA DO-355A, Керівництво з інформаційної безпеки для підтримання льотної придатності, видане у 2020 році.

За словами Джона Шрамма, колишнього пілота Delta Air Lines та інженера-електрика, який зараз є керуючим партнером консалтингової компанії Seatec, підсумком цього є те, що перевізники тепер повинні відповідати значно жорсткішим вимогам кібербезпеки та мати на це обмежений час.

Шрамм порівнює широту і складність нових правил із системою управління безпекою. Вони стосуються всіх аспектів роботи авіакомпанії: програмне забезпечення та компоненти, точки доступу до мережі, наземне допоміжне обладнання та його інформаційні системи, цифрові сертифікати, аналітика файлів

журналу, управління інцидентами безпеки, оцінка організаційних ризиків, ролі персоналу, обов'язки та навчання.

Особливо жорсткою новою вимогою є проведення оцінки організаційних ризиків (ORA). Існує два типи ORAs: один виконується згідно з керівництвом Національного інституту стандартів 800-30, а інший – згідно з ARINC 811. Шрамм каже, що FAA віддає перевагу першому підходу.

У будь-якому випадку Шрамм каже, що авіакомпанії важко виконати ORA, оскільки в ньому задіяно так багато відділів, зокрема технічне обслуговування та IT, які зазвичай не співпрацюють один з одним.

Ще одна жорстка нова вимога — цифровий підпис для нових частин або програмного забезпечення. «Це вимагає від технічної групи впровадження цілої інфраструктури відкритих ключів, що знову ж таки є великим підйомом і не входить у їхні типові навички», — зазначає Шрамм.

FAA дає перевізникам близько трьох років на виконання нових вимог, приділяючи особливу увагу скорішому виконанню ORA, каже Шрамм.

Зі свого величезного флоту MAX, що входить в дію, Southwest Airlines зараз у процесі виконання нових вимог. Зазначаючи, що нові вимоги містилися в редакції ANSOG компанії Boeing наприкінці 2021 року, представник Southwest каже, що перевізник працює над виконанням цих нових вимог до орієнтовної дати завершення в січні 2025 року. Він співпрацює з Airlines for America та іншими галузями. партнерів для вирішення технічних проблем, пов'язаних із відповідністю.

Речник підкреслює, що Southwest вже повністю відповідає старим вимогам кібербезпеки, які були встановлені переглядом Boeing ANSOG у 2019 році.

Інші перевізники, з якими зв'язалися, відмовилися повідомити про статус своєї відповідності, а FAA також відмовилося підсумувати, як перевізники працюють. Шрамм вважає, що кілька авіакомпаній, можливо, надто довго чекають, щоб почати роботу зі своїми ORA.

За словами Чейза Річардсона, провідного директора з питань кібербезпеки та конфіденційності даних у консалтинговій компанії Bridewell, Агентство авіаційної безпеки Європейського Союзу (EASA) було певним чином більш агресивним щодо

кібербезпеки, ніж FAA. Наприклад, європейський регулятор наполягає на тому, щоб стандарти кібербезпеки були встановлені на початку сертифікації нового літака, тоді як FAA чекає до середини процесу сертифікації, щоб узгодити ці стандарти з OEM.

EASA називає свої вимоги щодо кібербезпеки для операторів системою управління інформаційною безпекою, а не програмою безпеки мережі літака, як FAA, але правила схожі.

Організаційні ризики розглядаються відповідно до Part-IS, який був опублікований у лютому 2023 року. Представник EASA каже, що Part-IS стане обов'язковим до лютого 2026 року, і «авіакомпаніям рекомендується передбачити дотримання таких вимог».

Крім авіаційних регуляторів, з'являються нові кібервимоги. Річардсон зазначає, що в березні Управління транспортної безпеки США випустило нові правила кібербезпеки для аеропортів і операторів літаків, включаючи правила передачі даних між аеропортами та авіакомпаніями. Сподіваємося, ризики авіакомпаній тут уже розглядаються відповідно до кіберправил, встановлених FAA та EASA». ***(Henry Canaday. Airlines Face Tougher Cybersecurity Requirements // Informa Markets (https://aviationweek.com/mro/safety-ops-regulation/airlines-face-tougher-cybersecurity-requirements). 11.09.2023).***

***

«У травні 2022 року Департамент бізнесу, енергетики та промислової стратегії опублікував другу стратегію цивільної ядерної кібербезпеки. Він базується на розробках, зроблених у секторі з моменту публікації початкової стратегії в 2017 році, яка зосереджена на забезпеченні того, щоб цивільний ядерний сектор міг захищатися від нових кіберзагроз, відновлюватися від них і бути стійким до них. Це вимагає захисту застарілих об'єктів, нових будівельних проектів і цивільних ядерних ланцюгів постачання від кібератак, які можуть поставити під загрозу конфіденційну ядерну інформацію, перервати постачання електроенергії,

пошкодити об’єкти, затримати небезпеку та зменшити ризик, а також негативно вплинути на працівників, громадськість або навколишнє середовище.

Стратегія 2017 року визначила ролі, обов’язки, зобов’язання та очікування для Уряду Її Величності, Цивільних ядерних обов’язків Великобританії (відповідальних осіб на ядерних об’єктах, які підлягають регулюванню безпеки), цивільного ядерного ланцюга постачання та регуляторів, включаючи Управління ядерного регулювання (ONR) і Інформаційний уповноважений. Стратегія до 2022 року, розроблена спільно з британськими цивільними ядерними організаціями, ONR і Національним центром кібербезпеки, продовжує міжгалузеве партнерство, і на початку 2023 року ONR провело серію брифінгів правління в цивільному ядерному секторі Великобританії, включаючи лабораторії, виробництво палива. генерація та виведення з експлуатації.

Стратегія визначає, як сектор досягне чотирьох ключових цілей до 2026 року:

- Належне визначення пріоритетів кібербезпеки як частини цілісного підходу до управління ризиками, що базується на загальному розумінні ризиків і регулюванні, орієнтованому на результат
- Проактивні дії для пом’якшення кіберризиків перед обличчям загроз, що розвиваються, викликів у спадщину та впровадження нових технологій
- Підвищення стійкості шляхом підготовки та спільного реагування на кіберінциденти, мінімізації впливу та часу відновлення
- Співпрацюйте, щоб підвищити кіберзрілість, розвинути кібернавички та просувати позитивну культуру безпеки

Ця стаття, заснована на матеріалах, створених для підтримки виконавчих брифінгів ONR, висвітлює відповідну передову практику, пов’язуючи її з вимогами ядерного сектору, і має широке застосування для керівництва в інших організаціях.

вступ

Кібербезпека стала всеосяжним терміном із різними визначеннями та передбачуваними значеннями. Про це зазначає проект Cyber Security Body of Knowledge (CyBOK), що фінансується Національною програмою кібербезпеки Великобританії. У вступі до CyBOK робиться висновок, що стисле та широке

визначення залишається невловимим у цій новій галузі знань, що розвивається. Ймовірно, це буде проблемою для правлінь, де загальне розуміння є важливим. Однак використання визнаних інфраструктур кібербезпеки може допомогти в спілкуванні та управлінні кіберризиками.

Команда CyBOK підкреслює майже виключну увагу до інформації та пов'язаних із нею технічних заходів кібербезпеки, часто оминаючи ключові сфери людської поведінки та наслідки порушень через втрату інформації, безпеку або порушення операцій. Вони також розглядають мережеві системи керування, де обов'язковим є запобігання небажаним фізичним діям.

«Кіберпростір» зараз використовується для опису операційного середовища з віртуальним і реальним впливом. Ця тема була представлена ширшій аудиторії в Національній кіберстратегії Великобританії до 2022 року, починаючи з її початкового військового використання, описуючи унікальність кіберландшафту та його фізичний вплив:

«Кібердомен — це створене людиною середовище, яке фундаментально формується людською поведінкою. Це посилює таку поведінку на краще чи гірше, наслідки якої зазвичай також відчуваються у фізичному світі».

Зараз організації прагнуть до кіберстійкості, а не лише до захисту, за допомогою стратегій, які забезпечують довговічність і можливості, які вони можуть надати як стимул для бізнесу. Всесвітній економічний форум (ВЕФ) розрізняє кіберстійкість від кібербезпеки як такі, що мають більш стратегічну, довгострокову перспективу, керовану лідерами, які визнають важливість пом'якшення ризиків і проактивного управління ризиками. Лідери організацій, які визначають стратегію, несуть остаточну відповідальність і все частіше несуть відповідальність за кіберстійкість.

Кіберстійкість і стратегія

Кіберстійка організація поєднує в собі можливості кібербезпеки, безперервності бізнесу та стійкості підприємства. Він забезпечує безпеку всієї бізнес-екосистеми та застосовує гнучкі стратегії безпеки, щоб швидко реагувати на загрози, щоб мінімізувати шкоду та продовжувати працювати під час атаки. Як

наслідок, кіберстійка організація може безпечно впроваджувати інновації та операційні моделі по всьому ланцюжку створення вартості, зміцнюючи довіру та вселяючи впевненість.

Стратегія кібербезпеки визначає цілі щодо бажаного майбутнього стану безпеки організації та інтегрована з бізнес-стратегією. Це вимагає розуміння поточного стану, а стратегія встановлює курс на досягнення бажаного майбутнього стану протягом визначеного періоду.

Стратегія кіберстійкості вимагає:

Розуміння організаційного ризику

Діяльність із захисту персоналу та систем для запобігання та протидії кібератакам

Підготовка для забезпечення достатньої стійкості в разі кібератаки, щоб мінімізувати вплив і забезпечити можливість відновлення

Ядерна безпека не є підмножиною ядерної безпеки — вони взаємопов'язані, але інженерні дисципліни безпеки та безпеки є незалежними областями. Не можна припускати, що незрозумілі, спеціально розроблені системи або повітряні проміжки можуть запобігти атакам. Подібні проблеми спостерігаються у сфері безпеки на залізниці, інструкції з безпеки для інженерів і менеджерів опубліковано CPNI (нині Національне управління безпеки). Конвергенція була досягнута завдяки загальним технологіям, платформам і мережам, де безпечна робота складних систем вимагає відповідної безпеки. Ці дві дисципліни також можуть конфліктувати, створюючи нові функції, уразливості та небезпеки, які можуть вимагати додаткових пом'якшень, щоб зменшити ризик безпеки та безпеки під час надання критично важливих послуг.

Широко опубліковані інциденти в галузях промисловості продемонстрували закриті підходи, зосереджені на IT-безпеці та оминаючи, зокрема, операційні технології, які виявляють потенційно вразливі системи. Кодекс практики IET: Кібербезпека та безпека розглядає цю конвергенцію та необхідність інтеграції забезпечення безпеки та кібербезпеки. Публікація також розглядає, де можуть існувати суперечності між вимогами безпеки та безпеки, наприклад, створення

загроз безпеці, викликаних безпекою (наприклад, неможливість увійти в систему безпеки), і оцінка статичних ризиків безпеки, враховуючи при цьому швидко змінюване середовище безпеки в світлі динамічних загрози та нові слабкі місця.

Роль і значення стратегії кібербезпеки

Організації, які прагнуть до кібервідмовостійкості, вимагають від своїх старших зацікавлених сторін проактивного керування кіберризиками разом з іншими ризиками підприємства. Лідери встановлюють організаційні наміри та описують результати, які мають бути досягнуті в стратегії, яка документує рішення та використовується для контролю впровадження та прогресу, одночасно гарантуючи, що вона узгоджується з бізнес-стратегією організації.

Стратегія, орієнтована на стійкість, дає змогу організаціям скористатися перевагами цифровізації та технологічних змін, розробляючи підхід, який сприяє розвитку бізнесу та забезпечує джерело конкурентної переваги, зберігаючи цінність.

Узгодження стратегії кібербезпеки з пріоритетами бізнесу гарантує, що результати будуть пропорційними ризику, з яким стикається бізнес. Стратегія кількісно визначає схильність організації до кіберризику та толерантність, а також визначає загрози для організації. Використання визнаних кіберфреймворків сприяє застосуванню належної передової практики та дотриманню галузевих базових показників, і тому це також є нормативною вимогою для виконавців обов’язків, що має вирішальне значення для ефективної реалізації.

Принципи стратегії безпеки

Коли ми допомагаємо організаціям у впровадженні їхніх програм кіберстійкості, наш підхід завжди такий:

Орієнтований на бізнес: кіберстійкість має визначатися пріоритетами бізнесу та організації. Наше дослідження показало, що це була ключова відмінність кіберстійких організацій із значними фінансовими перевагами

У масштабах підприємства: кібернетична проблема є проблемою корпоративного рівня, до якої слід ставитися так само, як до інших організаційних ризиків. Це не лише питання IT, операційних технологій (OT) або технології. Це

робоче середовище з ризиком, так само як фізичне середовище працює з фізичними ризиками

Зосередженість на ризиках: ми повинні зосередитися не тільки на вимогах відповідності, але й на фактичному ризику, щоб бути кіберстійкими

Екстенсивний: впроваджені системи мають відповідати за вашу розширену екосистему, а не лише за безпосередній ланцюг поставок. Нещодавні події продемонстрували, що системні ризики випливають із складної природи цифрових систем і взаємозв'язку з іншими системами та організаціями. Інциденти Colonial Pipeline, Solarwinds і NotPetya ілюструють системні ризики

Гнучкість: ми прагнемо створювати організації з кібербезпеки, які можуть розвиватися та рости разом із бізнесом

Технологія підтримує: ми створюємо кіберстійку організацію, яка підтримує технології, а не просто повна технологій. Ваша стратегія має бути агностиком технологій, зосереджуючись на бажаних результатах, водночас забезпечуючи гнучкість, щоб йти в ногу з технологічними змінами

Загалом, стратегія кіберстійкості має узгоджуватися з бізнес-стратегією та її часовими рамками. До двох-трьох років – це принципово оперативне планування, яке не є стратегічним.

Управління та лідерство

Функція управління створює та підтримує організаційну структуру, використовуючи допоміжні процеси для забезпечення відповідності програми безпеки організаційним цілям і завданням. Наше дослідження показало, що сильніша взаємодія між методами кібербезпеки та бізнес-стратегією забезпечує кращі результати.

Правління та керівництво вищого рівня несуть остаточну відповідальність за кіберризики та стійкість вашої організації. Керівна команда повинна усвідомлювати свою роль і обов'язки, а також нести відповідальність за встановлення тону для виховання та підтримки організаційної культури безпеки, включаючи безпечне управління кіберризиками. Вкрай важливо, щоб усі співробітники розуміли свою відповідальність за безпеку та кіберстійкість.

Керівництво несе основну відповідальність за виконання законодавчих, нормативних та обов'язкових вимог, і тому недоліки в управлінні також можуть вплинути на особу — особливо там, де кіберризики OT можуть призвести до фізичної шкоди.

Підхід, що ґрунтується на результатах, як-от Принципи оцінки безпеки ONR і Структура оцінки кібербезпеки Національного центру кібербезпеки, покладає на правління обов'язок керувати ризиками та застосовувати відповідні судження для досягнення визначених результатів. Поєднання орієнтації на результат з управлінням ризиками та застосуванням визнаних інфраструктур кібербезпеки забезпечує більшу стійкість бізнесу та переваги, ніж просто гонитва за відповідністю; такі впровадження демонструють покращене розуміння ризиків та визначення сильних сторін і областей для вдосконалення, більш обґрунтовану толерантність до ризиків, чіткішу розстановку пріоритетів для відновлення безпеки та кращий розподіл ресурсів і налаштування бюджету безпеки.

Належне врядування має забезпечувати відповідальність за рішення, їх виконання та вимірювання прогресу за KPI, що дозволяє коригувати курс і надавати зворотній зв'язок старшим зацікавленим сторонам. Загальноорганізаційна структура управління та стратегія кібербезпеки підтримують забезпечення кіберстійкості та демонструють належну уважність і старанність.

Роль і значення стратегії кібербезпеки

Організації, які прагнуть до кібервідмовостійкості, вимагають від своїх старших зацікавлених сторін проактивного керування кіберризиками разом з іншими ризиками підприємства. Лідери встановлюють організаційні наміри та описують результати, які мають бути досягнуті в стратегії, яка документує рішення та використовується для контролю впровадження та прогресу, одночасно гарантуючи, що вона узгоджується з бізнес-стратегією організації.

Стратегія, орієнтована на стійкість, дає змогу організаціям скористатися перевагами цифровізації та технологічних змін, розробляючи підхід, який сприяє розвитку бізнесу та забезпечує джерело конкурентної переваги, зберігаючи цінність.

Узгодження стратегії кібербезпеки з пріоритетами бізнесу гарантує, що результати будуть пропорційними ризику, з яким стикається бізнес. Стратегія кількісно визначає схильність організації до кіберризику та толерантність, а також визначає загрози для організації. Використання визнаних кіберфреймворків сприяє застосуванню належної передової практики та дотриманню галузевих базових показників, і тому це також є нормативною вимогою для виконавців обов'язків, що має вирішальне значення для ефективної реалізації.

Принципи стратегії безпеки

Коли ми допомагаємо організаціям у впровадженні їхніх програм кіберстійкості, наш підхід завжди такий:

Орієнтований на бізнес: кіберстійкість має визначатися пріоритетами бізнесу та організації. Наше дослідження показало, що це була ключова відмінність кіберстійких організацій із значними фінансовими перевагами

У масштабах підприємства: кібернетична проблема є проблемою корпоративного рівня, до якої слід ставитися так само, як до інших організаційних ризиків. Це не лише питання IT, операційних технологій (OT) або технології. Це робоче середовище з ризиком, так само як фізичне середовище працює з фізичними ризиками

Зосередженість на ризиках: ми повинні зосередитися не тільки на вимогах відповідності, але й на фактичному ризику, щоб бути кіберстійкими

Екстенсивний: впроваджені системи мають відповідати за вашу розширену екосистему, а не лише за безпосередній ланцюг поставок. Нещодавні події продемонстрували, що системні ризики випливають із складної природи цифрових систем і взаємозв'язку з іншими системами та організаціями. Інциденти Colonial Pipeline, Solarwinds і NotPetya ілюструють системні ризики

Гнучкість: ми прагнемо створювати організації з кібербезпеки, які можуть розвиватися та рости разом із бізнесом

Технологія підтримує: ми створюємо кіберстійку організацію, яка підтримує технології, а не просто повна технологій. Ваша стратегія має бути агностиком

технологій, зосереджуючись на бажаних результатах, водночас забезпечуючи гнучкість, щоб йти в ногу з технологічними змінами

Загалом, стратегія кіберстійкості має узгоджуватися з бізнес-стратегією та її часовими рамками. До двох-трьох років – це принципово оперативне планування, яке не є стратегічним.

Управління та лідерство

Функція управління створює та підтримує організаційну структуру, використовуючи допоміжні процеси для забезпечення відповідності програми безпеки організаційним цілям і завданням. Наше дослідження показало, що сильніша взаємодія між методами кібербезпеки та бізнес-стратегією забезпечує кращі результати.

Правління та керівництво вищого рівня несуть остаточну відповідальність за кіберризики та стійкість вашої організації. Керівна команда повинна усвідомлювати свою роль і обов’язки, а також нести відповідальність за встановлення тону для виховання та підтримки організаційної культури безпеки, включаючи безпечне управління кіберризиками. Вкрай важливо, щоб усі співробітники розуміли свою відповідальність за безпеку та кіберстійкість. Керівництво несе основну відповідальність за виконання законодавчих, нормативних та обов’язкових вимог, і тому недоліки в управлінні також можуть вплинути на особу — особливо там, де кіберризики OT можуть призвести до фізичної шкоди.

Підхід, що ґрунтується на результатах, як-от Принципи оцінки безпеки ONR і Структура оцінки кібербезпеки Національного центру кібербезпеки, покладає на правління обов’язок керувати ризиками та застосовувати відповідні судження для досягнення визначених результатів. Поєднання орієнтації на результат з управлінням ризиками та застосуванням визнаних інфраструктур кібербезпеки забезпечує більшу стійкість бізнесу та переваги, ніж просто гонитва за відповідністю; такі впровадження демонструють покращене розуміння ризиків та визначення сильних сторін і областей для вдосконалення, більш обґрунтовану

толерантність до ризиків, чіткішу розстановку пріоритетів для відновлення безпеки та кращий розподіл ресурсів і налаштування бюджету безпеки.

Належне врядування має забезпечувати відповідальність за рішення, їх виконання та вимірювання прогресу за KPI, що дозволяє коригувати курс і надавати зворотній зв'язок старшим зацікавленим сторонам. Загальноорганізаційна структура управління та стратегія кібербезпеки підтримують забезпечення кіберстійкості та демонструють належну уважність і старанність.

Культура безпеки

Конвергенція збільшила потребу в управлінні кібербезпекою та розробці інформованого про безпеку підходу до безпеки, де міркування безпеки інтегровані в управління ризиками безпеки. Необхідно враховувати загрози безпеці, які впливають на безпеку, щоб забезпечити інженерний підхід, орієнтований на безпеку, який усуває загрози безпеці та вразливі місця протягом усього життєвого циклу.

Впровадження проактивної культури кібербезпеки та мислення має важливе значення для розвитку цифрового підприємства. Позитивна культура безпеки зменшить ризики безпеки там, де недостатньо лише технології. Людська помилка залишається основним джерелом порушень кібербезпеки через недостатню обізнаність і відповідну підготовку. Вище керівництво має визначити, продемонструвати та надихнути позитивну культуру безпеки та заохочувати співпрацю між дисциплінами.

Для створення проактивної культури кібербезпеки організації повинні зосередитися на таких сферах:

- Стратегічне узгодження керівників має вирішальне значення для побудови спільного володіння кібербезпекою в IT та OT та вирішення потенційно несумісних підходів до вирішення кіберризиків
- Підвищення кваліфікації спеціалістів «об'єднаної робочої групи» з кібербезпеки IT та OT, які мають відповідні навички для забезпечення та підтримки кібербезпеки в усій організації

- Встановлення заохочувальної та стримувальної політики для сприяння та впровадження кіберстійкої поведінки в усій організації
- Впровадження безперервних, інтерактивних і орієнтованих на людину програм підвищення обізнаності та навчання для підвищення пильності користувачів, включаючи нових учасників і третіх осіб
- Керуючись аналітикою даних, використовуйте прогнозні моделі на відміну від традиційних підходів для вимірювання змін у поведінці щодо вразливостей
- Лідери, які повинні бути прикладом і надихати свої команди демонструвати кіберстійку поведінку.

Необхідно встановити чіткі очікування щодо поведінки персоналу, погоджуючись на те, що інциденти виникатимуть, але персонал відчуватиме заохочення повідомляти про проблеми, щоб їх можна було швидко виправити без загрози звинувачень чи критики. Культура безпеки має бути основою повсякденного життя в організації, де погана кібербезпека просто неприйнятна, і для організацій важливо поставити собі такі запитання:

Чи існує відкритий підхід до оцінки безпеки без звинувачень?

Який рівень підготовки та обізнаності мають співробітники?

Як співробітники або внутрішня особа могли спричинити інцидент, навмисно чи випадково?

Чи дозволяє культура використовувати кіберстійкість як виправдання?

Чи існує підхід, орієнтований на безпеку для всього кіберсередовища?

Важливо, щоб обсяг стратегії охоплював усе кіберсередовище, включаючи інформаційні системи, системи управління, системи безпеки, системи безпеки, системи управління будівлями та Інтернет речей (датчики/приводи IoT). Інтегрований підхід повинен включати безпеку в обґрунтування безпеки для вирішення проблем безпеки, конвергенції технологій і вирішення потенційних суперечностей між безпекою та безпекою, які можуть виникнути. Це вимагає створення спільного розуміння між дисциплінами безпеки та безпеки, наголошуючи на важливості лідерства та позитивної культури безпеки. Команди

керівництва несуть юридичну відповідальність за управління ризиками безпеки та безпеки, а недоліки матимуть неминучі наслідки для відповідальних осіб». ***(Richard Piggin. Cyber Security Strategy for Executives in the UK Nuclear sector // BCS, The Chartered Institute for IT (https://www.bcs.org/articles-opinion-and-research/cyber-security-strategy-for-executives-in-the-uk-nuclear-sector/). 12.09.2023).***

***

«У 2021 році, в розпал епідемії програм-вимагачів, Colonial Pipeline зазнав історичної кібератаки, яка призвела до тижневого дефіциту газу. Цей інцидент підкреслив вразливість критичної інфраструктури до кібератак і став каталізатором відповіді уряду, включаючи виконавчі накази та директиви агентства.

З огляду на минуле тепер ми знаємо, що результати, засновані на ефективності, є більш ефективним підходом, ніж нормативні вимоги, і цей урок слід застосовувати в критичній інфраструктурі.

Відразу після атаки програм-вимагачів Darkside на Colonial Міністерство внутрішньої безпеки та Агентство транспортної безпеки видали директиву з кібербезпеки, яка вимагала від власників і операторів трубопроводів повідомляти про порушення в Агенцію з кібербезпеки та безпеки інфраструктури, створити координатора з кібербезпеки, доступного 24/7., переглянути свою поточну практику, виявити будь-які прогалини та подати план виправлення до TSA та CISA протягом 30 днів.

Пізніше DHS опублікував директиву, яка вимагала від власників і операторів трубопроводів застосовувати спеціальні методи пом’якшення для захисту IT- та OT-систем від програм-вимагачів, а також розробити та впровадити план відновлення кібербезпеки та перевірити дизайн архітектури кібербезпеки.

Ці початкові директиви широко критикувалися як за те, що вони були надто розпливчастими, так і за те, що вони були надто директивними. Наприклад, одне доручення вимагало виправлення вразливостей, що, безумовно, є ефективним підходом до пом’якшення атак, але також може бути виконано за допомогою

сегментації мережі та політики контролю доступу. Крім того, здавалося, що багато директив TSA спрямовані на захист IT-систем, наприклад, за допомогою використання антивірусного програмного забезпечення, яке не завжди ефективно в мережах OT.

Зосередженість на результатах

У 2022 році TSA повторно опублікував вимоги до кібербезпеки для власників і операторів трубопроводів, зосередивши увагу на результатах кібербезпеки на основі ефективності. До них належать сегментація мережі, контроль доступу, безперервний моніторинг і виявлення, а також зниження ризику експлуатації невиправлених систем.

Сегментація мережі може суттєво обмежити бічний рух атак, зокрема з IT-мереж на OT. Ефективний контроль доступу включає ретельне керування дозволами користувача, методами автентифікації та рівнями авторизації.

Постійний моніторинг забезпечує видимість у режимі реального часу аномальних дій, спроб несанкціонованого доступу та потенційних загроз. Стратегія керування виправленнями гарантує, що своєчасні оновлення компонентів програмного та апаратного забезпечення закривають уразливості, які інакше можна було б використати під час атаки.

Крім того, власники та оператори трубопроводів повинні були розробити та виконати схвалений TSA план впровадження кібербезпеки, розробити та підтримувати план реагування на інциденти кібербезпеки та створити програму оцінки кібербезпеки.

«Протягом цих двох років ми змінювалися, щоб, на наш погляд, стати ще ефективнішими в кібербезпеці разом з нашими партнерами в транспортному секторі», — визнав адміністратор TSA Девід Пекоске під час конференції Hack the Capitol у травні 2023 року.

Що буде далі?

Цього року TSA знову оновила та переглянула свої вимоги щодо кібербезпеки для власників і операторів трубопроводів. Це оновлення вимагає від власників і операторів трубопроводів подавати оновлений план оцінки

кібербезпеки до TSA для перевірки та затвердження, щорічно звітувати про результати попередніх оцінок і тестувати принаймні дві цілі Плану реагування на інциденти кібербезпеки.

«Попередні версії вимагали розробки процесів і планів впровадження кібербезпеки. Ця версія вимагає, щоб оператори перевірили та оцінили ці плани», — сказав Пекоске.

Один із найпереконливіших уроків, отриманих під час цього процесу, полягає в тому, що коли TSA перейшло від директивних мандатів до результатів, що ґрунтуються на результативності, деякі з його найгучніших критиків звернулися до деяких із його найрішучіших прихильників. Здається, TSA визнає ефективність свого переглянутого підходу, оскільки розглядає можливість поширення цих директив на всі сектори критичної інфраструктури.

Однак той факт, що переглянутий підхід TSA був добре сприйнятий власниками й операторами трубопроводів, не означає, що важку роботу виконано. З останньою вимогою щодо щорічного тестування та звітності здається ймовірним, що деякі сліпі плями або прогалини можуть бути висвітлені

Наприклад, реалізація безперервного моніторингу та виявлення в складних середовищах OT може бути досить складною та дорогою. Подібним чином, нинішній час часу кібербезпеки зміщується в бік управління ризиками та ризиками – виходячи за рамки управління вразливістю. Однак, враховуючи, наскільки TSA було готове переглянути свої директиви, здається ймовірним, що вони продовжуватимуть коригувати свій курс на основі тестування та звітності. Насправді нинішня адміністрація почала впроваджувати комбінацію правил і стимулів для постачальників критичної інфраструктури, зосереджуючись на суворих вимогах до звітності.

Стимули спрямовані на те, щоб спонукати власників критичної інфраструктури інвестувати в рішення кібербезпеки. Якщо справи й надалі підуть добре, схоже, що будь-який сектор критичної інфраструктури може виграти від реалізації плану кібербезпеки, орієнтованого на результати, засновані на ефективності». ***(Shawn Taylor. In the pipeline: The impact of TSA cybersecurity***

directives // Federal Times (https://www.federaltimes.com/opinions/2023/09/27/in-the-pipeline-the-impact-of-tsa-cybersecurity-directives/). 27.09.2023).

***

Кіберзахист закладів охорони здоров'я

«15 серпня 2023 року Спільна комісія опублікувала сповіщення Sentinel Event Alert під назвою «Збереження безпеки пацієнтів після кібератаки», у якому надано «поради щодо того, що організації можуть зробити, щоб підготуватися до надання безпечної медичної допомоги пацієнтам у разі кібератаки».

У повідомленні описано зростання кількості кібератак і зламів інформаційних систем у галузі охорони здоров'я та їх зростання за останні кілька років. Про деякі кібератаки, включно з атаками програм-вимагачів, було повідомлено Спільній комісії, яка зазначила, що «деякі з цих подій були пов'язані із заподіянням шкоди пацієнтам (наприклад, затримки в лікуванні)».

У попередженні зазначається, що «весь персонал, а не лише IT, повинен бути готовий» до кібератаки, щоб організація могла працювати під час кібернебезпечної ситуації. На додаток до реалізації планів безперервності операцій і планів аварійного відновлення, лікарні «повинні щорічно оцінювати свою програму управління надзвичайними ситуаціями». Дії, запропоновані Спільною комісією, включають:

- Надайте пріоритет лікарняним службам, які забезпечують працездатність і безпеку протягом тривалого простою.
- Сформуйте комісію з планування простоїв.
- Розробіть плани простоїв, процедури та ресурси.
- Призначити групи реагування.
- Навчіть керівників груп, команди та весь персонал тому, як діяти під час простоїв.

- Встановіть ситуаційну обізнаність за допомогою ефективного спілкування всієї організації з пацієнтами та родинами.
- Після атаки перегрупуйтеся, оцініть і внесіть необхідні покращення.

Багато пунктів, запропонованих Спільною комісією, можуть бути включені до Плану реагування на інциденти організації, але конкретно планування простою та відсутності доступу до систем під час надзвичайної ситуації не завжди включається. Планування простоїв і поворотів під час атаки має вирішальне значення для того, щоб мати можливість реагувати на надзвичайну ситуацію в кібернетичному просторі та продовжувати працювати та надавати допомогу пацієнтам. Перегляд існуючих планів і процедур для конкретного усунення часу простою та визначення пріоритетності операційних областей, які передбачають критичний догляд за пацієнтами, є необхідним, щоб запобігти затримкам у догляді за пацієнтами у разі кібератаки». ***(Linn Foster Freedman. Joint Commission Issues Alert on Patient Safety After a Cyber-Attack // Robinson+Cole (https://www.dataprivacyandsecurityinsider.com/2023/09/joint-commission-issues-alert-on-patient-safety-after-a-cyberattack/). 07.09.2023).***

***

«Команда дослідників з Індійського інституту менеджменту (IIM) Лакхнау розробила модель захисту систем охорони здоров'я в усьому світі від кіберзагроз. Їхня «Модель оцінки кіберризиків у сфері охорони здоров'я» оцінює та зменшує ризики кібератак, забезпечуючи тим самим безпеку даних пацієнтів і безперервність цифрових медичних послуг для закладів охорони здоров'я.

Зростаюча складність і чутливість даних в організаціях охорони здоров'я підвищили їх сприйнятливість до кібератак, особливо через те, що під час пандемії Covid-19 сектор охорони здоров'я все більше покладається на цифрові дані.

Цифрові медичні записи містять конфіденційну особисту інформацію, як-от державні ідентифікаційні номери (наприклад, Aadhaar), історії хвороби, фінанси та страхові дані, які кіберзлочинці можуть використовувати для крадіжки особистих даних і шахрайства. На жаль, багатьом організаціям охорони здоров'я в усьому

світі бракує засобів кібербезпеки, що робить їх легкою мішенню для кіберзлочинців.

Команда мала на меті вирішити цю проблему, досліджуючи слабкі місця в безпеці медичних даних, якими користуються хакери. Вони припустили, що кіберзагрози стають більш вірогідними, коли медичний персонал не навчений протидіяти таким тактикам, як фішинг, і коли технології управління IT і безпеки не впроваджуються ефективно.

«Наші моделі оцінки ризиків і кількісної оцінки допомогли нам згрупувати 1788 медичних фірм США за «тепловою матрицею», яка показує ймовірність кібератаки та її потенційну тяжкість. Це дає нам чітке уявлення про те, наскільки фірми готові боротися з кіберзагрозами. Ми також пропонуємо план подолання ризиків, який налаштовується відповідно до позиції фірми в матриці», – сказав у заяві професор Арунабха Мухопадхяй з IIM-L, який керував дослідженням.

Модель, яку можна поширити на індійський сектор охорони здоров'я, може допомогти керівникам інформаційних технологій (CIO) закладів охорони здоров'я визначити вразливість закладу охорони здоров'я до кібератак. Він використовує колективне моделювання ризиків для оцінки потенційної серйозності кібератак, що може допомогти лікарням передбачити наслідки, а також пропонує рекомендації щодо пом'якшення та запобігання цим кібератакам.

Рекомендації походять від теорії раціонального вибору та стандартів, викладених Національним інститутом стандартів і технологій (NIST). Вони включають пріоритетність заходів кібербезпеки, таких як брандмауери та антивірусні рішення. Модель також пропонує практичні засоби захисту від кібератак для медичних фірм у квадрантах високого ризику теплової матриці.

Це також включає в себе резервне копіювання даних, навчання персоналу антифішингу, залучення вищого керівництва, пропаганду законів про кібербезпеку та інвестиції в технології кібербезпеки, такі як виявлення кінцевих точок і реагування (EDR), розширене виявлення та реагування (XDR), брандмауер нового покоління (NGFW), антивірус, управління інцидентами та подіями безпеки (SIEM) і оркестрування безпеки, автоматизація та реагування (SOAR)». ***(IIM Lucknow's new***

model to mitigate cybersecurity risk in healthcare // Fusion Media Limited (https://in.investing.com/news/iim-lucknows-new-model-to-mitigate-cybersecurity-risk-in-healthcare-3829921). 29.09.2023).

***

Захист персональних даних та соціальні мережі

«У метавсесвіті, царстві, де реальність знаходить нове вираження та відкриваються чудові віртуальні пейзажі, ви ніколи не загубитесь, але ваші дані можуть бути.

Уявіть себе, як ви прогулюєтеся галасливим цифровим ринком в оточенні аватарів у новітньому цифровому вбранні. Поки ви насолоджуєтеся всіма видами та звуками, на темній стороні метавсесвіту прихована таємна підземна мережа. Тут хакери та торговці даними збилися разом, перешіптуючись про останні цифрові експлойти та кіберрозкрадання.

Але як хакери продають і торгують вашими даними в метавсесвіті?

Що таке Темна сторона Метавсесвіту, тобто Darkverse?

Якщо ви не впевнені, що таке темний всесвіт, уявіть собі дикий захід цифрового світу — темний всесвіт — це беззаконний ландшафт, де процвітають злі дії. Це тіньове царство містить кіберзлочинців, хакерів і зловмисників, які діють поза межами закону та етики, серйозно загрожуючи безпеці та стабільності метавсесвіту.

У темному всесвіті крадіжка особистих даних, шахрайство та витік даних — це звичайний процес, який полює на мимовільних користувачів, які використовують свій шанс на цій підступній території. Автоматизовані боти працюють безкоштовно, розсилаючи спам і обманюючи нічого не підозрюючих користувачів, у той час як складний штучний інтелект і технологія deepfake створюють оманливий вміст, мутять воду правди та довіри.

Щоб захистити метавсесвіт від цих небезпек, надзвичайно важливі заходи кібербезпеки та навчання користувачів.

Темна мережа та ринки даних у Метавсесвіті

Темна мережа — це підпільна онлайн-сфера, недоступна через традиційні пошукові системи, відома своєю анонімністю та часто пов'язана зі злочинною діяльністю, такою як продаж викрадених даних і незаконних товарів. Тим не менш, там все ще є пристойний вміст, тому варто ознайомитися з найкращими пошуковими системами темної мережі.

Темна мережа стала процвітаючим центром для торгівлі вкраденими даними. Від облікових даних для входу до даних кредитної картки та навіть цифрових ідентифікаційних даних, змішаний мішок незаконно отриманих доходів доступний для захоплення.

Навігація цим цифровим чорним ринком не для слабонервних, оскільки і покупці, і продавці використовують псевдоніми, зашифровані комунікації та операції з криптовалютою. Хакери продають свою здобич, а ті, хто хоче використовувати вкрадене, шукають собі шлях крізь лабіринт веб-сайтів і форумів.

Коротше кажучи, цей зловісний симбіоз між темною мережею та метавсесвітом створює серйозну загрозу кібербезпеці.

Які вкрадені дані продаються в Метавсесвіті?

Кіберзлочинці пристосувалися до цього ландшафту, продаючи всі типи вкрадених даних тим, хто запропонує найвищу ціну, тоді як ринки даних метавсесвіту так само жваві.

Першими в списку є особисті дані, які можуть включати ваше ім'я, адресу, номер телефону та багато іншого. Крадіжка особистих даних досить популярна в метавсесвіті, оскільки зловмисники можуть присвоїти вашу онлайн-персону заради прибутку чи з інших причин. Отже, перш ніж зайти, варто дізнатися про найпоширеніші злочини метавсесвіту.

Фінансові дані є ще одним популярним товаром. Дані кредитної картки, інформація про банківський рахунок і цифрові гаманці користуються великим попитом: кіберзлочинці можуть використовувати ці дані для несанкціонованих транзакцій, зливаючи рахунки жертв миттєво.

Облікові дані доступу є ще одним основним продуктом на чорному ринку. Якщо хакери заволодіють вашими іменами користувачів і паролями, вони проникнуть у ваше цифрове життя та спричинять хаос у ваших соціальних мережах, електронних листах чи більш важливих облікових записах.

А у віртуальних світах та іграх на основі блокчейну рідкісні скіни, потужну зброю та унікальні предмети колекціонування викрадають і продають за реальні прибутки.

Нарешті, приватні розмови, що містять конфіденційну інформацію, є золотою жилою для хакерів. Вони намагатимуться проникнути у ваші особисті повідомлення, збираючи компрометуючу інформацію, щоб використати проти вас або продати її найкращому покупцеві.

Як оцінюються дані на віртуальних ринках?

Дані – це дорогоцінний товар, і його вартість визначається кількома факторами...

Свіжість: чим свіжіші та релевантніші дані, тим вища ціна. Наприклад, дані про місцезнаходження в реальному часі від користувачів metaverse є дуже цінними для маркетологів, які орієнтуються на потенційних клієнтів у сфері.

Точність: високоякісні дані, перевірені та вільні від помилок, цінніші за неточні аналоги.

Кількість: оскільки більші набори даних можуть забезпечити глибше розуміння та всебічний аналіз, вони можуть отримати вищі ціни.

Унікальність: унікальні дані, які важко отримати, як-от ексклюзивна інформація про вподобання, поведінку чи тенденції користувачів, мають більшу цінність.

Попит і дефіцит: якщо є високий попит на певні типи даних, а їх не вистачає, їх цінність різко зростає. Навпаки, якщо певних даних багато, їх значення падає.

Потенціал прогнозування: не дивно, що дані, які можуть передбачити майбутні тенденції чи поведінку, дуже затребувані.

Згода користувача: цікаво, що дані, отримані за чіткої та інформованої згоди користувача, іноді вважаються більш цінними, ніж дані, зібрані сумнівними способами.

Як відбувається обмін даними та торгівля ними в Метавсесвіті?

Законні обміни даними також відбуваються в метавсесвіті, і вони зазвичай передбачають використання даних користувачів для кількох цілей, наприклад для покращення віртуального досвіду для досліджень. Наприклад, платформи соціальних медіа можуть збирати дані про ваші вподобання для коригування реклами чи інших умов віртуального світу.

З іншого боку, хакери та кіберзлочинці часто використовують уразливості безпеки, щоб викрасти особисту інформацію, яка потім продається на підпільних ринках даних. Покупці можуть використовувати отримані дані для крадіжки особистих даних, шахрайства або інших зловмисних дій.

Новою тенденцією є використання криптовалют (таких як Bitcoin, Ethereum і Tether) і незамінних токенів (NFT) для транзакцій даних у метавсесвіті. Вони додають рівень анонімності та безпеки, що робить їх привабливими для тих, хто займається операціями з сумнівними даними.

Ця нова межа незаконного обміну даними викликає багато занепокоєння серед експертів з кібербезпеки, які борються з моніторингом і регулюванням транзакцій для захисту користувачів та їхніх даних. З еволюцією метавсесвіту змінюватимуться й методи та механізми торгівлі даними, тому залишатися на крок попереду кіберзлочинців стає складним завданням.

Хто такі покупці та які їхні мотиви?

По-перше, кіберзлочинці шукають різні форми даних для зловісних цілей, таких як крадіжка особистих даних, шахрайські дії та корпоративне шпигунство.

Законний бізнес також відіграє значну роль в екосистемі даних метавсесвіту. Вони мотивовані шансами отримати цінну інформацію про поведінку споживачів, ринкові тенденції та стратегії конкурентів. Ці дані можуть дати їм шанс відшліфувати свої продукти, послуги та маркетингові стратегії.

Керуючись прагненням посилити онлайн-безпеку, дослідники даних, етичні хакери та дослідники безпеки досліджують ці ринки, щоб краще зрозуміти вразливості, покращити заходи та покращити загальний досвід метавсесвіту.

Тим часом, подібно до компаній, маркетологи та рекламодавці використовують дані метавсесвіту, щоб створювати персоналізовані та ефективніші рекламні кампанії. Уряди, основними рушійними силами яких є громадська безпека, можуть непомітно брати участь у торгівлі даними, щоб відстежувати й пом'якшувати потенційні загрози в метавсесвіті.

А деякі колекціонери мотивовані цікавістю або бажанням накопичувати цифрові артефакти й активно беруть участь у цих ринках даних.

Які реальні наслідки торгівлі вкраденими даними в Metaverse?

Наслідки торгівлі вкраденими даними в цьому цифровому ландшафті можуть виходити далеко за межі царства одиниць і нулів.

Якщо їхня особиста інформація потрапляє в руки зловмисників, це відкриває двері для крадіжки особистих даних, шахрайства та вимагання. Мимовільні жертви можуть виявити, що їхні банківські рахунки вичерпані, кредитні рейтинги різко впадуть, а їхнє приватне життя стане відкритим для громадськості.

Для бізнесу наслідки такі ж серйозні. Хакери, які торгують викраденими корпоративними даними, можуть призвести до серйозних фінансових втрат, шкоди репутації та юридичних проблем. Порушення даних може підірвати конкурентоспроможність компанії, підірвати довіру клієнтів і розбити бюджет.

Через взаємопов'язану природу метавсесвіту одне порушення даних може мати ефект доміно, вплинувши на кілька сфер життя людини чи організації.

Захист вашої інформації у віртуальних світах

Темний ринок даних метавсесвіту є яскравим нагадуванням про ландшафт кіберзагроз, що постійно розвивається. Коли ми крокуємо цим чарівним новим віртуальним світом, захист наших конфіденційних даних стає не просто пріоритетом, а необхідністю». ***(Sead Fadilpašić. How Do Hackers Sell and Trade Your Data in the Metaverse? // MUO (https://www.makeuseof.com/how-hackers-sell-trade-data-in-***

metaverse/?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 10.09.2023).

***

«Caesars Entertainment підтвердила в четвер, що хакер проник в її комп'ютерну систему та викрав дані клієнтів під час недавньої кібератаки.

Після розслідування, яке завершилося минулого тижня, компанія Caesars «визначила, що несанкціонований актор отримав копію, серед інших даних, нашої бази даних програми лояльності», — повідомила компанія в регулятивній заявці в четвер.

Це включало номери водійських прав та/або номери соціального страхування «для значної кількості членів бази даних», сказав Caesars.

У результаті компанія пропонує послуги кредитного моніторингу та захисту від крадіжки особистих даних усім учасникам своєї програми лояльності.

На сьогоднішній день компанія не підозрює, що будь-які паролі, PIN-коди, інформацію про банківський рахунок або платіжну картку були отримані хакером.

Проте він все ще з’ясовує ступінь витоку даних і чи була викрадена інша конфіденційна інформація.

Після того, як компанія помітила підозрілу активність, вона заявила, що «здійснила ряд заходів із стримування та відновлення, щоб посилити безпеку нашої мережі інформаційних технологій». вона також звернулася до фірм з кібербезпеки та повідомила правоохоронні органи та державні регулятори ігор. Згідно з заявою,

Повідомляється, що компанія також заплатила десятки мільйонів доларів, щоб не дати хакерам оприлюднити дані компанії, повідомили Bloomberg джерела, знайомі з цією справою.

У заяві Caesars Entertainment підтвердила, що вона понесла та може й надалі нести певні витрати, пов’язані з цією атакою.

«Ми вжили заходів, щоб переконатися, що вкрадені дані будуть видалені несанкціонованим учасником, хоча ми не можемо гарантувати цей результат», — заявили в компанії. «Ми стежимо за Інтернетом і не бачили жодних доказів того,

що ці дані надалі розповсюджувалися, публікувалися чи іншим чином зловживали».

Компанія також підтвердила, що цей інцидент не вплинув на її «операції, орієнтовані на клієнтів, включаючи наші фізичні властивості та наші онлайнові та мобільні ігрові програми, і вони тривають без збоїв»…». ***(Daniella Genovese. Caesars confirms hacker stole Social Security numbers, other data in cyberattack // FOX News Network, LLC. (https://www.foxbusiness.com/lifestyle/caesars-confirms-hacker-stole-social-security-numbers-other-data-cyberattack). 14.09.2023).***

***

«Щодня ви залишаєте цифрові сліди того, що ви робили, куди ходили, з ким спілкувалися, що купували, що збираєтеся купити та багато іншого. Ця маса даних слугує бібліотекою підказок для персоналізованої реклами, яку надсилає вам складна мережа – автоматизований ринок рекламодавців, видавців і рекламних брокерів, який працює блискавично.

Рекламні мережі створені для захисту вашої особи, але компанії та уряди можуть поєднувати цю інформацію з іншими даними, зокрема з даними про місцезнаходження телефону, щоб ідентифікувати вас і відстежувати ваші пересування та онлайн-активність. Ще більш агресивним є шпигунське програмне забезпечення – шкідливе програмне забезпечення, яке державний агент, приватний детектив або злочинець встановлює на чийсь телефон або комп’ютер без його відома чи згоди. Шпигунське програмне забезпечення дозволяє користувачеві переглядати вміст цільового пристрою, включаючи дзвінки, текстові повідомлення, електронну та голосову пошту. Деякі форми шпигунського програмного забезпечення можуть контролювати телефон, зокрема вмикати його мікрофон і камеру.

Тепер, згідно з розслідуванням ізраїльської газети Haaretz, ізраїльська технологічна компанія під назвою Insanet розробила засоби доставки шпигунського програмного забезпечення через онлайн-рекламні мережі, перетворюючи деякі

цільові оголошення на троянських коней. Згідно зі звітом, захисту від шпигунського ПЗ немає, і уряд Ізраїлю дав Insanet дозвіл на продаж цієї технології.

Прокрадається невидимим

Шпигунське програмне забезпечення Insanet, Sherlock, не перше шпигунське програмне забезпечення, яке можна встановити на телефон без необхідності змусити власника телефону натиснути шкідливе посилання або завантажити шкідливий файл. NSO Pegasus від для злому iPhone є одним із найбільш суперечливих шпигунських інструментів, які з'явилися за останні п'ять років. Наприклад,

Pegasus покладається на вразливості в iOS від Apple, операційній системі iPhone, щоб непомітно проникнути в телефон. Apple випустила оновлення безпеки для останньої вразливості 7 вересня 2023 року.

Коли ви бачите рекламу на веб-сторінці, за лаштунками рекламна мережа щойно автоматично проводить аукціон, щоб визначити, який рекламодавець отримав право представити вам свою рекламу. Ерік Цзен, CC BY-ND

Те, що відрізняє Шерлок від Insanet від Pegasus, так це використання рекламних мереж, а не вразливості телефонів. Користувач Sherlock створює рекламну кампанію, яка вузько зосереджується на демографічних показниках і місцеположенні цільової групи, і розміщує рекламу, завантажену шпигунським програмним забезпеченням, на біржі реклами. Після того, як реклама показується

на веб-сторінці, яку переглядає цільова особа, шпигунське програмне забезпечення таємно встановлюється на її телефон або комп'ютер.

Хоча ще занадто рано визначати повний обсяг можливостей і обмежень Шерлока, звіт Haaretz показує, що він може заразити комп'ютери на базі Windows і телефони Android, а також iPhone.

Шпигунське програмне забезпечення проти шкідливого ПЗ

Рекламні мережі роками використовувалися для розповсюдження зловмисного програмного забезпечення, ця практика називається шкідливою рекламою. У більшості випадків зловмисне програмне забезпечення націлене на комп'ютери, а не на телефони, є невибірковим і призначене для блокування даних користувача в рамках атаки програм-вимагачів або крадіжки паролів для доступу до облікових записів в Інтернеті чи організаційних мереж. Рекламні мережі постійно шукають шкідливу рекламу та швидко блокують її, якщо її виявляють.

З іншого боку, шпигунське програмне забезпечення, як правило, орієнтоване на телефони, націлене на конкретних людей або вузькі категорії людей і призначене для таємного отримання конфіденційної інформації та моніторингу чиєїсь діяльності. Щойно шпигунське програмне забезпечення проникає у вашу систему, воно може записувати натискання клавіш, робити знімки екрана та використовувати різні механізми відстеження, перш ніж передати ваші викрадені дані розробнику шпигунського програмного забезпечення.

Хоча його фактичні можливості все ще досліджуються, згідно з повідомленням Haaretz, нове шпигунське програмне забезпечення Sherlock принаймні здатне до проникнення, моніторингу, захоплення та передачі даних.

Хто використовує шпигунське програмне забезпечення

З 2011 по 2023 рік принаймні 74 уряди уклали контракти з комерційними компаніями на придбання шпигунського програмного забезпечення або цифрових криміналістичних технологій. Національні уряди можуть використовувати шпигунське програмне забезпечення для стеження та збору розвідувальних даних, а також для боротьби зі злочинністю та тероризмом. Правоохоронні органи також можуть використовувати шпигунське програмне забезпечення під час

розслідування, особливо у справах про кіберзлочинність, організовану злочинність або загрози національній безпеці.

Компанії можуть використовувати шпигунське програмне забезпечення для моніторингу комп'ютерної діяльності співробітників, нібито для захисту інтелектуальної власності, запобігання витоку даних або забезпечення дотримання політики компанії. Приватні детективи можуть використовувати шпигунське програмне забезпечення для збору інформації та доказів для клієнтів з правових чи особистих питань. Хакери та діячі організованої злочинності можуть використовувати шпигунське програмне забезпечення для викрадення інформації для використання в схемах шахрайства чи вимагання.

На додаток до відкриття того, що ізраїльські фірми з кібербезпеки розробили надійну технологію, яка використовує онлайн-рекламу для цивільного спостереження, головне занепокоєння полягає в тому, що передове шпигунське програмне забезпечення Insanet було законно дозволено ізраїльським урядом для продажу ширшій аудиторії. Це потенційно ставить під загрозу практично кожного.

Срібна підкладка в тому, що Шерлок, здається, дорогий у використанні. Згідно з внутрішнім документом компанії, цитованим у звіті Haaretz, одне зараження Sherlock обходиться клієнту компанії, яка використовує цю технологію, у значні 6,4 мільйона доларів США». ***(Claire Seungeun Lee. Spyware can infect your phone or computer via the ads you see online – report // The Conversation Media Group Ltd (https://theconversation.com/spyware-can-infect-your-phone-or-computer-via-the-ads-you-see-online-report-213685?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 22.09.2023).***

***

«Дослідники з кібербезпеки з Wiz виявили величезну розблоковану Microsoft Azure базу даних хмарного сховища, у якій зберігається конфіденційна інформація про сотні людей, включаючи закриті ключі та паролі.

База даних, як виявилося, належала дослідникам Microsoft, які працюють над штучним інтелектом (ШІ). Хороша новина полягає в тому, що база даних була заблокована до того, як будь-які хакери змогли до неї дістатися.

Як пояснили дослідники Wiz, вони досліджували випадковий доступ до даних, розміщених у хмарі, коли знайшли репозиторій Microsoft GitHub із відкритим вихідним кодом для моделей ШІ, які використовуватимуться для розпізнавання зображень. Моделі були розміщені на URL-адресі сховища Azure, але через очевидну людську помилку сховище також містило дані, до яких ніхто не повинен мати доступу.

Ці дані включають 38 терабайт інформації, включаючи резервні копії комп'ютерів двох співробітників Microsoft, паролі до служб Microsoft і понад 30 000 повідомлень чату Teams, якими обмінюються співробітники Microsoft. Обліковий запис зберігання не був доступний напряму, пояснили дослідники. Натомість команда Microsoft AI згенерувала маркер підпису спільного доступу (SAS), який надав забагато дозволів. За допомогою токенів SAS, пояснює TechCrunch, користувачі Azure можуть генерувати посилання для спільного використання для даних облікового запису Azure Storage.

Wiz повідомив Microsoft про свої висновки 22 червня, а через два дні маркер SAS було відкликано. Компанії знадобилося майже три тижні, щоб провести ретельне розслідування, після чого було зроблено висновок, що неавторизовані сторонні особи не отримали доступу до даних, повідомляє TechCrunch.

Щоб переконатися, що подібні речі більше не повторяться, Microsoft розширила секретну службу GitHub, яка відстежує всі зміни загальнодоступного коду з відкритим кодом для облікових даних та інших секретів, відкритих у відкритому тексті.

На жаль, незахищені бази даних є поширеним явищем. Раніше цього року відносно популярна програма голосового чату для Android OyeTalk зробила те саме. Він використовував платформу Google для розробки мобільних додатків Firebase, яка також пропонує хмарні бази даних. За словами дослідників із Cybernews, примірник OyeTalk Firebase не був захищений паролем, тобто його

вміст був доступний для всіх». ***(Sead Fadilpašić. Bad news - Microsoft employees leaked 38TB worth of private data, including Teams chats // Future US, Inc. (https://www.techradar.com/pro/security/microsoft-ai-researchers-leaked-38tb-worth-of-private-company-data?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 19.09.2023).***

***

«До кінця серпня 2023 року закон Каліфорнії про захист даних, Каліфорнійський закон про конфіденційність споживачів, або «CCPA», передбачав у майбутньому лише створення правил щодо автоматизованого прийняття рішень, зокрема профілювання, оцінки ризиків і перевірок кібербезпеки. Однак під час засідання правління, яке відбулося минулої п'ятниці, 8 вересня тис, Каліфорнійське агентство із захисту конфіденційності («CPPA» або «Агентство»), яке поділяє повноваження щодо виконання CCPA з Генеральним прокурором Каліфорнії, обговорило новий набір проектів нормативних актів («Regs»), які воно оприлюднило для обговорення в Агентстві наприкінці серпня. 2023. Хоча проект ще не є частиною офіційної нормотворчості, проект і обговорення навколо нього визначають напрямок майбутньої нормотворчості з цих тем. Ми називатимемо проект і відповідний коментар «дорожньою картою». Зокрема, Дорожня карта пропонує подавати до CPPA скорочені версії оцінок і аудитів, проведених підприємствами відповідно до їхніх зобов'язань CCPA, і встановлює детальні зобов'язання щодо таких оцінок і аудитів. Наслідком цього є те, що Агентству може стати очевидним, які компанії проводять чи не проводять оцінку чи аудит і, таким чином, дотримуються своїх зобов'язань CCPA. Це також може надати Агентству легкодоступний спосіб перегляду практик оцінки бізнесу, особливо щодо діяльності з обробки з високим ризиком. Крім того, Дорожня карта Агентства пропонує вимоги до оцінки, які не тільки включають, але й перевищують те, що вимагається в нормативних актах штату Колорадо, включаючи оцінку

ризику/шкоди будь-якого моніторингу персоналу чи студентів або моніторингу споживачів у громадських місцях...

Засідання ради CPPA

На засіданні правління 8 вересня Агентство обговорило свою Дорожню карту щодо кібербезпеки та оцінки ризиків, не починаючи офіційної нормотворчості. Агентство планує додатково переглянути Дорожню карту на основі дискусій і коментарів, отриманих під час зустрічі, і заявило, що воно має на меті оприлюднити запропоновані Регламенти поза процесом підкомітету до правління CPPA для подальшого обговорення на наступному засіданні правління, запланованому на грудень 8, 2023. Відповідно, Дорожня карта не стане нормативно-правовим актом, що має обов'язкову силу, не раніше, ніж у 1 кварталі 2024 року.

Під час зустрічі члени Правління Агентства оцінили плюси та мінуси різних положень, оцінивши переваги для споживачів від захисту конфіденційності, запропонованого Дорожньою картою, проти тягаря для компаній, які повинні дотримуватися.

Щодо аудитів кібербезпеки Рада CPPA обговорила кілька тем, зокрема:

Поріг, який визначатиме, коли компанії доведеться проводити аудит кібербезпеки. Рада агентств обговорювала, чи має ця межа відповідати пороговій сумі для компаній у CCPA, включаючи ще не визначену кількість споживачів, особиста інформація яких обробляється компанією. Інші обговорювані варіанти встановлюють порогове значення на рівні певного річного валового доходу підприємства або певної кількості працівників. Для цього поріг CCPA, кількість споживачів, особиста інформація яких оброблялася, і річний валовий дохід були найпопулярнішими варіантами. Агентство підкреслило, що ризик для безпеки є найважливішим фактором при визначенні того, чи повинен бізнес проводити аудит кібербезпеки, але визнало, що дорогі аудити кібербезпеки можуть бути обтяжливими, особливо для невеликих підприємств з меншими ресурсами.

Обсяг аудитів кібербезпеки. Рада агентства розглянула два варіанти обсягу аудиту кібербезпеки. Один із розглянутих варіантів передбачає, що аудит

кібербезпеки повинен оцінити та задокументувати ризики, які суттєво впливають або можуть суттєво вплинути на споживачів. Інший варіант передбачає, що перевірки кібербезпеки повинні захищати від певних перелічених негативних впливів на безпеку споживача, таких як економічна шкода та репутаційна шкода. Один із членів Правління Агентства запропонував об'єднати два варіанти, включивши ризики шкоди разом із пороговим значенням «суттєвого впливу». Під час обговорень Рада агентств також підкреслила, що для бізнесу важливо враховувати не лише ризики для себе під час проведення аудитів кібербезпеки, а й ризики для споживачів.

Запобіжні заходи, які підприємства повинні враховувати під час проведення аудитів кібербезпеки. Дорожня карта передбачає, що підприємства повинні документувати запобіжні заходи, які будуть запроваджені для мінімізації ризиків. Рада Агентства зазначила, що не всі запобіжні заходи можуть бути застосовані до кожного бізнесу, а перелічені запобіжні заходи є міркуваннями, а не чіткими мандатами.

Що стосується оцінки конфіденційності, рада CPPA обговорила:

Деталі, необхідні для оцінки. Правління агентства оцінило переваги та недоліки вимоги включення певних деталей до оцінювання, як-от перелік імен і посад усіх осіб у компанії, які готували, брали участь у оцінюванні чи переглядали його, описуючи кваліфікацію тих, хто брав участь, і визначення кількості годин, витрачених на проведення оцінювання. Правління агентства зазначило, що це може бути надто обтяжливим і може спричинити занепокоєння конфіденційності, пов'язане з зобов'язанням осіб у бізнесі ділитися такою інформацією. Деякі члени Правління CPPA запропонували змінити зобов'язання таким чином, щоб ці деталі реєструвалися всередині компанії без необхідності включати їх у форму оціночної документації, яка подається до CPPA.

Переваги в оцінці. Члени правління Агентства висловили зацікавленість в оцінках, включно з інформацією про те, чи отримує бізнес пряму фінансову вигоду від продажу або поширення особистої інформації, а не в ширшому дослідженні переваг обробки.

Час оновлення оцінок. Правління розглянуло питання про те, чи слід проводити оцінювання кожні три роки, чи вимагати від підприємств переглядати й оновлювати оцінки за необхідності, а також чи слід надавати їх Агентству у скороченій чи повній формі. Деякі члени правління зауважили, що вимога оновлення кожні три роки може бути непотрібною, але частіші оновлення можуть бути важливими для технології автоматизованого прийняття рішень («ADM»), враховуючи потенційні дискримінаційні результати. Члени Правління відзначили, що повна оцінка ризику, а не скорочена оцінка ризику, яка подається до Агентства за будь-яких обставин, може призвести до створення бази даних оцінок ризиків, яка буде дуже великою та важкою для керування.

Які дії з обробки вимагають оцінки ризику?

Потенційні правила Дорожньої карти зобов'яжуть компанії, на які поширюється дія CCPA, проводити оцінку, якщо обробка особистої інформації споживачів становить значний ризик для їх конфіденційності. Така обробка включає:

- продаж або передача особистої інформації;
- обробка конфіденційної особистої інформації;
- використання технології автоматизованого прийняття рішень для сприяння прийняттю рішення, яке призводить до надання або відмови у наданні фінансових чи кредитних послуг, житла, страхування, вступу до освіти чи можливості, кримінального правосуддя, можливостей працевлаштування чи укладання контрактів чи компенсації, послуг охорони здоров'я чи доступу до основних товарів, послуг або можливості;
- обробка особистої інформації споживачів про те, що бізнес фактично знає, що вони молодші 16 років;
- обробка особистої інформації споживачів, які є працівниками, незалежними підрядниками, претендентами на роботу або студентами, з використанням технологій для моніторингу працівників, незалежних підрядників, претендентів на роботу або студентів;

- обробка особистої інформації споживачів у загальнодоступних місцях з використанням споживачів технологій для моніторингу поведінки, місцезнаходження, переміщень або дій; і
- обробка особистої інформації споживачів для навчання штучного інтелекту («AI») або ADM технології.

Яку інформацію має містити оцінювання?

Оцінка згідно з Дорожньою картою має брати участь усіх осіб з організаційної структури підприємства, які відповідають за підготовку, участь у оцінюванні або її перегляд, а також може включати зовнішні сторони для виявлення, оцінки та пом'якшення ризиків (наприклад, ті, що є частиною команда із запобігання шахрайству, група продуктів або команда відповідності). Оцінки повинні включати короткий виклад обробки, інформацію про контекст і цілі обробки та особисту інформацію, яка підлягає обробці, а також ризики, переваги та вжиті заходи безпеки.

Для порівняння, штат Колорадо вимагає, щоб оцінки включали аналіз ризиків і переваг, включаючи обговорення запобіжних заходів, вжитих для компенсації ризиків. Положення штату Колорадо також містять список із 12 явних запитів, які необхідно обговорити, а також додаткові 12, які є обов'язковими, якщо компанія бере участь у профілюванні. Вимоги штату Колорадо до оцінювання наразі є найсуворішими, хоча нам ще належить побачити, що остаточно запропонує CPPA...

Що в Дорожній карті сказано про AI та ADM?

Щодо технології штучного інтелекту та ADM, у Дорожній карті ще не сформульовано тригер, коли штучний інтелект чи ADM вимагають оцінки. Однак Дорожня карта визначає штучний інтелект як «спроектовану або машинну систему, яка розроблена для роботи з різними рівнями автономності та яка може для явних або неявних цілей генерувати результати, такі як прогнози, рекомендації або рішення, які впливають на фізичні або віртуальні середовищ».

Дорожня карта також визначає ADM у широкому сенсі, як «будь-яку систему, програмне забезпечення або процес, включно з машинним навчанням, статистикою, іншими методами обробки даних або штучним інтелектом, які

обробляють особисту інформацію та використовують обчислення як частину або повністю. система для прийняття або виконання рішення або полегшення прийняття рішень людиною. Технологія автоматизованого прийняття рішень включає профілювання». Це визначення охоплює широкий спектр автоматизованих дій з прийняття рішень, вимагаючи від підприємств проведення оцінки ризиків перед використанням таких систем.

На додаток до проведення оцінок, якщо виконуються тригери, які ще не визначені, Дорожня карта передбачає наявність кількох інших зобов'язань, пов'язаних із ШІ та автоматизованим прийняттям рішень. Наприклад, у Дорожній карті пропонується, щоб під час надання технології штучного інтелекту іншим підприємствам бізнес мав надати всі факти, необхідні компаніям-одержувачам для проведення оцінки ризиків для компаній-одержувачів. Якщо це положення Дорожньої карти буде прийнято, воно стане в нагоді для процесу перевірки постачальників і під час розробки угод про захист даних («DPA»).

Чи є якісь зобов'язання щодо подання згідно з проектом Регламенту?

Оцінки, проведені відповідно до проекту потенційних нормативних актів Дорожньої карти, повинні бути надані CPPA або Генеральному прокурору Каліфорнії за запитом. Підприємства також повинні будуть щорічно подавати скорочені версії оцінки ризиків, включаючи сертифікат уповноваженого керівника про те, що підприємство відповідає вимогам цих проектів нормативних актів. Як зазначалося вище, деякі члени Правління виступають за подання повних звітів, принаймні в деяких випадках.

Чи вимагають інші державні закони про конфіденційність оцінки ризиків?

Згідно з іншими чинними законами штату США про конфіденційність, зокрема Законом Вірджинії про захист даних споживачів («VCDPA»), Законом штату Коннектикут № 22-15 («CTPA») і Законом Колорадо про конфіденційність («CPA»), практика конфіденційності даних необхідні оцінки для певних дій обробки з високим ризиком. Така діяльність включає продаж особистої інформації, обробку конфіденційної особистої інформації, участь у цільовій рекламі та профілювання, що загалом визначається як «будь-яка форма автоматизованої

обробки персональних даних для оцінки, аналізу або прогнозування особистих аспектів, пов'язаних з економічним становищем особи, її здоров'ям, особистими уподобання, інтереси, надійність, поведінка, місцезнаходження чи рухи». Профілювання не обов'язково стосується ШІ. Однак він може використовувати ШІ для аналізу даних і групування споживачів, наприклад, для створення релевантної реклами. У таких випадках і при використанні штучного інтелекту в цілому важливо провести оцінку ризиків перед використанням системи штучного інтелекту. Для отримання додаткової інформації про вимоги до оцінки ризиків див публікація в блозі.

Аудити кібербезпеки

На додаток до потенційних проектів нормативно-правових актів у Дорожній карті, пов'язаних з оцінкою ризиків, CPPA також окреслив дорожню карту нормотворення для нормативно-правових актів аудиту кібербезпеки. Початковий проект для обговорення, якщо врешті-решт буде прийнятий, вимагатиме від компаній проведення аудиту кібербезпеки, якщо обробка особистої інформації споживачів становить значний ризик для безпеки споживачів. Аудити кібербезпеки повинні проводитися за участю кваліфікованого, об'єктивного та незалежного аудитора. Аудит повинен:

- Оцінити, задокументувати та підсумувати кожен відповідний компонент програми кібербезпеки бізнесу;
- Конкретно визначте будь-які прогалини або недоліки в програмі кібербезпеки підприємства;
- Конкретно звернути увагу на статус будь-яких прогалин або недоліків, виявлених під час будь-якого попереднього аудиту кібербезпеки; і
- Конкретно вкажіть будь-які виправлення або поправки до будь-яких попередніх аудитів кібербезпеки.

Постачальники послуг і підрядники компанії повинні будуть співпрацювати з цією компанією в проведенні нею аудиту кібербезпеки. Підприємства матимуть 24 місяці з дати набрання чинності постановами для проведення першого аудиту кібербезпеки, а потім аудити повинні проводитися щорічно…» ***(Sasha Kiosse, Alan***

L. Friel, Niloufar Massachi. California's Potential Approach to Regulations on Risk Assessments and Cybersecurity Audits Could Be a Game Changer // Squire Patton Boggs (https://www.privacyworld.blog/2023/09/californias-potential-approach-to-regulations-on-risk-assessments-and-cybersecurity-audits-could-be-a-game-changer/#page=1). 12.09.2023).

***

«National Student Clearinghouse, некомерційна освітня організація, яка надає звіти, верифікацію та дослідницькі послуги, розкрила, що її було зламано та що дані з майже 900 університетів і коледжів були викрадені.

За даними NSC, компрометація сталася через уразливість в одному зі сторонніх програмних інструментів MOVEit Transfer. У повідомленні про порушення даних NSC стверджує, що 31 травня його поінформували про проблему Progress Software, виробники MOVEit, і, дізнавшись про це, розпочали розслідування та координували дії з правоохоронними органами. 20 червня некомерційна організація дізналася, що неавторизована сторона отримала певні файли з інструменту MOVEit.

Викрадена особиста інформація включала імена, дати народження, контактну інформацію, номери соціального страхування, студентські ідентифікаційні номери та деякі шкільні записи. У повідомленні про порушення зазначено, що викрадені дані різняться між особами.

Скільки саме студентів могло постраждати, не розголошується, NSC лише каже, що йдеться про 890 університетів і коледжів, яким він надає послуги. Було опубліковано список постраждалих університетів і коледжів, серед яких є Каліфорнійський державний університет, Гарвардський університет і Стенфордський університет. Потенційно кількість викрадених записів може становити сотні тисяч, якщо не значно більше.

MOVEit — це програмне забезпечення для керованої передачі файлів, призначене для забезпечення безпечної та сумісної передачі файлів конфіденційних даних усередині та між організаціями. Уразливість у програмному забезпеченні,

виявлена на початку цього року, офіційно позначена як CVE-2023-34362, дозволяє неавтентифікованому віддаленому зловмиснику надіслати спеціально створений SQL-ін'єкцію до вразливого екземпляра MOVEit Transfer.

Незважаючи на те, що NSC не назвала групу, яка стоїть за атакою, попередні атаки, пов'язані з уразливістю MOVEit, стосувалися банди програм-вимагачів Clop. Наразі Clop не містить компромісу NSC на своєму сайті витоків темної мережі, але це може змінитися.

Попередніми жертвами банди програм-вимагачів Clop через уразливість MOVEit є BBC, British Airways Plc і мережа аптек Boots UK Ltd., Міністерство енергетики США, Shell Plc, UnitedHealthcare Student Resources, Університет Джорджії, Університетська система Джорджії., Heidelberger Druckmaschinen AG і Landal Greenparks.

«Оскільки ще одна організація приєднується до довгого списку жертв MOVEit, висвітлюються вразливі місця та недоліки традиційних оборонних методів кібербезпеки, на які організації все ще покладаються», — сказав Даррен Вільямс, засновник і виконавчий директор компанії BlackFog Inc., яка займається запобіганням програм-вимагачів. SiliconANGLE. «Освітній сектор залишається одним із секторів, які найбільше підпадають під кібератаки, що підкреслює потребу шкіл інвестувати в новітні технології, які дозволяють їм йти в ногу з техніками, які швидко розвиваються, які зловмисники використовують проти них. Мине деякий час, перш ніж ми дізнаємося повний масштаб цього порушення, а тим часом список жертв експлойту MOVEit неминуче зростатиме».

Даррен Гуччіоне, співзасновник і генеральний директор компанії з керування паролями та секретами Keeper Security Inc., підкреслив ризик, який представляють уразливості нульового дня або невиправлені вразливості, зазначивши, що вони можуть призвести до крадіжки даних, компрометації системи або інших зловмисних дій.

«Оскільки кіберкоманди продовжують боротися з цією хвилею атак, ця новина має послужити тривожним сигналом для кожної організації про те, що цю серйозну вразливість нульового дня необхідно негайно усунути», — пояснив

Гуччіоне. «Усі організації повинні застосовувати проактивний підхід до регулярного оновлення програмного забезпечення та негайного виправлення вразливостей, які активно використовуються в дикій природі». ***(Duncan Riley. 890 universities and colleges affected in latest MOVEit attack // SiliconANGLE Media Inc. (https://siliconangle.com/2023/09/25/890-universities-colleges-affected-latest-moveit-attack/?utm_source=flipboard&utm_content=SiliconANGLE%2Fmagazine%2FSiliconANGLE). 25.09.2023).***

***

«OpenSea, один із найпопулярніших у світі ринків невзаємозамінних токенів (NFT), було зламано: конфіденційні дані користувачів викрадено.

Компанія підтвердила цю новину в електронному листі, надісланому постраждалим сторонам, повідомляючи користувачам, що в одного з її постачальників стався інцидент безпеки, «який міг розкрити інформацію про ваш ключ OpenSea API».

«Ми не очікуємо, що це матиме якийсь негайний вплив на вашу інтеграцію з нашою платформою», — йдеться далі в повідомленні компанії. «Однак ваш ключ може використовуватися зовнішніми сторонами, які використовуватимуть виділений ліміт швидкості».

Відсутні деталі

Щоб вирішити цю проблему, OpenSea попросила користувачів замінити існуючі ключі, термін дії яких закінчився 2 жовтня.

Інші подробиці інциденту не розголошуються, тому ми не знаємо, хто був виконавцем загрози та які їхні мотиви. Ми також не знаємо, скількох людей постраждало від злому та чи було отримано будь-яку іншу конфіденційну інформацію.

Це не перший випадок злому OpenSea. Насправді таких інцидентів було багато. Наприклад, у квітні 2022 року сотні NFT були викрадені з облікових записів користувачів OpenSea після серії успішних фішингових атак.

Список, складений компанією з безпеки блокчейнів PeckShield, свідчить про те, що було вкрадено понад 250 NFT, включаючи предмети з популярних колекцій, таких як Bored Ape Yacht Club. Незважаючи на те, що деякі з них були знайдені, аналіз гаманців показує, що вкрадені токени принесли зловмиснику приблизно 1,7 мільйона доларів США.

У липні того ж року компанія попередила своїх користувачів бути обережними щодо можливих фішингових атак після того, як в результаті витоку даних було виявлено адреси електронної пошти, прикріплені до облікових записів користувачів.

ОНОВЛЕННЯ 27 вересня. Відповідаючи на наш запит, речник OpenSea сказав, що зламано було третю сторону, а не саму компанію, але все ще не підтвердив, скільки людей могло постраждати.

«Один із наших сторонніх постачальників зіткнувся з інцидентом безпеки, який міг розкрити інформацію про ключі OpenSea API», — йдеться в заяві. «Ключі не надають доступу або можливості змінювати будь-яку інформацію користувача OpenSea. Скоріше вони надають доступ до нашого загальнодоступного API із підвищеними обмеженнями швидкості. Несанкціоноване використання ключа API може означати, що розробник не зможе насолоджуватися їхні повні обмеження швидкості. Ми повідомили розробників про те, щоб вони припинили підтримку та замінили їхні ключі API, щоб вони могли зберегти свої обмеження швидкості.» ***(Sead Fadilpašić. Third-party breach leaks OpenSea API key data // Future US, Inc. (https://www.techradar.com/pro/security/nft-marketplace-opensea-hacked-again-in-yet-another-blow?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 27.09.2023).***

***

«FraudGPT, новий генеративний інструмент штучного інтелекту на основі підписки для створення зловмисних кібератак, сигналізує про нову еру майстерності атак. Виявлена озброєного ШІ дослідницькою групою Netenrich у липні 2023 року в каналах Telegram темної мережі, вона має потенціал для масштабної демократизації. генеративного

Розроблений для автоматизації всього, починаючи від написання шкідливого коду та створення невиявлених зловмисних програм до написання переконливих фішингових електронних листів, FraudGPT дає передові методи атак у руки недосвідчених зловмисників.

Додатки та інструменти зі штучним інтелектом із застосуванням зброї є бестселерами темної мережі

Провідні постачальники засобів кібербезпеки, зокрема CrowdStrike, IBM Security, Ivanti, Palo Alto Networks і Zscaler, попередили, що зловмисники, включно зі спонсорованими державою підрозділами кібертерористів, почали використовувати генеративний штучний інтелект ще до випуску ChatGPT наприкінці листопада 2022 року.

VentureBeat нещодавно взяв інтерв'ю у Свена Крассера, головного наукового співробітника та старшого віце-президента CrowdStrike, про те, як зловмисники прискорюють спроби створити зброю для LLM та генеративного ШІ. Крассер зазначив, що кіберзлочинці використовують технологію LLM для фішингу та зловмисного програмного забезпечення, але «хоча це збільшує швидкість і обсяг атак, які може здійснити зловмисник, це суттєво не змінює якість атак»

Крассер каже, що застосування штучного інтелекту як озброєння ілюструє, чому «хмарна безпека, яка корелює сигнали з усього світу за допомогою ШІ, також є ефективним захистом від цих нових загроз. Коротко кажучи: Generative AI не піднімає планку вище, коли справа доходить до цих шкідливих методів, але він підвищує середній показник і полегшує менш досвідченим супротивникам бути більш ефективними».

Визначення FraudGPT і штучного інтелекту

FraudGPT, стартовий набір для кібератаків, використовує перевірені інструменти атаки, такі як спеціальні посібники з хакерства, пошук вразливостей і експлойти нульового дня. Жоден із інструментів у FraudGPT не вимагає передових технічних знань.

За 200 доларів США на місяць або 1700 доларів США на рік FraudGPT надає передплатникам базовий рівень майстерності, який інакше мав би створити початківець зловмисник. Можливості включають:

- Написання фішингових електронних листів і контенту соціальної інженерії
- Створення експлойтів, шкідливих програм і інструментів злому
- Виявлення вразливостей, скомпрометованих облікових даних і сайтів, які можна підключити
- Надання консультацій щодо методів злому та кіберзлочинності

FraudGPT сигналізує про початок нової, більш небезпечної та демократичної ери озброєних генеративних інструментів і програм ШІ. національно-державні штурмові команди та масштабні операції, такі як Департамент 121 елітного відділу кібервійни Головного розвідувального бюро північнокорейської армії. Поточна ітерація не відображає передового ремесла, яке створюють і використовують Але те, чого не вистачає FraudGPT і подібним, у глибині генерації ШІ, вони з лишком компенсують здатністю навчати наступне покоління зловмисників.

Завдяки моделі підписки за кілька місяців у FraudGPT може бути більше користувачів, ніж у найдосконаліших державних армій проти кібератак, у тому числі Департаменту 121, який, за даними New York Times, нараховує приблизно 6800 кібервоїнів — 1700 хакерів у семи різних підрозділах і 5100 співробітників технічної підтримки.

Хоча FraudGPT може не становити такої неминучої загрози, як більші, більш досвідчені групи національних держав, його доступність для зловмисників-початківців призведе до експоненціального збільшення кількості вторгнень і спроб

злому, починаючи з найм'якших цілей, таких як освіта, охорона здоров'я та виробництво.

Як розповів VentureBeat Джон Бамбенек, головний дослідник загроз Netenrich, FraudGPT, ймовірно, було створено на основі відкритим кодом моделей штучного інтелекту з і усунення етичних обмежень, які запобігають зловживанням. Хоча він, ймовірно, все ще знаходиться на ранній стадії розробки, Бамбенек попереджає, що його поява підкреслює необхідність постійних інновацій у захисті на основі ШІ для протидії ворожому використанню ШІ.

Озброєний генеративний штучний інтелект, що сприяє швидкому зростанню червоних команд

Враховуючи зростаючу кількість генеративних чат-ботів і магістерських програм на основі штучного інтелекту, з об'єднання в команду вправи мають важливе значення для розуміння слабких сторін цих технологій і встановлення огорож, щоб спробувати запобігти їх використанню для створення інструментів кібератак. Корпорація Майкрософт нещодавно представила посібник для клієнтів, які створюють програми за допомогою моделей Azure OpenAI, який надає основу для початку роботи з red-teaming.

Минулого тижня DEF CON організував першу публічну генеративну командну подію AI у партнерстві з AI Village, Humane Intelligence та SeedAI. Моделі, надані Anthropic, Cohere, Google, Hugging Face, Meta, Nvidia, OpenAI і Stability, були протестовані на платформі оцінювання, розробленій Scale AI. Румман Чоудхурі, співзасновник некомерційної організації Humane Intelligence та співорганізатор Generative Red Team Challenge, написав у нещодавній статті Washington Post про чат-ботів зі штучним інтелектом і LLM, що об'єднують команди, що «кожного разу, коли я це робив, я щось бачив». Я не очікував побачити, дізнався те, чого не знав».

Для чат-ботів червоної команди вкрай важливо випереджати ризики, щоб забезпечити етичний розвиток цих нових технологій, а не стати шахраями. «Професійні червоні команди навчені знаходити слабкі місця та використовувати лазівки в комп'ютерних системах. Але з чат-ботами штучного інтелекту та

генераторами зображень потенційна шкода суспільству виходить за межі недоліків безпеки», — сказав Чоудхурі.

П'ять способів FraudGPT передвіщає майбутнє збройного штучного інтелекту

Генеративні інструменти кібератак на основі штучного інтелекту спонукають постачальників кібербезпеки та підприємства, які вони обслуговують, набирати темп і залишатися конкурентоспроможними в гонці озброєнь. Оскільки FraudGPT збільшує кількість кібератак і прискорює їхній розвиток, один із впевнених результатів полягає в тому, що ідентифікаційні дані будуть ще більше в облозі.

Generative AI становить реальну загрозу безпеці на основі ідентифікації. Він уже довів свою ефективність у видаванні себе за керівників за допомогою глибоко підроблених технологій та організації атак соціальної інженерії для отримання облікових даних привілейованого доступу за допомогою претексту. Ось п’ять способів, якими FraudGPT пророкує майбутнє збройного штучного інтелекту:

1. Автоматизована соціальна інженерія та фішингові атаки

FraudGPT демонструє здатність генеративного штучного інтелекту підтримувати переконливі сценарії тексту, які можуть ввести жертв в оману, змусити їх скомпрометувати їхні особи, права доступу та їхні корпоративні мережі. Наприклад, зловмисники просять ChatGPT написати науково-фантастичні історії про те, як спрацювала успішна стратегія соціальної інженерії або фішингу, обманом змусивши LLM надати вказівки щодо атаки.

VentureBeat дізнався, що банди кіберзлочинців і національні держави регулярно надсилають запити ChatGPT та іншим LLM іноземними мовами, щоб модель не відхиляла контекст потенційного сценарію атаки так само ефективно, як це було б англійською мовою. У дарк-мережі є групи, присвячені швидкому розробці, які навчають зловмисників, як обходити огорожі в LLM для створення атак соціальної інженерії та допоміжних електронних листів.

Незважаючи на те, що виявити ці атаки складно, лідери кібербезпеки у сфері штучного інтелекту, машинного навчання та генеративного штучного інтелекту мають найкращі шанси зберегти своїх клієнтів на паритеті в гонці озброєнь. Серед

провідних постачальників, які володіють глибоким досвідом штучного інтелекту, машинного навчання та генеративного штучного інтелекту, є ArticWolf, Cisco, CrowdStrike, CyberArk, Cybereason, Ivanti, SentinelOne, Microsoft, McAfee, Palo Alto Networks, Sophos і VMWare Carbon Black.

2. Зловмисне програмне забезпечення та експлойти, створені ШІ

FraudGPT довів здатність генерувати шкідливі сценарії та код, адаптований до конкретної мережі жертви, кінцевих точок і ширшого IT-середовища. Зловмисники, які тільки починають, можуть швидко освоїти найновіші загрози, використовуючи генеративні системи на основі штучного інтелекту, такі як FraudGPT, щоб вивчати та розгортати сценарії атак. Ось чому організації повинні зосередитися на кібергігієні, включаючи захист кінцевих точок.

Зловмисне програмне забезпечення, створене штучним інтелектом, може уникнути давніх систем кібербезпеки, які не призначені для виявлення та припинення цієї загрози. На вторгнення без зловмисного програмного забезпечення припадає 71% усіх виявлень, проіндексованих CrowdStrike Threat Graph, що додатково відображає зростаючу витонченість зловмисників ще до широкого впровадження генеративного ШІ. Нещодавні повідомлення про нові продукти та послуги в галузі показують, яким пріоритетом є боротьба зі зловмисним програмним забезпеченням. Amazon Web Services, Bitdefender, Cisco, CrowdStrike, Google, IBM, Ivanti, Microsoft і Palo Alto Networks випустили вдосконалення платформи на основі штучного інтелекту для виявлення шаблонів атак зловмисних програм і, таким чином, зменшення помилкових спрацьовувань.

3. Автоматизоване виявлення ресурсів кіберзлочинності

Генеративний штучний інтелект скоротить час, необхідний для завершення ручного дослідження для пошуку нових вразливостей, пошуку та збору скомпрометованих облікових даних, вивчення нових інструментів злому та опанування навичок, необхідних для запуску складних кампаній кіберзлочинності. Зловмисники будь-якого рівня кваліфікації використовуватимуть його, щоб виявляти незахищені кінцеві точки, атакувати незахищені поверхні загроз і запускати кампанії атак на основі інформації, отриманої з простих підказок.

Разом з ідентифікаторами, кінцеві точки бачитимуть більше атак. Керівники CISO повідомляють VentureBeat, що самовідновлювані кінцеві точки — це ставки, особливо в змішаних IT-середовищах і середовищах операційних технологій (OT), які покладаються на датчики IoT. У нещодавній серії інтерв'ю CISO розповіли VentureBeat, що кінцеві точки самовідновлення також є основою їхніх стратегій консолідації та мають важливе значення для покращення кібервідмовостійкості. Серед провідних постачальників кінцевих точок із самовідновленням для корпоративних клієнтів є Absolute Software, Cisco, CrowdStrike, Cybereason, ESET, Ivanti, Malwarebytes, Microsoft Defender 365, Sophos і Trend Micro.

4. Ухилення від захисту за допомогою ШІ тільки починається, і ми ще нічого не бачили

Озброєний генеративний штучний інтелект все ще перебуває в зародковому стані, а FraudGPT — це його молоді кроки. З'являються більш досконалі — і смертоносні — інструменти. Вони використовуватимуть генеративний штучний інтелект, щоб уникнути виявлення кінцевих точок і систем реагування, а також створювати варіанти зловмисного програмного забезпечення, які можуть уникнути виявлення статичного підпису.

З п'яти факторів, які вказують на майбутнє збройного штучного інтелекту, здатність зловмисників використовувати генеративний штучний інтелект для випередження інновацій у постачальників кібербезпеки та підприємств є найбільш стійкою стратегічною загрозою. Ось чому інтерпретація поведінки, виявлення аномалій на основі даних телеметрії в реальному часі в усіх примірниках хмари та моніторинг кожної кінцевої точки є основними завданнями.

Постачальники засобів кібербезпеки повинні надавати пріоритет уніфікації кінцевих точок і ідентифікаторів для захисту поверхонь атак на кінцеві точки. Використання штучного інтелекту для захисту ідентичності та кінцевих точок має важливе значення. Багато CISO прагнуть поєднати стратегію, орієнтовану на правопорушення, з технологічною консолідацією, щоб отримати більш уніфіковане уявлення про всі загрози в реальному часі, одночасно роблячи стеки технологій більш ефективними. Дев'яносто шість відсотків CISO планують консолідувати свої

платформи безпеки, причому 63% кажуть, що розширене виявлення та реагування (XDR) є їхнім найкращим рішенням.

Провідні постачальники платформ XDR включають CrowdStrike, Microsoft, Palo Alto Networks, Tehtris і Trend Micro. Тим часом постачальники EDR прискорюють плани своїх продуктів, щоб випустити нові випуски XDR, щоб залишатися конкурентоспроможними на зростаючому ринку.

5. Складність виявлення та атрибуції

FraudGPT і майбутні генеративні додатки та інструменти штучного інтелекту, створені як зброя, будуть розроблені, щоб зменшити виявлення та атрибуцію до анонімності. Оскільки жорстке кодування не вимагається, командам безпеки буде важко віднести атаки, керовані штучним інтелектом, до певної групи загроз або кампанії на основі криміналістичних артефактів або доказів. Більша анонімність і менше виявлення призведуть до довшого часу перебування та дозволять зловмисникам виконувати «низькі та повільні» атаки, які є типовими для розширених атак постійної загрози (APT) на цільові цілі високої цінності. Генеративний штучний інтелект із застосуванням зброї згодом зробить це доступним для кожного зловмисника.

SecOps і команди безпеки, які їх підтримують, повинні розглянути, як вони можуть використовувати AI і ML для виявлення тонких індикаторів потоку атак, керованих генеративним AI, навіть якщо вміст виглядає законним. Провідні постачальники, які можуть допомогти захистити від цієї загрози, включають Blackberry Security (Cylance), CrowdStrike, Darktrace, Deep Instinct, Ivanti, SentinelOne, Sift і Vectra.

Ласкаво просимо до нової гонки озброєнь ШІ

FraudGPT сигналізує про початок нової ери озброєного генеративного ШІ, де основні інструменти кібератак доступні будь-якому зловмиснику з будь-яким рівнем досвіду та знань. З тисячами потенційних передплатників, у тому числі державами, найбільша загроза FraudGPT полягає в тому, як швидко він розширить глобальну базу зловмисників, які прагнуть потрапити на незахищені м’які цілі в освіті, охороні здоров’я, уряді та виробництві.

З огляду на те, що CISO просять робити більше з меншими витратами, а багато хто зосереджується на консолідації своїх технологічних стеків для підвищення ефективності та видимості, настав час подумати про те, як ця динаміка може сприяти підвищенню кіберстійкості. Настав час перейти в наступ із генеративним штучним інтелектом і йти в ногу в абсолютно новій, швидшій гонці озброєнь». ***(How FraudGPT presages the future of weaponized AI // VentureBeat (https://venturebeat.com/security/how-fraudgpt-presages-the-future-of-weaponized-ai/). 14.09.2023).***

***

«…кібербезпека — це укріплена стіна, яка стоїть між нашим цифровим життям і потенційними загрозами. Будь то секрети компанії, ваші особисті електронні листи чи критична інфраструктура, усе є потенційною мішенню для кібератак. Щоб захиститися від таких загроз, ми використовуємо низку інструментів, у тому числі системи виявлення та реагування на кінцеві точки («EDR»), такі як SentinelOne, засоби безпеки та управління подіями («SIEM»), такі як Splunk, і рішення для запобігання втраті даних («DLP»). як McAfee MVISION. У кожного своя роль, але як ці традиційні засоби захисту протистоять новому кордону кіберзагроз?

Новий рубіж: виявлення та реагування на загрози за допомогою ШІ

Ось де ШІ та машинне навчання змінюють правила гри. Традиційні антивірусні рішення мають фатальну ваду — вони покладаються на заздалегідь визначені «сигнатури» відомих вірусів. Це як мати охоронця, який розпізнає грабіжників лише за їхніми фотографіями. У світі, де кіберзагрози миттєво змінюють вигляд, покладатися виключно на застарілі методи — це рецепт катастрофи. Інструменти, керовані ШІ, не просто відстежують знайомі обличчя; вони ретельно перевіряють поведінку, відстежують аномалії та адаптуються в режимі реального часу до нових типів загроз.

Проактивне майбутнє: використання можливостей ШІ

Оскільки ми йдемо далі в ландшафт, де домінує ШІ, цілком логічно врівноважувати використання ШІ в кіберзлочинності кібербезпекою на основі ШІ. Автоматизовані системи можуть аналізувати колосальні обсяги даних, які неможливо просіяти людині. Це не тільки прискорює процес виявлення загроз, але й дозволяє експертам з кібербезпеки швидко розробляти ефективніші контрзаходи. З ШІ на чолі ми не просто реагуємо; ми активно зміцнюємо наші цифрові домени.

Збалансований погляд: двосічний меч ШІ в кібербезпеці

Однак дуже важливо визнати, що штучний інтелект не є панацеєю. Автоматизація заходів безпеки іноді може призвести до самовдоволення та ментальності «встановив і забув». Крім того, ці системи можуть помилково «навчатися» на скомпрометованій поведінці, надаючи хибні негативи та пропускаючи загрози. І не забуваймо: ШІ все ще не замінить людське мислення. Є глибоке розуміння та обізнаність про ситуацію, яку можуть принести лише люди, як-от команда центру безпеки (SOC).

Трансформаційна сила: тривалий вплив ШІ на кібербезпеку

Хоча ШІ не позбавлений перешкод, його внесок у кібербезпеку неоціненний. З розвитком технологій обсяг і складність кіберзагроз лише зростатимуть. AI пропонує динамічне рішення проблеми, яка постійно змінюється. Продовжуючи інтегрувати штучний інтелект у наші стратегії кібербезпеки та використовувати його можливості та обмеження, ми можемо будувати майбутнє, яке буде безпечнішим, ніж будь-коли». ***(Unlocking the Cyber Vault: The Dynamic Dance Between AI and Cybersecurity // Nexstar Media Inc. (https://www.snntv.com/story/49715939/unlocking-the-cyber-vault-the-dynamic-dance-between-ai-and-cybersecurity). 24.09.2023).***

***

«Тема дедалі більшої участі штучного інтелекту в нашому цифровому світі та пов’язані з цим можливості та виклики були головними темами обговорення на багатьох конференціях і подіях з безпеки останнім часом.

Немає жодних сумнівів, що людство стоїть на порозі ери експоненційного технологічного прогресу, і штучний інтелект лідирує в новому цифровому світі.

Ця технологічна тенденція має наслідки для кібербезпеки. Простіше кажучи, штучний інтелект діє як потужний каталізатор і засіб забезпечення кібербезпеки в нашій підключеній екосистемі.

Те, що підключено, має бути безпечним і стійким. Це охоплює майже всі галузі чи вертикалі світової економіки. Як штучний інтелект і кібербезпека поєднуються для досягнення цієї мети?

Обчислювальні системи, які використовують штучний інтелект (AI) і машинне навчання (ML), стають все більш важливими для кібероперацій і стали основною сферою досліджень кібербезпеки. Оператори служби безпеки повинні бути в курсі всього у вашій системі та мати можливість швидко виявляти аномалії, такі як зловмисне програмне забезпечення або неправильні конфігурації, щоб зупинити порушення в сучасному гіперз'єднаному цифровому світі. У цілісному розумінні технології штучного інтелекту можуть допомогти в захисті від програм-вимагачів, соціальної інженерії та зловмисного програмного забезпечення, яке стає все більш складним і руйнівним…

Як штучний інтелект може сприяти кібербезпеці:

Системи штучного інтелекту (ШІ) спрямовані на те, щоб перевершити людську швидкість і обмеження, імітуючи людські характеристики та обчислювальні здібності комп'ютера. Розставляючи пріоритети та діючи на основі даних, алгоритми ШІ можуть сприяти більш ефективному прийняттю рішень, особливо у великих мережах із великою кількістю користувачів і факторів. Пошук, класифікація та об'єднання даних є неймовірно корисними навичками для зниження ризиків кібербезпеки.

Кібербезпека може виграти від застосування штучного інтелекту та машинного навчання в сферах аналізу загроз і мережевого спостереження. Інтелектуальні алгоритми можна використовувати, щоб стежити за аномаліями в мережі, виявляти нові небезпеки без встановлених ознак і виявляти їх. Крім того, його можна використовувати для кореляції даних із силосів для оцінки мережевих

ризиків і вразливостей, а також для розуміння природи атак. Шляхом перехресної перевірки точності даних у численних розосереджених базах даних штучний інтелект і машинне навчання можуть допомогти в управлінні ідентифікацією.

Шляхом аналізу даних і файлів для виявлення незаконних з'єднань, небажаних спроб зв'язку, випадкового або зловмисного використання облікових даних, спроб входу грубою силою, аномальної передачі даних і викрадання даних ШІ може контролювати мережеву активність у режимі реального часу. Це дає змогу компаніям, які забезпечують кіберзахист, робити статистичні висновки та захищатися від аномалій до того, як вони будуть виявлені та виправлені.

Штучний інтелект і машинне навчання можуть допомогти створити автоматизовані та адаптовані мережеві програми. Сканування горизонту та моніторинг мережі, які можуть надавати звіти про відхилення та аномалії в реальному часі, стали можливими завдяки автоматизації. Пристрої Інтернету речей, хмара, центри обробки даних і робочі мережі можуть бути охоплені рішеннями пошуку загроз ШІ. Він автоматично оновлює діагностику кібербезпеки та криміналістичний аналіз, а також рівні мережі, корисного навантаження, кінцевої точки, брандмауера та антивірусного програмного забезпечення.

Поєднуючи процедури оркестровки, автоматизацію, керування інцидентами та співпрацю, візуалізацію та звітність в одному інтерфейсі, AI та ML також можуть допомогти продуктам автоматизації оркестровки безпеки та реагування (SOAR). Крім того, SOAR може надати працівникам центру безпеки (SoC) швидший і точніший підхід до керування величезними обсягами даних, створених системами кібербезпеки, а також допомогти у виявленні та вирішенні потенційних або активних атак.

У криміналістиці злому на запитання «що сталося» можна відповісти за допомогою описової аналітики, яку пропонують технології мережевого спостереження та виявлення загроз; питання «чому і як це сталося» можна вирішити за допомогою аналітики діагностики інцидентів із підтримкою ШІ. Щоб знайти відповіді на ці запити, програмне забезпечення та платформи на основі

штучного інтелекту (ШІ) можуть аналізувати історичні набори даних, щоб переглянути зміни та показники аномалій у мережевій активності.

Прогностична аналітика може надати інформацію про наслідки виявлення вразливості системи, якщо її виявить розслідування інциденту (на відміну від зловмисного використання). Наказову аналітику можна використовувати для реагування на подію на основі рекомендацій щодо локалізації та остаточного усунення її причин після того, як ці причини визначено. Ці пропозиції можна використати для багатьох різних цілей, наприклад, прийняти нову політику чи процедури, змінити тактику або прийняти цілеспрямовані заходи…

Хакери-злочинці використовують ШІ швидше, ніж більшість комерційних команд з кібербезпеки, і вони можуть використовувати його для власних цілей. Твердження «Вже є випадки, коли зловмисники та хакери використовують технології штучного інтелекту для посилення своїх атак і зловмисного програмного забезпечення» можна знайти в дослідницькій роботі Forrester «Використання штучного інтелекту для зла: посібник із того, як кіберзлочинці будуть використовувати зброю та використовувати штучний інтелект для атаки на ваш бізнес».

Го Сер Юн, експерт з IT та кібербезпеки, стверджує, що генеративний штучний інтелект може швидко створювати новий матеріал на основі таких вхідних даних, як текст, зображення та звук, використовуючи глибокі алгоритми машинного навчання нейронних мереж. Результати генеративних моделей AI, які включають текст, аудіо та відео, а також фотографії, дуже реалістичні, каже він. Зловмисник успішно використав мовні файли, згенеровані штучним інтелектом, щоб імітувати генерального директора, щоб незаконно отримати інформацію про банківський рахунок, оскільки результат був таким реалістичним.

Штучний інтелект (ШІ) може використовуватися державами та/або учасниками злочинних організацій для приховування зловмисного програмного забезпечення в програмах, які часто завантажуються. Після завантаження зловмисне програмне забезпечення активується через заданий проміжок часу одним або кількома елементами. Атаки, виконання яких потребує багато часу,

дають шанс зібрати дані користувача (функції керування ідентифікацією, процес автентифікації). Інтелектуальне зловмисне програмне забезпечення, яке вчиться як на успішних, так і на невдалих спробах, потенційно може отримувати допомогу зловмисного штучного інтелекту (Deep Exploit). Згодом інтелектуальне зловмисне програмне забезпечення може розмножуватися, виявляючи та користуючись слабкими місцями в системах і пристосовуючись до контрзаходів, запускаючи нові атаки. Шкідливий штучний інтелект також здатний запускати приховані атаки, адаптуючись до середовища безпеки організації шляхом обслуговування системи.

Цілком ймовірно, що одним із найскладніших завдань кібербезпеки буде не відставати від досвідчених супротивників, які бажають використовувати штучний інтелект (і квантові технології) для шкідливих або незаконних дій. Уже існує термінова необхідність усунути такі потенційні вразливості з боку цих учасників, особливо щодо критичної інфраструктури. Дослідження та розробки в області штучного інтелекту між державним і приватним секторами, а також державами-союзниками, необхідно прискорити, і вони мають важливе значення для вдосконалення передових можливостей і заповнення кіберпрогалин, зокрема щодо асиметричних технологічних загроз.

У найближчому майбутньому ШІ матиме руйнівний вплив на робочі моделі кібербезпеки. Підходи до управління ризиками та впровадження технологій доведеться постійно адаптувати зі швидкістю розумних алгоритмів. У найближчі роки боротьба з новими та дедалі складнішими загрозами буде мати важливе значення для підтримки безперервності бізнесу та кіберстійкості. Для майбутнього кібербезпеки необхідно глибоке розуміння потенційних застосувань, переваг і недоліків ШІ». ***(Chuck Brooks. A Primer On Artificial Intelligence And Cybersecurity // Forbes (https://www.forbes.com/sites/chuckbrooks/2023/09/26/a-primer-on-artificial-intelligence-and-cybersecurity/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA&sh=64b7ee7575d2). 26.09.2023).***

***

«Ви коли-небудь замислювалися, що відбувається в голові кіберзлочинця? Як вони планують і здійснюють напади на нічого не підозрюючих жертв? Які інструменти та методи вони використовують для проникнення в комп'ютери та мережі та викрадення даних?

Знання цих відповідей може допомогти вам виключити цільовий список хакерів. Кіберзлочинність — це серйозна та зростаюча загроза, яка вражає мільйони людей і компаній у всьому світі, не кажучи вже про те, що кіберзлочинці постійно знаходять нові способи атакувати нас.

Щоб ви знали, з чим ви стикаєтеся, дозвольте мені викласти чотири кроки, які часто виконує кіберзлочинець, плануючи кібератаку. Тоді ви станете сильнішими завдяки деяким важливим порадам щодо того, як захистити себе від того, щоб стати їхньою наступною мішенню.

Це 4 кроки, які кіберзлочинець завжди зробить, плануючи кібератаку.

1. Знайти свою ціль

Кіберзлочинець повинен знайти конкретну особу чи організацію для атаки, перш ніж він зможе зробити щось інше. Вони використовують для цього різні способи; однак зазвичай вони ціляться в тих, хто здається найлегшою та найвразливішою ціллю. Ось кілька способів, якими вони можуть націлитися на особу чи компанію.

Соціальні медіа: кіберзлочинці можуть використовувати соціальні медіа-платформи, такі як Facebook, Instagram, Twitter або Threads, щоб знайти особисту інформацію, таку як місцезнаходження, професія, хобі, інтереси тощо, яка може допомогти їм адаптувати свої атаки чи шахрайство.

Темна мережа: кіберзлочинці також можуть використовувати темну мережу, щоб купувати чи продавати викрадені дані, такі як номери кредитних карток, паролі, імена користувачів тощо, які можна використовувати для доступу до облікових записів в Інтернеті або крадіжки особистих даних.

Інформаційні брокери: кібершахраї використовують інформаційних брокерів, щоб отримати дані, зібрані з відкритих джерел, таких як записи про транспортні засоби, судові звіти та списки реєстрації виборців. Ця глибоко інтимна інформація може розкрити особисті дані, такі як ваше повне ім'я, адреса та номер телефону, які можуть бути використані для націлювання або видавання себе за вас.

Сканування мережі: кібершахраї використовують інструменти сканування мережі, щоб прочесувати Інтернет на наявність пристроїв або систем, які мають вразливість або слабкий захист. Вони використовують ці вразливості, щоб отримати доступ або розпочати атаки.

Цей перший крок є, мабуть, найважливішим у хакерській маніпуляційній грі, оскільки він створює або ламає хакерську гру. Розумієте, без мішені неможливо вчинити злочин.

2. Дослідження своєї мети

Знайшовши потенційну ціль, кіберзлочинець, швидше за все, проведе деякі дослідження, щоб зібрати якомога більше інформації, щоб викрасти ваші облікові дані. Для цього вони використовуватимуть різні інструменти та методи, як-от:

Інструменти розвідки: вони можуть розгорнути інструменти розвідки для сканування мережі цілі та виявлення її IP-адреси, відкритих портів, операційної системи, служб тощо. Це може допомогти їм виявити будь-які вразливості для подальшого використання.

Соціальна інженерія: це використовується, щоб обманом змусити ціль розкрити конфіденційну інформацію, таку як паролі, таємні запитання чи особисті дані. Вони роблять це, видаючи щось або когось, кому ціль довіряє, наприклад, друга, колегу або представника служби підтримки клієнтів зі знайомої організації. Ці інструменти включають фішингові електронні листи або телефонні дзвінки, щоб спонукати цільову особу перейти за шкідливими посиланнями чи вкладеннями чи завантажити небезпечне шкідливе програмне забезпечення.

Кейлоггери. Ця популярна підступна техніка використовується кіберзлочинцями, щоб таємно записувати натискання клавіш цільовою версією та перехоплювати облікові дані для входу, повідомлення та електронні листи. Вони

часто встановлюють клавіатурні шпигуни на цільовому пристрої, використовуючи зловмисне програмне забезпечення або фізичний доступ, щоб продовжувати шпигувати протягом тривалого періоду часу, викопуючи номери рахунків, кредитні картки та будь-які цінні дані.

Досліджуючи свою ціль, кіберзлочинець може краще зрозуміти її звички, уподобання та вразливі місця. Це може допомогти їм спланувати та здійснити більш ефективну та індивідуальну атаку.

3. Злом в мережу

Саме тоді хакер дійсно починає проявляти творчість. Найпоширеніший спосіб проникнення хакера в мережу – це фішинг.

Фішингові листи та веб-сайти

Це може бути фішинговий електронний лист із вкладеними шкідливими посиланнями або навіть фішинговий веб-сайт, створений так, щоб виглядати як законна компанія, щоб жертва потрапила на нього та передала свою інформацію.

Це одна з найпопулярніших атак зараз, коли хакери використовують інструменти фішингу як послуги, які фактично виконують всю брудну роботу за них. Даючи цим хакерам куленепробивний шаблон, який міг би обдурити будь-кого, вони просто повинні сидіти склавши руки і дозволити жертві потрапити на цей трюк.

Оцифрований волосяний фолікул людини

Серед інших хитрих інструментів, якими може скористатися хакер, є моторошний спосіб відображення оцифрованого волосяного фолікула людини на екрані телефону чи планшета жертви, щоб, коли вони намагалися його прибрати, зловмисне програмне забезпечення негайно завантажувалося.

Фальшиві оголошення

Хакери можуть використовувати підроблені оголошення та розміщувати їх у соціальних мережах, таких як Facebook, сподіваючись, що жертва попадеться на них. Замість того, щоб перейти до справжньої компанії, це веде нас з вами прямо в лапи злочинців. Можливості справді безмежні для хорошого хакера.

4. Взяття під контроль мережі

Це завершальний етап атаки хакерів і найвигідніший для них. Отримавши доступ до системи, вони якнайшвидше вилучають будь-яку цінну інформацію, яку можуть отримати, за допомогою інструментів після експлуатації, таких як AdFind і Cobalt Strike, які призначені для збору та передачі даних із скомпрометованих мереж. Вони або зникнуть із викраденими даними, або використають їх для вимагання грошей у своїх жертв, залежно від мети та мотиву нападу.

Що я можу зробити, щоб захиститися від цих хакерів?

На щастя, є запобіжні заходи, які ви можете вжити, щоб не стати наступною жертвою цих кіберзлочинців.

Інвестуйте в послуги з перевезення

Хакер не може легко використовувати вас як мішень, якщо він не може знайти вашу інформацію в Інтернеті. Сайти брокерів даних, керовані шахраями, отримують особисті дані, які хакери викрадають у вас, зокрема адреси електронної пошти, номери соціального страхування тощо. Вони роблять це для того, щоб продавати інформацію третім особам і отримувати прибуток.

Хоча жодна служба не обіцяє видалити всі ваші дані з Інтернету, підписка на хорошу службу видалення є найефективнішим способом постійного моніторингу та автоматизації процесу постійного видалення вашої інформації із сотень сайтів.

Ознайомтеся з моїми порадами та найкращими способами вилучення з Інтернету на сайті CyberGuy.com/Delete.

Майте хороше антивірусне програмне забезпечення

Установлення потужного антивірусного програмного забезпечення може допомогти захистити ваш телефон, планшет і комп’ютер від хакерів. Це також запобіжить вам натискати шкідливі посилання з метою встановлення зловмисного програмного забезпечення, дозволяючи хакерам отримати доступ до вашої особистої інформації.

Перегляньте мій експертний огляд найкращого антивірусного захисту для ваших пристроїв Windows, Mac, Android та iOS на сайті CyberGuy.com/LockUpYourTech.

Використовуйте захист від крадіжки особистих даних

Компанії, які займаються крадіжкою особистих даних, можуть контролювати особисту інформацію, як-от титул вашого будинку, номер соціального страхування, номер телефону та адресу електронної пошти, і повідомляти вас, коли вони продаються в темній мережі або використовуються для відкриття облікового запису на ваше ім'я. Вони також можуть допомогти вам заморозити ваші банківські рахунки та рахунки кредитних карток, щоб запобігти подальшому несанкціонованому використанню зловмисниками.

Переважна частина деяких компаній, що займаються крадіжкою особистих даних, полягає в тому, що вони часто включають страхування від крадіжки особистих даних на суму до 1 мільйона доларів США для покриття збитків і судових зборів, а також команду з розв'язання шахрайства в білих рукавичках, коли менеджер із справ із США допомагає вам відшкодувати будь-які збитки…» ***(Kurt Knutsson. The very first thing hackers do as criminals // FOX News Network, LLC. (https://www.foxnews.com/tech/first-thing-hackers-do-criminals?utm_source=flipboard&utm_content=FoxNews%2Fmagazine%2FLatest+News). 04.09.2023)***

***

«Кіберзлочинцям вдалося порушити роботу двох найсучасніших телескопів у світі, змусивши світову астрономічну спільноту занепокоїтися безпекою життєво важливої наукової інфраструктури.

Точна природа та походження цих кібератак залишаються загадкою, але обсерваторії були змушені тимчасово припинити дослідницьку діяльність.

Національна дослідницька лабораторія оптично-інфрачервоної астрономії Національного наукового фонду, відома як NOIRLab, виявила, що руйнівний інцидент з кібербезпекою 1 серпня змусив їх припинити роботу як на телескопі Gemini North на Гаваях, так і на телескопі Gemini South в Чилі. Менші телескопи на Серро Тололо в Чилі також стали жертвами хакерів.

У заяві, опублікованій 24 серпня, NOIRLab висловила свою прихильність швидкому вирішенню проблеми: «Наші співробітники співпрацюють з експертами

з кібербезпеки, щоб якнайшвидше відновити всі постраждалі телескопи та наш веб-сайт, і ми надихаємося прогресом, досягнутим на даний момент». Однак через розслідування, яке триває, лабораторія залишається обережною щодо розголошення деталей щодо природи та походження атак.

«Ми плануємо надати спільноті більше інформації, коли зможемо, відповідно до нашого зобов'язання щодо прозорості, а також нашої відданості безпеці нашої інфраструктури», – додається в заяві.

Ці кібератаки проти NOIRLab розгорнулися лише за кілька днів до того, як Національний центр контррозвідки та безпеки США (NCSC) попередив американські космічні компанії та дослідницькі організації про загрозу кібератак і шпигунства.

NCSC підкреслив, що іноземні шпигуни та хакери чітко усвідомлюють критичну роль комерційної космічної галузі в економіці та національній безпеці США. Вони визнають зростаючу залежність від космічних активів, розглядаючи американські космічні інновації та активи як потенційну загрозу та можливість придбати основні технології та досвід.

Як пише Space, це вже не перший випадок, коли астрономічні обсерваторії опиняються під прицілом кібератак. У жовтні 2022 року хакери перервали роботу великого міліметрового/субміліметрового масиву Атакама (ALMA) у Чилі, а NASA, головне космічне агентство Сполучених Штатів, протягом кількох років потерпало від кібератак.

У 2021 році NASA зіткнулося з далекосяжними наслідками всесвітнього злому SolarWinds, що стало головним тривожним дзвінком для керівництва агентства з питань кібербезпеки». ***(Alex Baker. Cyberattacks paralyze the world's two most advanced telescopes // DIYPhotography (https://www.diyphotography.net/cyberattacks-paralyze-the-worlds-two-most-advanced-telescopes/?utm_source=flipboard&utm_content=maryljohnso122n%2Fmagazine%2F6+Degrees+Goes+Under+The+Radar). 04.09.2023).***

***

«Коли справа доходить до кібербезпеки, це можуть бути найпростіші речі, які зачіпають бізнес, а не кричущі, великі речі, які, на вашу думку, є причиною витоку даних. Можливо, облікові дані доступу, які надаються через незахищені канали, або все ще підключене застаріле мережеве обладнання, яке ніхто не помітив, або навіть погано налаштована операційна система.

Прості проблеми можуть бути цокаючими бомбами уповільненої дії, які просто чекають, поки зловмисник помітить їх. Кіберзловмисники постійно оновлюють і вдосконалюють способи компрометації систем, і хоча підприємствам доводиться підвищувати рівень складного захисту, який вони мають, вони не можуть ігнорувати прості речі, які вони можуть зробити, щоб захистити себе.

Атака нульового дня

Відкриття в травні про те, що Barracuda, великий постачальник засобів безпеки з понад 200 000 бізнес-клієнтів, зазнав значної атаки нульового дня, є лише останнім прикладом цієї правди. Уразливість нульового дня багато в чому є золотим яйцем спільноти кіберзлочинців: термін, що описує недолік, про який постачальник програмного забезпечення не знає, який можна використовувати для доступу до систем і викрадання даних із відносно невеликим опором. У гіршому випадку (або, для зловмисника, найкращому випадку) такими вразливими місцями можна користуватися протягом місяців або навіть років, перш ніж проблему буде виявлено та усунено.

У цьому випадку виявлена вразливість нульового дня безпосередньо вплинула на продукт постачальника Email Security Gateway, викликавши запитання щодо ширшого профілю ризику організації, що повинно хвилювати клієнтів Barracuda. Підприємства не можуть і не повинні просто сидіти склавши руки і думати, що це певне, що колись вони стануть жертвами атаки нульового дня. Важливо бути готовим до перевіреної оборони та знати кожному свою роль і обов’язки. Готовність до реагування, стратегічний дизайн безпеки та підтримка співробітників відіграють важливу роль у зменшенні шкоди, яку може завдати атака нульового дня.

Ви ніколи не дізнаєтеся, коли станеться атака нульового дня. Це може бути о 21:00 у п’ятницю ввечері, коли всі старші люди будуть у літаку протягом наступних шести годин або посеред ночі – отже, потрібно знати, хто, що і коли робить. Команди організаційної безпеки повинні мати чітко визначені процеси та платформи, які визначають відповідальних осіб як контактні особи, які будуть дотримуватися методології для ізоляції уражених систем, проведення криміналістичного аналізу, щоб зрозуміти ступінь порушення та, зрештою, усунути вразливість, в ідеалі в реальних умовах. час.

Після початку атаки ви не можете втрачати дорогоцінний час, вирішуючи, хто де і коли повинен бути або якого партнера слід викликати першим. Сучасний, добре обладнаний відділ безпеки повинен бути стурбований поглибленням свого розуміння цілісного мережевого трафіку, а також посиленням конкретних потенційних місць уразливості. зонди на основі штучного інтелекту Аналітичні, розгорнуті на межі загальнодоступної мережі, можуть відстежувати та позначати потік трафіку для аналітиків і автоматизувати перші кроки щодо виявлення порушення, зрештою нейтралізуючи збитки швидше.

Робота, яку має виконати команда безпеки, буде легшою та швидшою, якщо масштаб порушення буде меншим – що зазвичай відбувається, коли компанія виконала всі стримування та противаги, згадані вище. Але коли йдеться про корпоративної електронної пошти компрометацію, це може включати додаткові рішення безпеки, які виявляють і блокують підозрілі електронні листи за допомогою протоколів автентифікації електронної пошти та більш спеціалізованих інструментів, які сканують загрози, як-от фішинг.

Охоронна поза

Компанії можуть подумати про ідентифікацію та захист імовірних точок входу, які можуть отримати зловмисники, коли вашу електронну пошту успішно зламано. Суворий внутрішній контроль за фінансовими операціями, наприклад, передбачатиме кілька рівнів внутрішнього схвалення, що значно ускладнить виконання переказів коштів без чийогось втручання.

Навчання користувачів також може бути вирішальним, коли справа доходить до виявлення того, що «просто не так». Це величезний ресурс, і важко переоцінити важливість викладацького складу для раннього виявлення проблем і якнайшвидшого передання їх команді безпеки.

Ризик уразливостей нульового дня нікуди не подінеться, і, фактично, у міру того, як цифровізація продовжується, а інфраструктура IT, Інтернету речей і OT стає все більш широкою, цілком імовірно, що в майбутньому вони будуть робити все більше заголовків. Але це не означає, що боротьба з кіберзагрозами програна; ні, регулярне оновлення систем може випередити загрози, що розвиваються.

Як я вже згадував, добре підтримана безпека, коли кожен знає свою роль і партнерів, готових реагувати, залишається одним із найкращих засобів захисту, навіть якщо мова йде про атаку нульового дня. Уразливість нульового дня, хоча вона потенційно може призвести до збитків і втрат, рідко є скелетним ключем для всієї IT-інфраструктури, і чим надійнішими є інші системи, тим складніше зловмисникам буде повністю використати свою перевагу.

Урок таких подій, як уразливість нульового дня Barracuda, полягає в тому, що ми всі можемо зробити більше, щоб шукати покращення та готуватися до неминучих атак і ймовірних порушень. З кібербезпекою ви ніколи не можете бути впевнені, що зможете відбити будь-які атаки, але ви можете зробити все можливе, щоб спробувати випередити тих, хто має намір завдати вам шкоди». ***(Mike Loginov. Why a response to zero-day attacks starts right now // Future US, Inc. (https://www.techradar.com/pro/why-a-response-to-zero-day-attacks-starts-right-now?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 06.09.2023).***

***

«Згідно з дослідженням, опублікованим у понеділок, майже половина великих підприємств Швейцарії стали жертвами кібератак, часто з катастрофічними наслідками.

У звіті SwissVR Monitor виявлено, що 45% швейцарських компаній із 250 і більше співробітниками стверджують, що зазнали принаймні однієї кібератаки.

Дослідження, проведене з середини травня до початку липня консалтинговою компанією Deloitte та Люцернським університетом прикладних наук, показує, що чим менша компанія, тим менша ймовірність, що вона стане об'єктом серйозної атаки.

Опитування, яке охопило 400 членів правління великих компаній, а також малих і середніх підприємств (МСП), показало, що лише 18% компаній з менш ніж 50 співробітниками зазнали значного кіберзлому.

«Зв'язок між розміром компанії та частотою атак очевидний: великі компанії мають більший глобальний вплив і ширшу потенційну цільову сферу для кіберзлочинців», – зазначили автори звіту.

Вони також припустили, що менші компанії можуть бути менш схильні інформувати свою раду директорів про будь-які потенційні напади.

Флоріан Шутц, який відповідає за реалізацію національної стратегії кіберзахисту Швейцарії, підтвердив, що «всі компанії піддаються ризику, незалежно від їх розміру чи сектора».

Цитований у звіті він сказав, що «багатьом малим і середнім підприємствам не вистачає фінансових і людських ресурсів для вжиття ефективних заходів кібербезпеки, тому їх досвід та інфраструктура обмежені або взагалі відсутні».

Кібератаки шкодять як клієнтам, так і компаніям

Загалом опитування показало, що компанії недостатньо готові до боротьби з кіберзагрозами.

Лише 57% опитаних членів правління сказали, що їхнє правління розробило чітку стратегію кібербезпеки, і лише близько третини отримували регулярні звіти від керівництва про основні ризики.

Це хвилюватиме багатьох керівників підприємств, оскільки кібератаки можуть мати серйозні наслідки для діяльності компанії. Згідно з дослідженням, 42% постраждалих компаній зазнали певної форми перерви у своєму бізнесі.

Витоки даних і збої в ланцюгах поставок або виробництва також є поширеними, іноді з наслідками, які стосуються не лише компанії.

Близько 11% респондентів сказали, що клієнти були об'єктами наступних атак.

«Крім втрати доходу через перебої в бізнесі, також можуть виникнути високі витрати на відновлення, наприклад, на відновлення даних», — зазначили автори опитування». ***(Half of Switzerland's large companies have been the victim of a cyber attack // euronews (https://www.euronews.com/2023/09/04/half-of-switzerlands-large-companies-have-been-the-victim-of-a-cyber-attack?utm_source=flipboard&utm_content=euronews%2Fmagazine%2FNews). 04.09.2023).***

***

«…З удосконаленням технологій зростають і кібератаки. У своєму останньому Глобальному дослідженні економічної злочинності та шахрайства PwC виявила, що серед 19 категорій економічних злочинів кіберзлочинність виділялася як не лише найпоширеніша, але й найбільш руйнівна економічна злочинність у США та в усьому світі.

Атаки програм-вимагачів, спроби фішингу та атаки соціальної інженерії є одними з найпоширеніших тактик, які використовують кіберзлочинці для проникнення в мережі фінансових установ. Постійна складність кібератак робить важливою для вашої організації бути на крок попереду в заходах кібербезпеки.

Хоча фінансова вигода залишається основною метою, почали з'являтися спонсоровані державою атаки, спрямовані на підрив фінансових систем у політичних цілях. Популярність криптовалют також призвела до сплеску атак програм-вимагачів, під час яких хакери вимагають цифрові валюти як викуп за розблокування зашифрованих даних.

Вживайте профілактичних заходів

Однією з найбільших вразливостей фінансових установ є належне керування їх програмним забезпеченням. Багато кібератак використовують уразливе або

«невиправлене» програмне забезпечення для входу в мережі та доступу до конфіденційних даних. Впровадження ретельного обслуговування програмного забезпечення, також відомого як плановий процес керування виправленнями, має важливе значення для пошуку й усунення потенційних уразливостей.

Співробітники, підрядники або постачальники, які мають доступ до мережі вашої організації, можуть ненавмисно або зловмисно порушити безпеку. У наші дні Zoom і Teams, а також спільного доступу до екрана, працівник може випадково поділитися інформацією про клієнта, просто показавши не той екран.

Навчання співробітників належним методам безпеки шляхом регулярного навчання з кібербезпеки та впровадження засобів контролю доступу, таких як додаткові паролі та контроль фізичного доступу (де це можливо), може допомогти зменшити ці ризики. В Ulrich ми регулярно проводимо тренінги з кібербезпеки, а також перевіряємо знання наших співробітників, надсилаючи фальшивий спам і фішингові листи.

Паролі та PIN-коди виявилися вразливими до кіберризиків, таких як фішинг і атаки грубої сили. Біометрія відбитків пальців і розпізнавання обличчя є більш безпечною та зручною альтернативою. Багатофакторна автентифікація додає додатковий рівень захисту, поєднуючи два або більше елементів автентифікації, наприклад пароль і відбиток пальця. MFA може бути таким же простим, як завантаження програми, яка надсилає push-сповіщення користувачеві, коли виконується спроба входу. Банківські установи впроваджують біометрію та MFA, щоб обмежити небезпеку незаконного доступу та крадіжки особистих даних, гарантуючи безпеку банківських рахунків та особистої інформації своїх клієнтів.

Зростаюча кількість кіберзагроз привернула увагу регуляторних органів у всьому світі. Останніми роками було створено більше вказівок і стандартів, які гарантують, що фінансові установи визнають кібербезпеку серйозною проблемою та впроваджують належні заходи безпеки, необхідні для захисту даних клієнтів. Наприклад, у нашій фірмі ми використовуємо безпечні електронні листи з шифруванням для передачі конфіденційної інформації клієнтам, що також дозволяє їм безпечно надсилати та вкладати особисту інформацію членам нашої команди. І

багато разів найкращою практикою є просто взяти трубку, щоб підтвердити запит клієнта.

Регуляторні органи, зокрема Рада Федеральної резервної системи, Федеральна корпорація страхування депозитів і Комісія з цінних паперів і бірж, мають вирішальне значення для заохочення покращення кібербезпеки в галузі. Вони співпрацюють з фінансовими установами, щоб надавати рекомендації та контролювати відповідність для створення безпечнішої кібер-екосистеми.

Майте план реагування на порушення

Однак впровадження потужних превентивних заходів не робить фірму повністю захищеною від кіберзагроз. Щоб зменшити вплив порушення та сприяти швидкому поверненню до нормального стану, переконайтеся, що у вас є чітко визначений план реагування на інцидент і відновлення.

Ефективний план реагування на інциденти визначає ролі та обов’язки ключових зацікавлених сторін, створює канали зв’язку та надає покрокові методи виявлення, стримування та пом’якшення кіберзагроз. Обов’язково регулярно тестуйте та оновлюйте свій план інцидентів, щоб переконатися, що він відповідає новим ризикам і змінам в інфраструктурі вашої організації.

Прозорість і оперативне спілкування є критично важливими складовими ефективного плану реагування на інциденти. Своєчасне повідомлення про події внутрішнім командам, клієнтам, регуляторним органам і правоохоронним органам допомагає розвинути довіру споживачів і сприяє скоординованим діям для ефективного контролю проблеми.

Після порушення виконайте огляд після інциденту, щоб визначити основні причини, оцінити ефективність вашої реакції та запровадити заходи щодо усунення, які зміцнять кібербезпеку вашої організації та зменшать ймовірність подібних подій у майбутньому.

Майбутнє фінансової галузі залежить від безпечної та надійної інфраструктури кібербезпеки. Кіберзагрози продовжуватимуть зростати, і фінансові установи повинні бути готові до впровадження інноваційних технологій, сприяти розвитку сильної культури кібербезпеки та стратегічно інвестувати для

захисту своїх операцій і інтересів своїх клієнтів. Оскільки кібербезпека є головним пріоритетом, фінансова індустрія може створити безпечніший цифровий світ, який принесе користь усім зацікавленим сторонам». ***(John Ulrich. Cybersecurity In Finance: Protecting Client Data And Mitigating Risks // Forbes (https://www.forbes.com/sites/forbesfinancecouncil/2023/09/11/cybersecurity-in-finance-protecting-client-data-and-mitigating-risks/?utm_source=flipboard&utm_content=user%2Fforbes&sh=5235637b3c51). 11.09.2023).***

***

«Мережа казино та готелів MGM Resorts International заявила в понеділок, що «проблема кібербезпеки» вплинула на деякі її онлайн-системи, викликаючи збої в роботі клієнтів, особливо в Лас-Вегасі, де, за словами експертів з кібербезпеки, компанія, ймовірно, стала жертвою поширеної кібератаки.

MGM Resorts не поділилися подробицями збоїв або не розкрили, коли почалася проблема або коли її було виявлено, але сказали, що правоохоронні органи були повідомлені. У заяві компанія заявила, що вжила «швидких заходів для захисту наших систем і даних, включаючи закриття певних систем».

«Наше розслідування триває, і ми старанно працюємо над визначенням характеру та масштабу справи», – опублікували MGM Resorts у соціальних мережах.

Були деякі ознаки збоїв у компанії, яка не відповідала на електронні листи з проханням про коментарі. Її веб-сайт не працював у понеділок увечері, а коментарі користувачів групи Facebook стверджували, що ігрові автомати не працюють і що є проблеми з доступом до готельних номерів на курортах компанії.

KTNV 13, телевізійна станція в Лас-Вегасі, повідомила, що кілька гральних автоматів у готелях вийшли з мережі, і що кілька гостей не можуть нічого стягувати зі своїх номерів, робити бронювання або використовувати цифрові ключі від номерів.

У понеділок пізно ввечері MGM Resorts заявила., що її курорти «продовжують дарувати враження, якими відома MGM», включаючи заклади харчування, розваги та ігри

«Наші гості залишаються в змозі отримати доступ до своїх готельних номерів, а наші співробітники стійки реєстрації готові допомогти нашим гостям у разі потреби», — заявили в компанії. «Ми цінуємо ваше терпіння».

Невідомо, скільки людей постраждали від збоїв у кібербезпеці. MGM — це відома казино та готельна компанія, яка має тисячі готельних номерів у Лас-Вегасі, зокрема Mandalay Bay, Aria, Bellagio та MGM Grand Las Vegas.

Грег Муді, ад'юнкт-професор інформаційних систем і кібербезпеки в Університеті Невади, Лас-Вегас, заявив у понеділок, що «проблема кібербезпеки» зазвичай означає, що особа або група атакували мережу компанії.

У випадку з MGM, зловмисник або зловмисники могли «знайти якусь прогалину у своїй броні» та використати її, щоб зламати системи компанії, сказав доктор Муді, який працював з компанією та членами її технічної команди над кількома проектами.

За його словами, такі атаки зазвичай здійснюються хакерами, які прагнуть отримати прибуток. Зловмисники зазвичай викрадають дані компанії та тримають їх у заручниках, доки компанія не заплатить ціну за їх повернення. Зловмисники також продаватимуть викрадені дані на підпільному онлайн-ринку, де покупці шукатимуть дані, що містять інформацію, яка дозволить викрасти особисті дані, як-от імена, номери чи адреси.

MGM є великою компанією з величезним набором даних і тому є мішенню, сказав доктор Муді.

Артур Салмон, професор обчислювальної техніки та інформаційних технологій у Коледжі Південної Невади, де він також є директором програми кібербезпеки, заявив у понеділок, що великі компанії часто стають жертвами кібератак.

Проте три галузі часто стають об'єктами таких атак через додатковий тиск, пов'язаний із поверненням систем до нормального стану, сказав доктор Салмон.

Це: комунальні підприємства, оскільки скарги клієнтів часто стають новинами; лікарнях через ризики, які становлять порушення для пацієнтів; і казино, через репутаційний удар, який може виникнути внаслідок витоку особистої інформації клієнтів.

«Їхня команда безпеки має мати рацію 100 відсотків часу», — сказав доктор Салмон. «І загрози постійно зростають, постійно адаптуються, постійно ускладнюються. Нападник просто повинен бути правий один раз».

Юван Кім, професор мережевої безпеки в Університеті Невади, Лас-Вегас, сказав, що зловмисники іноді викрадають дані у великої та фінансово безпечної компанії, вимагають викуп за ключ для розшифровки їхніх систем, а потім чекають, поки компанія зробить це. платити.

Доктор Салмон сказав, що сума викупу може бути різною, але зазвичай вона становить сотні тисяч або невеликі мільйони для великих компаній.

Експерти кажуть, що відновлення після масштабної атаки на кібербезпеку може зайняти місяці або роки.

Нещодавні кібератаки по всьому світу призвели до припинення роботи бензопроводу, лікарень і мереж продуктових магазинів і потенційно скомпрометували деякі спецслужби. У 2019 році MGM стала жертвою витоку даних, від якого постраждали близько 10,6 мільйонів людей». ***(Eduardo Medina. ‘Cybersecurity Issue’ Forces Systems Shutdown at MGM Hotels and Casinos // The New York Times Company (https://www.nytimes.com/2023/09/11/us/cyberattack-mgm-hotel-las-vegas.html). 11.09.2023).***

***

«Материнська компанія The Weather Network каже, що на неї вплинув інцидент з кібербезпекою, який виніс з ладу деякі її системи даних.

У заяві Pelmorex Corp. йдеться, що інцидент був пов’язаний зі стороннім постачальником програмного забезпечення.

Схоже, збій системи почався у вівторок вранці.

Компанія заявляє, що постраждали системи даних про погоду як The Weather Network, так і її франкомовного еквівалента MeteoMedia.

Pelmorex заявляє, що працює над якнайшвидшим повним відновленням послуг.

Компанія каже, що зв'язалася з експертами з кібербезпеки щодо інциденту, і розслідування триває». ***(Weather Network affected by cybersecurity incident, some data systems down // National Post (https://nationalpost.com/news/canada/weather-network-cybersecurity). 13.09.2023).***

***

«Рівень кіберзлочинності зріс у Туреччині через приплив хакерів-мігрантів, переважно російських програмістів, які виїхали з Росії, тікаючи від мобілізації. Про це повідомляє Financial Times.

Згідно з джерелами в турецькій поліції та експертами з кібербезпеки, початково ці хакери займалися онлайн-шахрайством, співпрацюючи з місцевими хакерами для продажу вкрадених даних та легалізації прибутку. Але нещодавно турецька поліція розпочала розслідування, оскільки російські та місцеві хакери почали формувати угруповання, в яких використовували свої вміння.

Наприклад, експерт з кібербезпеки, який захотів залишитися анонімним, заявив газеті, що проник у телеграм-групу, в якій росіяни навчали турецьких колег роботі з великими обсягами даних, а турки надавали вигідні угоди завдяки своїм контактам у Західній Європі. Інші хакери обговорювали способи конвертації вкраденої криптовалюти в готівкові кошти та способи отримання громадянства Туреччини. За даними джерел газети, вони використовують шкідливу програму Redline, яка обходить більшість антивірусів». ***(Ярослав Жахалов. У Туреччині зростає рівень кіберзлочинності. Все через російських хакерів // Інформаційне агентство ЛІГАБізнесІнформ (https://tech.liga.net/ua/technology/novosti/v-turtsii-rastet-uroven-kiberprestupnosti-vse-iz-za-rossiyskih-hakerov). 11.09.2023).***

***

«Колумбія повідомила про масштабну кібератаку, яка вразила десятки державних веб-сайтів і країни Латинської Америки.

У четвер місцеві ЗМІ повідомили, що такі ключові веб-сайти, як міністерства юстиції, охорони здоров'я та культури, а також кілька лікарень, постраждали від атаки програм-вимагачів.

У заяві президента в середу йдеться про те, що атака була спрямована на американську компанію IFX Networks, яка надає послуги веб-хостингу в 17 країнах Америки.

Уряд президента Густаво Петро створив надзвичайний командний пункт "для оцінки збитків і ліквідації наслідків інциденту", який почався у вівторок.

У заяві йдеться, що атака зачепила 762 компанії по всій Латинській Америці.

Місцеві ЗМІ повідомили, що постраждали 34 колумбійські організації, а також інші в таких країнах, як Аргентина, Панама та Чилі.

«В руках злочинців знаходиться значна кількість інформації», — сказав Noticias Caracol TV радник президента з цифрових технологій Саул Каттан.

Атаки програм-вимагачів зазвичай отримують доступ до вразливих комп'ютерних систем і шифрують або викрадають дані, перед тим як надіслати повідомлення про викуп із вимогою оплати в обмін на розшифровку даних або їх нерозголошення.

«Це можна вважати найбільшою атакою на інфраструктуру Колумбії за останні роки», — написав Каттан у соцмережах». ***(Colombia Reports Cyberattack With Impact Across Latin America // Dow Jones & Company, Inc. (https://www.barrons.com/news/colombia-reports-cyberattack-with-impact-across-latin-america-f6c0db3b?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 14.09.2023).***

***

«Згідно з останніми інцидентами кібербезпеки, про які повідомляє Центр реагування на кіберінциденти Cyber999 CyberSecurity Malaysia, із січня по серпень цього року було зафіксовано 3837 інцидентів.

Заступник міністра зв'язку та цифрових технологій Тео Ні Чін сказав, що першими чотирма інцидентами є шахрайство (2400), вторгнення (396), пов'язане з контентом (378) і шкідливий код (359).

Тео сказав, що ці інциденти показали, що рівень обізнаності користувачів Інтернету в Малайзії потребує покращення, оскільки люди все ще стають жертвами кіберзагроз.

«Озброєні новітніми технологіями, кіберзлочинці тепер використовують інструменти AI (штучного інтелекту) для злому паролів, витоку інформації та шахрайства користувачів, спричиняючи витік даних і фінансові збитки», — сказала вона у своїй програмній промові на 10-му національному дискурсі безпеки ІКТ CyberSAFE Challenge. Гранд-фінал Trophy 2023 або NICTSeD 2023 відбувся сьогодні в Auditorium Perdana Angkasapuri, Media City.

За словами Тео, під час переходу Малайзії до інформаційно-центричного суспільства пріоритетність цифрової безпеки в системі освіти мала вирішальне значення через потенційні ризики та небезпеки, такі як шахрайство та крадіжка особистих даних, які створює Інтернет.

Вона сказала, що такий дискурс, як NICTSeD 2023, розвиває критичне мислення, отримання знань, креативність та інновації серед студентів, що охоплює знання кібербезпеки, конфіденційності даних, захисту інформації та управління цифровими ризиками.

Тео сказав, що формування кіберстійкості передбачає, що кожен член спільноти дотримується цілісної кібергігієни, від впровадження найкращих практик кібербезпеки до постійного навчання, співпраці та обміну інформацією.

«Що стосується уряду та індустрії кібербезпеки, нам потрібно постійно інвестувати в дослідження та розробки, планування реагування на інциденти, дотримання нормативних вимог і міжнародну співпрацю», — додала вона.

Тим часом, голова ради директорів Cybersecurity Malaysia General (Rtd) Тан Шрі Зулкифелі Мохд Зін у своїй промові сказав, що швидка еволюція штучного інтелекту, особливо генеративного штучного інтелекту, принесла значні досягнення в ключових галузях і секторах, і, за іронією долі, та сама технологія, яка живить у нашому повсякденному житті, може зараз стати зброєю кіберзлочинців.

«Generate AI використовує машинне навчання для створення тексту, відео, аудіо та зображень, схожих на людину. Хоча ці інструменти мають багато корисних застосувань, і вони також використовуються зловмисниками для здійснення більш ефективної складної соціальної інженерії та кібератак», – сказав він.

Зулкифелі сказав, що NICTSeD, який був запущений у 2013 році, розпочався як національний конкурс дебатів з безпеки ІКТ на тему кібербезпеки для середніх шкіл по всій країні.

За його словами, за останнє десятиліття в NICTSeD взяли активну участь 2264 школярі з 693 шкіл по всій країні, а в NICTSeD 2023 брали участь 133 школи, з яких три команди сьогодні стали великими фіналістами.

Секола Сері Путері був оголошений чемпіоном NICTSeD 2023 і виграв 5 000 рингітів, а потім Секола Тенга Кебангсан (SMK) Амінуддін Бакі, Селангор став першим учасником і взяв додому 3 500 рингітів, а SMK Кота Кемунінг був оголошений другим учасником- вгору вгору.

NICTSeD був організований кібербезпекою Малайзії та Відділом освітніх ресурсів і технологій (BSTP) Міністерства освіти з партнерами, а саме Департаментом телерадіомовлення, який організував захід, а також Інститутом Пеньяран дан Пенеранган Тун Абдул Разак за розміщення учасників». ***(Teo Nie Ching: 3,837 cyber security incidents reported from January to August this year; fraud, intrusion among top four // Malay Mail (https://www.malaymail.com/news/malaysia/2023/09/13/teo-nie-ching-3837-cyber-security-incidents-reported-from-january-to-august-this-year-fraud-intrusion-among-top-four/90696). 13.09.2023).***

***

«Минулого тижня понад 50 колумбійських державних установ і приватних компаній постраждали від кібератаки, повідомив журналістам у Нью-Йорку президент Колумбії Густаво Петро.

Інтернет-провайдер IFX Networks минулого тижня повідомив, що став жертвою атаки програм-вимагачів, унаслідок якої постраждали десятки колумбійських організацій.

Не називаючи компанію, Петро сказав, що ширший вплив атаки показав, що IFX Networks не вжила належних «заходів кібербезпеки», і компанія порушила свої контракти.

Раніше в понеділок міністр інформації, технологій і комунікацій Колумбії Маурісіо Ліскано заявив на платформі обміну повідомленнями X, що він наказав розпочати адміністративні дії проти IFX Networks.

«Ми координуємо... цивільний позов і, можливо, кримінальну справу (проти компанії)», - сказав Ліскано.

IFX Networks розуміє всю складність інциденту та проблеми, які він спричинив для постраждалих клієнтів, йдеться у заяві компанії на її веб-сайті.

«Завдяки швидкому виявленню та діям нашої команди ми змогли обмежити потенційний охоплення атаки та значно стримати кількість постраждалих систем», — йдеться у заяві». ***(More than 50 Colombian state, private entities hit by cyberattack –Petro // Reuters (https://www.reuters.com/world/americas/more-than-50-colombian-state-private-entities-hit-by-cyberattack-petro-2023-09-18/). 19.09.2023).***

***

«Хакери, які зламали гіганти казино MGM Resorts International (MGM.N) і Caesars Entertainment (CZR.O) протягом останніх тижнів, також зламали системи трьох інших компаній у сфері виробництва, роздрібної торгівлі та технологій сказав керівник служби безпеки, знайомий із ситуацією.

Девід Бредбері, керівник служби безпеки компанії Okta з управління ідентифікацією, сказав, що п’ять клієнтів компанії, включаючи MGM і Caesars, стали жертвами хакерських груп, відомих як ALPHV і Scattered Spider з серпня.

В інтерв'ю Reuters Бредбері не назвав інших компаній, але сказав, що Okta співпрацює з офіційними розслідуваннями порушень.

Ці хакерські атаки привернули увагу до атаки програм-вимагачів – кібервторгнень, які щороку вражають сотні компаній, від постачальників медичних послуг до телекомунікаційних компаній. Минулого тижня MGM і Caesars втратили ринкову вартість через падіння цін на акції, і MGM ще не оговталася після різних операцій, зруйнованих у готелях і ігрових закладах, які їй належать від Лас-Вегаса до Макао.

Компанія Okta, що базується в Сан-Франциско, має понад 17 000 клієнтів по всьому світу, надає послуги ідентифікації, такі як багатофакторна автентифікація, яка використовується для надання користувачам безпечного доступу до онлайн-додатків і веб-сайтів. За словами Бредбері, численні порушення, виявлені у своїх клієнтів минулого місяця, спонукали компанію випустити попередження.

«Ми побачили, що це сталося за такий короткий проміжок часу, і ми подумали, що нам слід звернутися до галузі в цілому та пояснити, що тут відбувається», — сказав він.

У той час Okta заявила, що її клієнти в США повідомляють про постійну схему атак, коли хакери видавали себе за співробітників фірми-жертви та переконали свою службу підтримки інформаційних технологій надати їм дублікат доступу.

«Протягом останніх шести-дванадцяти місяців ми постійно спостерігаємо зростання кількості таких атак», — сказав Бредбері.

MGM не прокоментувала цю заяву чи злом, окрім того, що минулого тижня заявила, що має справу з «проблемою кібербезпеки». Caesars раніше заявила, що розслідує порушення.

Фінансово вмотивована хакерська група ALPHV заявила про злом MGM у дописі на своєму веб-сайті в п'ятницю та попередила MGM про подальші атаки, якщо вона не укладе угоду. Незрозуміло, скільки викупу вимагає ALPHV.

Бредбері сказав, що група зламала MGM і отримала доступ до її клієнта Okta, що дозволило отримати подальший доступ до більшої кількості облікових даних у системі фірми з керування ідентифікацією.

Схоже, Scattered Spider працював з ALPHV над останніми зломами, сказав Бредбері, посилаючись на дослідження аналітиків безпеки, які відстежували обидві групи. «Думайте про них більше як про ділових партнерів або афілійованих осіб», - сказав він.

Минулого тижня Mandiant Intelligence Google назвала Scattered Spider, також відомий як UNC3944, однією з найбільш руйнівних хакерських організацій у Сполучених Штатах. Бредбері сказав, що опис Mandiant тактики групи узгоджується з тим, що Okta спостерігав під час нещодавніх хакерів». ***(Zeba Siddiqui. Hackers who breached casino giants MGM, Caesars also hit 3 other firms, Okta says // Reuters (https://www.reuters.com/technology/hackers-who-breached-casino-giants-mgm-caesars-also-hit-3-other-firms-okta-says-2023-09-19/). 19.09.2023).***

***

«У вівторок Міжнародний кримінальний суд (ICC) заявив, що його комп'ютерну систему було зламано, що стало зломом в одній із найвідоміших міжнародних установ світу, яка обробляє дуже конфіденційну інформацію про військові злочини.

ICC заявив, що наприкінці минулого тижня виявив незвичайну активність у своїй комп'ютерній мережі, що спонукало до реагування, яке все ще триває. Прес-секретар відмовився коментувати, наскільки серйозним був злом, чи його повністю вирішено та хто може стояти за ним.

«Були вжиті негайні заходи для реагування на цей інцидент кібербезпеки та пом'якшення його впливу», — йдеться в короткій заяві ICC.

ICC є постійним трибуналом з військових злочинів у нідерландському місті Гаага, створеним у 2002 році для розгляду воєнних злочинів і злочинів проти людства. Прокурори суду зараз проводять 17 розслідувань ситуацій в Україні, Уганді, Венесуелі, Афганістані та на Філіппінах, серед інших.

У березні суд потрапив у заголовки газет, коли видав ордер на арешт президента Росії Володимира Путіна за підозрою в незаконній депортації дітей з України. У Кремлі звинувачення та юрисдикцію суду відкидають.

Дуже конфіденційні документи в ICC можуть включати будь-що, починаючи від кримінальних доказів і закінчуючи іменами захищених свідків, хоча суд не розкриває, до якої частини його систем був доступ.

У своїй заяві суд зазначив, що він продовжує «аналізувати та пом'якшувати вплив цього інциденту» за сприяння уряду Нідерландів. У компанії заявили, що також вживають заходів для посилення своєї кібербезпеки.

Речник міністерства юстиції Нідерландів підтвердив, що Національний центр кібербезпеки країни підтримує розслідування, але відмовився від подальших коментарів.

Президент асоціації адвокатів ICC Марі-Елен Прулькс сказала, що адвокати підсудних і потерпілих постраждали «так само, як і персонал суду» через невизначені заходи безпеки, вжиті у відповідь на інцидент.

«Ми високо оцінюємо зусилля... щодо захисту інформаційних систем суду і сподіваємося, що ситуація буде швидко вирішена», - сказала вона.

Нідерландське розвідувальне агентство (AIVD) у своєму щорічному звіті за 2022 рік заявило, що МКС «становить інтерес для Росії, оскільки він розслідує можливі військові злочини Росії в Грузії та Україні». У червні 2022 року AIVD оголосила, що знайшла російського військового агента, який видавався за бразильця, і намагався проникнути в суд.

У серпні 2023 року прокурор ICC Карім Хан заявив, що кібератаки можуть бути частиною майбутніх розслідувань військових злочинів. Він попередив, що сам ICC може бути вразливим і повинен посилити свою оборону.

«Дезінформація, знищення, зміна даних і витік конфіденційної інформації можуть перешкоджати здійсненню правосуддя в ICC і, як такі, становити злочини в межах юрисдикції ICC, які можуть бути розслідувані або переслідувані», — написав він у звіті Foreign Policy Analytics, фінансованому Microsoft…» ***(Toby Sterling, Stephanie van den Berg. War crimes tribunal ICC says it has been hacked // Reuters (https://www.reuters.com/world/international-criminal-court-reports-cybersecurity-incident-2023-09-19/). 19.09.2023).***

***

«У нещодавньому звіті Norton, провідний бренд споживчої кібербезпеки під Gen™ (NASDAQ: GEN), пролив світло на зростаючу загрозу кібершахрайства в сучасному цифровому світі. Оскільки штучний інтелект (ШІ) стає все більш поширеним, кіберзлочинці використовують цю технологію для створення все більш витончених шахрайств, що призводить до різкого зростання їх поширеності.

Згідно з даними Gen, зараз приголомшливі 75% усіх кіберзагроз на настільних комп'ютерах є шахрайством. Експерти Norton виявили кілька відомих онлайн-шахрайств, з якими зараз стикаються люди, починаючи від шахрайства в Інтернет-магазинах і закінчуючи сексуальним здирством і шахрайством із технічною підтримкою.

Поширена загроза кібершахрайства

З розповсюдженням штучного інтелекту кіберзлочинці мають змогу створювати шахрайства, які є не тільки більш переконливими, але й надзвичайно реалістичними. Ця підвищена складність ускладнює виявлення шахрайства, створюючи серйозну проблему для споживачів. Проповідник безпеки Norton, Луїс Корронс, наголосив на необхідності обізнаності та пильності серед споживачів. Корронс заявив: «Ми виявили, що шахраї покладаються на старі методи, щоб заманити жертв, але тепер вони мають у своєму розпорядженні більш складний арсенал, щоб зробити ці схеми більш реалістичними».

Розкриття ключових категорій шахрайства

У звіті Нортона висвітлюється кілька ключових категорій шахрайства, які зараз полюють на нічого не підозрюючих жертв:

1. Шахрайство в інтернет-магазині

У E-Shop Scams шахраї створюють шахрайські інтернет-магазини, які пропонують товари за неймовірно низькими цінами. Однак після здійснення покупки товар ніколи не доставляється, а веб-сайт зникає, залишаючи жертв з порожніми руками.

2. Сексуальне шахрайство

Шахрайство з сексуальним здирництвом включає кіберзлочинців, які погрожують оприлюднити конфіденційну або компрометуючу інформацію, якщо не буде сплачено викуп. Ці шахрайства часто починаються з фішингових електронних листів, використовуючи емоції жертв, як-от страх і сором, для маніпулювання ними.

3. Шахрайство з техпідтримкою

Під час шахрайства з технічною підтримкою шахраї видають себе за агентів технічної підтримки від авторитетних компаній. Вони обманом змушують жертв надати віддалений доступ до їхніх комп'ютерів, що може призвести до крадіжки даних або вимоги викупу.

Рішення Norton для боротьби з шахрайством

Norton прагне допомогти споживачам захистити себе від цих нових кіберзагроз. З цією метою Norton нещодавно представив Norton Genie, безкоштовний інструмент виявлення шахрайства на основі штучного інтелекту. Genie розроблено для виявлення шахрайства через текстові повідомлення, соціальні мережі та електронну пошту, надаючи користувачам надійний засіб визначення потенційної небезпеки повідомлень, з якими вони стикаються.

Norton Genie йде ще далі, пропонуючи інформативні відповіді на наступні запитання, наприклад «Як ви знаєте, що це шахрайство?» і «Що мені робити далі?» Це дає користувачам знання, необхідні для ефективного виявлення шахрайства та вжиття відповідних заходів.

Поради щодо безпеки в Інтернеті

Norton також пропонує ряд практичних порад, які допоможуть людям захистити себе від різних типів шахрайства:

1. Перевірте перед покупкою

Перш ніж робити покупку в інтернет-магазині, важливо перевірити автентичність веб-сайту за допомогою оглядів і рейтингів. Будьте обережні, зустрічаючи угоди, які здаються занадто хорошими, щоб бути правдою.

2. Ще раз перевірте невідомі виклики

Отримавши дзвінки від невідомих осіб або організацій, особливо тих, хто представляється технічною підтримкою, перевірте їхню особу, зв'язавшись із відповідною компанією безпосередньо через офіційні канали. Не розголошуйте особисту чи фінансову інформацію по телефону.

3. Додайте рівні безпеки до покупок

Надайте пріоритет безпеці під час здійснення фінансових операцій в Інтернеті. Застосуйте багатоетапну перевірку для додаткового захисту та використовуйте безпечні методи оплати, як-от кредитні картки, які забезпечують захист від шахрайства.

4. Будьте обережні з особистою інформацією

Незалежно від платформи чи одержувача, завжди будьте обережні, надаючи особисту інформацію в Інтернеті. Двічі подумайте, перш ніж розголошувати конфіденційні дані, щоб не стати жертвою крадіжки особистих даних або фішингових атак.

У той час як кіберзлочинці використовують можливості штучного інтелекту для вдосконалення своїх шахрайств, Norton використовує ту ж технологію, щоб розширити можливості споживачів у боротьбі з онлайн-загрозами. Norton Genie зі своїми можливостями штучного інтелекту надає користувачам цінний інструмент для виявлення та боротьби з шахрайством у різних цифрових каналах зв'язку». ***(Benson Mawira. Norton's Latest Report Reveals Alarming Rise in Cyber Scams // Cryptopolitan (https://www.cryptopolitan.com/nortons-reveals-alarming-rise-in-cyber-***

scams/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 20.09.2023).

***

«За останні два роки серія відомих порушень кібербезпеки має одну спільну рису: залучення невеликої онлайн-спільноти переважно молодих людей, присвячених зухвалим вторгненням.

Виступаючи в кулуарах другої щорічної конференції SentinelOne з аналізу кіберзагроз LABScon, команда дослідників, які вивчали ці онлайн-спільноти, описала CyberScoop, як онлайн-спільнота, яка називає себе «Com», виділила собі ключову роль у ширшому Інтернеті кримінальна екосистема — зокрема, беручи участь у недавніх нападах на курорти Лас-Вегаса, які покалічили кілька відомих готелів і казино.

Говорячи на умовах анонімності, щоб описати дії хакерської групи з історією насильства проти своїх передбачуваних ворогів, дослідники кажуть, що поява Com ілюструє необхідність політиків і спільноти кібербезпеки зайняти набагато жорсткішу позицію проти молоді.

Підлітки та зловмисники у віці близько 20 років все частіше здійснюють гучні хакерські атаки, використовуючи передові навички та голосно вихваляючись своїми подвигами мовою, сповненою расизму та женоненависництва, при цьому Com є середовищем радикалізації для деяких із цих кіберзлочинців.

«Якщо відкинути всю дурницю і просто поглянути на можливості, — сказав дослідник, — це неймовірно потужно».

Політики та захисники мереж у деяких найбільших світових компаніях схильні відкидати цю екосистему кіберзлочинців як щабель нижче загрози, яку створюють підтримувані державою хакери, але нещодавні злами ясно показують, що це нове покоління хакерів має високі здібності.

Особи в одній із підгруп Com, відомих як «Star Fraud», ймовірно, брали участь у недавніх резонансних атаках на Caesars Entertainment і MGM Resorts,

кажуть дослідники, що демонструє серйозність і небезпеку, яку представляє більша екосистема.

ALPHV, створена операція програм-вимагачів як послуга, яка, як вважають, базується в Росії та пов'язана з атаками на десятки організацій, взяла на себе відповідальність за атаки на Caesars і MGM у примітці, опублікованій на її веб-сайті на початку цього місяця. Експерти стверджують, що атаки були результатом роботи групи, яку по-іншому відстежують як UNC 3944 або Scattered Spider, яка була описана як філія, що працює з ALPHV, що складається з людей у Сполучених Штатах і Великобританії, які перевершують соціальну інженерію.

Але термін «Розсіяний павук» не є точним, кажуть дослідники з LABScon, оскільки він об'єднує діяльність кількох різнорідних, а іноді й суперницьких груп із екосистеми Com в одне ціле. За словами дослідника, групи копіюють і навчаються тактиці одна в одної і можуть виглядати як одна й та сама річ, але вони різні. Людина, яка стверджувала, що є учасником Scattered Spider, поспілкувалася з кількома новинними виданнями, включно з CyberScoop, і взяла на себе відповідальність за злом MGM, але не Caesars, що є прикладом нестабільної екосистеми Com.

Атаки, що походять від екосистеми Com, виходять далеко за межі нещодавно постраждалих курортів Лас-Вегаса. Раніше цього тижня керівник Okta, компанії з управління ідентифікацією, повідомив Reuters, що крім Caesars і MGM ще три клієнти фірми постраждали від того самого кластера активності. За останні два роки великі корпорації від Nvidia до Samsung і Microsoft стали мішенню групи, відомої як Lapsus$, деякі з членів якої вийшли з екосистеми Com, сказав дослідник.

Оголошення

У серпневому 2023 році звіт Комітету з огляду кібербезпеки щодо Lapsus$ рекомендував Конгресу вивчити можливість фінансування програм запобігання кіберзлочинності серед неповнолітніх як частину загальносуспільного підходу до боротьби з кіберзлочинністю серед молоді.

ФБР бере участь у кількох розслідуваннях за участю людей, пов'язаних з Комітетом, за ймовірну насильницьку діяльність Як повідомляв Vice у травні,. У

свідченнях під присягою від травня 2023 року агент ФБР описав Com як «групу кіберзлочинців», яка є «географічно різноманітною» і організовується в різні підгрупи, щоб «брати участь у різних видах злочинної діяльності, включаючи кібервторгнення, обмін SIM-картами, викрадення криптовалюти, замовлення насильства в реальному житті та Swatting», практика відправлення озброєних груп екстреного реагування на місце жертви під фальшивими приводами.

Фірми з кібербезпеки описали цю групу онлайн-кіберзлочинців як висококваліфікованих у сфері соціальної інженерії, зокрема тому, що серед їхніх членів є велика кількість носіїв англійської мови, які вміють дзвонити в службу підтримки IT і переконувати техніків передати облікові дані компанії.

Дослідники, які виступали на LabsCON, попередили, що ці молоді кіберзлочинці зараз працюють разом із глобальними синдикатами програм-вимагачів, які мають досвід вимагань по всьому світу та виплачують десятки мільйонів доларів у вигляді викупу.

За словами одного з дослідників, роль Com у втягненні цих молодих хакерів у злочинне життя схожа на добре задокументовану проблему того, як токсичні онлайн-спільноти можуть радикалізувати дітей. «Радикалізація — це кіберзлочинність і бути найгіршою людиною, якою тільки можна бути», — сказав дослідник». ***(AJ Vicens. Youth hacking ring at the center of cybercrime spree // CyberScoop (https://cyberscoop.com/youth-hacking-ring-at-the-center-of-cybercrime-spree/?utm_source=flipboard&utm_content=other). 22.09.2023).***

***

«Бермудські острови працюють над відновленням громадських послуг, які були припинені минулого тижня після «складної та навмисної» кібератаки на державні системи, заявив у понеділок прем'єр-міністр острова Е. Девід Берт.

Влада розслідує, хто стоїть за атакою, і виконавці, «швидше за все, з Росії», сказав Берт на прес- конференції минулого тижня. Він відмовився повідомити додаткові подробиці розслідування, пославшись на національну безпеку.

«Зусилля по відновленню повністю тривають, і ми працюємо над тим, щоб опублікувати графік, за яким люди зможуть слідкувати, який використовуватиметься для безпечного відновлення наших систем», — сказав він.

Порушення сталося ввечері в середу, а поліцейські помітили його вранці в четвер. Поліція Бермудських островів і урядовий Департамент інформаційних і цифрових технологій намагалися ізолювати точку вторгнення і вимкнути її, але були змушені вимкнути всі пристрої, підключені до мережі, а потім відключити саму мережу, пояснив Берт.

Транспорт, освіта та лікарня працюють без перебоїв». ***(Margi Murphy. Bermuda Public Services Remain Disrupted After Cyberattack // Bloomberg L.P. (https://www.bloomberg.com/news/articles/2023-09-26/bermuda-public-services-remain-disrupted-after-cyberattack?utm_source=flipboard&utm_content=user%2Fbloomberg). 26.09.2023).***

***

«Johnson Controls постраждала від інциденту кібербезпеки. Представник Johnson Controls поділився заявою для TMJ4 News, що вони «зазнали збоїв у частині [його] внутрішньої інфраструктури інформаційних технологій і додатків у результаті інциденту кібербезпеки».

Відтоді Johnson Controls розпочала розслідування за участю експертів з кібербезпеки та координує свої дії зі своїми страховиками.

«Ми продовжуємо оцінювати, яка інформація зазнала впливу, і виконуємо наш план управління інцидентами та захисту, включаючи впровадження заходів з усунення наслідків інциденту, і продовжуватимемо вживати додаткових заходів, якщо це необхідно», — йдеться в заяві.

Станом на вечір середи компанія Johnson Controls заявила, що багато її додатків «значною мірою не вплинули» і залишаються в роботі. Однак інцидент спричинив і, як очікується, продовжуватиме спричиняти збої в частині його бізнес-операцій.

У заяві продовжувалося: «Наскільки це було можливо та відповідно до наших планів забезпечення безперервності бізнесу, ми запровадили обхідні шляхи для певних операцій, щоб зменшити збої та продовжити обслуговування наших клієнтів... Ми оцінюємо, чи вплине цей інцидент на нашу здатність своєчасно випускати наші результати четвертого кварталу та повного фінансового року, а також вплив на наші фінансові результати». ***(Madison Goldbeck. Johnson Controls experiencing disruptions after hit with cybersecurity 'incident' // Scripps Media, Inc (https://www.tmj4.com/news/local-news/johnson-controls-experiencing-disruptions-after-hit-with-cybersecurity-incident). 27.09.2023).***

***

«Спонсоровані державою хакери, які зламали маршрутизатори великих брендів та інше мережеве обладнання, наразі не є чимось новим. Проте, якщо спільні консультації з кібербезпеки від США та Японії підвищать обізнаність проти китайських кіберзлочинців, все може стати досить цікавим.

Відома група китайських кіберзлочинців, відома як «BlackTech», активно націлена на маршрутизатори Cisco для викрадання конфіденційних даних. Розвідувальне агентство США NSA, ФБР і Агентство з кібербезпеки та безпеки інфраструктури (CISA) опублікували спільну консультацію разом з поліцією Японії та органами кібербезпеки, де детально описується діяльність BlackTech і надаються рекомендації щодо пом’якшення атак.

Команда BlackTech, також відома як Palmerworm, Temp.Overboard, Circuit Panda та Radio Panda, працює з 2010 року. Кіберзлочинців безпосередньо спонсорує комуністична диктатура Китаю, і вони історично нападали на урядові організації, промисловість, ЗМІ, електроніка, телекомунікації та оборонні підрядники в США та Східній Азії.

Кіберактор спеціалізується на розробці спеціального шкідливого програмного забезпечення та «спеціалізованих механізмів збереження» для компрометації популярних брендів маршрутизаторів. США та Японія попереджають, що ці спеціальні шкідливі програми включають небезпечні функції

для відключення журналювання, зловживання стосунками довірених доменів і компрометації конфіденційних даних. Повідомлення містить список конкретних штамів шкідливого програмного забезпечення, таких як BendyBear, Bifrose, SpiderPig і WaterBear, які використовуються для націлювання на операційні системи Windows, Linux і навіть FreeBSD.

Повідомлення не дає жодної підказки щодо методів, використовуваних BlackTech для отримання початкового доступу до пристроїв жертви, які можуть включати звичайні викрадені облікові дані або навіть якусь невідому, «дико складну» 0-денну вразливість безпеки. Коли вони входять, кіберзлочинці зловживають інтерфейсом командного рядка (CLI) Cisco IOS, щоб замінити офіційне мікропрограмне забезпечення маршрутизатора скомпрометованим образом мікропрограмного забезпечення.

Процес починається, коли мікропрограмне забезпечення змінюється в пам’яті за допомогою техніки «гарячого виправлення», попереджає консультація, яка є точкою входу, необхідною для встановлення модифікованого завантажувача та модифікованого мікропрограмного забезпечення. Після завершення інсталяції змінене мікропрограмне забезпечення може обійти функції безпеки маршрутизатора та ввімкнути бекдор-доступ, який не залишає слідів у журналах і уникає обмежень списку контролю доступу (ACL).

Щоб виявити та запобігти зловмисній діяльності BlackTech, компаніям і організаціям рекомендується дотримуватися деяких «найкращих практик пом’якшення». IT-спеціаліст повинен вимкнути вихідні з’єднання, застосувавши команду конфігурації «transport output none» до ліній віртуального телетайпу (VTY), контролювати як вхідні, так і вихідні з’єднання, обмежити доступ і контролювати журнали.

Організаціям також слід оновити мережеві пристрої за допомогою останніх версій мікропрограми, змінити всі паролі та ключі, якщо існує занепокоєння, що один пароль було зламано, періодично виконувати перевірку файлів і пам’яті та стежити за змінами мікропрограми. США та Японія застерігають від скомпрометованих маршрутизаторів Cisco, але методи, описані в спільній

консультації, можна легко адаптувати для націлювання на інші відомі бренди мережевих пристроїв». ***(Alfonso Maruccia. Government-sponsored Chinese hackers are "hiding" inside Cisco routers // TechSpot, Inc. (https://www.techspot.com/news/100330-government-sponsored-chinese-hackers-hiding-inside-cisco-routers.html). 29.09.2023).***

***

Діяльність хакерів та хакерські угруповування

«Північнокорейські хакери атакували російських дипломатів і успішно зламали російський аерокосмічний науково-дослідний інститут на початку цього року, повідомляє корпорація Microsoft у блозі, опублікованому в четвер.

Корпорація Майкрософт не назвала жодної з жертв по імені та надала небагато деталей чи доказів, але заявила, що злом стався в березні.

«Північнокорейські загрозливі суб’єкти можуть скористатися можливістю проводити збір розвідданих про російські організації через те, що країна зосереджена на своїй війні в Україні», – йдеться у звіті.

Місія Північної Кореї в ООН не відразу відповіла на повідомлення з проханням прокоментувати. Російське посольство у Вашингтоні не відразу відповіло на електронний лист.

Стеження за військовими та дипломатичними організаціями конкурентів є стандартною операційною процедурою для хакерських загонів, які працюють у світових спецслужбах. Північну Корею неодноразово звинувачували в застосуванні хакерів проти оборонних і дипломатичних цілей у Південній Кореї, Сполучених Штатах та інших країнах.

Але звинувачення в тому, що Пхеньян шпигує за своїми російськими союзниками, є потенційно більш незграбними, оскільки країни зближуються на тлі війни в Україні.

Минулого місяця агентство Reuters і дослідники з фірми з кібербезпеки SentinelOne Inc розкрили, як північнокорейські шпигуни проникали в компанію

великого російського розробника ракет протягом щонайменше п’яти місяців минулого року, надаючи їм можливість збирати розвідувальні дані про російські гіперзвукові ракети та технології ракетного палива.

Звинувачення Microsoft були висловлені у звіті про кібершпигунство у Східній Азії, який також охоплював попередні звіти американського технологічного гіганта про китайських хакерів, які атакували критичну інфраструктуру США за допомогою штучного інтелекту та впливових осіб, а також нові звинувачення щодо пропагандистських операцій Китаю, які, за його словами, Пекін «продовжував нарощувати».

Посольство Китаю не відразу відповіло на повідомлення з проханням прокоментувати. Пекін регулярно заперечує звинувачення в кібервивертках». ***(Raphael Satter. North Korea Hackers Going After Russian Targets, Microsoft Says // U.S. News & World Report L.P. (https://www.usnews.com/news/technology/articles/2023-09-07/north-korea-hackers-going-after-russian-targets-microsoft-says?utm_source=flipboard&utm_content=Riskope%2Fmagazine%2FRisk+and+Crisis+Management+in+Modern+Society). 07.09.2023).***

***

«Іноземні хакери зламали аеронавігаційну організацію США, скориставшись уразливістю в IT-програмному забезпеченні компанії Zoho, попередив уряд США в четвер.

У четвер Агентство з кібербезпеки та безпеки інфраструктури США опублікувало спільне консультування з кібербезпеки, попереджаючи про загрози з ФБР і кіберкомандуванням США.

«Це [рекомендація] містить інформацію про інцидент в організації авіаційного сектору, де зловмисна діяльність мала місце ще в січні 2023 року», — йдеться в заяві CISA в четвер. CISA повідомила, що хакери, названі «національними державними передовими постійними загрозами», отримали

несанкціонований доступ до програмного забезпечення Zoho ManageEngine ServiceDesk Plus. Експлойти відомі як «CVE-2022-47966 і CVE-2022-42475».

«Виконавці постійних загроз часто сканують пристрої, що підключаються до Інтернету, на наявність вразливостей, якими можна легко скористатися, і продовжуватимуть це робити», — заявило Кіберкомандування США в окремому релізі.

За даними галузевих видань The Hacker News і Bleeping Computer, заява кіберкомандування США натякала на причетність іранських хакерів.

CISA порадила всім організаціям, які можуть постраждати, повідомляти ФБР про підозрілу чи злочинну діяльність.

У січні CISA додала CVE-2022-47966 до свого каталогу відомих використаних уразливостей, що фактично наказало федеральним агентствам захистити свої системи від конкретного експлойту. Північнокорейська державна хакерська група Lazarus використовує ту саму вразливість з початку цього року». ***(Adam Schrader. Foreign hackers attacked IT software to breach U.S. aeronautical organization // The McClatchy Company, LLC (https://www.miamiherald.com/news/nation-world/national/article279154754.html?utm_source=flipboard&utm_content=MiamiHerald%2Fmagazine%2FNews). 09.09.2023).***

***

«Недавній шквал онлайн-шпигунських кампаній показує, що висококласні хакери все частіше націлюються та використовують інструменти кібербезпеки, призначені для того, щоб не допустити їх.

Успішна атака на програму кібербезпеки пропонує хакерам високорівневий доступ до ІТ-мережі, у якій вона встановлена, відкриваючи шлях до коштовностей комп’ютерної корони. І ці мережі, як правило, належать організаціям, які найбільше піклуються про безпеку: державні установи та компанії, що працюють у таких важливих сферах діяльності, як банківська справа, телекомунікації та

електроенергетика – привабливі мішені як для хакерів із національних держав, так і для тих, хто має фінансові мотиви, наприклад банди програм-вимагачів.

В одній нещодавній хакерській кампанії, яку офіційні особи США приписують Китаю, використовувалися вразливості брандмауера Fortinet Fortigate, який продається як рішення безпеки нового покоління. Хакери намагалися встановити приховану присутність в IT-мережах постачальників життєво важливих послуг, таких як телекомунікаційні та електроенергетичні компанії на території американського тихоокеанського острова Гуам, де розташовані військові бази США, які будуть життєво важливими логістичними центрами в будь-якому конфлікті з Китаєм. Корпорація Майкрософт, яка ідентифікувала кампанію в травні, разом із агентствами з кібербезпеки США та їхніх союзників назвали хакерів Volt Typhoon.

А в липні було виявлено ще дві кампанії онлайн-шпигунства, під час яких зловмисники проникли в комп'ютерні мережі союзників США, скориставшись вразливими місцями в продуктах кібербезпеки від кіберкомпаній Ivanti та Citrix.

Кампанія Volt Typhoon ілюструє те, як IT-мережі стали критичною територією у змаганнях великих держав 21-го століття. Злом ворога — це вже не просто крадіжка секретів, це стало ключем до перемоги на полі бою. За словами офіційних осіб США, відключення комунікацій або живлення американських баз на Гуамі може бути частиною китайської превентивної атаки в Інтернеті, спрямованої на обмеження здатності американських військових переміщувати сили навколо великого тихоокеанського театру.

«Те, що ми починаємо бачити... це цілі, які не так стосуються шпигунства, а більше зриву та руйнування», — нещодавно сказала директор Агентства кібербезпеки та безпеки інфраструктури США (CISA) Джен Істерлі, відповідаючи на запитання про атаки Volt Typhoon. «У разі конфлікту Китай майже напевно використовуватиме агресивні кібероперації, щоб переслідувати нашу критично важливу інфраструктуру, включаючи трубопроводи та залізничні лінії, як для затримки розгортання військ, так і для виклику суспільної паніки», — сказала вона 12 червня на заході в Інститут Аспена у Вашингтоні, округ Колумбія.

Volt Typhoon та інші хакерські кампанії також ілюструють переваги, які національні державні хакерські групи можуть отримати, націлившись на програми безпеки, сказав Брайан Вер, колишній помічник директора CISA з кібербезпеки. Це "цікава іронія", - сказав Уор. «Організації, які найбільше піклуються про безпеку, піддаються найбільшому ризику, коли продукти безпеки скомпрометовані».

Збройні сили, уряди та корпорації покладаються на компанії приватного сектору для захисту власних систем і цього року витратять понад 219 мільярдів доларів у всьому світі на продукти та послуги кібербезпеки, згідно з даними компанії IDC, що займається аналізом ринку.

Окрім кампанії Volt Typhoon, цього літа було виявлено ще два порушення:

24 липня уряд Норвегії заявив, що в IT-мережі 12 міністерств проникли хакери, які скомпрометували програмне забезпечення безпеки Ivanti, встановлене на державних мобільних телефонах. У серпні офіційні особи оголосили про закриття систем електронної пошти та календаря для цих міністерств і їх міграцію на нову платформу, яку вони не назвали. За словами Гейра Арільда Енг-Хеллесвіка, директора департаменту Управління національної безпеки Норвегії, після того як хакери отримали доступ до сервера електронної пошти, найкращі практики вимагали переходу на нову систему. Чітким натяком є те, що електронні листи всіх 12 міністерств були скомпрометовані щонайменше чотири місяці.

Близько 2000 пристроїв Citrix, які використовувалися для безпечного масштабування комп’ютерних ресурсів у великих організаціях, включаючи державні установи та бізнес-сектори, які піклуються про безпеку, як-от банківська справа та телекомунікації, були зламані хакерами в липні та серпні, головним чином у Німеччині, а також у Японії та інших країнах. ЄС, за словами дослідників кібербезпеки Fox-IT. Згідно з попередженням влади Німеччини, ця вразливість дозволила хакерам встановити задні двері в системах, захищених пристроями Citrix, які залишалися навіть після усунення вразливостей. Вони не оприлюднили жодної інформації про те, які агентства чи компанії постраждали.

За даними ZeroFox, приватного підрозділу з кібербезпеки, де Вер зараз є головним спеціалістом з розвитку, ці порушення, хоча наразі не пов'язані з жодною конкретною країною, мають усі ознаки хакерів національної держави.

«Актори, націлені на інфраструктуру безпеки, як правило, мають довгострокові стратегічні цілі, — йдеться у звіті розвідки ZeroFox. — На відміну від типових кіберзлочинців, які схильні поспішати у своїх операціях, щоб отримати швидкі результати, ці актори демонструють терпіння, тихо зберігаючи свою присутність у скомпрометованих системах і вивчаючи їхнє оточення», щоб підготуватися до будь-якого лиха, яке вони мають намір заподіяти.

Поведінка є важливим маркером, який кібераналітики шукають, щоб зрозуміти, ким можуть бути зловмисники в системі. Оскільки інструменти, які називаються експлойтами, які використовують хакери, поширюються настільки безладно, використання експлойтів, як правило, не є хорошим способом ідентифікації зловмисника. Щойно кіберзахисники виявляють новий експлойт, вони оприлюднюють його, щоб інші захисники могли захистити власні мережі від нього.

Але це часто означає, що тепер інші зловмисники також можуть використовувати цей експлойт, спонукаючи будь-кого, хто намагається ідентифікувати конкретного зловмисника або навіть параметри конкретної кампанії – тепер кожен може використовувати цю нову зброю у власних хакерських кампаніях, атакуючи будь-які обраних ними цілей, які використовують використане програмне забезпечення.

Коли ці атаки спрямовані проти програмного забезпечення безпеки, вони ілюструють кібербезпеку, еквівалентну принципу Віллі Саттона, кажуть експерти. Подібно до знаменитого Саттона, який грабував банки, оскільки «саме там гроші», хакери атакують програми безпеки, оскільки вони зазвичай використовуються організаціями, які найбільше піклуються про безпеку, і вони користуються довіреним доступом високого рівня до систем, де вони встановлені.

Томер Бар, віце-президент із досліджень безпеки кіберпідрозділу SafeBreach: «Але якщо зловмисник може контролювати систему, Подумайте про програму

кібербезпеки, як-от система протиракетної оборони «Залізний купол», яку Ізраїль використовує для збивання ракет, випущених по його містах, сказав Newsweek він може націлити ракети не на наближаючі ракети, а на школи чи лікарні».

Дослідники SafeBreach представили три атаки з використанням цього доступу на серпневому щорічному літньому таборі хакерів у Лас-Вегасі, місці злиття провідних американських конференцій з кібербезпеки, які цього року включали велику кількість таких презентацій, зосереджених на програмному забезпеченні безпеки.

«Постачальники засобів безпеки, як і будь-які інші постачальники, вбудовуватимуть недоліки у своє програмне забезпечення... У програмі будуть помилки», — сказав Гай Бейжерано, генеральний директор SafeBreach. Він сказав, що дослідники SafeBreach, як і інші хакери, які виступають на конференції, працювали з компаніями, чиї продукти вони зламали, щоб виявлені ними недоліки в програмуванні, які називаються вразливими місцями, можна було виправити або виправити до здійснення атак. громадськість.

Але він сказав, що дослідники виконували «місію викликати [охоронні компанії]», щоб переконатися, що вони «виконують свою обіцянку». ***(Shaun Waterman. Cybersecurity Tools Are New Targets For Nation-State Hackers // NEWSWEEK DIGITAL LLC (https://www.newsweek.com/hackers-cybersecurity-volt-typhoon-guam-china-anti-virus-1823608). 01.09.2023).***

***

«Хакери, ймовірно пов’язані з урядом Ірану, використовували просту техніку, щоб спробувати зламати тисячі організацій у очевидній глобальній шпигунській кампанії.

Хакери використовували стратегію «розпилення паролів», коли вони намагалися одним і тим же простим паролем відкрити кілька облікових записів, перш ніж перейти до наступного командного пароля, повідомили дослідники Microsoft у блозі в четвер.

Microsoft пов'язала цю операцію з хакерською командою, яку підтримує іранський уряд, яку Microsoft називає «Peach Sand Storm», і заявила, що вторгнення групи, ймовірно, використовуються «для полегшення збору розвідданих на підтримку державних інтересів Ірану».

За словами Microsoft, хакери «нещодавно переслідували організації в супутниковому, оборонному та фармацевтичному секторах по всьому світу».

Коли іранські хакери знайшли один із цих облікових записів і зламали його, за словами Microsoft, вони застосували «комбінацію загальнодоступних і спеціальних інструментів» для відображення комп'ютерних систем своїх жертв, залишаючись прихованими та переходячи до інших частин жертв. мережі.

Компанія не повідомила подробиць щодо потенційних жертв кампанії. Але це підтвердило, що хакери вкрали дані в «невеликій кількості» випадків.

Розпилення паролів є поширеною та ефективною технікою злому, оскільки, незважаючи на багаторічні попередження, багато людей використовують схожі паролі, які легко вгадати.

Microsoft заявила, що публічно розкриває діяльність Peach Sandstorm, щоб підвищити обізнаність користувачів про необхідність надійних паролів та інших базових засобів захисту.

Розпорошення паролів є улюбленою технікою цієї іранської групи, яка раніше використовувала її в 2019 році в період загострення напруженості між адміністрацією Трампа та іранським режимом.

Але Peach Sandstorm також, здається, стає розумнішим. Microsoft заявила, що багато методів групи «матеріально більш складні», ніж її попередні стратегії.

«На відміну від атак грубої сили, спрямованих на один обліковий запис із використанням багатьох паролів, атаки розпиленням паролів допомагають зловмисникам максимізувати свої шанси на успіх і мінімізувати ймовірність автоматичного блокування облікового запису», — заявили в Microsoft.

«Навіть один зламаний обліковий запис може дозволити супротивнику проводити розвідку, рухатися вбік або отримати доступ до конфіденційних ресурсів, часто не привертаючи уваги захисників». ***(Eric Geller. Hackers Backed by***

Iran Caught in Apparent Global Spy Campaign // JAF Communications Inc (https://themessenger.com/tech/hackers-backed-by-iran-caught-in-apparent-global-spy-campaign?utm_source=flipboard&utm_content=waral01%2Fmagazine%2FRumors+Of+War). 14.09.2023).

***

«Правоохоронні органи США та Японії та органи кібербезпеки попереджають про те, що китайські хакери «BlackTech» зламають мережеві пристрої, щоб встановити спеціальні бекдори для доступу до корпоративних мереж.

Спільний звіт надійшов від ФБР, АНБ, CISA, японського NISC (кібербезпека) і NPA (поліція), які пояснюють, що спонсорована державою хакерська група зламує мережеві пристрої в міжнародних дочірніх компаніях, щоб перейти до мереж корпоративних штаб-квартир.

BlackTech (вона ж Palmerworm, Circuit Panda та Radio Panda) — спонсорована державою китайська група APT (передова постійна загроза), відома тим, що проводить кібератаки на японські, тайванські та гонконзькі організації принаймні з 2010 року.

Цільові сектори BlackTech включають уряд, промисловість, технології, ЗМІ, електроніку, телекомунікації та оборонну промисловість.

Спеціальне шкідливе програмне забезпечення на мережевих пристроях

У повідомленні ФБР попереджається, що хакери BlackTech використовують спеціальне, регулярно оновлюване шкідливе програмне забезпечення для бекдорів мережевих пристроїв, які використовуються для збереження, початкового доступу до мереж і для викрадення даних шляхом перенаправлення трафіку на сервери, контрольовані зловмисниками.

Повідомлення попереджає, що спеціальне шкідливе програмне забезпечення іноді підписується за допомогою вкрадених сертифікатів підпису коду, що ускладнює виявлення програмного забезпечення безпеки.

Використовуючи вкрадені облікові дані адміністратора, зловмисники скомпрометують широкий спектр марок, моделей і версій маршрутизаторів, встановлюють постійність і переміщуються по мережі.

Як пояснюється в спільній консультації з кібербезпеки:

«Зокрема, отримавши початкову точку опори в цільовій мережі та отримавши доступ адміністратора до периферійних мережевих пристроїв, кіберучасники BlackTech часто модифікують мікропрограму, щоб приховати свою активність на периферійних пристроях для подальшої підтримки стабільності в мережі. Щоб розширити свою точку опори на Учасники BlackTech націлюються на маршрутизатори філій — як правило, менші пристрої, які використовуються у віддалених офісах філій для підключення до штаб-квартири компанії, — а потім зловживають довіреними відносинами маршрутизаторів філій у цільовій корпоративній мережі. Потім учасники BlackTech використовують скомпрометовану публічну філію маршрутизатори як частину їхньої інфраструктури для проксі-серверу трафіку, змішування з корпоративним мережевим трафіком і передачі іншим жертвам у тій самій корпоративній мережі».

Модифікована прошивка дозволяє зловмисникам приховувати зміни конфігурації та історію виконаних команд. Це також дозволяє їм деактивувати журналювання на скомпрометованому пристрої, поки вони активно беруть участь у зловмисних операціях.

Зокрема, для маршрутизаторів Cisco дослідники спостерігали, як зловмисники вмикають і вимикають бекдор SSH за допомогою спеціально створених пакетів TCP або UDP, які надсилаються на пристрої. Цей метод дозволяє зловмисникам уникнути виявлення та активувати бекдор лише за необхідності.

Зловмисники також спостерігали за латанням пам’яті пристроїв Cisco, щоб обійти функції перевірки підпису Cisco ROM Monitor. Це дозволяє зловмисникам завантажувати модифіковане мікропрограмне забезпечення, яке попередньо інстальовано з бекдорами, які дозволяють нереєстрований доступ до пристрою.

У випадках зламаних маршрутизаторів Cisco хакери також змінюють політики EEM, які використовуються для автоматизації завдань, видаляючи певні

рядки з законних команд, щоб блокувати їх виконання та перешкоджати криміналістичному аналізу.

Створення спеціального зловмисного програмного забезпечення не є новим для групи BlackTech APT, у двох звітах 2021 року від NTT і Unit 42 висвітлюється використання цієї тактики зловмисниками.

У старішому звіті Trend Micro конкретно згадувалося про тактику компрометації вразливих маршрутизаторів для використання їх як серверів C2.

Рекомендації щодо захисту

Повідомлення радить системним адміністраторам стежити за несанкціонованими завантаженнями завантажувача та образів прошивки та незвичними перезавантаженнями пристроїв, які можуть бути частиною завантаження модифікованої прошивки на маршрутизаторах.

Трафік SSH, який спостерігається на маршрутизаторі, також слід ставитися з великою підозрою.

Рекомендуються наступні методи пом’якшення:

Використовуйте команду «transport output none», щоб запобігти небажаним зовнішнім підключенням.

Контролюйте вхідний/вихідний трафік на пристроях, особливо неавторизований доступ, і розділяйте адміністративні системи за допомогою VLAN.

Дозволяйте лише певні IP-адреси для адміністраторів мережі та відстежуйте спроби входу.

Перехід на пристрої з розширеним безпечним завантаженням і пріоритетне оновлення застарілого обладнання.

Негайно змініть усі паролі та ключі, якщо є підозра на порушення.

Уважно перевірте журнали на наявність аномалій, як-от несподівані перезавантаження чи зміни конфігурації.

Використовуйте методологію цілісності мережевого пристрою (NDI), щоб виявити несанкціоновані зміни.

Постійно порівнюйте завантажувальні записи та мікропрограми з надійними версіями.

Cisco також опублікувала пораду щодо безпеки на цю тему, підкресливши, що немає жодних ознак того, що BlackTech використовує вразливість у своїх продуктах або вкрадений сертифікат для підпису свого шкідливого програмного забезпечення.

Крім того, Cisco зазначає, що метод атаки, який передбачає зниження версії мікропрограми для обходу заходів безпеки, застосовується лише до старих, застарілих продуктів.

Протягом останнього року націлювання на мережеві пристрої зросло, причому китайські загрозливі особи також націлюються на Fortinet, TP-Link і SonicWall за допомогою спеціального шкідливого програмного забезпечення. мережеві пристрої

У квітні США, Велика Британія та Cisco попередили про атаки на пристрої Cisco iOS з боку російської хакерської групи APT28 (Fancy Bear, STRONTIUM), спонсорованої державою, яка розгорнула спеціальне шкідливе програмне забезпечення для крадіжки даних і передачі даних на внутрішні пристрої.

Оскільки периферійні мережеві пристрої зазвичай не підтримують рішення безпеки EDR (виявлення кінцевих точок і реагування), вони є основними цілями для зловмисників, які використовують для крадіжки даних і початкового доступу до мережі.

«Існує повторювана тема про те, що кібершпигунство, пов’язане з Китаєм, зосереджено на мережевих пристроях, пристроях IOT тощо, які не підтримують рішення EDR», — сказав технічний директор Mandiant Чарльз Кармакал BleepingComputer у травні.

Тому мережеві адміністратори повинні інсталювати всі доступні виправлення безпеки на периферійних пристроях, щойно вони стануть доступними, і не розкривати публічні консолі керування». ***(Bill Toulas. US and Japan warn of Chinese hackers backdooring Cisco routers // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/us-and-japan-warn-of-chinese-***

hackers-backdooring-cisco-routers/?utm_source=flipboard&utm_content=other). 27.09.2023).

***

Вірусне та інше шкідливе програмне забезпечення

«Індія попередила своїх громадян про вдосконалене шкідливе програмне забезпечення, націлене на користувачів Android, здатне отримати доступ до конфіденційних даних і дозволити хакерам контролювати заражені пристрої.

Головний контролер оборонних рахунків, департамент Міністерства оборони Індії, опублікував консультацію щодо трояна віддаленого доступу під назвою DogeRAT, про який спочатку повідомив стартап з кібербезпеки CloudSEK. У примітці говориться, що зловмисне програмне забезпечення, націлене переважно на користувачів Android в Індії, поширюється через соціальні мережі та платформи обміну повідомленнями як законні програми, такі як ChatGPT, Opera Mini, і навіть як «преміум-версії» YouTube, Netflix і Instagram.

«Після встановлення на пристрої жертви зловмисне програмне забезпечення отримує несанкціонований доступ до конфіденційних даних, включаючи контакти, повідомлення та банківські облікові дані», — йдеться в повідомленні від 24 серпня.

Зловмисне програмне забезпечення може заволодіти зараженими пристроями, дозволяючи хакерам надсилати спам, ініціювати неавторизовані платежі, змінювати файли та навіть знімати фотографії та натискання клавіш; він також може відстежувати місцезнаходження користувача та записувати аудіо, йдеться у примітці.

Хоча походження загрози залишається невідомим, у повідомленні підкреслюється, що група кіберзлочинців використовувала Telegram для поширення підроблених версій популярних додатків, таких як ChatGPT, Instagram, Opera Mini та YouTube у недавньому інциденті.

Міністерство оборони попросило свої відомства та чиновників утримуватися від завантаження додатків із неперевірених сторонніх платформ і переходів за

посиланнями від невідомих відправників. Їм також рекомендовано постійно оновлювати смартфони за допомогою найновішого програмного забезпечення та патчів безпеки та встановлювати антивірусну програму.

У своєму блозі наприкінці травня CloudSEK заявив, що зловмисне програмне забезпечення Android з відкритим кодом, засноване на Java, націлене на клієнтів у багатьох галузях, включаючи банківську справу та розваги. Стартап також зазначив, що хоча більшість кампанії спочатку були націлені на користувачів в Індії, вона має на меті мати глобальне охоплення.

За словами дослідників CloudSEK, автор DogeRAT показав у публікації на GitHub, що кампанію зловмисного програмного забезпечення можна запустити за допомогою бота Telegram і платформи NodeJS з відкритим кодом.

Про надзвичайну ситуацію консультації вперше повідомило місцеве видання Moneycontrol.

Із зростанням оцифровки в Індії зросли випадки кібербезпеки в цій країні, яка зараз є другим за величиною інтернет-ринком у світі після Китаю. Міністерство інформаційних технологій Індії повідомило про збільшення на 171% інцидентів кібербезпеки, що стосуються державних відомств, до 192 439 у 2022 році з 70 798 у 2018 році.

Один із значних інцидентів кібербезпеки стався торік в Нью-Делі в найбільшій державній медичній установі Індії, Всеіндійському інституті медичних наук (AIIMS). Атака програмного забезпечення-вимагача вразила п’ять серверів, які містили 1,3 терабайта даних, повідомив уряд у своїй відповіді парламенту в грудні». ***(Jagmeet Singh. India warns of malware attacks targeting its Android users // Yahoo (https://techcrunch.com/2023/09/05/india-advisory-dogerat-malware-android-users/?utm_source=flipboard&utm_content=user%2FTechcrunch&guccounter=1&guce_referrer=aHR0cHM6Ly9mbGlwYm9hcmQuY29tL3JlZGlyZWN0P3VybD1odHRwcyUzQSUyRiUyRnRlY2hjcnVuY2guY29tJTJGMjAyMyUyRjA5JTJGMDUlMkZpbmRpYS1hZHZpc29yeS1kb2dlcmF0LW1hbHdhcmUtYW5kcm9pZC11c2VycyUyRiUzRnV0bV9zb3VyY2UlM0RmbGlwYm9hcmQlMjZ1dG1fY29udGVudCUzRHVzZXIlMjUyRlRlY2hjcnVuY2gmdj1QckJJU2NOU3otMDRKOGFQeDY0S1VKa1lJdklVNllLTm5SV2FT***

MFEyRTFFQUFBR0taZzg3UlE&guce_referrer_sig=AQAAAIi6C3b3K6hWAKyeggs7FYl7jn_SKZZeD91Z_vviMUMRuWyOqqLPJtZiVSdNKnBOfTZGUAFjyx1m9VfC2VnAoKxtLzE9LgjdfXkBz-A9qDU9z_srKWhtomcmfmqvluLIgslwkvTbowI14B3OqM7rTCwHJWfkV9-ugutW7ZzSLMcm). 05.09.2023).

***

«Новий штам зловмисного програмного забезпечення під назвою ValleyRAT розгортається серед великих організацій у всьому світі, попереджають дослідники.

Експерти з кібербезпеки з Proofpoint опублікували звіт, у якому стверджується, що китайські підприємства на материку, а також інші фірми в інших країнах стають мішенями кількох нових штамів зловмисного програмного забезпечення, які, ймовірно, використовуються більш ніж одним новим суб'єктом загрози.

Серед них – новий інструмент під назвою ValleyRAT: «Кампанії розповсюдження цього зловмисного ПЗ проводилися китайською мовою, і, слідуючи тенденції інших китайських кампаній зловмисного програмного забезпечення, більшість використовувала теми рахунків-фактур, пов'язані з різними китайськими підприємствами», – сказали дослідники, заявивши, що вони побачили кілька кампаній, що розповсюджують саме це зловмисне програмне забезпечення.

Електронні листи, заражені RAT

ValleyRAT було вперше помічено в березні 2023 року, зазначає далі Proofpoint, і хоча це, мабуть, найцікавіший, це навряд чи єдиний варіант, який розгортається. Дослідники також помітили Sainbox (варіант сумнозвісного Gh0stRAT), а також Purple Fox. За допомогою останнього нападники здебільшого переслідували японські цілі:

«Хоча історична діяльність узгоджується з тим, що Proofpoint вважає китайською, вона рідко спостерігається в наших даних про загрози», — сказали

дослідники, обговорюючи Purple Fox. «Примітно, що в одній спостережуваній кампанії використовувалися теми рахунків-фактур японською мовою, націлені на організації в Японії, щоб доставляти заархівовані вкладення, які призводили до встановлення, тоді як інші використовували повідомлення на тему рахунків-фактур китайською мовою з URL-адресами».

Наразі Proofpoint каже, що виявив понад два десятки таких кампаній. У них зловмисники видавали себе за великі корпорації та зверталися до їхніх співробітників електронною поштою, намагаючись змусити їх завантажити та запустити деякі з вищезгаданих RAT.

Хоча докази здаються непереконливими, коли йдеться про особи зловмисників, дослідники припускають, що це може бути робота кількох груп, які, швидше за все, ділять цінні ресурси. Вони засновують ці висновки на тому факті, що «деякі кластери діяльності дійсно перетинаються».

Мотиви нападників наразі також невідомі». ***(Sead Fadilpašić. A mysterious new Chinese malware strain is targeting large firms across the globe // Future US, Inc. (https://www.techradar.com/pro/security/a-mysterious-new-chinese-malware-strain-is-targeting-large-firms-across-the-globe?utm_source=flipboard&utm_content=rubertus%2Fmagazine%2FInnovation%2C+Business+%26+Creativity+%7C+Innovaci%C3%B3n+y+Creatividad). 21.09.2023).***

***

«Дослідники з кібербезпеки виявили нову партію шкідливих пакетів у реєстрі пакетів npm, які призначені для викрадання конфігурацій Kubernetes і ключів SSH із скомпрометованих машин на віддалений сервер.

Sonatype повідомляє, що наразі виявлено 14 різних пакетів npm: @am-fe/hooks, @am-fe/provider, @am-fe/request, @am-fe/utils, @am-fe/watermark, @am-fe/watermark-core, @dynamic-form-components/mui, @dynamic-form-components/shineout, @expue/app, @fixedwidthtable/fixedwidthtable, @soc-fe/use, @spgy/eslint-plugin-spgy- fe, @virtualsearchtable/virtualsearchtable і shineouts.

«Ці пакунки [...] намагаються імітувати бібліотеки та компоненти JavaScript, такі як плагіни ESLint та інструменти TypeScript SDK», — повідомила фірма з безпеки ланцюга постачання програмного забезпечення. «Але після інсталяції було помічено, що кілька версій пакетів запускають обфусцований код для збору та перекачування конфіденційних файлів із цільової машини».

Разом із конфігурацією Kubernetes і ключами SSH, модулі також здатні збирати системні метадані, такі як ім’я користувача, IP-адреса та ім’я хоста, які передаються в домен із назвою app.threatest[.]com.

Розкриття сталося трохи більше ніж через тиждень після того, як Sonatype виявив підроблені пакети npm, які використовують техніку, відому як плутанина залежностей, щоб імітувати внутрішні пакети, нібито використовувані розробниками PayPal Zettle та Airbnb у рамках етичного дослідницького експерименту.

Тим не менш, зловмисники продовжують націлюватися на реєстри з відкритим кодом, такі як npm і PyPI, за допомогою криптоджекерів, інформаційних викрадачів та іншого нового шкідливого програмного забезпечення, щоб скомпрометувати системи розробників і, зрештою, отруїти ланцюг постачання програмного забезпечення.

В одному випадку, описаному Phylum на початку цього місяця, модуль npm під назвою hardhat-gas-report залишався безпечним протягом більше восьми місяців з 6 січня 2023 року, перш ніж отримати два послідовних оновлення 1 вересня 2023 року, щоб включити шкідливі JavaScript здатний викрадати закриті ключі Ethereum, скопійовані в буфер обміну, на віддалений сервер.

«Цей цілеспрямований підхід вказує на складне розуміння безпеки криптовалют і передбачає, що зловмисник має на меті захопити та викрасти конфіденційні криптографічні ключі для несанкціонованого доступу до гаманців Ethereum або інших захищених цифрових активів», — заявили в компанії.

Готові вирішувати нові виклики кібербезпеки, спричинені ШІ? Приєднуйтесь до нашого проникливого вебінару з Zscaler, щоб розглянути зростаючу загрозу генеративного ШІ в кібербезпеці.

Інший випадок спроби атаки на ланцюжок постачань стосувався хитрого пакета npm під назвою gcc-patch, який, як виявилося, видавався за спеціальний компілятор GCC, але насправді містив майнер криптовалюти, який «таємно використовує обчислювальну потужність невинних розробників, щоб отримати прибуток від їх витрати.»

Але в знак того, що такі загрози стають надто частими, схожа кампанія криптозловмисників, націлена на PyPI, використовувала шахрайський пакет Python під назвою Culturestreak для викрадення системних ресурсів і майнінгу криптовалюти Dero, завантажуючи корисне навантаження зі сховища GitLab, згідно з Checkmarx.

Більше того, такі кампанії охоплюють екосистеми Javascript (npm), Python (PyPI) і Ruby (RubyGems), а зловмисники завантажують кілька пакетів із можливостями збору та викрадання даних, а потім публікують нові версії зі зловмисними корисними навантаженнями.

Кампанія спеціально націлена на користувачів Apple macOS, вказуючи на те, що зловмисне програмне забезпечення в сховищах пакунків з відкритим кодом не тільки стає все більш поширеним, але й виділяє інші операційні системи, окрім Windows.

«Автор цих пакетів організовує широку кампанію проти розробників програмного забезпечення», — зазначив Phylum в аналізі. «Кінцева мета цієї кампанії залишається незрозумілою». ***(Fresh Wave of Malicious npm Packages Threaten Kubernetes Configs and SSH Keys // The Hacker News (https://thehackernews.com/2023/09/fresh-wave-of-malicious-npm-packages.html). 20.09.2023).***

***

«Дослідники кібербезпеки з Proofpoint нещодавно виявили нову частину зловмисного програмного забезпечення, яке імітує Bitwarden у спробі викрасти конфіденційну інформацію з кінцевої точки жертви.

Отримавши інформацію від старшого директора відділу аналізу загроз у Malwarebytes Жерома Сегури, дослідники виявили, що шкідливе програмне забезпечення під назвою ZenRAT маскується під підроблену версію популярного менеджера паролів.

Зловмисники купили домен «bitwariden[.]com» — домен з орфографічною помилкою, але навмисно схожий на законний сайт за допомогою техніки, відомої як типосквотінг — і створили веб-сайт, здавалося б, ідентичний веб-сайту Bitwarden.

Крадіжка даних, що зберігаються в браузері

Невідомо, як зловмисники просували веб-сайт, але дослідники підозрюють, що SEO, шкідлива реклама або соціальна інженерія. найімовірнішими векторами є або отруєння

У будь-якому випадку, коли жертва відвідує веб-сайт із пристрою Mac або Linux і натискає відповідне посилання для завантаження, нічого зловмисного не станеться. Вони просто будуть перенаправлені на зовсім іншу, безпечну сторінку. Однак користувачі Windows будуть заражені ZenRAT.

Після встановлення з’єднання зі своїм сервером керування та керування (C2) зловмисне програмне забезпечення виконає ряд дій, зокрема збиратиме системну інформацію та краде паролі.

Використовуючи запити WMI, ZenRAT намагатиметься дізнатися ім’я процесора жертви, ім’я графічного процесора, версію ОС, встановлену оперативну пам’ять, IP-адресу та шлюз, а також будь-які встановлені антивірусні програми та інші програми. Крім того, він викраде всі дані браузера, включаючи будь - які облікові дані, що зберігаються там.

Хоча Proofpoint закликає споживачів бути обережними під час завантаження програмного забезпечення та переконатися, що вони отримують його лише з надійних джерел, проблема полягає в тому, що споживачів можна легко обдурити.

Через зловмисну рекламу можливо, що фальшива реклама Bitwarden потрапила в Google – зазвичай це надійне джерело. Непідготовлене око може легко

пропустити зайве «і» в URL-адресі, і оскільки веб-сайт майже ідентичний законному, кампанія може бути досить успішною.

Точно невідомо, скільки людей наразі завантажили зловмисне програмне забезпечення та втратили свої паролі та інші конфіденційні дані в процесі. (Sead Fadilpašić. This destructive malware is targeting Windows users as a fake password manager, so beware // Future US, Inc». ***(https://www.techradar.com/pro/security/this-destructive-malware-is-targeting-windows-users-as-a-fake-password-manager-so-beware?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 27.09.2023).***

***

«Дослідники кібербезпеки Cyble нещодавно виявили новий штам шкідливого програмного забезпечення, яке атакує користувачів Windows і здатне викрадати конфіденційні дані із заражених пристроїв.

Зловмисне програмне забезпечення називається Exela і, як повідомляється, використовує Discord для доставки викраденої інформації своїм операторам. Дані, які він прагне викрасти, включають облікові дані для входу, особисті дані та фінансову інформацію, а також деталі сеансу з різних онлайн-додатків, служб соціальних мереж та ігрових платформ.

Хоча дослідники вперше помітили Exela в середині вересня 2023 року, аналіз показав, що вона була розроблена в травні. Відтоді він виріс і отримав нові функції, а також власний канал у Telegram.

Користувачі Chrome під загрозою

Exela намагатиметься викрасти дані з усіх основних браузерів на ринку сьогодні, включаючи Chrome, Edge, Brave, Opera та Vivaldi. Крім того, він викрадає дані кредитної картки, сеансові файли cookie та інші дані, а також робить знімки екрана.

Що стосується сеансів у соціальних мережах, він може захоплювати ті з Instagram, Twitter, TikTok і Reddit. І коли справа доходить до ігор, користувачі

гігантської роздрібної платформи Steam і гравці популярного Roblox, здається, найбільш вразливі.

Інші подробиці про зловмисне програмне забезпечення наразі невідомі, тому ми не знаємо, хто його розробники або на кого саме вони намагаються націлитися, хоча поки що в полі зору його знаходяться геймери та розробники програмного забезпечення.

Ми також не знаємо, як зловмисне програмне забезпечення доставляється жертвам і наскільки воно успішне. Очевидно, його скидають через фішингові сторінки та веб-сайти, що рекламують безкоштовне програмне забезпечення.

Якщо ви боїтеся зараження, найкращий спосіб забезпечити безпеку – завантажувати програмне забезпечення лише з перевірених джерел. Отримання посилань через канали соціальних мереж, електронну пошту чи щось подібне завжди є проблемою.

Крім того, допомагає встановлене антивірусне програмне забезпечення, а також брандмауер. Нарешті, багато інформаційних викрадачів захоплюють інформацію, що зберігається в браузері, тому, можливо, було б непоганою ідеєю зберігати конфіденційну інформацію в одному з найкращих рішень для керування паролями». ***(Sead Fadilpašić. Exela Stealer malware uses Discord to steal Windows users data // Future US, Inc. (https://www.techradar.com/pro/security/exela-stealer-malware-uses-discord-to-steal-windows-users-data?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 27.09.2023).***

***

Програми-вимагачі

«Невідомі зловмисники націлені на погано захищені сервери Microsoft SQL, намагаючись заразити їх новим штамом програм-вимагачів.

Новий звіт дослідників кібербезпеки Securonix описує кампанію, під час якої хакери спочатку намагаються грубою силою проникнути на сервери MS SQL.

Коли їм це вдається, вони роблять ряд речей, включаючи розгортання маяка Cobalt Strike, латеральний рух по цільовій мережі та кінцевих точках і, зрештою, розгортання штамів програм-вимагачів під назвою FreeWorld.

Програма-вимагач FreeWorld

FreeWorld, здається, є варіантом відомого шифрувальника під назвою Mimic. Хоча мета кампанії така, як очікувалося (викрадення конфіденційних даних і шифрування кінцевих точок), спосіб, яким хакери використовують інструменти та інфраструктуру, щоб потрапити туди, досить унікальний. Securonix пояснив у своєму звіті: «Деякі з цих інструментів включають програмне забезпечення для перерахування, корисні навантаження RAT, програмне забезпечення для експлуатації та крадіжки облікових даних і, нарешті, програмне забезпечення-вимагач».

Успіх кампанії залежить виключно від надійності пароля, який використовується для захисту сервера MS SQL, підсумували дослідники. «Важливо підкреслити важливість надійних паролів, особливо на публічних службах». Зрештою, саме сервери зі слабкими паролями були зламані.

Програмне забезпечення-вимагач є одним із найпопулярніших видів кіберзлочинності. Згідно з даними Coveware, після відносно мирного 2022 року кількість атак програм-вимагачів стрімко зросла. У той же час обізнаність серед потенційних жертв зростає, в результаті чого менше організацій сплачують вимогу викупу. Відсоток скомпрометованих організацій, які в кінцевому підсумку сплатили вимогу викупу, впав до рекордно низького рівня в 34%, стверджує те ж джерело.

Ті, хто платили – в підсумку заплатили досить багато. Середня сума перевищила $700 000, що на 126% більше, ніж у першому кварталі 2023 року». ***(Sead Fadilpašić. Microsoft SQL servers hijacked to deliver Cobalt Strike and ransomware // Future US, Inc. (https://www.techradar.com/pro/security/microsoft-sql-servers-hijacked-to-deliver-cobalt-strike-and-ransomware?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 04.09.2023).***

***

«Агентство з кібербезпеки та інфраструктури США (CISA) і Федеральне бюро розслідувань (ФБР) опублікували рекомендації щодо безпеки, які попередили організації про операцію з програмою-вимагачем Snatch.

Порада є частиною парної кампанії #StopRansomware, у якій двоє детально описують тактику, техніку та процедури (TTP), а також індикатори компрометації (IOC) активних і руйнівних операцій програм-вимагачів, сподіваючись допомогти організаціям. захищати від загроз трохи краще.

Незважаючи на те, що Snatch вперше з'явився десь у 2018 році, дані, які надають дві організації, відносно нові, деякі дані розслідування датуються початком червня цього року. Згідно з консультацією, Snatch — це модель програми-вимагача як послуги, за якою різні групи загроз здають в оренду шифрувальник та інфраструктуру, щоб запускати кампанії програм-вимагачів.

У той час як суб'єкти загроз Snatch продовжували «послідовно» розвивати свою тактику загроз, йдеться в повідомленні, вони дотримувалися того, що робила більшість – вони викрадали та шифрували конфіденційні дані, а потім вимагали плату в обмін на ключ дешифрування та в обмін на те, щоб не витікати. дані в темній мережі.

«ФБР і CISA заохочують організації виконувати рекомендації в розділі «Пом'якшення» цього CSA, щоб зменшити ймовірність і вплив інцидентів з програмами-вимагачами», — сказали вони.

Ще в грудні 2019 року було виявлено, що програма-вимагач Snatch перезавантажує заражені комп'ютери в безпечний режим, щоб обійти рішення безпеки. Цю версію виявили дослідники безпеки з команди Sophos Managed Threat Response і SophosLabs, які заявили, що жоден інструмент безпеки не працює в безпечному режимі, що дозволяє Snatch безперервно шифрувати файли.

У звіті на SiliconANGLE сказано, що останніми жертвами Snatch є Департамент у справах ветеранів Флориди, Zilli, CEFCO Inc., Міністерство оборони Південної Африки та Briars Group Ltd.

Майкл Мумкуоглу, співзасновник і виконавчий директор компанії CardinalOps Ltd., що займається управлінням позиції, розповів тому ж виданню, що оператори Snatch були більш активними за останні півтора року». ***(Sead Fadilpašić. FBI and CISA issue warning about dangerous new ransomware strain // Future US, Inc. (https://www.techradar.com/pro/security/fbi-and-cisa-issue-warning-about-dangerous-new-ransomware-strain?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 21.09.2023).***

***

«За даними Cybersecurity Ventures, до 2031 року програми-вимагачі коштуватимуть своїм жертвам приблизно 265 мільярдів доларів. У першій половині 2023 року, у середньорічному звіті Check Point Research за 2023 рік, було виявлено, що 48 груп програм-вимагачів визнали порушення та публічне вимагання понад 2200 жертв у всьому світі. Сорок п’ять відсотків атак були спрямовані на організації, що базуються в США – це значно більше, ніж у будь-якій іншій країні.

Згідно зі звітом Verizon DBIR за 2023 рік, 24% усіх порушень кібербезпеки стосувалися програм-вимагачів. І ці атаки програм-вимагачів непропорційно зосереджені на виробництві, роздрібній торгівлі та послугах програмного забезпечення. Цікаво відзначити, що хоча уряд, охорона здоров’я та освіта є найбільш атакуваними галузями, вони не є головним центром програм-вимагачів.

Програмне забезпечення-вимагач визначається як зловмисне програмне забезпечення, призначене для заборони організації доступу до файлів або даних на її комп’ютері. Кіберзлочинці шифрують дані та вимагають викуп за ключ розшифровки, сподіваючись, що жертва заплатить, щоб відновити доступ.

У подвійних атаках програм-вимагачів, якщо викуп не буде сплачено, зловмисники продадуть викрадені дані або опублікують їх на публічних форумах. Дедалі частіше кіберзлочинці вдаються до потрійного вимагання, коли вони шантажують окремих співробітників або жертв, щоб вони заплатили за їхні дані. Останнім прикладом є клініка пластичної хірургії, де клініка відмовилася платити

викуп, тож хакери зв'язалися з пацієнтами та погрожували оприлюднити їхні медичні записи, якщо вони не заплатять. Щонайменше 70 пацієнтів опублікували дані про стан здоров'я та фотографії, а один пацієнт подав до суду на клініку.

Щоб запобігти атакам програм-вимагачів, організаціям необхідно дотримуватися гігієни безпеки в локальних, хмарних і гібридних мережах аж до рівня правління. Є кілька дій, які лідери можуть вжити, щоб мінімізувати вплив і потенційні наслідки атаки.

1. Надійне резервне копіювання даних

Мета програми-вимагача — змусити жертву заплатити викуп, щоб відновити доступ до своїх зашифрованих даних. Однак це ефективно, лише якщо мета фактично втрачає доступ до своїх даних. Надійне, безпечне рішення для резервного копіювання даних є ефективним способом пом'якшити наслідки атаки програм-вимагачів.

2. Навчання кіберобізнаності

Фішингові електронні листи є одним із найпопулярніших способів поширення зловмисного програмного забезпечення з вимогою викупу. Обманом змушуючи користувача перейти за посиланням або відкрити шкідливе вкладення, кіберзлочинці отримують доступ до комп'ютера співробітника та починають процес встановлення та запуску на ньому програми-вимагача. Часте навчання з питань кібербезпеки має вирішальне значення для захисту організації від програм-вимагачів, залучаючи власний персонал як першу лінію захисту для забезпечення захищеного середовища. Цей тренінг має навчити працівників класичним знакам і мові, які використовуються у фішингових електронних листах.

3. Актуальні патчі

Оновлення комп'ютерів і застосування виправлень безпеки, особливо тих, які позначені як критичні, може допомогти обмежити вразливість організації до атак програм-вимагачів, оскільки такі виправлення зазвичай не помічаються або відкладаються занадто довго, щоб забезпечити необхідний захист.

4. Посилення аутентифікації користувачів

Застосування політики надійних паролів, вимога використання багатофакторної автентифікації та навчання співробітників щодо фішингових атак, призначених для викрадення облікових даних для входу, — усе це критично важливі компоненти стратегії кібербезпеки організації.

5. Рішення для захисту від програм-вимагачів

Ці програми відстежують запущені на комп'ютері підозрілу поведінку, яку зазвичай демонструють програми-вимагачі; якщо така поведінка буде виявлена, програма може вжити заходів, щоб зупинити шифрування, перш ніж буде завдано подальшої шкоди.

6. Використовуйте засоби запобігання загрозам на основі ШІ

Більшість атак програм-вимагачів можна виявити та усунути, поки не стане надто пізно. Автоматичне виявлення та запобігання загрозам може збільшити ваші шанси на захист, включаючи сканування та моніторинг електронних листів, а також сканування та моніторинг активності файлів на наявність підозрілих файлів. ШІ став незамінним союзником у боротьбі з кіберзагрозами. Збільшуючи рівень людського досвіду та зміцнюючи заходи захисту, керовані штучним інтелектом рішення з кібербезпеки забезпечують надійний захист від широкого спектру атак. Оскільки кіберзлочинці постійно вдосконалюють свою тактику, симбіотичний зв'язок між штучним інтелектом і кібербезпекою, безсумнівно, матиме вирішальне значення для захисту нашого цифрового майбутнього.

Хоча атаки програм-вимагачів справді можуть бути страшними, можна запобігти або принаймні зменшити їхній вплив, виконавши шість кроків, наведених вище. І перш ніж заплатити викуп, пам'ятайте, що немає гарантії, що ви повернете свої дані або що хакер не оприлюднить їх. Насправді, сплачуючи викуп, ви фінансуєте зусилля хакерів і даєте зрозуміти іншим злочинцям, що ви готові заплатити. Тож насамперед зосередьтеся на запобіганні порушенням». ***(Itai Greenberg. 6 steps to stop ransomware taking you hostage // World Economic Forum (https://www.weforum.org/agenda/2023/09/6-key-steps-ransomware/?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 20.09.2023).***

***

«Очікується, що цей рік стане другим за вартістю атак програм-вимагачів, оскільки суб'єкти загроз покладаються на нові оманливі підходи до соціальної інженерії в поєднанні зі штучним інтелектом зі зброєю. Нещодавнє порушення MGM почалося з того, що зловмисники вивчали профілі працівників служби підтримки в соціальних мережах, а потім телефонували в службу підтримки та видавали їх за них, щоб отримати облікові дані привілейованого доступу та логіни.

Безпека з нульовою довірою має бути думкою, яка пронизує все, від консолідації технологічних стеків до управління ідентифікацією в масштабі. CISO та їхні команди повинні почати з припущення, що злам уже відбувся, і мережа організації повинна бути спроектована таким чином, щоб обмежити радіус і глибину вторгнення.

«Для нульової довіри потрібен захист скрізь, а це означає, що деякі з найбільших вразливостей, як-от кінцеві точки та хмарні середовища, автоматично та завжди захищені», — сказав Капіл Райна, віце-президент із маркетингу нульової довіри та проповідник ідентифікації, хмари та спостережуваності) у CrowdStrike. «Оскільки більшість загроз проникають у корпоративне середовище або через кінцеву точку, або через робоче навантаження, захист має починатися там, а потім розвиватися, щоб захистити решту IT-стеку».

Gartner представляє новий Hype Cycle для Zero Trust Networking

Перший Hype Cycle for Zero Trust Networking від Gartner відбувається в той час, коли CISO та організації, які вони обслуговують, знаходяться в облозі майже рекордних атак програм-вимагачів. Усі цикли ажіотажу та ринкові структури мають обмеження, але вони допомагають відфільтрувати шум від постачальників і тих, хто перебільшує свої можливості нульової довіри. Hype Cycle вивчає 19 ключових технологій, включаючи мікросегментацію, мережу Kubernetes, безпечний доступ (SASE) і безпеку (SSE), і визначає рівень їх зрілості та позицію в циклі реклами.

VentureBeat вважає, що десять основних технологій у Hype Cycle мають потенціал, щоб забезпечити найбільшу цінність для CISO. Вони включають безпеку контейнерів, корпоративні браузери, мережу Kubernetes, керований SASE, мікросегментацію, OpenID Connect, віддалену ізоляцію браузера (RBI), край служби безпеки (SSE), уніфіковану безпеку кінцевих точок і стратегію нульової довіри.

Що таке мережа нульової довіри?

Gartner визначає нульової довіри (мережу ZTN) як те, як концепції нульової довіри застосовуються та інтегруються в мережеву інфраструктуру. Відповідно до стандарту безпеки NIST з нульовою довірою, ZTN надає користувачам і пристроям доступ до мережі лише на основі перевірки ідентифікації та контексту в реальному часі. Інфраструктура ZTN корпоративного класу надає доступ до автентифікованих і авторизованих ідентифікаторів і дотримується найменш привілейованого доступу до будь-якого мережевого ресурсу.

Керівники CISO кажуть VentureBeat, що чим більшого прогресу досягають їхні організації у впровадженні Zero Trust Network Access (ZTNA), тим ефективнішим стає впровадження ZTN. Мета полягає в тому, щоб захистити віртуальні команди та розширити нові проекти цифрової трансформації, щоб їх не зламали одразу після запуску. Нові програми є магнітом для атак, і ZTNA допомагає зменшити поверхню загрози та захистити від крадіжки облікових даних привілейованого доступу, одночасно посилюючи політики динамічного контролю доступу на основі ризиків.

Десять технологій нульової довіри, на які варто звернути увагу

Визначення стратегії безпеки нульової довіри, яка забезпечує швидкі перемоги, має важливе значення для контролю над бюджетами та отримання більших інвестицій. Один із керівників CISO сказав VentureBeat, що вони запланували швидкі, вимірні перемоги на початку своїх дорожніх карт нульової довіри спеціально для цієї мети. Сучасні CISO прагнуть захистити та збільшити бюджети для інвестицій у нові технології.

VentureBeat визначає десять основних технологій, які приносять найбільшу цінність для CISO, які дотримуються стратегії нульової довіри.

Безпека контейнера

Інструменти безпеки контейнерів розробників завчасно виявляють уразливості та неправильні конфігурації. Ці засоби виробництва захищають від відкритих контейнерів і скомпрометованих зображень під час виконання. Сегментація мережі та моніторинг поведінки під час виконання безпечних динамічних контейнерних середовищ. Серед провідних постачальників – Aqua Security, Orca Security, Red Hat, Sysdig, Trend Micro і Palo Alto Networks.

Корпоративні браузери

Керовані захищені браузери консолідують доступ, щоб зменшити ризик шкідливих сайтів або завантажень. Безпечний перегляд веб-сторінок стає все більш популярним серед розосереджених працівників. Деталізований контроль політики щодо веб-вмісту, завантажень і розширень є важливим. Програмне забезпечення Check Point, Ermes Cyber Security, Google, Island, Microsoft, Perception Point, Seraphic Security, SlashNext, SURF і Talon Cyber Security є одними з провідних постачальників.

Мережа Kubernetes

Мережа Kubernetes відповідає вимогам Kubernetes щодо масштабу, безпеки та видимості. Балансування навантаження, виявлення служб, підключення до кількох кластерів і мікросегментація — це ключові функції. Серед провідних постачальників Amazon Web Services, Avesha, Azure, Cisco, F5, HashiCorp, Isovalent, Juniper Networks, Tetrate і VMware.

Керував SASE

Керований SASE прискорює розгортання з інтегрованою мережею та безпекою як послугою, використовуючи ресурси та досвід постачальників. Основні переваги включають зниження ризиків щодо персоналу, швидше ввімкнення можливостей SASE та інтегроване керування. VentureBeat продовжує бачити переваги SASE від швидшої консолідації мережі та безпеки. AT&T, Cato Networks, Comcast, Expereo, KDDI, MetTel, Orange Business Services, Palo Alto Networks, Verizon, VMware і Windstream Enterprise є провідними постачальниками SASE.

Мікросегментація

Мікросегментація є основою стандарту нульової довіри NIST SP800-207 і надає багато переваг, у тому числі застосування політик доступу на основі ідентичності між робочими навантаженнями для обмеження бокового переміщення після порушень. Він також забезпечує детальне керування трафіком зі сходу на захід на основі ідентифікації робочого навантаження, а не лише зонування мережі. Серед провідних постачальників – Airgap Networks, Akamai Technologies, Cisco, ColorTokens, Fortinet, Illumio, Palo Alto Networks, VMware, Zero Networks і Zscaler.

OpenID Connect

OpenID Connect — це протокол автентифікації, який покращує взаємодію з користувачем, безпеку та конфіденційність. Він набуває поширення, щоб увімкнути єдиний вхід на всіх пристроях, програмах і API. Серед провідних постачальників – Auth0, Cloudentity, Curity, ForgeRock, Gluu, Google, IBM, Microsoft, Okta, Ping Identity і Red Hat.

Віддалена ізоляція браузера (RBI)

RBI ізолює браузери, щоб зменшити поверхню атаки шляхом дистанційного виконання веб-коду, перешкоджаючи таким загрозам, як випадкові завантаження, фішинг і викрадання даних. Провідні постачальники зосереджують свої інновації на вдосконаленні методів ізоляції та інтеграції з Secure Web Gateway (SWG) і ZTNA для вирішення більшої кількості випадків використання.

Для аналізу загроз, виявлених під час ізольованих сеансів веб-перегляду, додано детальні елементи керування завантаженням і завантаженням та інтеграцію

з Cloud Access Security Brokers (CASB), запобігання втраті даних (DLP) і пісочниці. Провідні постачальники включають Authentic8; Broadcom; Cloudflare; Ericom Software, підрозділ кібербезпеки компанії Cradlepoint; Forcepoint; гарнізонний; Безпека Менло; Netskope; Proofpoint; Skyhigh Security; і Zscaler.

Security Service Edge (SSE)

SSE об'єднує SWG, CASB і ZTNA в хмарну платформу для захисту Інтернету, SaaS і приватних додатків, забезпечуючи при цьому послідовність і масштабність керування системою. Тісна інтеграція забезпечує стандартизовані політики, автоматизовані робочі процеси та обмін даними між інтегрованими інструментами. SSE також покращує роботу віддаленого користувача завдяки уніфікованій архітектурі. SSE підвищує ефективність і узгодженість шляхом спрощення адміністрування та координації між технологіями безпеки. Серед провідних постачальників – Broadcom, Cisco, Cloudflare, Forcepoint, Fortinet, iboss, Lookout, Netskope, Palo Alto Networks, Skyhigh Security і Zscaler.

Уніфікована безпека кінцевих точок (UES)

UES поєднує в собі захист і керування кінцевими точками, щоб забезпечити політику безпеки з урахуванням ризиків і автоматизоване виправлення. Він дає змогу визначати пріоритетність виправлень на основі ризиків і безперервно перевіряти конфігурації кінцевих точок для більш ефективного керування безпекою шляхом інтеграції телеметричних даних про загрози в реальному часі в робочі процеси. Серед провідних постачальників – Absolute, BlackBerry, CrowdStrike, IBM, Ivanti, Microsoft, Sophos, Syxsense, Tanium і VMware.

Стратегія нульової довіри

Стратегія нульової довіри встановлює основи та заходи програми нульової довіри. Він забезпечує найменш привілейований доступ для кожного ресурсу та запиту ідентифікації. Це зменшує радіус вибуху вторгнень і проломів. Стратегії повинні узгоджуватися з цілями підприємства та толерантністю до ризику. Щоб стратегії нульової довіри були ефективними, їх потрібно налаштувати для кожної організації…

Прогнозування майбутнього без довіри

Масштабна атака програми-вимагача MGM, яка почалася з простого телефонного дзвінка, демонструє, наскільки важливо мати безпеку на основі ідентифікації та мікросегментацію, посилену перевіркою облікових даних у реальному часі, щоб обмежити радіус вибуху. Нульова довіра припускає, що порушення вже відбулося, і служить основою для його стримування.

Нульова довіра не є панацеєю від зловмисників, які використовують генеративний штучний інтелект для вдосконалення своєї майстерності та запускають атаки на основі соціальної інженерії, які нищать жертв. Як нещодавно сказав VentureBeat один із керівників CISO: «Нульова довіра повинна забезпечити стійкість. Це його комерційне обґрунтування, і чим стійкішим він є та здатний обмежити атаку, тим більше нульова довіра доводить його цінність як бізнес-рішення». ***(Why CISOs need zero trust as a ransomware shield // VentureBeat (https://venturebeat.com/security/why-cisos-need-zero-trust-as-a-ransomware-shield/). 18.09.2023).***

***

«Дослідники безпеки виявили інфраструктуру, що належить загрозливому суб'єкту, якого зараз відслідковують як ShadowSyndicate, який, імовірно, використовував сім різних сімей програм-вимагачів для атак протягом останнього року.

Аналітики Group-IB, які працюють разом з Bridewell і незалежним дослідником Майклом Кочварою, з різним ступенем впевненості приписують використання ShadowSyndicate програм-вимагачів Quantum, Nokoyawa, BlackCat/ALPHV, Clop, Royal, Cactus і Play у численних зломах, які спостерігалися з липня 2022 року.

Ґрунтуючись на своїх висновках, дослідники вважають, що суб'єктом загрози може бути брокер початкового доступу (IAB), хоча дані свідчать про те, що ShadowSyndicate є філією кількох операцій програм-вимагачів.

Дослідники засновують свої висновки на чіткому SSH-відбитку, який вони виявили на 85 IP-серверах, більшість із яких позначено як командні та контрольні машини Cobalt Strike.

«Ми назвали загрозу, яка використовує відбиток SSH, 1ca4cbac895fc3bd12417b77fc6ed31d ShadowSyndicate (попередня назва Infra Storm)» - Group-IB

Аналітики вперше побачили відбиток пальця 16 липня 2022 року, і він все ще використовувався в серпні 2023 року.

Команда дослідників покладалася на різні інструменти для свого дослідження, які включали механізми виявлення, такі як Shodan і Censys, а також різні методи OSINT. Це дозволило їм виявити великий слід діяльності ShadowSyndicate.

Переглядаючи сервери ShadowSyndicate, ідентифіковані на основі відбитка SSH, дослідники «натрапили на вісім різних водяних знаків Cobalt Strike [ліцензійних ключів]».

Вісім серверів Cobalt Strike спілкувалися з програмами-вимагачами Cactus, Royal, Quantum, Nokoyawa, Play, Clop і BlackCat/ALPHV, розгорнутими в різних мережах жертв.

Дослідники також виявили конфігурації Cobalt Strike, розгорнуті на двох серверах, але лише один із них на машині з SSH-відбитком ShadowSyndicate.

У деяких атаках ShadowSyndicate використовував інструмент проникнення Sliver, який раніше вважався потенційною заміною Cobalt Strike.

Інші інструменти, помічені в атаках ShadowSyndicate, включають завантажувач зловмисних програм IcedID, завантажувач Matanbuchus MaaS і корисне навантаження Meterpreter Metasploit.

Аналітики перевірили гіпотезу про те, що всі 85 серверів з однаковим відбитком ключа SSH, пов’язаного з ShadowSyndicate, підключені до одного хостинг-провайдера, але виявили 18 різних власників, 22 різні імена мережі та 13 різних місць.

Аналіз параметрів Cobalt Strike C2, таких як дата виявлення, водяні знаки або налаштування часу сну, допоміг отримати високонадійні докази, які пов'язують ShadowSyndicate із програмами-вимагачами Quantum, Nokoyawa та ALPHV/BlackCat.

Зокрема, аналітики пов'язали сервери з атакою Quantum у вересні 2022 року, трьома атаками Nokoyawa у 4 кварталі 2022 року та квітні 2023 року та атакою ALPHV у лютому 2023 року.

Group-IB і згадані сторони, що співпрацюють, знайшли додаткові докази, які менш впевнено пов'язують ShadowSyndicate із діями шкідливих програм Ryuk, Conti, Trickbot, Royal, Clop і Play.

Зокрема, щодо Клопа у звіті Group-IB згадується, що принаймні 12 IP-адрес, які раніше були пов'язані з горезвісними операторами програм-вимагачів, були передані ShadowSyndicate із серпня 2022 року та тепер використовуються для Cobalt Strike.

Незважаючи на численні висновки, які свідчать про потенційний зв'язок, достовірний прямий зв'язок між ShadowSyndicate і Clop залишається невловимим.

Експерти з розвідки Group-IB дійшли висновку, що ShadowSyndicate, ймовірно, є афілійованою компанією, яка працює з різними операціями програм-вимагачів як послуг (RaaS). Однак на підтримку цієї теорії потрібні додаткові докази.

Тим не менш, ця робота має вирішальне значення для виявлення та боротьби з кіберзлочинністю, і в цьому дусі фірма кіберрозвідки запрошує зовнішніх дослідників відкрито співпрацювати з ними та допомогти розкрити незрозумілі частини, що залишилися.

Щодо деталей, які можуть допомогти захисникам виявити та приписати дії ShadowSyndicate, Group-IB опублікувала сьогодні звіт із технічними даними свого дослідження». ***(Bill Toulas. ShadowSyndicate hackers linked to multiple ransomware ops, 85 servers // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/shadowsyndicate-hackers-linked-to-multiple-ransomware-ops-85-***

servers/?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology). 26.09.2023).

***

Програми-трояни

«Було виявлено абсолютно нового загрозливого актора, який видавав себе за Червоний Хрест, щоб розгортати троянів, здатних викрадати дані та запускати шкідливий код.

Виявлений дослідниками кібербезпеки з NSFOCUS Security Labs, загроза була названа AtlasCross і описана як така, що має «високий технічний рівень і обережне ставлення до атак».

Вектор зараження є досить старим, якщо не застарілим – за допомогою ще невідомих засобів зловмисники видають себе за некомерційну організацію, щоб поширювати документ Word із вбудованою функцією макросу. Документ, здавалося б, надходив від Червоного Хреста і містив би інформацію про донорство крові.

Дуже міцний і зрілий процес

Корпорація Майкрософт давно вимкнула макроси у файлах, завантажених з Інтернету, і користувачам потрібно буде зробити кілька додаткових кроків, щоб їх активувати.

Запуск макросу ініціював би завантаження трояна під назвою DangerAds. Це зловмисне програмне забезпечення- завантажувач, основною метою якого є виявлення хост-оточення та запуск вбудованого шелл-коду, який використовується для завантаження кінцевого корисного навантаження. Виявляючи середовище хосту, DangerAds шукатиме певні рядки в іменах користувачів і локальних доменних іменах і продовжуватиме, лише якщо їх знайде.

«Ця схема вказує на те, що зловмисник використовує цей процес атаки для проникнення всередину домену після успішного вторгнення в цільову мережу», — додали дослідники. Остаточне корисне навантаження називається AtlasAgent, і

його основна функція полягає в отриманні інформації про хост, виконанні шелл-коду, завантаженні та виконанні.

Наразі дослідники не знають, кого переслідують нападники. Вони знають, що спостережувана фішингова активність є «частиною цілеспрямованого удару зловмисника по конкретних цілях і є його основним засобом досягнення проникнення в домен».

«На поточному етапі AtlasCross має відносно обмежений обсяг діяльності, головним чином зосереджуючись на цілеспрямованих атаках на конкретні хости в межах мережевого домену», — йдеться у звіті. «Однак процеси атаки, які вони використовують, дуже надійні та зрілі». ***(Sead Fadilpašić. Phishing scam pretends to be the Red Cross to trick victims into installing malware // Future US, Inc. (https://www.techradar.com/pro/security/phishing-scam-pretends-to-be-the-red-cross-to-trick-victims-into-installing-malware). 29.09.2023).***

***

Фішингові атаки

«Зловмисник, відомий як W3LL, розробив набір для фішингу, який може обійти багатофакторну автентифікацію разом з іншими інструментами, які скомпрометували понад 8000 корпоративних облікових записів Microsoft 365.

За десять місяців дослідники з безпеки виявили, що утиліти та інфраструктура W3LL використовувалися для налаштування близько 850 фішингових дій, націлених на облікові дані для понад 56 000 облікових записів Microsoft 365.

Розвиток бізнесу

Обслуговуючи принаймні 500 кіберзлочинців, спеціальні інструменти W3LL для фішингу використовувалися в атаках на компрометацію бізнес-електронної пошти (BEC), що призвело до фінансових втрат на мільйони доларів США.

Дослідники кажуть, що інвентар W3LL охоплює майже весь ланцюжок знищення BEC і може керуватися «кіберзлочинцями будь-якого рівня технічної кваліфікації».

У сьогоднішньому звіті компанія з кібербезпеки Group-IB надає подробиці про W3LL і те, як вона стала одним із найдосконаліших розробників шкідливих програм для груп BEC.

Перше свідчення активності W3LL датується 2017 роком, коли розробник почав пропонувати спеціальний інструмент для масової розсилки електронної пошти під назвою W3LL SMTP Sender, який використовувався для спаму.

Популярність і бізнес актора почали зростати, коли він почав продавати спеціальний набір для фішингу, орієнтований на корпоративні облікові записи Microsoft 365.

У 2018 році W3LL запустила свій W3LL Store, англомовний ринок, де він міг просувати та продавати свої інструменти закритій спільноті кіберзлочинців, кажуть дослідники.

Арсенал W3LL для атак BEC

Крім панелі W3LL, яка була розроблена для обходу багатофакторної автентифікації (MFA), актор надає ще 16 інструментів, усі вони призначені для атак BEC. Каталог включає:

- Відправники SMTP PunnySender і W3LL Sender
- Зловмисне посилання W3LL Redirect
- Сканер вразливостей під назвою OKELO
- Утиліта автоматичного виявлення облікових записів під назвою CONTOOL
- Валідатор електронної пошти під назвою LOMPAT

Відповідно до Group-IB, W3LL Store пропонує рішення для розгортання атаки BEC від початкової стадії вибору жертв, фішингових приманок із вкладеними засобами (за замовчуванням або налаштованими) до запуску фішингових електронних листів, які потрапляють у вхідні скриньки жертв.

Дослідники кажуть, що W3LL достатньо навчений, щоб захистити свої інструменти від виявлення або знищення, розгортаючи та розміщуючи їх на скомпрометованих веб-серверах і службах.

Однак клієнти також мають можливість використовувати сканер OKELO від W3LL, щоб самостійно знаходити вразливі системи та отримувати до них доступ.

Обхід фільтрів і агентів безпеки

Деякі методи, які W3LL використовує для обходу фільтрів електронної пошти та агентів безпеки, включають різні методи обфускації заголовків електронної пошти та основного тексту (Punycode, теги HTML, зображення, посилання з віддаленим вмістом).

Початкові фішингові посилання також доставляються за допомогою кількох методів, які уникають виявлення. Один – через фішингові вкладення замість того, щоб вставляти їх у тіло електронного листа.

Дослідники виявили, що посилання розміщується у файлі HTML, який додається як вкладення. Коли жертва запускає шкідливий HTML, який може бути замаскований під документ або голосове повідомлення, вікно браузера відкривається з «справжньою анімацією MS Outlook».

Це фішингова сторінка W3LL Panel, яка готова збирати облікові дані облікового запису Microsoft 365.

Аналізуючи фішинговий вкладення W3LL, виявлене в дикій природі, Group-IB помітила, що це був HTML-файл, який відображав веб-сайт в iframe за допомогою JavaScript, обфускованого за допомогою кодування base64…

У новішій версії, оновленій наприкінці червня, W3LL додав кілька рівнів обфускації та кодування. Він завантажує сценарій безпосередньо з панелі W3LL, а не включає його в HTML-код…

Викрадення корпоративних облікових записів Microsoft 365

Дослідники Group-IB пояснюють, що початкове посилання у фішинговій приманці не веде на підроблену сторінку входу Microsoft 365 на панелі W3LL, і це лише початок ланцюжка перенаправлення, призначеного для запобігання виявленню фішингових сторінок панелі W3LL.

Щоб скомпрометувати обліковий запис Microsoft 365, W3LL використовує техніку супротивника/людини посередині (AitM/MitM), де зв'язок між жертвою та сервером Microsoft проходить через панель W3LL і магазин W3LL, які діють як серверна частина. система.

Мета — отримати файл cookie сеансу автентифікації жертви. Щоб це сталося, W3LL Panel має пройти кілька кроків, які включають:

- Пройдіть перевірку CAPTCHA
- Налаштуйте правильну підроблену сторінку входу
- Перевірте обліковий запис жертви
- Отримайте бренд цільової організації
- Отримайте файли cookie для процесу входу
- Визначте тип облікового запису
- Перевірте пароль
- Отримайте одноразовий пароль (OTP)
- Отримайте автентифікований сеансовий файл cookie

Після того, як W3LL Panel отримує файл cookie сеансу автентифікації, обліковий запис скомпрометовано, і жертві показується PDF-документ, щоб зробити запит на вхід легітимним.

Етап відкриття облікового запису

Використовуючи CONTOOL, зловмисник може автоматизувати пошук електронних листів, номерів телефонів, вкладень, документів або URL-адрес, які використовувала жертва, що може допомогти на стадії бічного руху.

Інструмент також може відстежувати, фільтрувати та змінювати вхідні електронні листи, а також отримувати сповіщення в обліковому записі Telegram на основі конкретних ключових слів.

Відповідно до Group-IB, типові результати такої атаки:

- Крадіжка даних
- Підроблений рахунок з платіжною інформацією зловмисника
- Видача себе за професійні послуги для надсилання шахрайських платіжних запитів клієнтам

- Класичне шахрайство BEC – доступ до топ-менеджера та дія від його імені, щоб дати вказівки працівникам здійснювати банківські перекази або купувати товари
- Розповсюджувати шкідливі програми
- Робити гроші

Звіт Group-IB глибоко занурюється в функціональність панелі W3LL, описуючи на технічному рівні, як деякі функції працюють для досягнення наміченої мети, будь то уникнення виявлення або збір даних.

Панель W3LL є перлиною корони розробника, її вартість становить 500 доларів США на три місяці та ціна оновлення 150 доларів США на місяць. Також необхідно купити ліцензію на його активацію…

Загрозливий актор W3LL існує близько п’яти років і накопичив клієнтську базу з понад 500 кіберзлочинців, які мають у своєму магазині понад 12 000 товарів на вибір.

Окрім інструментів, пов’язаних із фішингом і BEC, W3LL також надає доступ до скомпрометованих веб-сервісів (веб-оболонка, електронна пошта, системи керування вмістом) і серверів SSH і RDP, облікових записів хостингу та хмарних служб, доменів бізнес-електронної пошти, облікових записів VPN і зламаних облікових записів електронної пошти.

Дослідники Group-IB кажуть, що з жовтня 2022 року по липень 2023 року W3LL продала понад 3800 одиниць товару з орієнтовним оборотом, що перевищує 500 000 доларів США». ***(Ionut Ilascu. W3LL phishing kit hijacks thousands of Microsoft 365 accounts, bypasses MFA // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/w3ll-phishing-kit-hijacks-thousands-of-microsoft-365-accounts-bypasses-mfa/?utm_source=flipboard&utm_content=erik6408%2Fmagazine%2FCybersecurity+and+Information+Security+Articles). 06.09.2023).***

***

«Повідомлення Microsoft Teams використовуються як вектор для нової фішингової кампанії, призначеної для того, щоб змусити користувачів завантажити вкладений файл, що містить зловмисне програмне забезпечення.

Починаючи з минулого місяця, шкідливі повідомлення надсилалися з кількох скомпрометованих облікових записів Office 365. Вони містили ZIP-файл під назвою «зміни в графіку відпусток».

Якщо натиснути це, файл буде завантажено з URL-адреси SharePoint. Усередині стисненого файлу знаходиться те, що виглядає як PDF-файл, але насправді це файл LNK, який сам по собі містить небезпечний VBScript, який призводить до встановлення шкідливого програмного забезпечення, відомого як DarkGate.

Фірма з кібербезпеки Truesec розпочала розслідування кампанії та виявила, що завантаження використовує Windows cURL для отримання коду зловмисного програмного забезпечення, причому сценарій попередньо скомпільований, а небезпечні елементи приховані в середині файлу, щоб уникнути виявлення.

Сценарій також перевіряє, чи встановлено популярне антивірусне рішення Sophos на кінцевій точці жертви. Якщо ні, то додатковий код розкривається, і запускається шелл-код, щоб запустити виконуваний файл DarkGate і завантажити його в системну пам’ять.

Це не перший випадок, коли повідомлення Microsoft Teams викликають занепокоєння. Нещодавно було виявлено помилку, через яку повідомлення із зовнішніх облікових записів надходили до папки «Вхідні» організації, чого не мало бути. Схоже, ця нова кампанія DarkGate використовує цей недолік.

Корпорація Майкрософт не усунула недолік безпосередньо; все, що він зробив, це рекомендував організаціям створити списки дозволених у Teams, щоб лише певні зовнішні організації могли спілкуватися з ними, або взагалі вимкнути зовнішні зв’язки.

DarkGate існує з 2017 року, але його використання було обмежено лише невеликою кількістю кіберзлочинців проти конкретних цілей. Це потужний і всеосяжний інструмент, здатний викрадати файли, дані браузера та вміст буфера

обміну, а також здійснювати криптомайнінг, клавіатурні журнали та дистанційне керування кінцевими точками». ***(Lewis Maddison. This Microsoft Teams phishing campaign could infect your PC with malware // Future US, Inc. (https://www.techradar.com/pro/software-services/this-microsoft-teams-phishing-campaign-could-infect-your-pc-with-malware?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 11.09.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«У четвер Міністерство юстиції США оголосило про пред'явлення звинувачень дев'ятьом чоловікам у роботі на сумнозвісну мережу кіберзлочинців, яка ймовірно пов'язана з російською розвідкою, яка утримувала американські лікарні за викуп і отримала понад 100 мільйонів доларів США.

Це кульмінація багаторічного розслідування ФБР угруповання програм-вимагачів, яке присягнуло на вірність Росії, розпочавши напад на Україну минулого року, і члени якого нібито обговорювали хакерську атаку на журналіста, який розслідував отруєння критика Кремля Олексія Навального.

Згідно з обвинувачувальними документами, дев'ять чоловіків – вісім росіян і українець – залишаються на волі, але офіційні особи США сподіваються, що багатомільйонна програма винагород, яку проводить Державний департамент, може дати інформацію про місцезнаходження чоловіків, якщо і коли вони покинуть Росію.

«Доведено, що ця пропозиція є дуже цінною для нас і для наших операцій проти кіберзлочинців», — сказав CNN високопоставлений чиновник ФБР.

Міністерство фінансів також наклало санкції на чоловіків, перекривши їм доступ до долара.

Це останній крок в агресивній кампанії США та їхніх союзників за останні два роки, спрямованої на знищення банд програм-вимагачів у Росії та Східній Європі, які вивели з ладу школи та медичних закладів.

Без будь-якої співпраці з російським урядом у затриманні ймовірних кіберзлочинців Міністерство юстиції США покладалося на публічне викриття тактики хакерів, захоплення їхньої комп'ютерної інфраструктури, якщо вона розміщена на західних технологічних фірмах, і сподіваючись, що хакери підуть у відпустку до країна готова видати їх до США.

Незважаючи на тривалі шанси на арешт, у США перебувають під вартою кілька обвинувачених російських хакерів, у тому числі 42-річний чоловік, якого американський суддя засудив у четвер до дев'яти років ув'язнення за його ймовірну участь у схемі торгівлі цінними паперами на суму 93 мільйони доларів.

Американські чиновники розглядають ймовірних російських хакерів, які перебувають під вартою в США, як потенційних кандидатів у переговорах про обмін ув'язненими для американців, ув'язнених у Росії.

Дев'ять чоловіків, чиї звинувачення були розкриті в четвер, нібито використовували два типи хакерських інструментів, пов'язаних з російськомовними кіберзлочинцями: один, відомий як TrickBot, для початкового злому жертв, а інший, відомий як Conti, щоб блокувати їхні комп'ютери та вимагати непомірні платежі. (Люди, пов'язані з TrickBot і Conti, збігаються, і офіційні особи США іноді називають їх окремою бандою.)

За словами високопоставленого чиновника ФБР, програмне забезпечення-вимагач Conti використовувалося в сотнях організацій по всьому світу, включаючи майже 300 у США. Згідно з розкритими в четвер звинуваченнями, це включає відділ шерифа та службу екстреної медичної допомоги в Теннессі.

За даними британських чиновників, Conti зібрали 180 мільйонів доларів у вигляді викупу, оперативники також оголосили про санкції проти деяких імовірних кіберзлочинців у четвер.

У лютому 2022 року угруповання Conti зібрало міжнародні заголовки, коли пообіцяло «повну підтримку» російського уряду під час нападу на Україну.

Український дослідник кібербезпеки у відповідь оприлюднив тисячі внутрішніх документів групи, включно з доказами, які свідчать про те, що оперативники Conti мають контакти в російському уряді.

Тоді український дослідник розповів CNN, що агент ФБР зв'язався з ним, щоб сказати припинити витік інформації. Теоретично викриття інфраструктури Conti могло б ускладнити ФБР відстеження групи, оскільки це могло створити нові комп'ютерні системи. ФБР відмовилося коментувати будь-яку взаємодію з дослідником.

Код Conti не використовувався в останніх атаках програм-вимагачів, але це не означає, що хакери мовчали. «Конті пішов, але актори не обов'язково», - визнав високопоставлений чиновник ФБР.

Представник ФБР відмовився коментувати поточне місцеперебування дев'ятьох нових обвинувачених осіб або те, як ФБР їх стежить. «Це триває. Ми ще не закінчили з цим». ***(Sean Lyngaas. US indicts nine alleged members of Russian cybercrime gang that targeted hospitals // Cable News Network. (https://edition.cnn.com/2023/09/07/politics/us-indicts-alleged-cybercriminals?utm_source=flipboard&utm_content=user%2FCNN). 07.09.2023).***

***

«На початку цього тижня Міністерство юстиції висунуло звинувачення дев'ятьом російським громадянам, які, за їх словами, використовували російське шкідливе програмне забезпечення в кібератаках, щоб викрасти гроші американських компаній, урядів і шкільних округів.

За даними Міністерства юстиції, Михайло Царьов, Андрій Жуйков, Максим Галочкін, Дмитро Путлін, Сергій Логунцов, Макс Михайлов, Макіс Руденський, Валентин Карягін і Маским Халіуллін нібито використовували шкідливі інструменти Trickbot і Conti для проникнення на пристрої американців.

Обвинувачені стоять за «одним із найпоширеніших варіантів програм-вимагачів, які використовуються для кібератак у Сполучених Штатах, включаючи атаки на місцеві поліцейські відділи та служби екстреної медичної допомоги»,

заявив генеральний прокурор Меррік Гарленд у заяві, опублікованій Міністерством юстиції.

Згідно з одним обвинуваченням, розкритим у Північному окрузі Огайо, дев'ять чоловіків нібито заразили комп'ютери жертв шкідливим програмним забезпеченням Trickbot, призначеним для захоплення особистих даних жертв, таких як банківські облікові дані, а також паролі та ідентифікаційні дані для таких речей, як кредитні картки та електронні листи. Потім хакери заразили інші комп'ютери та використали облікові дані для входу, щоб викрасти кошти з банківських рахунків жертв, а потім встановили програми-вимагачі на комп'ютери жертв, йдеться в обвинуваченні.

Програми-вимагачі – це різновид зловмисного програмного забезпечення, яке загрожує оприлюднити особисті дані жертви або заблокувати доступ, якщо викуп не буде сплачено.

Згідно з обвинуваченням, обвинувачені надсилали фішингові листи компаніям із вбудованим шкідливим посиланням або вкладеним файлом. Коли нічого не підозрююча особа клацне на ньому, це заражатиме його мережу.

Потім чоловіки просили гроші, щоб розблокувати систему, згідно з документами. Чоловіки підтримували програмне забезпечення, яке ФБР вивело з мережі минулого року, починаючи з 2015 року, повідомило міністерство юстиції.

Згідно з судовими документами, обвинувачені переводили гроші з рахунку компанії, використовуючи викрадену банківську інформацію, яку вони отримали під час розгортання шкідливого програмного забезпечення.

«Сьогоднішнє оголошення свідчить про нашу постійну відданість притягненню до відповідальності найогидніших кіберзлочинців – тих, хто присвятив себе завданню шкоди американській громадськості, нашим лікарням, школам і підприємствам», – сказав директор ФБР Крістофер Рей у заяві Міністерства юстиції.

«Кіберзлочинці знають, що ми використовуватимемо всі законні засоби, які є в нашому розпорядженні, щоб ідентифікувати їх, невтомно переслідувати їх і перешкоджати їхній злочинній діяльності. Ми, разом із нашими федеральними та

міжнародними партнерами, продовжуватимемо стягувати витрати через спільні операції незалежно від того, де ці злочинці намагатимуться сховатися», – додав Рей.

У своїй заяві Гарленд зазначив, що звинувачення, висунуті проти чоловіків, показують, «що вони не можуть сховатися від Міністерства юстиції Сполучених Штатів».

Декільком обвинуваченим висунули звинувачення в кіберзлочинах у Теннессі та Каліфорнії, а також в Огайо.

Звинувачення в Південному окрузі Каліфорнії стверджує, що Галочкін, один із організаторів змови, зламав мережу Scripps Healthcare за допомогою шкідливого програмного забезпечення Conti, відгалуження шкідливого програмного забезпечення Trickbot. За допомогою злому Scripps Healthcare вони пошкодили комп'ютери понад 900 людей, йдеться в звинуваченні. Хакери також викрали дані 150 000 пацієнтів, повідомляє Scripps Healthcare.

Згідно з судовими документами, злом Scripps Healthcare призвело до затримки отримання інформації про пацієнтів і оглядів.

Федеральне велике журі в Середньому окрузі штату Теннессі повернуло обвинувальний акт, який звинувачує Галочкіна, Руденського, Царьова та Жуйкова у змові з метою використання того самого програмного забезпечення-вимагача Conti для нападу на підприємства, некомерційні організації та уряди в США протягом двох років, починаючи з 2020 року.

Згідно з даними Міністерства юстиції, усі вони перебувають у Росії та не мають американських адвокатів.

Джавед Алі, колишній старший директор з боротьби з тероризмом у Раді національної безпеки, сказав ABC News, що малоймовірно, що ці чоловіки коли-небудь постануть перед судом, але їхня можливість виїжджати за межі Росії зараз серйозно обмежена.

«Останні висунуті Міністерством юстиції звинувачення дев'яти особам, пов'язаним з російською хакерською групою Trickbot, підкреслюють, що Сполучені Штати продовжують використовувати розслідування правоохоронних

органів і кримінальне переслідування як політичний інструмент для здійснення тиску та притягнення злочинців до відповідальності за кібератаки з використанням програм-вимагачів. та інші методи», - сказав Алі, який зараз є доцентом Школи публічної політики Форда Мічиганського університету.

«За останні кілька років Сполучені Штати висунули аналогічні обвинувачення проти інших східноєвропейських кіберзлочинців, які також включали екстрадицію деяких із цих осіб, щоб фактично постати перед кримінальним судом тут». ***(Luke Barr. 9 Russians charged with cyberattacks targeting US companies // ABC News Internet Ventures (https://abcnews.go.com/Politics/9-russians-charged-cyberattacks-targeting-us-companies-doj/story?id=103033736&utm_source=flipboard&utm_content=Insights2016%2Fmagazine%2FUKRAINE+SOVEREIGNTY+%3ARUSSIAN+%2CCHECHEN+%2CIRANIAN+%26+BELARUS+AGGRESSION+202++3%F0%9F%87%BA%F0%9F%87%A6%F0%9F%87%BA%F0%9F%87%A6%F0%9F%87%BA%F0%9F%87%A6). 08.09.2023).***

***

Технічні аспекти кібербезпеки

«Якщо ви перебуваєте поза домом і не користуєтеся мобільним широкосмуговим зв'язком, громадський Wi-Fi є одним із ваших єдиних варіантів.

Майже напевно, що в якийсь момент вам знадобиться підключитися до публічної Wi-Fi. На щастя, більшість постачальників публічних точок доступу Wi-Fi роблять їх «відкритими», що означає, що будь-хто може приєднатися до мережі без пароля. Однак це має свою ціну. Коли ви перебуваєте в мережі, зловмисники, як-от хакери та викрадачі особистих даних, можуть атакувати ваші дані.

У цьому посібнику ви дізнаєтеся про 5 основних способів, за допомогою яких хакери намагатимуться зламати вашу особисту інформацію, і про те, як захистити

себе. Також не забудьте приділити трохи часу, щоб прочитати наш посібник про те, навіщо потрібен VPN під час доступу до загальнодоступної мережі Wi-Fi.

1. Підробка ARP

Коли ви підключаєтеся до загальнодоступної мережі Wi-Fi для доступу в Інтернет, ви ніколи не знаєте, хто ще підключений до неї.

Якщо хакер підключає свій пристрій до тієї ж мережі, що й ви, він може використати отруєння протоколу розпізнавання адрес (ARP), щоб спробувати отримати доступ до ваших даних.

Хакер може використовувати спеціальні інструменти для сканування вашого пристрою, загальнодоступної мережі Wi-Fi на предмет унікальної IP-адреси а також основного маршрутизатора Wi-Fi. Надсилаючи фальшиві ARP-повідомлення, вони можуть виявити MAC-адресу (Media Access Control) як вашого пристрою, так і маршрутизатора. Це дозволяє хакеру видавати себе за ваш пристрій і таємно отримувати всі дані, які передаються між вами та веб-сайтами, які ви відвідуєте.

Ці типи атак відомі як атаки «Людина посеред» і залишають вас уразливими, лише якщо веб-сайти чи служби, до яких ви підключені, не використовують шифрування.

Ви можете захистити себе, коли вам потрібно використовувати публічну Wi-Fi, переконавшись, що ви отримуєте доступ лише до сторінок, захищених шифруванням SSL/TLS. А ще краще, зареєструйтеся в будь-якій із найкращих служб VPN, і всі ваші дані в Інтернеті будуть зашифровані, перш ніж вони покинуть ваш пристрій, що значно ускладнить доступ до них для хакерів.

2. Отруєння DNS

Отруєння DNS або «спуфінг DNS» може бути надзвичайно небезпечним типом атаки, оскільки більшість людей не підозрюють про це.

DNS- сервери діють як свого роду віртуальна телефонна книга для Інтернету. Вони беруть зрозумілі людині назви веб-сайтів, які ви вводите в адресний рядок, наприклад, www.techradar.com, і перетворюють їх на машинозчитувані IP-адреси.

Удома ваш інтернет-провайдер зазвичай надає вам DNS-сервери, які допомагають спрямовувати ваші запити на з'єднання, але якщо зловмиснику вдасться отримати доступ до вашого пристрою, наприклад через ARP Spoofing, або втрутитися в публічний маршрутизатор Wi-Fi, ви можете легко ввести адресу легітимний веб-сайт, наприклад www.amazon.com, який перенаправляється на фішинговий сайт, створений хакером.

В адресному рядку все ще відображається правильна веб-адреса веб-сайту, який ви хочете відвідати, тож ви нічого не зрозумієте, коли введете свої паролі чи іншу конфіденційну інформацію.

Ви можете налаштувати власну мережу Wi-Fi на використання більш безпечної форми DNS, як-от DNSSEC, або використовувати загальнодоступний DNS-сервер, як-от запропонований Google. Однак, якщо ви використовуєте загальнодоступний Wi-Fi, ви не можете робити ці дії.

Найпростіший спосіб убезпечитися — використовувати надійного постачальника VPN, наприклад ExpressVPN, який направляє всі запити на підключення через власні сервери, звідки б ви не підключалися.

3. Видалення SSL

Коли зловмисник підключений до тієї ж мережі Wi-Fi, що й ви, він може використовувати видалення SSL, щоб відкрити ваші конфіденційні особисті дані.

SSL/TLS — це набір протоколів безпеки, які шифрують з'єднання між вашим пристроєм і веб-сервером. Отже, якщо ваші дані буде перехоплено, хакеру буде майже неможливо їх прочитати. Ви можете дізнатися більше в нашому посібнику Що таке TLS і як він працює?

Якщо хакер може маніпулювати вашим з'єднанням, наприклад, за допомогою ARP Poisoning, він може спробувати змусити ваш пристрій використовувати незашифровані версії безпечних веб-сайтів, а не захищені сертифікатом SSL.

Якщо ви використовуєте загальнодоступну Wi-Fi, будьте в безпеці, перевіряючи, щоб кожен веб-сайт, який ви використовуєте, починався з «https://» в адресному рядку, а не з «http://». Більшість браузерів також відображають замок біля адресного рядка, щоб показати, що сайт безпечний.

Майже всі найкращі браузери тепер можна налаштувати на використання лише захищених з'єднань HTTPS, де вони доступні.

Всесвітня павутина повільно починає створювати безпечні веб-сайти, але тим часом за допомогою VPN увесь ваш трафік зашифровано, як HTTP, так і HTTPS.

4. Шкідливе програмне забезпечення

Хакери можуть впровадити зловмисне програмне забезпечення на ваш пристрій через незахищену мережу та іншими способами. Наприклад, якщо ви клацнете посилання з підозрілого електронного листа. Вони також можуть намагатися активно зламати ваш пристрій, але вони, швидше за все, використовуватимуть такі методи, як ARP Spoofing і DNS Poisoning, щоб перенаправити вас за шкідливими посиланнями, які завантажать шкідливе програмне забезпечення на ваш пристрій.

Це дуже небезпечно, оскільки зловмисник не тільки може отримати доступ до всіх даних на вашому пристрої, але й після зараження комп'ютера він цілком може отримати до нього доступ, навіть якщо ви від'єднаєтеся від загальнодоступної точки доступу Wi-Fi і під'єднаєтеся до іншої, скажімо, у твій дім. На щастя, найкращий засіб для видалення зловмисного програмного забезпечення має працювати з більшістю форм шкідливого програмного забезпечення на вашому комп'ютері.

Для додаткової безпеки ми рекомендуємо вибрати будь-який із найкращих блокувальників реклами, щоб запобігти завантаженню більшості шкідливих посилань на зловмисне програмне забезпечення. І обов'язково встановіть та оновіть найкраще антивірусне програмне забезпечення для свого пристрою (так, навіть якщо ви використовуєте Apple Mac).

5. Медовий горщик

Враховуючи, наскільки популярним є публічний Wi-Fi, деякі хакери та викрадачі особистих даних йдуть далі, створюючи власну точку доступу «приманка» або «злий близнюк». Сьогодні це дуже легко зробити, використовуючи обладнання, яке є у вільному доступі в Інтернеті, і це має дуже страшні наслідки.

В аеропорту хакер може налаштувати незахищену бездротову мережу під назвою «FREE AIRPORT Wi-Fi». Тоді особа, яка налаштувала мережу, збиратиме дані кожного, хто підключається до цієї мережі.

Перший спосіб убезпечитися — перевірити в адміністрації приміщення, чи ви маєте правильну назву мережі Wi-Fi.

Знову ж таки, якщо ви використовуєте захищену VPN для підключення до Інтернету, увесь ваш трафік зашифровано, включаючи запити DNS для відвідування веб-сайтів незалежно від того, у якій мережі ви перебуваєте. Це ускладнить зловмиснику отримання будь-якої корисної інформації про вас, навіть якщо ви випадково підключилися до honeypot». ***(Nate Drake. 5 ways hackers can steal your data on public Wi-Fi // Future US, Inc. (https://www.techradar.com/pro/vpn/5-ways-hackers-can-steal-your-data-on-public-wi-fi?utm_source=flipboard&utm_content=aj7iohv%2Fmagazine%2FCONCEPT+%21++++++++++++++++++SPACE+%21++++++++++++++++++++++++++++++++++++TECH+.+.+.). 08.09.2023).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Численні хакерські групи національних держав використовують відомі недоліки в програмному забезпеченні Zoho ManageEngine і брандмауерах Fortinet, для яких доступні виправлення, попереджають представники кібербезпеки.

У новому попередженні Агентство з кібербезпеки та безпеки інфраструктури США надає подробиці того, як обидві вразливості використовуються за допомогою розслідування, яке воно проводило з лютого по квітень в неназваній організації в авіаційному секторі.

CISA виявила, що, починаючи з січня, кілька груп APT окремо використовували дві різні критичні вразливості для отримання несанкціонованого доступу та вилучення даних з організації.

Обидва непов'язані недоліки – CVE-2022-47966 у Zoho ManageEngine та CVE-2022-42475 у Fortinet FortiOS SSL VPN – були класифіковані як такі, що мають критичний рівень серйозності, тобто їх можна використати для віддаленого виконання коду, дозволяючи зловмисникам отримати контроль над систему та перейти до інших частин мережі. Кожен із постачальників наприкінці 2022 року випустив оновлення, виправляючи свої недоліки. Дослідники називають їх уразливістю N-day, що означає відомі недоліки, на відміну від уразливостей нульового дня, для яких ще немає виправлень.

У попередженні, опублікованому CISA, ФБР і Кібернаціональними силами кіберкомандування США, міститься інформація про те, як зловмисники використовували кожну з вад, щоб отримати ширший доступ до мереж жертв. У повідомленні не зазначено, яка нація чи групи APT були пов'язані з відомими використанням цих недоліків. Звіти приватного сектору раніше прив'язували хакерів, пов'язаних із Китаєм, Іраном і Північною Кореєю, до відомих випадків використання цих вразливостей.

Ціль: Zoho ManageEngine

У жовтні минулого року Zoho попередив, що кілька продуктів ManageEngine OnPremise, включаючи такі інструменти управління IT, як ServiceDesk Plus і Vulnerability Manager Plus, мають «уразливість неавтентифікованого віддаленого виконання коду» — CVE-2022-47966 — через використання «застарілої третьої сторони». залежність» за участю Apache Santuario. Постачальник випустив виправлення для постраждалих продуктів у жовтні та листопаді минулого року. 19 січня з'явився тестовий код для використання вади.

У випадку зі зламаною аеронавігаційною компанією, у звіті CISA та інших урядових розслідувачів США йдеться, що зловмисники використали вразливість 20 січня, щоб отримати кореневий доступ до веб-сервера фірми, на якому розміщено загальнодоступну програму Zoho ManageEngine ServiceDesk Plus. Звідти

зловмисники завантажували подальше зловмисне програмне забезпечення, досліджували мережу, використовували Mimikatz для викрадення облікових даних адміністратора, встановлювали варіант Metasploit під назвою Meterpreter, додавали постійність через SSH, запускали з'єднання протоколу віддаленого робочого столу тощо.

Урядові слідчі «не змогли визначити, чи була конфіденційна інформація доступна, змінена чи викрадена», йдеться у звіті. «Це сталося через те, що організація не чітко визначила, де їхні дані розташовані в центрі, а CISA мала обмежене покриття мережевих датчиків».

Хоча у звіті не згадується причина атаки, Microsoft повідомила, що іранські хакери почали запускати атаки, націлені на вразливість, того самого дня, коли було опубліковано код POC. Технологічний гігант простежив деякі з цих атак до групи з кодовою назвою Mint Sandstorm, яка включає участь Корпусу вартових ісламської революції та також відома як APT42, Cobalt Illusion і TA453.

«Виправлення цієї вразливості є корисним за межами цієї конкретної кампанії, оскільки кілька зловмисників використовують CVE-2022-47966 для початкового доступу», — повідомила тоді Microsoft.

Зловмисники продовжували зловживати недоліком. Минулого місяця Cisco Talos детально розповіла про шпигунську кампанію, яка, здається, вела до північнокорейської Lazarus Group і була спрямована на вразливість Zoho ManageEngine для розгортання трояна під назвою QuiteRAT. У Cisco Talos повідомили, що кампанія почалася в травні та, здається, була зосереджена на ураженнях магістральної інфраструктури Інтернету та медичних установ США та Європи.

Ціль: Fortinet FortiOS

Авіаційна компанія також стала жертвою атаки, запущеної не тією групою, яка використовувала її програмне забезпечення Zoho ManageEngine, яка отримала доступ до брандмауера Fortinet, повідомляє CISA.

Експлуатована вразливість CVE-2022-42475 у пристроях FortiOS SSL VPN є «вразливістю переповнення буфера на основі динамічної пам'яті», яку

зловмисники можуть використовувати для віддаленого виконання коду або команд, повідомила Fortinet під час випуску виправлень для цієї вади 12 грудня 2022 року. При цьому час, він сказав, що вразливість вже активно використовується в дикій природі.

Хакер авіаційної фірми скористався недоліком, щоб отримати доступ до брандмауера організації, а потім створив кілька VPN-з'єднань із завідомо зловмисних IP-адрес, повідомляє CISA. Зловмисники також використовували законні облікові дані для вимкненого облікового запису адміністратора, який раніше був призначений колишньому підряднику, виявили слідчі.

«Організація підтвердила, що користувача було вимкнено до спостережуваної активності», — повідомили вони, додавши, що зловмисники повторно активували обліковий запис, а також видалили журнали з кількох серверів. «Це запобігло можливості виявити подальшу експлуатацію або викрадання даних», що посилилося через те, що організація не змогла ввімкнути протоколювання IP-адрес трансляції мережевої адреси, сказали вони. Зберігання IP-журналів NAT допомагає дослідникам відстежувати, як пакети надходять із зовнішніх IP-адрес і портів до внутрішніх клієнтів.

Як і у випадку з використанням уразливості Zoho, у звіті атака не приписується жодній групі APT. Кілька груп можуть бути спрямовані на цей недолік.

У січні минулого року відділ реагування на інциденти Google Mandiant повідомив про атаки, націлені на вразливість FortiOS SSL-VPN Fortinet, яка, як підозрюється, пов'язана з китайською хакерською групою. «Цей інцидент продовжує китайську схему використання пристроїв, що виходять в Інтернет, зокрема тих, що використовуються для цілей керованої безпеки», включаючи брандмауери, системи запобігання та виявлення вторгнень тощо, повідомляє Mandiant.

«Докази свідчать про те, що експлуатація мала місце ще в жовтні 2022 року», — сказав Мандіант, додавши, що «ідентифіковані цілі включають європейську державну установу та керованого постачальника послуг, розташованого в Африці».

Повторні цілі

Це не перший раз, коли зловмисники націлюються на вразливості, для яких доступні виправлення в продуктах Zoho ManageEngine і Fortinet SSL VPN. Минулого місяця США та їхні партнери по розвідці «П'ять очей» – Австралія, Канада, Нова Зеландія та Велика Британія – випустили спільну консультацію щодо безпеки, в якій детально описано 12 уразливостей, які злочинці та групи APT найчастіше використовували у 2022 році (див.: Patching Conundrum: 5- Year- Old Flaw Again очолює список найпопулярніших).

Одним із них є неправильна помилка автентифікації в Zoho ManageEngine, позначена CVE-2021-40539, яку постачальник виправив у вересні 2021 року.

Ще одна з 12 найпоширеніших уразливостей — це помилка проходження шляху у Fortinet SSL VPN, позначена як CVE-2018-13379, яку постачальник виправив у травні 2019 року.

Чотири роки по тому, попередили чиновники, зловмисники продовжують зловживати недоліком FortiOS, щоб отримати легкий доступ до корпоративних мереж. «Постійна експлуатація вказує на те, що багато організацій не змогли вчасно виправити програмне забезпечення та залишаються вразливими для зловмисників», — йдеться в повідомленні». ***(Mathew J. Schwartz. Feds Urge Immediate Patching of Zoho and Fortinet Products // Information Security Media Group, Corp. (https://www.databreachtoday.com/feds-urge-immediately-patching-zoho-fortinet-products-a-23038?utm_source=flipboard&utm_content=AWC%2Fmagazine%2FOur+Electronic+%26+Digital+Lives.). 08.09.2023).***

***

«У четвер Cisco підтвердила існування невиправленої вразливості нульового дня, яку хакери використовують для отримання несанкціонованого доступу до двох широко використовуваних пристроїв безпеки, які вона продає.

Уразливість міститься в програмному забезпеченні Cisco Adaptive Security Appliance і його Firepower Threat Defense, які зазвичай скорочено називають ASA та

FTD. Cisco та дослідники з минулого тижня знали, що злочинний синдикат програм-вимагачів під назвою Akira отримував доступ до пристроїв за допомогою розпилення паролів і грубої форсування. Розпорошення паролів, також відоме як надсилання облікових даних, передбачає спробу кількох часто використовуваних паролів для великої кількості імен користувачів, щоб запобігти виявленню та наступному блокуванню. Під час атак методом грубої сили хакери використовують значно більший масив підгаданих паролів проти більш обмеженої кількості імен користувачів.

Атаки тривають (принаймні) з березня

«Зловмисник може використати цю вразливість, вказавши профіль підключення/групу тунелів за замовчуванням під час проведення атаки грубою силою або під час встановлення безклієнтського сеансу SSL VPN з використанням дійсних облікових даних», — написали представники Cisco в повідомленні. «Успішний експлойт може дозволити зловмиснику досягти одного або обох із наведеного нижче:

Визначте дійсні облікові дані, які потім можна використати для встановлення неавторизованого сеансу VPN віддаленого доступу.

Встановіть безклієнтський сеанс SSL VPN (тільки під час запуску програмного забезпечення Cisco ASA версії 9.16 або ранішої).

ASA — це універсальний пристрій безпеки, який забезпечує брандмауер, антивірус, захист від вторгнень і захист віртуальної приватної мережі. FTD — це пристрій Cisco наступного покоління, який поєднує в собі можливості ASA з більш детальною консоллю керування та іншими розширеними функціями. Уразливість, яка відстежується як CVE-2023-20269, виникає внаслідок неправильного розподілу на пристроях функцій автентифікації, авторизації та обліку під час віддаленого доступу між функціями VPN, керування HTTPS і VPN між сайтами. Він має рейтинг серйозності 5,0 з 10 можливих.

Минулого тижня дослідники з охоронної фірми Rapid7 повідомили, що вони спостерігали атаки з використанням облікових даних і грубою силою проти пристроїв ASA принаймні з березня минулого року. За словами дослідників, атаки

виходили з Akira та були націлені на пристрої, які не мали багатофакторної автентифікації для деяких або всіх користувачів.

«Rapid7 виявив принаймні 11 клієнтів, які зіткнулися з вторгненнями, пов'язаними з Cisco ASA, у період з 30 березня по 24 серпня 2023 року», — йдеться в повідомленні від 29 серпня під заголовком «В облозі: спостережувана Rapid7 експлуатація Cisco ASA SSL VPN». «Наша команда відстежила зловмисну активність до пристрою ASA, який обслуговує SSL VPN для віддалених користувачів. Патчі пристроїв ASA відрізнялися для зламаних пристроїв — Rapid7 не визначив жодної конкретної версії, яка була б надзвичайно сприйнятливою до експлуатації».

Атаки, як показано на зображенні, включеному в публікацію Rapid7, часто спрямовували кілька спроб входу на ціль у швидкій послідовності. Хоча обидві спроби входу, зафіксовані в зображеному журналі активності, були невдалими, у деяких випадках зловмисники «успішно пройшли автентифікацію з першої спроби, що може означати, що облікові записи жертви використовували слабкі облікові дані або облікові дані за замовчуванням».

Дослідники продовжили:

У більшості інцидентів, які ми розслідували, зловмисники намагалися ввійти в пристрої ASA за допомогою загального набору імен користувачів, зокрема:

адмін

adminadmin

адміністратор резервного копіювання

час

cisco

гість

облік

розробник

користувач ftp

навчання

тест

принтер

луна

безпеки

інспектор

тестовий тест

snmp

Вище наведено досить стандартний список облікових записів, які можуть вказувати на використання інструменту підбору. У деяких випадках імена користувачів під час спроб входу належали фактичним користувачам домену. Хоча ми не маємо конкретних доказів витоку облікових даних жертви, ми усвідомлюємо, що можлива спроба підбору послуги Cisco ASA за допомогою шляху +CSCOE+/logon.htm. Назви груп VPN також відображаються у вихідному коді сторінки входу в кінцеву точку VPN і можуть бути легко витягнуті, що може допомогти в атаках підбір.

Після успішної автентифікації внутрішніх активів зловмисники розгорнули set.bat. Виконання set.bat призвело до встановлення та запуску програми віддаленого робочого столу AnyDesk із встановленим паролем greenday#@!. У деяких випадках nd.exe запускався в системах для створення дампу NTDS.DIT, а також вуликів SAM і SYSTEM, що могло надати зловмиснику доступ до додаткових облікових даних користувача домену. Зловмисники здійснили подальше бічні переміщення та двійкові виконання в інших системах у цільових середовищах, щоб збільшити обсяг компрометації. Як згадувалося раніше, кілька вторгнень завершилися розгортанням і запуском двійкових файлів програм-вимагачів, пов’язаних із Akira або LockBit.

Далі дослідники опублікували посібник зі злому корпоративних облікових записів, рекламованих на продаж на кримінальних форумах. У посібнику продавець стверджував, що скомпрометував 4865 служб Cisco SSL VPN і 9870 служб Fortinet VPN за допомогою комбінації імені користувача та пароля test:test. У дописі було припущення, що розповсюдження посібника сприяло сплеску атак облікових даних на Cisco ASA.

Звіт Rapid7 був опублікований через п’ять днів після того, як головний інженер групи реагування на інциденти безпеки продукту Cisco попередив клієнтів, що компанія знала про атаки облікових даних на ASA. Він порадив клієнтам використовувати надійні паролі та застосовувати MFA для всіх користувачів.

Наразі невідомо, коли буде випущено патч для CVE-2023-20269. У повідомленні Cisco у четвер сказано, що на додаток до наведених вище вказівок щодо паролів і MFA, клієнти можуть вжити таких кроків, щоб захистити себе від поточних атак:

Налаштуйте політику динамічного доступу для припинення встановлення тунелю VPN, коли використовується профіль підключення/група тунелю DefaultADMINGroup або DefaultL2LGroup

Заборонити віддалений доступ VPN за допомогою елемента керування груповою політикою за замовчуванням

Обмежити користування у ЛОКАЛЬНІЙ базі даних користувачів

Блокувати користувачів лише до певного профілю підключення/групи тунелів

Заборонити користувачам встановлювати сесії VPN віддаленого доступу

Обхідні шляхи можливі не у всіх випадках. Інструкції та додаткові відомості доступні в публікації в четвер. Однак найефективнішим захистом залишається суворе дотримання MFA, оскільки ця вимога запобігатиме доступу, навіть якщо зловмисник володіє правильною комбінацією імені користувача та пароля». ***(Dan Goodin. Cisco security appliance 0-day is under attack by ransomware crooks // Condé Nast (https://arstechnica.com/security/2023/09/ransomware-crooks-exploit-unpatched-0-day-in-cisco-security-appliances/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 08.09.2023).***

***

«У багатьох найкращих веб-переглядачах та інших програмах є серйозний недолік безпеки, який потрібно усунути якомога швидше, щоб запобігти атаці хакерів на ваш пристрій.

Уразливість, яка відстежується як CVE-2023-4863, спричинена переповненням буфера купи в бібліотеці коду WebP (libwebp) і може призвести до збою вашої системи або виконання довільного коду в разі використання.

Постраждалі програми включають Chrome, Firefox, Brave і Edge, а також інші програми, такі як Telegram, Thunderbird і Gimp.

Більшість браузерів на базі Chromium випустили свої оновлення, включно з чотирма згаданими вище, тоді як очікується, що інші незабаром випустять виправлення. Ми радимо вам стежити за сповіщеннями про оновлення та якнайшвидше застосувати виправлення для веб-переглядача.

Переповнення буфера купи дозволяє зловмиснику заповнити область пам'яті системи зловмисною діяльністю, у свою чергу дозволяючи йому взяти під контроль пристрій, отримати дані або просто поширити зловмисне програмне забезпечення.

Алекс Іванов із Stack Diary, який, поряд із поглибленим технічним поясненням недоліку, також зазначив, що вразливість вплинула не лише на браузери, зауважив, що Apple виправила macOS Ventura, щоб усунути недолік у версії 13.5.2.

Команда безпеки та архітектури Apple (SEAR) і Citizen Lab школи Мунка Університету Торонто вперше повідомили про помилку 6 вересня.

Відмова від оновлення може призвести до пошкодження комп'ютера жертви та навіть до втрати особистих даних». ***(Craig Hale. Huge security breach affects Chrome, Firefox, Brave, Edge, and plenty more apps besides - here's what you need to know // Future US, Inc. (https://www.techradar.com/pro/security/huge-security-breach-affects-chrome-firefox-brave-edge-and-plenty-more-apps-besides-heres-what-you-need-to-know?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 14.09.2023).***

***

«Експерти попереджають, що помилка в графічних процесорах усіх основних виробників може дозволити хакерам читати конфіденційні дані, що відображаються в браузерах.

Уразливість, про яку йдеться, називається GPU.zip і дозволяє здійснювати перехресні атаки. По суті, хакер може створити зловмисний веб-сайт, який відстежує, скільки часу потрібно графічному процесору для відтворення окремого веб-сайту, і використовувати цю інформацію для реконструкції другої сторінки, піксель за пікселем. Таким чином шкідливий веб-сайт міг читати конфіденційний вміст, наприклад імена користувачів, паролі та інші конфіденційні дані….

Однак постачальники графічних процесорів применшують важливість висновків і стверджують, що це не те, що потребує вирішення - принаймні не з їхнього боку.

Навіть засоби масової інформації припускають, що зловживання вразливістю є довгостроковою спробою, оскільки для успішної атаки потрібно виконати багато умов.

По-перше, веб-переглядач має дозволяти завантажувати фрейми iframe із перехресним походженням із файлами cookie, фільтри SVG для їх відтворення та делегувати завдання відтворення графічному процесору. Варто також зазначити, що недолік працює лише в браузерах Chrome і Edge; І Safari, і Firefox безпечні.

Google уже відповів на претензії, заявивши, що «широко поширені заголовки можуть запобігти вбудовуванню сайтів, що запобігає цій атаці», додавши, що він не планує вносити будь-які зміни.

Intel також додала, що проблема не в самих графічних процесорах, а в програмному забезпеченні сторонніх розробників, і тому не буде вживати заходів. Для Qualcomm «проблема не в нашій моделі загроз», оскільки її «може вирішити програма браузера». ***(Sead Fadilpašić. Almost all top GPUs are at risk of this dangerous cyberattack - here's what you need to know // Future US, Inc. (https://www.techradar.com/pro/security/almost-all-top-gpus-are-at-risk-of-this-dangerous-cyberattack-heres-what-you-need-to-***

know?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 27.09.2023).

***

«Google надав уже відомій вразливості безпеки новий ідентифікатор CVE з найвищим рівнем серйозності. Причиною цього є те, що вразливість, спочатку класифікована як помилка Chrome, впливає на значно більше програм, оскільки натомість це вразливість WebP.

Формат файлу зображень WebP особливо популярний в Інтернеті, оскільки він пропонує хороший баланс між розміром і якістю зберігання. Але вразливість дозволяє зловмисникам використовувати спеціально створене зображення WebP для створення переповнення буфера купи та виконання шкідливого коду. Для цього зображення має бути відкрито в додатку; у браузерах достатньо просто відкрити веб-сайт. Код, який виконується у фоновому режимі, може потім інсталювати, наприклад, шкідливе програмне забезпечення.

Постраждало багато відомих програм

Уразливість, яку виявили відділ інженерії безпеки та архітектури Apple (SEAR) і Citizen Lab у школі Манка Університету Торонто, спочатку помилково класифікували як чисту помилку Chrome; поширені веб-браузери були швидко захищені оновленням безпеки. Але, як тепер виявилося, постраждало також значно більше додатків.

Уразливість пов’язана з відкритою бібліотекою Libwebp, яка використовується багатьма програмами. Таким чином, такі програми, як Gimp, Libreoffice, Telegram, 1Password та багато інших, також можуть стати об’єктами атаки. У результаті CVSS, стандартизований бал для оцінки вразливостей системи безпеки, було підвищено до найвищого рівня 10,0.

Як себе захистити

Як користувач, у вас є лише один спосіб захистити себе від цієї вразливості: переконайтеся, що у вас встановлено найновіші виправлення. Багато постраждалих

програм уже випустили оновлення безпеки, які закривають дірку в безпеці, включаючи браузери та Libreoffice.

В іншому випадку те, що завжди має застосовуватися під час серфінгу в мережі, все ще діє тут. Не завантажуйте файли з невідомих джерел і переконайтеся, що посилання в електронних листах ведуть лише на перевірені сайти». ***(Kris Wallburg. Risk level 10: Critical security hole affects widespread software // IDG Communications, Inc. (https://www.pcworld.com/article/2083926/highest-alert-level-security-vulnerability-affects-apps-like-telegram-and-1password.html?utm_source=flipboard&utm_content=PCWorld%2Fmagazine%2FPCWorld). 27.09.2023).***

***

«Уразливості програмного забезпечення дуже схожі на протипехотні міни в зоні бойових дій: вони приховані на видноті, здається всюди, і готові вибухнути, коли ви цього найменше очікуєте.

Однак, на відміну від однорідної руйнівної сили указу, не всі вразливі місця однакові. Спектр серйозності вразливості програмного забезпечення охоплює від нешкідливих неправильних налаштувань до руйнівних експлойтів нульового дня, які, якщо їх спрацювати, можуть призвести до згубних порушень даних і скомпрометувати цілісність цілих систем.

Як постачальник програмного забезпечення безпеки, Descope покладається на партнерів, користувачів та інших членів спільноти програмного забезпечення безпеки, щоб повідомляти нас про виявлення вразливостей у наших продуктах. Ми також час від часу виявляємо вразливі місця в інших продуктах. Нещодавно ми виявили та оприлюднили серйозну неправильну конфігурацію програм Microsoft Active Directory, що потенційно може вплинути на будь-яку програму, яка використовує «Вхід за допомогою Microsoft» у своїх потоках автентифікації.

Чому відповідальне розкриття інформації є критичним

Перевіривши довіру користувачів, які повідомляють про вразливості, ми розуміємо важливість визначення та дотримання програми відповідального

розкриття інформації. Відповідальне розголошення має досягти тонкого балансу між задоволенням негайної потреби захистити користувачів, які знаходяться під загрозою, та ширшими наслідками безпеки для всієї спільноти.

Агентство з кібербезпеки та безпеки інфраструктури (CISA) повідомило про рекордні 26 448 підтверджених уразливостей у 2022 році, при цьому кількість «критичних» уразливостей зросла на 59% порівняно з попереднім роком. Проте це лише невелика частина звітів, надісланих постачальникам, особливо за останні кілька років, оскільки все більше постачальників програмного забезпечення покращили свої програми винагород за помилки.

Постачальники програмного забезпечення не завжди сприймали пошук уразливостей у третіх сторін. У 2015 році CSO Oracle написав відкритий лист із 3000 слів, у якому благав клієнтів припинити зворотне проектування та оприлюднювати недоліки в програмному забезпеченні. У деяких екстремальних випадках особам, які повідомляли про вразливі місця, навіть погрожували кримінальним переслідуванням.

Постачальники програмного забезпечення оцінили цінність краудсорсингового тестування на проникнення. Багато хто створив стимули для винагороди користувачів і дослідників загроз за виявлення вразливостей і повідомлення про них. Однак, незважаючи на те, що ці програми винагород за помилки стають все більш поширеними, залишаються проблеми, щоб зробити процес оптимізованим, прозорим і вигідним для всіх сторін. Велика кількість звітів про вразливості також підкреслює необхідність структурованого та відповідального підходу до управління, усунення та усунення цих вразливостей.

Головною метою звітування про вразливості залишається зробити програмне забезпечення максимально безпечним для кінцевих користувачів. Перехід від реактивної до проактивної позиції вимагає не лише відкритих каналів для звітування. Це потребує розробки всебічної структури, яка встановлює керівні принципи як для журналістів, так і для продавців.

4 ключові принципи відповідального розкриття інформації про кібербезпеку

Розробка програми відповідального розкриття інформації відповідає інтересам кожного члена спільноти програмного забезпечення. Розгляньте наступні чотири принципи як основні стовпи для побудови ефективної програми відповідального розкриття інформації.

1. Будьте чіткими та прозорими

Чіткий і прозорий процес комунікації має окреслювати ключові елементи процесу розкриття інформації, визначати призначені контактні особи та планувати очікувані часові рамки для відповіді. Важливим аспектом цього процесу є баланс між терміновістю негайного розкриття та наданням постачальнику програмного забезпечення достатнього часу для вирішення проблеми.

Загалом галузевий стандарт передбачає надання постачальнику програмного забезпечення 30 днів для усунення вразливості, хоча цей графік може коливатися залежно від масштабу та серйозності вразливості. Організаціям, які пропонують програму винагороди, важливо підтримувати прозорість щодо роботи програми, яка включає чітке визначення того, як і коли звіти будуть компенсовані, а також типи вразливостей, які мають право на винагороду.

2. Виховуйте довіру, а не страх

Послідовне та відкрите спілкування з дослідниками та етичними хакерами, які виявляють вразливі місця, є життєво важливим для формування середовища спільної відповідальності, відкритої розмови та взаємної довіри. Важливо запевнити учасників, що вони не зазнають юридичних наслідків за повідомлення про вразливість.

У сучасному середовищі взаємопов’язаного програмного забезпечення погано керована програма виявлення вразливостей може негативно вплинути на всю екосистему програмного забезпечення. Тому дуже важливо проявляти обережність, особливо коли йдеться про розкриття інформації про інших сторін, включаючи конкурентів, які можуть постраждати від подібної вразливості. Це не лише демонструє професійну повагу та справедливість, але й посилює дух співпраці, життєво важливий для підтримки безпеки в усій галузі.

3. Встановіть комплексний процес сортування

Інвестиції в добре задокументовану структуру сортування є наріжним каменем кожної зрілої програми управління вразливістю. Він надає групам безпеки структуру для визначення пріоритетів уразливостей на основі їх потенційного впливу та ймовірності використання.

Крім встановлення пріоритетів, надійний процес сортування також сприяє відповідальному спілкуванню та прийняттю рішень з низкою зацікавлених сторін — від розробників програмного забезпечення, які впроваджують виправлення, до користувачів, які повинні бути належним чином поінформовані про будь-який потенційний ризик. Процес сортування має надзвичайно важливе значення в суворо регульованих галузях, які підпадають під суворі правила та вимагають, щоб певні типи вразливостей повідомлялися та вирішувалися протягом визначеного періоду часу.

4. Безперервність має вирішальне значення

Сучасне середовище загроз є дуже динамічним і вимагає безперервного та адаптивного процесу для своєчасного виявлення вразливостей, звітування та виправлення. Також важливо регулярно переглядати та оновлювати програму розкриття інформації, щоб переконатися в її ефективності та відповідності в контексті поточної ситуації загроз. Це означає, що ваші процедури, інструменти та стратегії мають не лише усунути наявні вразливості, але й підготуватися до майбутніх.

Культура постійного вдосконалення має включати відгуки різних зацікавлених сторін і уроки, отримані з минулого досвіду. Використовуйте інформацію, отриману в результаті розвитку ландшафту загроз, щоб удосконалити свою програму розкриття інформації.

Ціле більше, ніж сума

Відповідальне розкриття інформації підкреслює, що в кібербезпеці колективна сила, отримана від співпраці дослідників, постачальників і користувачів, перевершує можливості будь-якого окремого компонента. Подібно до того, як ціле часто є більшим, ніж сума його частин, кібербезпека — це не просто турбота однієї організації чи окремої людини; це спільний обов’язок у

нашому спільному прагненні до безпечного цифрового світу». ***(Omer Cohen. 4 Pillars for Building a Responsible Cybersecurity Disclosure Program // Informa PLC (https://www.darkreading.com/risk/4-pillars-for-building-a-responsible-cybersecurity-disclosure-program?utm_source=flipboard&utm_content=DarkReading%2Fmagazine%2FDark+Reading). 26.09.2023).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Заснований в Ізраїлі стартап із кібербезпеки Legit Security заявив у середу, що отримав 40 мільйонів доларів від інвесторів, щоб допомогти компаніям захистити свої генеруючі додатки на основі штучного інтелекту від зловмисних атак і порушень безпеки.

Раунд фінансування серії B очолювала американська венчурна компанія CRV за участю існуючих інвесторів, ізраїльського фонду венчурного капіталу Cyberstarts, міжнародної інвестиційної компанії Bessemer Venture Partners і венчурної компанії Кремнієвої долини TCV. Свіжий капітал збільшив загальну суму зібраних Legit Security коштів до 77 мільйонів доларів.

В останні місяці шквал заснованих в Ізраїлі стартапів у сфері кібербезпеки, які прагнуть розробити рішення для задоволення швидкозростаючих потреб бізнесу в безпеці, досяг успіху в залученні капіталу, оскільки простір захоплює інтерес приватних інвесторів, незважаючи на глобальну кризу фінансування технологій.

Підприємства все більше покладаються на програмне забезпечення для ведення бізнесу, а цифрова трансформація переносить центри обробки даних у хмару. Швидкі темпи змін також відкрили більше незахищених каналів атак, на які націлені кіберзлочинці.

Legit Security зі штаб-квартирою в Пало-Альто, Каліфорнія, була заснована у вересні 2020 року генеральним директором Роні Фуксом, технічним директором Лявом Каспі та віце-президентом з досліджень і розробок Ліором Бараком, випускниками підрозділу 8200 Сил оборони Ізраїлю. Стартап розробив платформу безпеки, яка, за його словами, допомагає підприємства та організації захищають ланцюжки поставок програмного забезпечення та програми від атак загроз, виявляючи та пом'якшуючи вразливості від етапу розробки коду до розгортання хмари. Серед клієнтів Legit Security, які використовують платформу, є Google, NYSE, Kraft Heinz, Takeda Pharmaceuticals та інші компанії зі списку Fortune 500.

Ланцюжок постачання програмного забезпечення – це екосистема систем, інфраструктури, процесів і людей, залучених до розробки програмного забезпечення. Платформа Legit Security сканує конвеєри розробки програмного забезпечення на наявність прогалин і витоків, а також інфраструктуру розробки та системи в цих конвеєрах. Gartner, до 2025 року близько 45% підприємств і організацій у всьому світі зазнають атак на ланцюги поставок програмного забезпечення, що в три рази більше, ніж у 2021 році Згідно зі звітом.

Стартап заявив, що використовуватиме кошти серії B для розширення «продажів, маркетингу та досліджень і розробок, а також для вирішення нової загрози штучного інтелекту та великих мовних моделей (LLM) у розробці нових програм».

Команди розробників програмного забезпечення все більше використовують код, згенерований штучним інтелектом, і вбудовують LLM у свої додатки, «але ці технології штучного інтелекту також створюють клас нових загроз безпеці, що швидко зростає», — йдеться в заяві Legit Security.

«Ми заснували Legit Security з місією захистити світове програмне забезпечення за допомогою платформи, яка постійно керує безпекою додатків від коду до хмари», — сказав Фукс. «Завдяки цим інвестиціям наша місія отримує додаткову тягу та швидкість, включаючи нові можливості для розширення видимості, безпеки та керування кодом, створеним штучним інтелектом, і вбудованими моделями великих мов (LLM) у програми».

Цей крок відбувається, оскільки все більше і більше розробників програмного забезпечення, які працюють у хмарних середовищах, використовують помічники коду на основі штучного інтелекту, такі як GitHub Copilot або Tabnine, відкриваючи низку нових ризиків для конфіденційності даних і захисту конфіденційних даних. У результаті такі великі технологічні компанії, як Apple і Samsung, як повідомляється, обмежують своїх співробітників у використанні генеративних інструментів штучного інтелекту, таких як ChatGPT OpenAI і кодові помічники штучного інтелекту, щоб запобігти витоку приватної інформації». ***(Sharon Wrobel. Israeli-founded cybersecurity startup raises $40m to help mitigate threats to AI apps // The Times of Israel (https://www.timesofisrael.com/israeli-founded-cybersecurity-startup-raises-40m-to-help-mitigate-threats-to-ai-apps/?utm_source=flipboard&utm_content=TimesofIsrael%2Fmagazine%2FThe+Times+of+Israel). 20.09.2023).***

***

«…8 серпня 2023 року Національний інститут стандартів і технологій США (NIST) випустив пропозицію щодо нової версії (2.0) Framework Cybersecurity Framework (CSF), щоб забезпечити організації структурою для заходів кібербезпеки. З моменту свого першого випуску в 2014 році CSF став основним інструментом, який використовують компанії в усьому світі для підвищення своєї стійкості до кіберзагроз.

The Cybersecurity Framework — це високоякісний інструмент, який визначає загальну структуру, яка допомагає організаціям визначати, оцінювати та керувати ризиками кібербезпеки. Концепція кібербезпеки призначена для забезпечення організованого та узгодженого набору найкращих практик, інструкцій і стандартів, які повинні бути узгоджені з конкретними потребами різних секторів і організацій. З цієї причини він містить посилання на норми та спеціальні рекомендації, розроблені NIST, а також Міжнародною організацією зі стандартизації (ISO).

Основні зміни в оновленій версії фреймворку:

сфера застосування була переглянута та розширена – новий CSF розширює структуру, включаючи нові та діючі норми та рекомендації, роблячи її більш актуальною та повною;

допомога для тих, хто його впроваджує – також покращено поради щодо використання CSF 2.0 на практиці, що значно полегшить впровадження.

Важливо, що розробка інструментів, норм і інструкцій кібербезпеки має серйозні наслідки для комерційної практики. Це пояснюється тим, що вони є ключовими як засіб «м'якого права» – вони відіграють справді додаткову роль по відношенню до прийнятих законів, оскільки це закони, які мають враховувати швидкі темпи розвитку технологій і тривалі законодавчі процеси. Законодавці усвідомлюють це, і законодавство часто насправді містить загальні посилання на технічні норми та рекомендації. NIS 2 є лише одним із прикладів. Що стосується заходів з управління ризиками кібербезпеки, то посилаються, наприклад, на «сучасні» та «європейські та міжнародні норми».

З цієї причини як приватні, так і державні організації повинні вживати заходів для впровадження норм і стандартів кібербезпеки, щоб забезпечити більшу стійкість до кіберзагроз, а також дотримання законодавства. На практиці це, як правило, стандарти, розроблені NIST та ISO, і тому було б доцільно переглянути процедури та політику, що діють в організації, і визначити, чи потрібно їх оновлювати, тепер, коли нова версія фреймворку NIST було випущено». ***(Konrad Basaj and Marcin Ręgorowicz. Proposal for the new NIST Cybersecurity Framework now revealed // Traple Konarski Podrecki & Wspólnicy (https://www.traple.pl/en/proposal-for-the-new-nist-cybersecurity-framework-now-revealed/). 12.09.2023).***

***

«В епоху, коли кіберзагрози невблаганно розвиваються, традиційні захисні механізми часто не встигають. З кожним днем цифрова сфера спостерігає сплеск складних атак, які порушують роботу сервісів і загрожують цілісності та конфіденційності даних. У той час як підприємства, організації та

навіть окремі особи борються з непростою проблемою захисту своїх цифрових активів, з'являється маяк надії – система кібербезпеки на основі машинного навчання.

Цей потужний підмножина штучного інтелекту, відома своєю передбачуваною здатністю та адаптивністю, все більше займає центральне місце в рішеннях кібербезпеки. Але як поєднати складний світ алгоритмів із постійно складною сферою кібербезпеки? У цій статті ми розпочнемо комплексну подорож, починаючи від базових концепцій і закінчуючи тонкими кроками, щоб створити надійну систему кібербезпеки на основі машинного навчання. Незалежно від того, чи є ви досвідченим професіоналом у сфері кібербезпеки чи допитливим ентузіастом, приєднуйтесь до нас, коли ми заглибимося в план майбутнього, де машинний інтелект невтомно працює, щоб відбиватися від кіберсупротивників.

Розуміння основ

Розробляючи систему кібербезпеки на основі машинного навчання, ми повинні ознайомитися з основними концепціями.

За своєю суттю машинне навчання є підмножиною штучного інтелекту, який дає змогу комп'ютерам покращувати свою продуктивність у виконанні завдань за допомогою досвіду. Замість того, щоб бути явно запрограмованими для виконання конкретних завдань, розробники навчають ці системи, використовуючи величезні обсяги даних, що дозволяє їм вивчати шаблони, приймати рішення або навіть передбачати майбутні події.

У машинному навчанні існує два типи навчання. Контрольоване навчання передбачає навчання моделі з використанням позначених даних, що дозволяє передбачати результати на основі вхідних даних. З іншого боку, неконтрольоване навчання має справу з немаркованими даними. Система самостійно визначає структури та шаблони, сегментуючи дані на кластери або зменшуючи їх розміри.

На крок далі до складності глибоке навчання включає алгоритми, натхненні структурою людського мозку, які називаються нейронними мережами. Ці багаторівневі мережі можуть обробляти величезні обсяги даних, що робить їх неймовірно потужними для завдань розпізнавання зображень і мови. У сфері

кібербезпеки вони можуть відігравати важливу роль у виявленні раніше невидимих загроз або розумінні складних моделей зловмисної діяльності.

Отже, навіщо поєднувати машинне навчання з кібербезпекою? Причин багато:

Швидкість і ефективність: через величезний обсяг даних, що проходить через сучасні мережі, вручну аналізувати кожен пакет на наявність загроз неможливо. Моделі машинного навчання можуть швидко обробляти величезні набори даних, виявляючи аномалії та загрози в реальному часі.

Здатність розвиватися разом із загрозами. Традиційні системи кібербезпеки часто покладаються на попередньо визначені сигнатури або відомі поведінки загроз. Навпаки, машинне навчання може адаптуватися. Коли він стикається з новими загрозами або варіаціями старих, він навчається, забезпечуючи розвиток захисних механізмів у тандемі з кібернетичним ландшафтом, що постійно адаптується.

Просуваючись далі, пам’ятайте, що машинне навчання — це не просто інструмент, а союзник. На динамічному полі битви кіберпростору саме той, хто навчається, тримає супротивників на відстані. Маючи ці базові знання, тепер ми можемо заглибитися в дрібниці створення системи кібербезпеки, доповненої машинним навчанням.

Необхідність машинного навчання в кібербезпеці

Оскільки цифрова трансформація прискорюється в усьому світі, складність і обсяг кіберзагроз зросли тривожно. Ландшафт кібербезпеки — це постійні зміни, де старі загрози змінюються, а нові з’являються з дивовижною швидкістю. За такого сценарію традиційні, засновані на правилах заходи кібербезпеки часто не дають результатів; ось тут вступає машинне навчання, пропонуючи динамічну лінію захисту, що розвивається.

Робота з великими обсягами даних

Сучасні підприємства та мережі щодня обробляють величезні обсяги даних. Від поведінки користувачів до журналів транзакцій, кожна взаємодія залишає

цифровий слід. Контролювати ці сліди на наявність потенційних загроз вручну займає багато часу та майже неможливо.

Алгоритми машинного навчання, призначені для роботи з великими наборами даних, можуть просіювати ці дані в режимі реального часу, приймаючи рішення щодо потенційних загроз за частку секунди та забезпечуючи своєчасне реагування.

Проактивне виявлення загроз

Традиційні інструменти кібербезпеки часто покладаються на сигнатури – попередньо визначені шаблони відомих шкідливих програм або методів атак. Хоча вони ефективні проти відомих загроз, вони сліпі до нових, невідомих загроз.

Машинне навчання не просто виявляє; це передбачає. Аналізуючи минулі та поточні дані, можна передбачити майбутні загрози або розпізнати ранні ознаки кібератаки, дозволяючи вживати профілактичні заходи.

Адаптація до загроз, що розвиваються

Краса машинного навчання полягає в його адаптивності. Він навчається та адаптується, коли стикається з новими типами атак або незначними варіаціями, гарантуючи, що система не просто реагує на останню атаку, а готується до наступної.

Зменшення помилкових спрацьовувань

Частою проблемою в сфері кібербезпеки є помилкові спрацьовування – доброякісні дії, які помилково позначаються як загрози. Це може перевантажити команди безпеки та призвести до самовдоволення. Завдяки безперервному навчанню машинне навчання вдосконалює свої алгоритми виявлення, зменшуючи число помилкових тривог і забезпечуючи ефективність сповіщень.

Автоматизація рутинних завдань

Ефективність і експертна спрямованість: машинне навчання може виконувати рутинні повторювані завдання, як-от аналіз журналів або моніторинг мережевого трафіку. Автоматизація цих завдань гарантує, що люди-експерти можуть зосередитися на складніших проблемах безпеки з нюансами, роблячи весь процес кібербезпеки більш ефективним.

Оскільки кіберсупротивники використовують передові методи та використовують цифрові вразливості нашого часу, покладатися виключно на традиційні методи схоже на те, щоб брати з собою ніж у перестрілку. Завдяки динамічній адаптивності, можливостям прогнозування та величезній потужності обробки машинне навчання змінює правила гри, оснащуючи системи кібербезпеки інструментами, необхідними для ефективної протидії сучасним загрозам.

Кроки для створення системи кібербезпеки за допомогою машинного навчання

Використання майстерності машинного навчання в кібербезпеці полягає не в простому застосуванні формули; це вимагає організованої методології, ретельного керування даними, уточнення моделі та постійних оцінок для безпрецедентного кіберзахисту. Ось покрокова інструкція, яка допоможе вам зорієнтуватися в цьому:

Встановлення чітких цілей

Під час впровадження машинного навчання в кібербезпеку важливо мати чітку мету. Ви зосереджені на виявленні зловмисного програмного забезпечення, виявленні оманливих електронних листів або передбаченні потенційних загроз зсередини? Встановлення цієї ясності з самого початку буде керувати подальшими рішеннями. Наприклад, якщо основною метою є зменшення частоти помилкових сповіщень, тоді доцільно встановити конкретний цільовий відсоток зменшення.

Збір і уточнення даних

Сильна сторона будь-якої моделі машинного навчання полягає в якості її даних; це означає збір різноманітних і вичерпних даних для кібербезпеки для кращого прогнозування та виявлення загроз. Але збір даних – це лише початок. Не менш важливо забезпечити однорідність даних. Видалення аномалій або нерелевантних даних робить фазу навчання моделі машинного навчання більш оптимізованою та ефективною.

Вибір правильних методів машинного навчання

Ваші конкретні цілі будуть керувати вибором алгоритмів машинного навчання. Наприклад, прості аномалії, засновані на правилах, краще вирішувати за допомогою дерев рішень, тоді як для більш складних моделей можуть знадобитися

методи глибокого навчання. Якщо в цьому процесі прийняття рішень є невизначеність, доцільно проконсультуватися з експертами, які спеціалізуються на машинному навчанні та кібербезпеці.

Навчання та перевірка моделі

Коли ви підготуєте дані, наступним кроком стане введення їх у модель машинного навчання під час навчання. Перевірте цю модель за окремим набором даних, до якого вона раніше не піддавалася, щоб визначити її точність і надійність. Зворотній зв'язок від цього процесу перевірки допомагає вдосконалити модель для підвищення її продуктивності.

Забезпечення швидкого аналізу загроз

Інтеграція є вирішальним етапом. Удосконалене рішення машинного навчання має бездоганно інтегруватися з існуючою технологічною інфраструктурою. Крім того, система повинна забезпечувати моніторинг у реальному часі та миттєво реагувати на виявлені загрози.

Пріоритет безперервної еволюції моделі

Кібернетичний ландшафт постійно розвивається, як і системи кібербезпеки. Модель залишається гнучкою та актуальною, регулярно надаючи системі нові дані аналізу загроз та оновлюючи цикли навчання, навіть якщо негайних загроз немає.

Постійний моніторинг і вдосконалення

Встановлення контрольних показників і регулярне їх вимірювання має вирішальне значення. Якщо є якісь відхилення, це дає можливість перекалібрувати стратегію та внести необхідні корективи.

Відповідність і етичні міркування

У сучасну епоху цифрових технологій слід звернути увагу на положення про захист даних, такі як GDPR, особливо під час обробки конфіденційних даних користувачів. Більше того, відповідальне використання машинного навчання має першорядне значення, забезпечуючи етичне поводження з даними та поважаючи права особи на конфіденційність.

Залучення та навчання персоналу служби безпеки

Щоб підвищити ефективність системи машинного навчання, співробітники служби безпеки повинні добре знати її роботу. Пропонуємо регулярні навчальні сесії та сприяємо спільному середовищу, де спеціалісти з даних та експерти з безпеки, які працюють у тандемі, можуть використовувати свій спільний досвід.

Будьте в курсі розвитку галузі

Світ машинного навчання та кібербезпеки динамічний. Важливо бути в курсі найновіших стратегій, алгоритмів і передових практик. Бути активним учасником пов'язаних спільнот, форумів і подій може бути безцінним для обміну думками та навчання від колег-професіоналів галузі.

Інтеграція машинного навчання у вашу стратегію кібербезпеки — це плавне завдання, яке вимагає технічних знань і далекоглядного планування. Дотримуючись цього структурованого посібника та залишаючись напоготові до кіберзагроз, що постійно змінюються, підприємства можуть зміцнити свій захист, завжди випереджаючи кіберсупротивників.

Виклики та міркування

Машинне навчання з його величезним потенціалом стало ключовим інструментом у сфері кібербезпеки. Однак його інтеграція має складності та проблеми. Давайте розберемо ці аспекти, щоб краще зрозуміти:

Розуміння цілісності та обсягу даних

Успіх будь-якої системи машинного навчання незмінно пов'язаний з її даними. Але помилково ототожнювати обсяг і ефективність. Замість простої кількості найважливішими є якість, різноманітність і чистота даних. Ще більше ускладнює ситуацію ризик, пов'язаний із синтетичними або надмірно очищеними наборами даних, які можуть не відобразити непередбачувану природу справжніх кіберзагроз.

Звернення до переобладнання моделі

Поширеною проблемою машинного навчання є переобладнання; це відбувається, коли модель стає настільки точно налаштованою на певний набір даних, що їй важко ефективно працювати з незнайомими даними. Для боротьби з цим можна застосувати такі методи, як перехресна перевірка, що гарантує, що

модель залишається універсальною та актуальною для різноманітних сценаріїв даних.

Навігація в кіберзагрозах, що постійно змінюються

У кіберсфері стагнація дорівнює вразливості. Кіберзагрози знаходяться в безперервній еволюції, що робить моделі, навчені на сьогоднішніх загрозах, потенційно застарілими завтра. Отже, наголос повинен бути зроблений на моделях, що мають пріоритет на постійному навчанні та адаптації в реальному часі до останніх парадигм загроз.

Управління помилковими спрацьовуваннями

Хоча висока чутливість у виявленні може здатися бажаною, вона може ненавмисно призвести до шквалу помилкових тривог; це призводить до втоми попередження серед команд безпеки та ризикує справжнім загрозам загубитися в шумі. Досягнення балансу між точністю та запам'ятовуванням має вирішальне значення для пом'якшення цієї проблеми.

Оцінка потреб у ресурсах

Machine learning, particularly sophisticated deep learning models, can be resource-intensive. Beyond the computational demands, there's also a cost implication. Conducting a thorough cost-benefit analysis ensures that the returns justify the resource investment.

Збалансування автоматизації з людським розумінням

Повна залежність від автоматизації може здатися спокусливою, але може бути небезпечною. Незважаючи на всю свою майстерність, системи машинного навчання можуть пропустити нюанси загроз, які може вловити досвідчене людське око. Метою має бути симбіотичний зв'язок між системами машинного навчання та людським судженням.

Пріоритет конфіденційності даних

Використання машинного навчання в кібербезпеці вимагає збору великої кількості даних, що викликає законні занепокоєння щодо конфіденційності. Організації повинні бути добре обізнані з глобальними правилами

конфіденційності, такими як GDPR, і суворо їх дотримуватися, щоб забезпечити етичну та законну обробку даних.

Подолання розриву в навичках

Унікальний перетин кібербезпеки та машинного навчання потребує спеціалізованих знань, яких може бракувати. Організаціям слід надати пріоритет підвищенню кваліфікації існуючих команд і, якщо необхідно, найняти експертів у галузі або співпрацювати з ними.

Захист від ворожих загроз

Кібернедоброзичливці стають дедалі витонченішими, деякі з них мають досвід маніпулювання моделями машинного навчання, надаючи їм оманливі дані. Забезпечення надійності моделей за допомогою змагальності є проактивною стратегією захисту від такої тактики.

Забезпечення прозорості моделі

Одним із закидів проти складних моделей машинного навчання є їхня природа «чорної скриньки», що робить процеси прийняття рішень непрозорими. Важливо схилятися до моделей, які пропонують чітке вікно в їх операційну логіку, щоб створити довіру та спростити усунення несправностей.

Включення машинного навчання в кібербезпеку, безсумнівно, є прогресивним кроком. Однак розуміння цих викликів і активне їх вирішення є першорядним. Це поєднання інновацій, безперервного навчання та стратегічного планування, яке спрямовуватиме організації до міцної та надійної системи кібербезпеки на основі машинного навчання.

Висновок

У сучасній динамічній цифровій екосистемі важливість кібербезпеки для підприємств у всьому світі важко переоцінити. Оскільки кіберзагрози стають все більш заплутаними та експансивними, інтеграція машинного навчання в наш арсенал безпеки перетворилася з передової концепції на важливу стратегію. Використовуючи передбачувану майстерність машинного навчання, компанії тепер краще оснащені, щоб відбиватися від досвідчених кіберсупротивників і захищати свої цифрові активи.

Проілюстроване вражаючими історіями успіху та практичними ідеями, додаткова цінність машинного навчання для кібербезпеки очевидна. Він захищає від потенційних загроз і змінює спосіб запобігання та протидії компаніям цифрової вразливості. Машинне навчання та координація кібербезпеки ще більше зміцняться, оскільки цифрова сфера продовжує свою висхідну траєкторію, підкреслюючи їхню колективну роль у зміцненні наших цифрових горизонтів…» ***(Brian Koome. How to Create a Machine Learning-Based Cybersecurity System (Exclusive Report) // Cryptopolitan (https://www.cryptopolitan.com/machine-learning-based-cybersecurity-system/?utm_source=flipboard&utm_content=MattMagnuson%2Fmagazine%2FArtificial+Intelligence+%26+Machine+Learning). 25.09.2023).***

***

«…ZoomEye — це безкоштовна розвідувальна платформа, яку фахівці з кібербезпеки, дослідники та організації можуть використовувати для збору інформації про існуючі сервіси та пристрої, підключені до Інтернету, оцінки їх безпеки та виявлення потенційних уразливостей.

Незважаючи на те, що різні інструменти розвідки, такі як Nmap і Masscan, можуть забезпечити навіть більш глибокий аналіз певного діапазону IP-адрес та їхніх портів, ZoomEye є ширшим інструментом, який дає краще загальне уявлення про загальний ландшафт відкритого кіберпростору.

Як працює ZoomEye?

За допомогою ZoomEye фахівці з кібербезпеки можуть шукати та переглядати базу даних, яка індексує IPv4, IPv6 і бази даних доменів веб-сайтів, доступні в Інтернеті. Оскільки кіберпростір — це величезна мережа, яка постійно зростає, ZoomEye покладається на геодезичні вузли, розташовані по всьому світу, щоб ефективно сканувати значну частину кіберпростору.

Щоб розбити його, ZoomEye працює в чотири етапи: сканування, захоплення банера, індексування та пошук і запит.

Сканування: ZoomEye використовує свої геодезичні вузли, розташовані по всьому світу, для пошуку відкритих портів послуг і пристроїв, підключених до Інтернету.

Захоплення банерів: після того, як існування служби чи пристрою було перевірено, ZoomEye збирає інформацію про банер конкретного запущеного порту служби. Інформація про банер може включати деталі про службу, наприклад список запущених портів, утиліти, які вона використовує, версію таких утиліт, апаратне забезпечення, на якому працює служба, та інші ідентифікаційні характеристики

Індексація: Дані, зібрані на етапі захоплення банера, потім зберігаються та індексуються в базі даних ZoomEye.

Пошук і запит: база даних потім підключається до ZoomEye API, де користувачі можуть шукати та запитувати будь-яку інформацію, що зберігається в базі даних ZoomEye. Користувачі можуть здійснювати пошук за ключовими словами та застосовувати фільтри для пошуку певних типів пристроїв або послуг.

ZoomEye стягує різні комісії, якщо користувачі хочуть отримати доступ до додаткових видів даних. Наприклад, якщо ви хочете контролювати 50 IP-адрес щомісяця, це коштуватиме вам 70 доларів США. Якщо ви хочете контролювати 250 IP-адрес щомісяця, це коштуватиме 140 доларів США. Ви можете отримати доступ до 10 000 результатів щомісяця безкоштовно або отримати додаткові 20 000 результатів за 70 доларів США на місяць.

Чим ZoomEye корисний для вашої кібербезпеки?

Оскільки ZoomEye та подібні розвідувальні платформи, потенційно можуть отримати обсяг даних зловмисники можуть зловживати цією платформою. Однак приховування вразливих мереж мало допомагає захистити їх від хакерів. Натомість такі платформи, як ZoomEye, відкривають ці мережі для громадськості, щоб кожен міг перевірити свої мережі та пристрої на наявність будь-яких можливих слабких місць, якими може скористатися хакер.

Отже, як саме ZoomEye допомагає зробити безпечнішим кіберпростір?

Зовнішня видимість: виявлення ймовірно вразливих мереж і пристроїв на таких платформах, як ZoomEye, може допомогти попередити спільноту, а також власників про слабкі місця в їхній системі. Великі організації можуть використовувати ZoomEye, щоб краще бачити свою цифрову присутність з точки зору сторонньої людини.

Виявлення активів: налаштувати та провести інвентаризацію всіх пристроїв, підключених до мережі, може бути легко, якщо мережа невелика. Однак для великих мереж, таких як ті, що використовуються в урядах та інших організаціях, відстеження може бути неможливим. Наявність можливості зовнішньої перевірки можливих недоробок, таких як веб-камери, повторювачі та пристрої Інтернету речей, може допомогти персоналу з кібербезпеки ідентифікувати ці активи та тримати їх під контролем.

Оцінка вразливості: ZoomEye може допомогти виявити потенційні вразливості та неправильні конфігурації в мережі. Хоча спеціалісти з кібербезпеки можуть виконувати оцінку вразливості, розвідувальні платформи, такі як ZoomEye, можуть виявити проблеми, які могли бути пропущені, наприклад відкриті порти, застаріле програмне забезпечення або незахищені конфігурації.

Управління ризиками третіх сторін: ZoomEye дозволяє перевіряти безпеку сторонніх постачальників і партнерів, пов’язаних із вашим бізнесом. Переконавшись, що ваша система безпечна, перевірка партнерських мереж за допомогою ZoomEye та подібних платформ може допомогти вам попередити їх про будь-які проблеми, пов’язані з їх безпекою.

Дослідження та аналіз загроз: спеціалісти з кібербезпеки можуть використовувати ZoomEye, щоб знати, які типи технологій часто використовуються, нові загрози та досліджувати потенційні вектори атак.

Можливі небезпеки ZoomEye

ZoomEye — це безкоштовний онлайн-інструмент, призначений для підтримки кібербезпеки в сферах розвідки та оцінки загроз. Однак, як і будь-який

інструмент, доступний для будь-кого, ZoomEye потенційно може бути використаний хакерами та використовувати різні типи розвідувальних атак.

Завдяки об'єму інформації, яку можна отримати від ZoomEye, хакери потенційно можуть отримати несанкціонований доступ до пристроїв у мережі, установити зловмисне програмне забезпечення, порушити роботу служб і викрасти конфіденційні дані, які можуть бути використані для всіляких нечесних дій.

Крім того, кваліфіковані хакери можуть автоматизувати процес, безперервно скануючи через ZoomEye та інтегруючи отриману інформацію у свій інструментарій, щоб спробувати отримати несанкціонований доступ до будь-якої мережі.

Чи варто боятися ZoomEye?

З огляду на те, що ZoomEye потенційно зловживають хакерами для визначення можливих цілей, зрозуміло, що люди можуть боятися ZoomEye. Однак ви повинні пам'ятати, що всі набори даних у базі даних ZoomEye вже є загальнодоступними. ZoomEye — це просто масивний сканер портів, який індексує розкриті веб-сайти, служби та підключені пристрої в Інтернеті.

З ZoomEye або подібними платформами або без них, якщо ваша мережа вразлива, хакери завжди зможуть знайти спосіб знайти та атакувати вашу систему. Так, ZoomEye може полегшити хакерам пошук вразливих систем. Але насправді проблема не в цьому. Справжня проблема полягає в тому, що десь розташована мережа є вразливою, і власники не змогли її належним чином захистити.

ZoomEye може бути корисним з обох боків ігрового поля. Хакери завжди можуть знайти вразливу мережу, якщо вони достатньо стараються, але з іншого боку, люди без досвіду кібербезпеки можуть скористатися інструментом і перевірити, чи їхня мережа піддана впливу.

ZoomEye має свої плюси і мінуси

Незважаючи на те, що ZoomEye є потужною платформою для початкової розвідувальної роботи, обсягу інформації, яку можна отримати з платформи, часто бракує.

Враховуючи принцип роботи ZoomEye та його обмеження, фахівці з кібербезпеки часто використовують інші розвідувальні платформи, такі як Shodan, Censys, FOFA та LeakIX у поєднанні з ZoomEye. Потім вони збиратимуть ще більше даних за допомогою більш спеціалізованих інструментів, таких як Nmap, BurpSuit і WireShark, у певній мережі. Майте це на увазі, якщо ви хочете використовувати ZoomEye самостійно». ***(Jayric Maning. What Is ZoomEye and How Is It Useful for Your Cybersecurity? // www.makeuseof.com (https://www.makeuseof.com/what-is-zoomeye-how-is-it-useful-for-your-cybersecurity/?utm_source=flipboard&utm_content=muo_official%2Fmagazine%2FSECURITY). 25.09.2023).***

***

«Новий звіт IDC про кібербезпеку сигналізує про кінець ери SOAR, оскільки підприємства та постачальники переходять на гіперавтоматізацію.

IDC досліджує, як Torq Hyperautomation «прогнозує прогалини в безпеці, проактивно оцінює мережу та остаточно захищає її», забезпечуючи «видимість і контроль усіх середовищ для всіх процесів і рольових гравців».

Torq, лідер у сфері гіперавтоматизації безпеки, сьогодні оголосила, що IDC заявила, що Torq Hyperautomation забезпечує «автоматизацію всього, що можна і потрібно автоматизувати» в сучасних SecOps у новому «Як гіперавтоматизація використовується для зменшення прогалин і неефективності в мережевій кібербезпеці». Восьмисторінковий звіт є найдетальнішим дослідженням гіперавтоматизації кібербезпеки, опублікованим на сьогодні. У ньому підкреслюється зміна варти від застарілого SOAR до цього нового підходу, який швидко приймається підприємствами по всьому світу та зростаючою кількістю постачальників засобів автоматизації кібербезпеки.

«Існує справжнє занепокоєння, що поточні підходи до кібербезпеки недостатньо гнучкі, щоб встигати за розповсюдженням інструментів, новими поверхнями, перевантаженням даними та зловмисниками, посиленими генеративним штучним інтелектом», — йдеться у звіті, описуючи обмеження

застарілого SOAR. «Спільним для всіх цих платформ є те, що вони лише реакційні. Shift-left, ідея про те, що безпека починається з моменту розробки програми, не береться до уваги. Статистичні відомості про конфігурації, запобігання та правила й політику дрейфу з'являються лише в момент сповіщення. Незалежно від того, як ви це ділите, сучасні стратегії платформи кібербезпеки тримаються з невеликим відривом. Забагато процесів все ще виконується вручну».

Навпаки, у звіті досліджується, як Torq Hyperautomation, який тепер включає Torq Socrates, перший агент штучного інтелекту Tier-1 для аналізу кібербезпеки, перетворює SecOps за допомогою штучного інтелекту для гіперавтоматизації ключових операцій безпеки, включаючи сортування попереджень, контекстне збагачення даних, розслідування інцидентів, ескалацію., і відповідь.

За даними IDC, Torq Hyperautomation точно поєднує інтелектуальні сигнали з усіх корпоративних середовищ безпеки для забезпечення автономного відновлення. Він також навчається та розвивається, накопичуючи та аналізуючи події безпеки. Torq також представляє вражаючу нову ефективність і точність реагування на інциденти, які пом'якшують найбільш критичні проблеми, з якими стикаються аналітики безпеки, включаючи втому від сповіщень, помилкові спрацьовування, зниження видимості та виснаження роботи.

У звіті зазначено, що ключові переваги Torq Hyperautomation включають:

- Видимість і контроль гетерогенної нерухомості мережі та всіх середовищ для всіх процесів і рольових гравців
- Можливість передбачити прогалини в безпеці, завчасно оцінити стан мережі та в кінцевому підсумку захистити мережу
- Архітектура, керована подіями, на відміну від архітектури, керованої сповіщеннями SOAR, яка вирішує проблему втоми від сповіщень як прокляття існування операцій безпеки
- Розширювані можливості без використання коду, низького коду або повного коду з потенційним використанням генеративного ШІ для автоматизації ще більшої кількості завдань

- Проста, прозора модель розгортання, яка усуває приховані високі витрати на адаптацію SOAR, навчання та постійні професійні послуги

«Підхід гіперавтоматизації Torq є більш комплексним, ніж той, що пропонується в сучасних інструментах кібербезпеки», — підсумовується у звіті. «Кібербезпека повинна забезпечувати превентивні заходи, а також потужні можливості виявлення. Розчинний периметр є проблематичним, що лише посилює потребу в гнучкості та автоматизації. Torq будує філософію продукту, яка розглядає практичну конструкцію того, як виглядає сучасний бізнес, і те, як робочий процес і виявлення повинні виникати з цього».

«Як одна з найнадійніших і найвпливовіших аналітичних компаній у світі, IDC надала широку перевірку безпрецедентної цінності Torq Hyperautomation у автоматизації найскладніших корпоративних інфраструктур безпеки в надзвичайному масштабі», — сказав Леонід Белкінд, технічний директор і співзасновник Torq. «Цей звіт відображає неймовірний імпульс Torq, оскільки він забезпечує вкрай необхідну ефективність і підвищення продуктивності для команд SecOps. Простіше кажучи, Torq — це протиотрута від дедалі зростаючої неадекватності SOAR і приголомшливої втоми, яка виникає з цього. Ми пишаємося тим, що знаходимося в авангарді найважливіших інновацій, якими є гіперавтоматизація». ***(New IDC Cybersecurity Report Signals End of SOAR Era As Enterprises and Vendors Shift to Hyperautomation // Morningstar, Inc. (https://www.morningstar.com/news/business-wire/20230926641997/new-idc-cybersecurity-report-signals-end-of-soar-era-as-enterprises-and-vendors-shift-to-hyperautomation). 26.09.2023).***

***