**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

№ 4 (квітень)

Київ – 2024

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2024.– №4 (квітень) . – 320 с.

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

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

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

ЗМІСТ

«Голова СБУ Василь Малюк відсторонив керівника департаменту кібербезпеки Іллю Вітюка від виконання посадових обов'язків після розслідування журналістів «Слідства. Інфо».

Про це повідомили агентству Інтерфакс-Україна у пресслужбі СБУ.

На час проведення перевірок Вітюк проходитиме службу на фронті, де виконуватиме спецзавдання разом з «Альфою».

«Наразі він відряджений до підрозділу, сьогодні виїхав у район виконання бойових завдань», — повідомили у пресслужбі.

Розслідування «Слідства.Інфо»

Журналіст «Слідства.Інфо» Євгеній Шульгат 4 квітня оприлюднив розслідування про те, що дружина очільника департаменту кібербезпеки СБУ Іллі Вітюка у грудні 2023 року придбала квартиру у столичному житловому комплексі преміум-класу. У декларації посадовця зазначено, що за квартиру сплатили 12,8 мільйона гривень, хоча її ринкова її вартість перевищує 20 мільйонів.

«Слідство.Інфо» каже, що офіційного заробітку на цю квартиру Вітюку не вистачило б. Водночас його дружина Юлія почала займатися бізнесом невдовзі після призначення чоловіка на цю посаду. В СБУ запевнили, що її заробітку вистачає на придбану нерухомість.

Після цього агенція журналістських розслідувань заявила, що представники військкомату намагалися вручити повістку їхньому журналісту Шульгату Працівник СБУ міг давати вказівки представникам ТЦК вручити повістку журналісту «Слідство.Інфо» за вказівкою працівника СБУ. У такий спосіб спецслужбовці нібито хотіли «покарати» розслідувача.

У пресслужбі СБУ сказали, що перевіряють цю інформацію спільно з Міноборони та Генштабом ЗСУ. Офіс генерального прокурора відкрив кримінальне провадження Офіс генпрокурора почав провадження через інцидент з повісткою журналісту «Слідство.Інфо» за фактом інциденту. У командуванні Сухопутних військ заявили, що проводять службову перевірку, щоб встановити всі обставини події. Службову перевірку доручив провести й головнокомандувач ЗСУ Олександр

Сирський». ***(Софія Телішевська. Голова СБУ відсторонив керівника департаменту кібербезпеки Вітюка на час перевірки // Бабель (https://babel.ua/news/105855-golova-sbu-vidstoroniv-kerivnika-departamentu-kiberbezpeki-vityuka-pislya-publikaciji-rozsliduvannya). 09.04.2024).***

***

Національна система кібербезпеки

«Ізраїль все ж таки вирішив зробити з двох національних служб кібербезпеки одну, єдину. Про тамтешню систему і що було у них до того я детально розказував півроку тому.

То що ж змінилося?

Ще півроку тому в Ізраїлі один кібер-орган формував політики, стратегії, візії, затверджував стандарти та розробляв методики. А другий – виконував те все. Типу як законодавчий та виконавчий орган, тільки в кібер-сфері.

Аж ось тепер прийнято рішення злити їх в один-єдиний орган. Чому саме таке рішення прийнято – складно сказати. Думаю, прихильники жорсткої консолідації наявних ресурсів під час війни навели більше аргументів.

Але в Україні під час війни відбуваються чомусь рівно протилежні процеси. «Основних суб'єктів забезпечення кібербезпеки» - 11 (одинадцять, Карл!) Без довіри між ними, без єдиного центру, без координації, без якоїсь системності. Взаємодія між цими 11 няньками слабка і здебільшого декоративна, оскільки усі вони між собою активно конкурують, щоб більше сподобатися Самому Головному та отримати жирніший шматок бюджету. Закон «десь щось про кібербезпеку» вийшов у 2017 році вже кривим та непрацюючим, але за 5 років тотального домінування в усіх гілках влади зелені жижиталізатори так і не спромоглися написати хоча б якийсь притомний Закон про кібербезпеку.

Але у сфері «наступальної кібербезпеки» ситуація ще менш райдужна. Команди «бойових хакерів» існують не тільки у кожній силовій структурі, але навіть у деяких напів-цивільних та суто цивільних відомствах, типу Мінцирку. А

ще є багато суто волонтерських команд, і хоча б приблизну їх кількість (а тим більше склад та чисельність) не знає абсолютно ніхто. З одного боку, така децентралізація сприяє режиму секретності, і також це унеможливлює знищення всієї системи одним потужним ударом по її мозку. А з іншого боку, системи-то взагалі не існує як такої. І це досить часто заважає самим командам досягати поставлених цілей. Скажімо, серйозні хакери довго, обережно та непомітно «прокрадаються» всередину мережі ворожого військового заводу, аж тут з криками «егегей» на мережі цього ж заводу налітає мінциркова гопота, шкоди майже не наносить, але перепаскуджують довгу та складу операцію своїх колег. І подібних випадків прямої шкоди через нескоординованість дій – безліч. Деякі відповідальні групи намагаються домовлятися між собою, але це більше джентльменські домовленості, неформальні, на горизонтальному рівні. Які перестають працювати у випадку, скажімо, «сорі, наш головний дав команду херачити». І ще один момент поза увагою: аналіз технічних даних. Кожен грамотний хакер скаже вам, що головна проблема не стільки здобути дані з ворожих мереж, скільки проаналізувати здобуте. Усі ж чули щось на кшталт «Українські хакери зламали ворожу систему та витягли XXX-гігабайт даних»? А хтось знає, що зазвичай відбувається після такого «довго і щасливо»? А я вам скажу: більшість здобутою інформації не аналізується взагалі – немає людей, усі побігли знов «здобувати дані». Петабайти цінної розвідувальної інформації лежать на далеких серверах без діла. Тому що для аналізу даних потрібно у рази більше людей, ніж для їх здобуття. Тому що треба місяцями перебирати руками терикони інформаційного шлаку, щоб знайти золоту крупинку. І при цьому аналіз має проводити людина хоч з якимось з досвідом – бажано у кібер/розвідці/безпеці - яка здатна відрізнити шлак від скарбу. Та й з досвідом це не завжди просто насправді.

В Україні вирішити ці дві серйозні проблеми – координація кібер-операцій та аналіз масивів цифрових даних – могла б спеціалізована агенція. Наприклад, у США цими питаннями вже 72 роки займається National Security Agency, яку вважають найпотужнішою технічною розвідкою Світу. І питання створення щось типу Агентства технічної розвідки вже кілька місяців лунає у високих кабінетах.

Тому що це логічно, як на мене: консолідувати експертизу в єдиний кулак, а не «усі потроху хто як розуміє». Але поки що безрезультатно. Головна перепона – амбіції окремих начальників та конкуренція між відомствами, небажання ділитися бюджетами та славою «незламного кібербійця» в очах Самого. Тому поки що вся ця діяльність залишається напів-хаотичною партизанщиною, при тому, що наші західні союзники принципово не допомагають українським наступальним кібер-операціям. А от якщо б це була легальна державна інституція – могли б допомагати, хоча б досвідом, why not. За умови, що керівників призначатимуть за конкурсом на профпридатність, а також серйозно перевірятимуть доброчесність, щоб не вийшло чергове корупційне держспецніхуа.

Але поки в Україні замість інституцій керують незрозумілі «5-6 ефективних менеджерів» (С) без державницького підходу – не буде у нас «як в Ізраїлі», навіть близько. Буде вічне «маємо те, що маємо».

P.S.: Прошу не плутати систему національного кіберзахисту та «ударний кіберпотенціал» - це різні напрямки роботи, з різними підходами, методами, стратегією та з різною кінцевою метою. На мою думку, умовна «агенція кібербезпеки» має бути окремим цивільним органом, а умовне «відомство аналізу цифрових даних» - окремим розвідувальним органом. І при цьому тісно співпрацювати. Щоб побудувати збалансовану систему цього всього, потрібен мозковий штурм високорівневих експертів. А не ту, шо у нас: в основному випадкові невігласи, зайняти переважно розпилами». ***(Костянтин Корсун. Кібербезпека: Україна - не Ізраїль // Цензор.НЕТ (https://censor.net/ru/blogs/3483155/kiberbezpeka_ukrayina_ne_izrayil). 08.04.2024).***

***

Правове забезпечення кібербезпеки в Україні

«Законодавче визначення кібервійни потрібне, щоб захистити українських фахівців, які виконують наступальні операції проти російських загарбників у кіберпросторі.

Таку думку висловив Українському радіо інженер із кібербезпеки компанії OptiData Владислав Радецький, коментуючи ініціативу Міноборони із законодавчого визначення поняття «кібервійна».

Він наголосив, що на полі бою воїн ЗСУ є прозорим перед законом – він виконує свою функцію — захищає свою землю. Разом з тим люди, які здійснюють будь-які наступальні кібероперації проти загарбників, з позиції закону досі перебувають у сірій зоні.

Це дуже позитивний сигнал, і нам як державі це справді потрібно, - заявив Радецький, коментуючи ініціативу Міноборони щодо законодавчого визначення терміну «кібервійна». – Але треба зрозуміти, що тут є багато роботи. Мало просто ввести це поняття у правову сферу. Якщо є кібервійна, то потрібно мати кібервійсько та кіберкомандування, аби це поняття не було просто на папері. Що це може нам дати в короткостроковій перспективі? Як тільки все буде оформлено на законодавчому рівні, це дасть можливість захисту фахівців з нашого боку. У нас є підрозділи з кібероперацій у силових структурах, а також різні спільноти — «Кіберспротив», «Кіберальянс». Тобто визначення кібервійни нам потрібне, щоб ми могли захищати своїх фахівців, які виконують певні наступальні операції. Якщо порівняти з військовими на полі бою, то там усе зрозуміло: український захисник, який веде вогонь по піхоті чи машинах загарбників, прозорий перед законом, він виконує функцію — захищає свою землю. Зараз усі люди, які здійснюють будь-які наступальні кібероперації проти загарбників, з точки зору закону перебувають у сірій зоні. Тому нам це визначення потрібно для захисту наших сил кіберспротиву. І другий момент — це дозволить покращити і посилити притягнення до відповідальності російських угруповань та, сподіваюся, вплине на посилення санкцій у розрізі програмного забезпечення та послуг, які ще й досі можуть надаватися на території РФ», – сказав Радецький…» ***(Законодавче визначення кібервійни допоможе українському кібернаступу – експерт // Укрінформ (https://www.ukrinform.ua/rubric-technology/3847725-zakonodavce-viznacenna-kibervijni-dopomoze-ukrainskomu-kibernastupu-ekspert.html). 02.04.2024).***

***

«Міністерство оборони України затвердило рішення щодо основних засад інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах.

Про це повідомляє пресслужба Міноборони.

Відтепер усі системи, сервіси, застосунки та цифрові інструменти Міністерства оборони матимуть єдині, чітко визначені правила щодо кібербезпеки.

Правила враховуватимуть кращі підходи НАТО та міжнародні стандарти.

«Під час постійних кібератак ворога ми маємо приділяти особливу увагу кібербезпеці. Заходи з кібербезпеки повинні бути системними та постійно вдосконалюватись. Тому нова політика передбачає систематичний перегляд та оновлення вимог Міністерства у сфері кібербезпеки», — підкреслила Катерина Черногоренко, заступниця Міністра оборони з цифровізації, цифрових трансформацій та цифрового розвитку». ***(Іванна Капустянська. Міноборони затвердило основні засади інформаційної безпеки та кібербезпеки // LB.ua (https://lb.ua/news/2024/04/21/609526_minoboroni_zatverdilo_osnovni.html). 21.04.2024).***

***

Кібервійна проти України

«Українські хакери, які можуть бути пов'язані з кіберфахівцями Служби безпеки України, знищили дата-центр, яким користувалися російський військово-промисловий, нафтогазовий і телекомунікаційний комплекси, повідомило агентству «Інтерфакс-Україна» інформоване джерело.

«У хмарному сервісі OwenCloud.ru свої дані містили понад 10 тисяч юросіб - підприємства російського ВПК, нафтогазового, металургійного, авіакосмічного комплексів, а також телекомунікаційні гіганти», - розповів співрозмовник агентства в понеділок.

Він уточнив, що йдеться про такі підприємства: «Уральський завод цивільної авіації», «НВП «РУБІН» (входить до складу холдингу «Роселектроніка»), «Уральський завод спецтехніки», «Газпром», «Трансгаз», «Лукойл», «Роснафта», «Норильський нікель», «Ростелеком», «Телеком», «Мегафон».

Співрозмовник агентства зазначив: «Це була спільна операція української хакерської групи BLACKJACK і кібердепартаменту СБУ. Вони знищили понад 300 Тб даних. Це 400 віртуальних і 42 фізичні сервери, на яких розміщувалася внутрішня документація, резервні копії та інші програми, через які клієнти віддалено керували виробничими процесами на підприємствах».

Джерело додало, що знищення російського хмарного сервісу стало відплатою за атаку на український дата-центр «Парковий» у січні цього року». ***(Українські хакери знищили рашистський дата-центр // Агенція інформації та аналітики (https://galinfo.com.ua/news/ukrainski_hakery_znyshchyly_rashystskyy_datatsentr_416454.html). 08.04.2024).***

***

«Кіберфахівці та слідчі Служби безпеки України збирають доказову базу на хакерів головного розвідувального управління генерального штабу рф (більш відомого як гру), які здійснили атаку на одного з національних операторів мобільного зв'язку «Київстар». Після проведення всіх експертиз та оголошення підозр матеріали цього розслідування будуть передані до Міжнародного кримінального суду у Гаазі.

Про це повідомив начальник Департаменту кібербезпеки СБУ Ілля Вітюк в інтерв'ю інформаційному агентству «Укрінформ».

«Ми працюємо, щоб за нашим законодавством оголосити підозри, а у подальшому передати ці справи в МКС. Воєнних злочинців мають судити на міжнародному рівні!» - зазначив Ілля Вітюк, підкреслюючи, що кібератаки по цивільній інфраструктурі мають бути визнані воєнними злочинами.

Наразі СБУ встановила, що атаку на «Київстар» реалізувало хакерське угруповання SandWorm, яке є штатним підрозділом російського гру.

За словами очільника Департаменту кібербезпеки, зараз СБУ проводить низку експертиз щодо уражених хакерами систем і завданих збитків. Також спецслужба спрямувала запити на отримання додаткової інформації від міжнародних партнерів.

Ілля Вітюк підкреслив, що у межах кримінального провадження ДКІБ опрацьовує всіх учасників вертикалі, які були причетні до цієї атаки.

«Відповідати за скоєне має не лише конкретний хакер, але і, як мінімум, керівник військової частини і керівництво спецслужби, яка здійснює деструктивну діяльність», – переконаний керівник ДКІБ.

Водночас він підкреслив, що у світі налічується лише три кейси, коли оголошувалися підозри хакерам за кібератаки на інфраструктуру. При чому один із них – якраз результат СБУ.

Також Ілля Вітюк розповів, що загалом під час повномасштабної війни Служба безпеки блокує по 4,5 тис. кібератак щороку.

Особливим пріоритетом у кіберзахисті є Збройні сили України та Міноборони, оскільки спроби втручань ворога у військові системи відбуваються регулярно. Відповідні заходи Департамент кібербезпеки СБУ проводить у взаємодії з Департаментом військової контррозвідки СБУ, кіберцентром Міноборони, Генштабом та Командуванням військ зв'язку та кібербезпеки.

«Співробітники ДКІБ на постійній основі працюють у військових частинах, штабах, їздять на передову, перевіряють пристрої та системи на предмет несанкціонованого втручання», – зазначає Ілля Вітюк. Зокрема, СБУ запобігла технічному проникненню ворога на 1700 пристроїв українських військових.

Окрім кібератак російські спецслужби проводять ІПСО для дискредитації командування Сил оборони. Наприклад, були інформатаки і спроби зламу офіційних акаунтів, а також створення десятків фейкових сторінок головкома Олександра Сирського.

Подібні дискредитаційні атаки ворог проводить і стосовно співробітників СБУ: їм надходять погрози фізичної розправи, листи із ознаками вербування і

шантажу тощо. Ілля Вітюк відзначив, що й по ньому особисто вже були фейкові вкиди і можливі нові атаки.

«Інформацією дуже просто маніпулювати, щоб спробувати вплинути на когось, проте ми готові і до таких методів ведення війни», – резюмував він». ***(СБУ ідентифікувала хакерів російського гру, які атакували «Київстар», і передасть матеріали справи в Гаагу, – Ілля Вітюк // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-identyfikuvala-khakeriv-rosiiskoho-hru-yaki-atakuvaly-kyivstar-i-peredast-materialy-spravy-v-haahu-illia-vitiuk). 04.04.2024).***

***

«Російські хакери, які працюють у штаті спецслужб, намагалися заразити шкідливим програмним забезпеченням військові системи зв'язку «Кропива», «Дельта», «Гризельда» і «Графіт» Збройних Сил і Міністерства оборони України.

Про це розповів в інтерв'ю Укрінформу начальник Департаменту кібербезпеки СБУ Ілля Вітюк.

За його словами, фахівці департаменту провели кібероборонну операцію за стандартами НАТО, під час якої вичистили присутність російських хакерів з військових систем зв'язку «Кропива», «Дельта», «Гризельда», «Графіт». Завдяки цьому було припинено отримання ворогом важливої розвідінформації.

Вітюк уточнив, що лише у системі «Кропива» близько 1700 пристроїв могли бути заражені шкідливим програмним забезпеченням хакерського угруповання SandWorm, яке входить до структури ГРУ ГШ РФ.

«Угруповання хакерів працювало на території Донецької області, щоб мати потрібні доступи. Коли когось із наших захисників брали у полон, то забирали в них телефони чи планшети зі встановленими «Кропивою» і «Дельтою», вивчали як працюють ці системи і надалі розробляли під них шкідливе програмне забезпечення, щоб проникнути до листувань і документів.

Також у одного ШПЗ була спеціальна мета - отримати конфігурації зі Старлінків. Таким чином вони могли знати точні дані про кількість під'єднаних до

них пристроїв, з'ясувати розташування штабів, орієнтовну кількість осіб у певному місці, а тоді коригувати туди артилерійські чи ракетні удари», - розповів Вітюк.

За словами начальника Департаменту кібербезпеки СБУ, наразі Збройні сили України та Міністерство оборони є пріоритетом у кіберзахисті. Співробітники департаменту на постійній основі працюють у військових частинах, штабах, їздять на передову, перевіряють пристрої на предмет несанкціонованих втручань, спроби яких не припиняються». ***(Російські хакери намагалися вразити військові системи зв'язку Міноборони – СБУ // Укрінформ (https://www.ukrinform.ua/rubric-ato/3848405-rosijski-hakeri-namagalisa-vraziti-vijskovi-sistemi-zvazku-minoboroni-sbu.html). 04.04.2024).***

***

«Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, повідомляє про підвищену активність угруповання UAC-0184, яке намагається отримати доступ до комп'ютерів військовослужбовців з метою викрадення документів та даних месенджерів.

Зловмисники використовують популярні месенджери, соціальні мережі та інші платформи для знайомств та спілкування з метою розповсюдження шкідливих програм. Їхні методи включають:

- супровідні повідомлення-приманки: наприклад, про відкриття виконавчого провадження/кримінальної справи; відео бойових дій; запит на знайомство тощо;
- файли (архіви) з проханням допомогти у їх відкритті/обробці.

📩 Зловмисники застосовують такі шкідливі програми, в тому числі для викрадення та вивантаження даних з комп'ютера, зокрема повідомлень і контактних даних месенджера Signal, який є доволі популярним серед військових.

❗ Звертаємо увагу, що:

- зловмисники продовжуватимуть вдосконалювати способи доставки шкідливих програм через месенджери;

- будь-яка необачна онлайн-активність військовослужбовця (наприклад, публікація фото у військовій формі) полегшує зловмисникам визначення пріоритетних цілей для атак…» ***(CERT-UA попереджає про кіберзагрозу для Сил оборони України // Україна кримінальна (https://cripo.com.ua/news/war/cert-ua-poperedzhaye-pro-kiberzagrozu-dlya-syl-oborony-ukrayiny/). 17.04.2024).***

***

«Війна в Україні відбувається на всіх фронтах. Країна-агресор залучає всі можливі ресурси, щоб блокувати всі сфери життя українців. Це також стосується цифрових технологій та атак на них: кібервійна продовжує йти з першого дня вторгнення. Росіяни постійно проводять атаки на цифрову інфраструктуру, маючи різний успіх.

В умовах війни сторони використовують всі ресурси, але залишається відкритим юридичний бік цифрового протистояння. Європейська Асоціація програмної інженерії провела інтерв'ю з Максимом Курочко, керуючим партнером та адвокатом об'єднання MK Legal Service та його колегою Артемом Остапенко, керівник IT/TMT практики, щоб дізнатися, які сервіси найбільше наражені на небезпеку атак та чи є це законним.

В першу чергу, варто зазначити, що цілі та об'єкти атак в інших країнах та в мирний час відрізняються від того, що зараз відбувається в Україні. Зазвичай метою атаки на компанію може бути бажання отримати викуп будь-яким шляхом. Проте в умовах війни зловмисники мають іншу задачу: паралізувати всю можливу інфраструктуру та ускладнити життя громадян. Також атаки є невіддільною складовою інформаційної війни.

За спостереженнями експертів, найчастіше об'єктами кібератак є інформаційно-комунікаційні системи операторів критичної інфраструктури, адміністраторів державних реєстрів, та баз даних, компаній які надають масові загальнодоступні послуги через Інтернет. Найпомітнішим кейсом такої атаки було падіння «Київстару» в грудні минулого року, проте атаки менших масштабів відбуваються регулярно.

Хоча не завжди хакери відкрито беруть на себе відповідальність за атаку, ні для кого не секрет, що за ними стоять російські спецслужби. За допомогою атак хакери не тільки намагаються паралізувати критичну інфраструктуру та блокувати діяльність ресурсів державної влади, а також здобувати персональні дані українців та використовувати їх зі злочинними намірами.

Що стосується питання законності таких атак, то законодавство кожної країни регулює питання хакерства окремо. Проте не існує організації, яка б контролювала порушення на міжнародному рівні, тому притягти російських хакерів до відповідальності наразі складно. Однак варто згадати, що українські айтівці атакують ворожі ресурси не менш активно, тому це протистояння продовжується на рівних умовах.

В умовах постійних атак потрібен захист. На тлі цього експерти зазначають, що можливості українських фахівців з кібербезпеки значно зросли, як і технічні можливості. MK Legal Service також докладає зусиль до цього напрямку, маючи ряд успішних кейсів». ***(Герман Богапов. Які українські сервіси є головною мішенню кібератак // HiTech.Expert. (https://expert.com.ua/181094-yaki-ukrainski-servisy-ye-golovnoyu-mishennyu-kiberatak.html). 18.04.2024).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Національний банк України продовжує співпрацю з Міністерством фінансів Сполучених Штатів Америки у сфері забезпечення кібербезпеки в банківському та фінансовому секторах України. З цією метою сторони підписали Меморандум про взаємодію та співробітництво, повідомила пресслужба НБУ.

«Зміцнення кібербезпеки та спільна протидія актуальним кіберзагрозам вкрай важливі для стабільної та безперервної роботи українського фінансового сектору. Особливо актуальним це питання є в умовах гібридної війни, яку вже третій рік РФ

веде проти України на додачу до повномасштабної військової агресії», - наголосив голова НБУ Андрій Пишний.

За його словами, співпраця НБУ та Міністерства фінансів США в цьому напрямі дасть змогу й надалі підтримувати ефективну систему захисту банків та фінансових установ від кіберзагроз, зокрема в умовах воєнного стану, та забезпечувати сталість фінансових ринків.

Зазначається, що Меморандум набув чинності 4 квітня 2024 року. Він визначає методи обміну інформацією про загрози кібербезпеці та інциденти, учасників кіберзагроз, а також дає змогу сторонам проводити спільні навчання, експерті форуми тощо.

Метою цього документа є організація взаємодії між Національним банком України та Міністерством фінансів США для:

- реалізації механізмів обміну інформацією у сфері кібербезпеки та актуальних кіберзагроз;
- подальшого розвитку Центру кіберзахисту Національного банку (CSIRT-NBU);
- розроблення та реалізації заходів підтримки Національного банку з питань кібербезпеки в банківському та фінансовому секторах України…». ***(Юрій Мирний. США допоможуть захистити банки та фінустанови України від кіберзагроз: деталі // Деньги.ua (https://dengi.ua/ua/finance/7501735-ssha-pomogut-zaschitit-banki-i-finuchrezhdeniya-ukrainy-ot-kiberugroz). 08.04.2024).***

***

«З нагоди Міжнародного дня інтернету в Україні за підтримки ЄС запущено портал «Кібер Брама». Про це повідомляється на порталі Східного партнерства.

Проєкт було створено Консультативною місією Європейського Союзу (КМЄС) в Україні за ініціативи Департаменту кіберполіції Національної поліції України в партнерстві з ГО MINZMIN та за сприяння Міжнародного фонду «Відродження» й фінансової підтримки ЄС.

«Кібер Брама» допоможе українцям безпечно користуватись всесвітньою мережею, попереджати та протидіяти злочинним діям в інтернеті й не стати жертвою ворожої пропаганди.

Поради щодо безпеки та інформацію про поточні загрози можна знайти в розділах:

«Кібербезпека в освіті»,

«Кібербезпека в роботі»,

«Кібербезпека в повсякденному житті»,

«Кібербезпека в розвагах і спілкуванні»

та «Кібербезпека під час війни».

Команда порталу також створила путівник зі списком і описом ігор, програм і соціальних мереж в Україні та поясненням, як захистити вашу інформацію.

Портал дозволяє користувачам зв'язатися з Департаментом кіберполіції, щоб повідомити про кіберзлочин, а також звернутися до технічної підтримки популярних месенджерів і соціальних мереж, щоб повідомити про проблему». ***(Анна. В Україні за підтримки ЄС запущено новий портал з кібербезпеки «Кібер Брама» // МИГ (https://mig.com.ua/v-ukraini-za-pidtrymky-ies-zapushcheno-novyj-portal-z-kiberbezpeky-kiber-brama/). 07.04.2024).***

***

Світові тенденції в галузі кібербезпеки

«Bitdefender замовив Censuswide, сторонню опитувальну компанію, щоб оцінити мислення споживачів щодо кібербезпеки на трьох континентах. 7335 респондентів віком від 16 до 55 років із США, Великої Британії, Німеччини, Іспанії, Франції, Італії та Австралії поділилися своїм досвідом, страхами та занепокоєнням щодо поточного цифрового ландшафту та кіберзлочинності – від фішингу, викриття даних і зловмисного програмного забезпечення до SMS-шахрайства, штучного інтелекту та безпеки дітей в Інтернеті.

Подібності та відмінності в поведінці та поглядах споживачів у різних регіонах були цікавими, а часом і дивовижними.

Керуючи до десяти облікових записів кожен, чверть користувачів мережі кажуть, що зазнали принаймні одного інциденту безпеки за останні 12 місяців. Майже половина зіткнулися зі спробою шахрайства через текстові повідомлення, але значною мірою покладаються на свій телефон для здійснення конфіденційних транзакцій. Поведінка споживача не завжди відповідає висловленим страхам і занепокоєнням. Наприклад, виявилося, що хоча багато хто побоюється, що кіберзлочинці шукають їхню кредитну картку чи особисту інформацію, вони мало роблять для її захисту.

Опитування та аналіз проводилися з грудня 2023 року по січень 2024 року. Ось деякі основні висновки:

Сьогодні користувачі мережі мають у середньому від 3 до 5 онлайн-акаунтів (35%), хоча значна частка (31%) має 6 або більше. Однак респонденти, ймовірно, забули включити облікові записи, які вони створили з примхи – щоб насолодитися швидким обслуговуванням або одноразовою покупкою. Електронним громадянам важливо враховувати це в час, коли витоки даних стали повсякденним явищем, особливо якщо вони піддаються зручності використання одного пароля для кількох облікових записів.

Майже чверть респондентів (24,3%) сказали, що вони зазнали принаймні одну подію безпеки протягом останніх 12 місяців. Австралійці повідомили про найбільше зіткнень з кіберзлочинністю, 37,6%, або на 12% вище загального середнього, за ними йдуть Іспанія (27,9%), США (26,7%), Німеччина (26,3%), Франція (19,6%), Великобританія (17,2%) та Італії (16,1%). У 2023 році Австралія зазнала низки витоків даних, що допомагає пояснити, чому вона лідирує серед інцидентів, про які повідомляють споживачі.

SMS-шахрайство (45,4%) є найпоширенішою подією безпеки, за нею йдуть спроби шахрайства (44,4%) і фішингові електронні листи (42,1%). 27,5% повідомлених інцидентів викликало розкриття даних, за ним йшло зараження зловмисним програмним забезпеченням (16,4%) і doxxing (9,2%).

Респонденти, які кажуть, що можуть розпізнати шахрайство, частіше стикалися з інцидентом безпеки (29%), ніж ті, хто не завжди (24%) або ніколи (16%) не розпізнавали шахрайство. Це може означати, що ті, хто не може розпізнати шахрайство, стикалися з ним, не знаючи.

Майже 4 з 5 (78,3%) сказали, що використовують свій смартфон для банківських операцій, доступу до даних охорони здоров'я, управління інвестиціями, торгівлі криптовалютою – загалом, для керування важливими даними та проведення конфіденційних транзакцій. І це незважаючи на те, що споживачі найбільше бояться кібербезпеки через те, що хакери отримають доступ до їхніх фінансів, водночас нехтуючи адекватними методами безпеки.

Керування паролями залишається одним із найслабших місць споживачів: 37% користувачів мережі записують свої паролі, 18,7% використовують той самий пароль для трьох або більше облікових записів, а 15,8% використовують той самий пароль принаймні для двох облікових записів.

Перш ніж відповісти, для чого вони використовують VPN, 48,3% респондентів прямо сказали, що не користуються нею взагалі. З тих, хто користується VPN, 27% кажуть, що це для пошуку пропозицій на основі місцезнаходження або перегляду вмісту, недоступного в їхньому регіоні.

Переважна більшість сказали, що вони «стурбовані» або «дуже стурбовані» наслідками ШІ для безпеки та конфіденційності. Лише 8,4% відповіли, що їх це взагалі не турбує. Подібним чином близько 70% сказали, що вони стурбовані конфіденційністю та безпекою дітей в Інтернеті. Третій сказав, що вони дуже стурбовані.

Майже чверть користувачів мережі (24,2%) вважають, що вони є мішенню для кіберзлочинців.

Наш безкоштовний звіт розширює ці ключові висновки, а також інші з розподілом за регіонами, віком і статтю для кожної охопленої теми. Незалежно від того, чи є ви журналістом, спеціалістом із кібербезпеки чи звичайним користувачем мережі, звіт Bitdefender 2024 Consumer Cybersecurity Assessment Report є цінним ресурсом для всіх, хто цікавиться сучасними загрозами кібербезпеки, що

розвиваються». ***(Filip TRUȚĂ. Bitdefender Releases 2024 Consumer Cybersecurity Assessment Report // Bitdefender (https://www.bitdefender.com/blog/hotforsecurity/bitdefender-releases-2024-consumer-cybersecurity-assessment-report/?utm_source=flipboard&utm_content=rhudaur%2Fmagazine%2FCybersecurity%20Today%2F). 03.04.2024).***

***

«Південна Корея готується головувати на засіданні Ради Безпеки ООН з питань кібербезпеки в четвер, щоб пролити світло на наслідки кіберзагроз і зловмисної кібердіяльності, включаючи маневри Північної Кореї, спрямовані на порушення санкцій у кіберпросторі, на міжнародний мир і безпеку.

Головування на першому в Південній Кореї засіданні за формулою Аррія — неформальному зібранні, скликаному членом або членами Ради Безпеки — є важливою віхою для Кореї з моменту вступу на посаду непостійного члена Ради Безпеки в січні.

Хоча кібербезпека офіційно не входить до порядку денного Ради Безпеки, члени скликали зустрічі за формулою Арріа, окремо від офіційних сесій, щоб обговорити критичну проблему та її наслідки для міжнародного миру та безпеки. Головний обов'язок Ради Безпеки, який складається з 15 членів, полягає в підтримці міжнародного миру та безпеки.

Південна Корея організовує зустріч за формулою Арріа під назвою «Розвиток ландшафту кіберзагроз та його наслідки для підтримки міжнародного миру та безпеки», а Сполучені Штати та Японія виступають співорганізаторами.

Зустріч за формулою Аррія обговорюватиме мінливий ландшафт кіберзагроз, включаючи такі теми, як програмне забезпечення-вимагач і крадіжка криптовалюти, як зазначено в концептуальній записці зустрічі, наданій місіями Південної Кореї, США та Японії в ООН у середу.

Інші теми для обговорення включають поширення зловмисників у кіберпросторі та необхідність міжнародного співробітництва для протистояння зростаючій складності кіберзагроз.

Кібербезпека є одним із ключових тематичних питань, які Південна Корея прагне висвітлити в Раді Безпеки як член, поряд із підтриманням та розбудовою миру; жінки, мир і безпека; клімат і безпека.

Зосередженість Сеула на кібербезпеці є особливо актуальною, враховуючи, що в звітах ООН про ухилення Північної Кореї від санкцій у березні зазначено, що 40 відсотків програм зброї масового знищення в Північній Кореї фінансуються за допомогою незаконних кібермереж.

Метою зустрічі є «сприяти кращому розумінню впливу різних зловмисних кібер-дій, які характеризуються як кіберзлочинність, на міжнародний мир і безпеку, включаючи нерозповсюдження зброї масового знищення, що включає дії, що характеризуються як кіберзлочинність, та іншу існуючу архітектуру роззброєння, і санкцій Ради Безпеки", - йдеться в записці.

Концептуальна записка зустрічі також визначає кіберзлочини Північної Кореї, спрямовані на обхід резолюцій Ради Безпеки ООН, як ключовий пункт порядку денного для обговорення.

У концептуальній записці, зокрема, цитується звіт ООН, у якому стверджується, що «незаконні прибутки однієї держави-члена від зловмисної кіберактивності складають приблизно половину її доходів в іноземній валюті, і відомо, що близько 40 відсотків її програм зі зброї масового знищення (ЗМЗ) фінансуються незаконні кіберзасоби», без прямого назви Північної Кореї.

«Національні держави та недержавні суб’єкти, до яких введені санкції Ради Безпеки ООН, все більше використовують прибутки від кіберзлочинів як життєво важливий інструмент для ухилення від режимів санкцій, встановлених Радою Безпеки ООН, підриваючи ефективність колективної роботи Ради Безпеки», — йдеться в концептуальній записці. читати.

Іншою ключовою метою зустрічі є «обговорення та надання можливих рекомендацій щодо посилення ключової ролі Ради Безпеки ООН і всебічної участі у боротьбі з багатогранною природою кіберзагроз».

Посол Південної Кореї в ООН Хван Чжун Кук раніше підкреслював нагальну потребу в розгляді кіберпроблем у Раді Безпеки ООН, посилаючись на отримання незаконних доходів Північної Кореї в кіберпросторі як головну проблему.

«Кібербезпека ще офіційно не входить до порядку денного Ради Безпеки. Проте сьогодні існує широкий консенсус щодо того, що кібератаки становлять значну загрозу миру та безпеці для всіх країн на всіх рівнях», — сказав Хван під час заходу, організованого Нью-Йоркським університетом. штаб-квартиру Корейського товариства в березні.

Потім Хван заявив, що наразі Північна Корея отримує приблизно мільярд доларів щорічного доходу виключно за рахунок кіберзлому іноземних банків і криптовалютних бірж для фінансування своїх програм ЗМЗ.

«Незважаючи на відсутність консенсусу в Раді Безпеки щодо того, як вирішувати нові проблеми кібербезпеки, Республіка Корея прагне підвищити свій профіль у роботі Ради», — підкреслив Хван». ***(Ji Da-gyum. S. Korea to chair first UN Security Council meeting with focus on cyber threats // Herald Corporation (https://www.koreaherald.com/view.php?ud=20240404050732). 04.04.2024).***

***

«У четвер, 4 квітня 2024 р., відбулося останнє засідання Ради Безпеки ООН (РБ ООН) за формулою Арріа на тему, пов’язану з кібернетичною діяльністю. Організовано Республікою Корея (РК) та спільно організовано Японією та Сполученими Штатами (США), сесія була зосереджена на «Ландшафті кіберзагроз, що розвивається, і його наслідках для підтримки міжнародного миру та безпеки».

Неформальна зустріч включала виступи понад 30 делегацій, яким передували технічні брифінги заступника Верховного представника з питань роззброєння Адедеджі Ебо; Директор Інституту дослідження проблем роззброєння ООН

(UNIDIR) Робін Гайс; і Валері Кеннеді, директор відділу розвідувальних рішень для розслідувань і спеціальних програм компанії Chainalysis, що займається аналізом блокчейнів.

У своїй концептуальній записці до наради Південна Корея встановила цілі скликання: підвищити обізнаність членів щодо проблем, що розвиваються в кіберпространстві, сприяти кращому розумінню кіберзлочинності у зв'язку з міжнародним миром і безпекою, а також надати рекомендації щодо покращення роботи Ради роль у протидії цим загрозам у спосіб, який доповнює поточну роботу на Генеральній Асамблеї ООН (ГА ООН).

Ландшафт загроз, що розвивається

У заявах, зроблених на зустрічі Arria-formule, було охоплено широкий спектр загроз, що виникають і розвиваються, таких як криптовалюта та квантові обчислення, а також шкідливі кіберінструменти, такі як програми-вимагачі та комерційно доступні засоби вторгнення. Були також висловлені занепокоєння щодо використання цих інструментів кіберзлочинцями, і кілька делегацій висловили занепокоєння щодо кібертероризму. Про штучний інтелект (ШІ) також думали кілька держав, зокрема США, Словенія, Катар, Італія, Сьєрра-Леоне та Еквадор. Більшість із цих делегацій вказали на наслідки безвідповідального використання ШІ в інформаційній сфері для демократичних процесів і верховенства права; наприклад, Словенія охарактеризувала ШІ як «прискорювач» інших кіберзагроз. Проте кілька делегацій визнали потенційні позитивні переваги ШІ для кіберзахисту або стійкості.

Більшість підкреслювали серйозність атак програм-вимагачів, часто в контексті критичної інфраструктури. Коста-Ріка, яка оголосила надзвичайний стан після серії руйнівних кібератак проти урядових і фінансових установ у 2022 році, зазначила, що міжнародне гуманітарне право (МГП) забороняє невибіркові атаки на цивільні об'єкти. Він також визнав значні гуманітарні страждання, які є результатом атак на цивільну інфраструктуру, таку як лікарні та електромережі.

У своїх технічних брифінгах для членів доповідачі відзначили, що кіберзагрози більше не обмежуються окремими технологіями чи наступальними та

військовими застосуваннями. Продаж цих інструментів як послуг на відкритому ринку дозволяє поширювати їх серед нерегульованих учасників. Коста-Ріка закликала до універсального правового стандарту згідно з МГП, щоб усунути цю сіру зону та захистити малі держави від зловмисної кібер-діяльності, яка завдає шкоди функціональності цивільної інфраструктури.

Простір між малоінтенсивними фінансово вмотивованими кіберзлочинами та руйнівними великомасштабними кібератаками звужується, залишаючи позаду «сіру зону», де можливості та інструменти поєднуються для досягнення дестабілізуючих наслідків як під час конфлікту, так і в мирний час.

Як і у випадку з іншими векторами загроз, ці ризики є найбільш актуальними в контекстах, де спроможність до кіберстійкості нижча, а також для вразливих груп населення та груп ризику, включаючи жінок та інші меншини. Еквадор, Мальта, Бельгія-Нідерланди-Люксембург (BENELUX) і Канада-Австралія-Нова Зеландія (CANZ) коротко розповіли про гендерний вимір кіберактивності.

Відповідно до концептуальної записки зустрічі, багато делегацій прокоментували незаконну торгівлю цифровими активами, включаючи крадіжку та відмивання криптовалюти, з потенційними фінансовими та гуманітарними втратами. Зокрема, було зроблено наголос на крадіжці криптовалюти, як, наприклад, проведена Корейською Народно-Демократичною Республікою (КНДР) у зв’язку з її програмою зброї масового знищення (ЗМЗ).

Лише за кілька днів до зустрічі за формулою Аррія Росія наклала вето на рішення щодо продовження мандата групи експертів Комітету 1718. Група експертів, заснована відповідно до резолюції Ради Безпеки ООН (SCR) 1718 для надання допомоги у впровадженні санкцій РБ ООН проти КНДР згідно з резолюцією 1874, дослідила випадки невиконання у своєму щорічному звіті, опублікованому на початку цього року. Рішення кинуло тінь на засідання за формулою Аррії, коли багато держав і делегацій висловили свої погляди щодо використання права вето та/або цінності групи. Під час «формули Арріа» Росія у відповідь визнала нагальну необхідність «серйозної переоцінки» режиму глобальних санкцій проти КНДР. На їхню думку, ізоляція КНДР від світової

фінансової системи змусила її вдатися до незаконних засобів, щоб вижити, одночасно зменшуючи засоби регулювання такої поведінки та відчужуючи її від міжнародного співтовариства.

У нещодавньому звіті Групи детально описано явний зв'язок між зловмисними кіберкампаніями КНДР, які зосереджуються в основному на шпигунстві та атаках програм-вимагачів на глобальні криптовалютні компанії з метою отримання незаконних доходів, і її програмою створення ядерної зброї та ракет, яка швидко розвивається. Він виявив випадки невибіркового нападу КНДР на оборонно-промислову базу кількох країн, починаючи від європейських аерокосмічних компаній і закінчуючи російськими компаніями супутникового зв'язку. Кіберзлочинність стала для КНДР ефективним засобом обходу санкцій ООН, отримання доступу до світового ринку та фінансування свого зростаючого арсеналу, який Рада Безпеки визнала незаконним згідно з Договором про нерозповсюдження ядерної зброї. У 2023 році половина валютних активів КНДР була придбана через незаконні кіберактивності.

Цей зв'язок кіберзагроз і зловмисної діяльності з усталеними нормами нерозповсюдження є чимось на кшталт нового кута зору в кібердіалогах ООН, хоча діяльність КНДР вже давно є сферою уваги Ради. Використання КНДР кіберпотужностей для незаконної торгівлі та розповсюдження зброї масового знищення не тільки зміцнює зв'язок між міжнародною безпекою та кібербезпекою, але доповідачі також зазначали, що це становить загрозу для роботи Ради. Якщо кіберінструменти дозволять Пхеньяну перешкоджати поточному режиму санкцій, здатність Ради забезпечити виконання свого мандату відповідно до Статуту ООН буде серйозно скомпрометована, як зазначає РК.

Роль Ради

Одна з цілей зустрічі полягала в тому, щоб почути від держав можливі рекомендації щодо посилення ролі та участі Ради у боротьбі з кіберзагрозами у спосіб, який доповнює те, як це питання вирішується в інших частинах системи ООН, наприклад у ГА ООН та спеціалізованих установах. Протягом останніх кількох років Рада все більше бере участь у розгляді різних аспектів кібермиру та

безпеки, переважно в неформальних умовах. З 2016 року зустрічі за формулою Аррія розглядають кібербезпеку в контексті міжнародного миру та безпеки, гібридну війну, її наслідки для критичної інфраструктури та запобігання впливу на цивільне населення. Інші дискусії розглядали суміжні питання, такі як новітні технології, роль соціальних медіа в розпалюванні дискримінації, ворожнечі та насильства, а останнім часом і ШІ. Кібер також з'явився у зв'язку з операціями проти Грузії та в рамках регіональних зустрічей на Близькому Сході. У 2021 році Естонія скликала перші відкриті дебати на цю тему на високому рівні.

Незважаючи на нещодавнє залучення, існують різні погляди щодо того, чи повинна і як Рада вирішувати питання ІКТ та кібернетики.

Це стало очевидним із заяв, зроблених на засіданні, хоча більше делегацій висловили підтримку в цьому, і багато хто надав чіткі ідеї щодо ролей і дій, які може здійснити РБ ООН. У рамках цього було підтверджено зв'язок між кібербезпекою та відповідальністю Ради за підтримання міжнародного миру та безпеки.

Заступник директора UNODA Адедеджі Ебо зазначив, що минулі дискусії Ради щодо кіберзбагатили розуміння загроз і можуть закласти основу для ефективної відповіді. Він припустив, що Рада може вжити практичних заходів, таких як підвищення обізнаності щодо узгодженої нормативної бази відповідальної поведінки держави та сприяння відповідальності за зловмисну діяльність.

Директор UNIDIR Робін Гайс запропонував кілька конкретних пропозицій у рамках свого брифінгу: Рада може скликати щорічне обговорення спеціально для перегляду ландшафту загроз ІКТ; ГС ООН міг би підготувати щорічний звіт про тенденції для інформування про ці обговорення; і цю тему можна ширше інтегрувати в існуючі питання Ради, враховуючи її транскордонний характер.

Посилаючись на типи зловмисної кіберактивності та інструменти, такі як атаки програм-вимагачів на уряд, ухилення від санкцій, крадіжка криптовалюти для фінансування тероризму та як виклик нерозповсюдженню, РК підкреслив, що існує «сіра зона» перетину традиційних концепцій. кіберзлочинності та

кібербезпеки. Південна Корея припустила, що РБ ООН міг би розглядати такі загрози в рамках свого основного мандату та на додаток до зусиль у ГА ООН.

Франція, Японія, Словенія, Швейцарія та країни БЕНІЛЮКСу запропонували підтримку для розгляду Радою цього питання таким чином, щоб, загалом кажучи, було зосереджено на зборі інформації чи вивченні конкретних загроз чи інцидентів, при цьому деякі з цих держав посилалися на контекст санкцій, зокрема. Японія закликала постійно оновлювати роботу Комітету 1540, щоб відобразити використання ІКТ, і відзначила зростаючу кіберзагрозу контролю над озброєннями та режиму нерозповсюдження.

Сполучене Королівство запропонувало всебічну взаємодію з відповідними комітетами Генасамблеї ООН і спеціалізованими установами для вирішення проблеми зміни природи кіберзагроз.

Латвія висловила думку, що було б корисно, якби Рада могла координувати розробку інструментів у ГА ООН, таких як кіберпрограма дій, і щоб Рада була в курсі подій у РГО. Філіппіни визнали ключову роль Ради у вирішенні мінливого характеру загроз у межах своїх повноважень, але заявили, що надають перевагу обговоренням у OEWG.

Словенія стверджувала, що Рада повинна розглядати інциденти, коли кібер-/ІКТ-діяльність загострює конфлікт, так само, як вона буде розслідувати загрози, створені звичайними засобами, і розглядати дії, які впливають на цивільне населення та спричиняють гуманітарні страждання.

Ліхтенштейн, Словенія, Швейцарія та CANZ запропонували пропозиції щодо ролі Ради у підтвердженні міжнародного права та рамок ООН для відповідальної поведінки держав. Пакистан нагадав, що Статут ООН чітко визначає принципи суверенітету та невтручання, і що це має застосовуватися до кіберпростору, що підтримав Бангладеш.

Китай, Естонія, Мальта та США заявили про свою підтримку продовження участі Ради. Китай привітав активну роль Ради у забезпеченні «мирного та більш безпечного кіберпростору». Росія заявила, що не розуміє додаткової цінності обговорення кібернетичних проблем у РБ ООН, вважаючи це контрпродуктивним і

дублюючим інші зусилля ООН. Тут Росія посилалася на Робочу групу відкритого складу з ІКТ (OEWG), створену через Перший комітет ГА ООН, відповідно до резолюцій, які вона внесла. Росія традиційно займається питаннями ІКТ у Першому комітеті, ініціювавши резолюції, які створили п'ять із шести Груп урядових експертів (GGE) з цієї теми, а нещодавно дві послідовні РГО. Для Росії велике питання, яке залишається невирішеним, полягає в тому, які випадки зловмисного використання ІКТ можна впевнено віднести до «прямих загроз міжнародному миру та безпеці».

Щоб зберегти імпульс, Рада має розробити ціннісну пропозицію

Хоча більшість заяв, зроблених під час Arria, підтримували те, що Рада відіграє більшу роль у цьому питанні, також ясно, що це не універсальна точка зору.

Незважаючи на відсутність підтримки та схвалення з боку постійних членів, таких як Росія, країни-члени, які підтримують, розійшлися в думці про ступінь, масштаби та характер керівництва Ради, яке могло б ефективно боротися з цими кіберзагрозами, що розвиваються.

Є кілька шляхів вперед, як було окреслено під час Arria різними ідеями та втручаннями на цю тему. Члени Ради могли б частіше посилатися на проблеми, події чи загрози, пов'язані з кібернетичною мережею, у заявах і діях щодо пріоритетних питань або щодо роботи в країні та регіоні, або отримувати брифінги щодо загроз. Робота Ради може бути спрямована на активне посилення та розширення рішень кіберфорумів на базі Генеральної асамблеї ООН, включаючи важливість дотримання міжнародного права та норм. Інший підхід може бути зосереджений на моніторингу ролі кіберзлочинів в обході санкцій, які дозволяють РБ ООН виконувати свій мандат або розслідувати виклики режимам нерозповсюдження з боку кіберзагроз.

Більш амбітним, але потенційно суперечливим шляхом було б спробувати викроїти нову нішу для Ради щодо кібербезпеки та ризиків ІКТ для міжнародного миру та безпеки, потенційно в поєднанні з суміжними технологічними проблемами, такими як ШІ.

Майбутня участь Ради потребуватиме визначення її унікальної ролі та цінності, а також того, як будь-яка майбутня робота чи впровадження можуть доповнити інші процеси ООН.

Багато хороших ідей було висунуто під час Arria, але кожна з них заслуговує на подальше опрацювання та розгляд як здійсненності, так і впливу. Тим не менш, зустріч стала корисним барометром для розуміння поглядів і позицій

Раді слід використати поточну динаміку серед держав для більш конструктивного вирішення цього питання. Кібербезпека та кіберзлочинність не існують у вакуумі, а мають масштабний вплив, який впливає на міжнародне співтовариство в цілому. Розглядати ці наслідки на таких форумах, як РБ ООН, є цінним, оскільки це дає державам можливість відіграти роль у розробці відповідей на ці загрози та пом'якшенні цих загроз, які також впливають на їх національну безпеку.

Проект Центру Стімсона

Центр Стімсона реалізує нову ініціативу, яка вивчає роль РБ ООН у вирішенні питань міжнародного кібермиру та безпеки. Проект досліджує потенційні шляхи, за допомогою яких Рада безпеки ООН може більш надійно та регулярно розглядати вплив ІКТ та цифрових технологій на міжнародний мир і безпеку шляхом досліджень, консультацій та побудови партнерства. Він також вивчає, як питання, які представляють подібні транснаціональні або нетрадиційні загрози миру та безпеці, такі як стрілецька зброя та легка зброя, зміна клімату та ґендер, розглядаються методами роботи Ради.

Ми з нетерпінням чекаємо публікації наших перших висновків у найближчі місяці та нашого постійного діалогу з державами та зацікавленими сторонами». ***(Allison Pytlak, Shreya Lad. The UN Security Council Discusses Cyber Threats to International Security // The Henry L. Stimson Center (https://www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/). 15.04.2024).***

***

«В епоху, коли домінують цифрові інновації та технологічний прогрес, важливість кібербезпеки ніколи не була такою виразною. Наближаючись до 2024 року та далі, ландшафт кібербезпеки продовжує швидко розвиватися, відкриваючи багато можливостей для професіоналів, які шукають динамічну та вдячну кар'єру. З огляду на те, що кіберзагрози стають дедалі складнішими та поширеними, організації в усіх секторах усвідомлюють критичну важливість захисту своїх цифрових активів і конфіденційної інформації. У цьому блозі ми заглиблюємось у широку кар'єру в галузі кібербезпеки, вивчаємо зростаючий попит на кваліфікованих спеціалістів, нові тенденції та неперевершені перспективи, які чекають на тих, хто наважується на цю захоплюючу сферу.

Сфера кар'єри в галузі кібербезпеки демонструє експоненційне зростання, оскільки цифровий ландшафт розширюється, а кіберзагрози стають все більш складними. Організації в усьому світі надають пріоритет надійним заходам кібербезпеки для захисту своїх даних і систем, створюючи високий попит на кваліфікованих фахівців. Проходження курсу з кібербезпеки озброює людей основними навичками та знаннями, необхідними для досягнення успіху в цій динамічній сфері. Від вивчення методів виявлення загроз і реагування на інциденти до освоєння мережевої безпеки та протоколів шифрування, такі курси забезпечують повне розуміння принципів і практик кібербезпеки. Крім того, практичний досвід, отриманий під час практичних вправ і симуляцій, готує людей до ефективної боротьби з реальними проблемами, що робить їх цінними ресурсами для захисту організацій від кіберзагроз.

Передбачаючи шлях: уявлення про кар'єру в галузі кібербезпеки

Кар'єра в галузі кібербезпеки пропонує динамічні виклики та можливості постійного навчання. Професіонали захищають цифрові активи, виявляють уразливості та пом'якшують кіберзагрози в різних секторах, як-от фінанси, охорона здоров'я та уряд. Ключові ролі включають етичних хакерів, аналітиків безпеки та служб реагування на інциденти. Необхідні навички охоплюють технічну майстерність у сфері мережевої безпеки, криптографії та аналізу зловмисного програмного забезпечення, а також здатність до критичного мислення та вирішення

проблем. Здатність адаптуватися та бути в курсі нових технологій мають вирішальне значення в умовах постійного розвитку загроз. Кар'єра в галузі кібербезпеки обіцяє конкурентоспроможну зарплату, стабільну роботу та задоволення від захисту критично важливої інформаційної інфраструктури у світі, що стає все більш цифровим.

Кар'єрні шляхи кібербезпеки, які ви можете вибрати

Архітектор кібербезпеки:

Роль: архітектори кібербезпеки є ідейними головами розробки та впровадження надійних інфраструктур безпеки в організаціях. Вони несуть відповідальність за створення та підтримку схем безпечних систем, мереж і програм. Ці професіонали передбачають і створюють складні системи безпеки, які охоплюють різні рівні захисту для захисту від низки кіберзагроз.

Обов'язки: до їхніх обов'язків входить проведення комплексної оцінки безпеки для виявлення вразливостей і ризиків, розробка стратегічних планів для усунення цих знахідок і проектування архітектур безпеки, адаптованих до конкретних потреб і цілей організації. Вони тісно співпрацюють із зацікавленими сторонами, такими як IT-групи та керівництво, щоб забезпечити відповідність бізнес-цілям і нормативним вимогам. Крім того, архітектори кібербезпеки постійно оцінюють нові технології та ландшафти загроз, що розвиваються, щоб завчасно адаптувати та вдосконалювати заходи безпеки.

Навички: архітектори кібербезпеки повинні мати глибоке розуміння принципів безпеки, технологій і найкращих практик. Їм потрібні міцні аналітичні навички та навички вирішення проблем, щоб оцінити складні системи та виявити потенційні слабкі місця. Вміння керувати ризиками, стандартами відповідності та інструментами безпеки є важливими. Здібності до ефективного спілкування та управління проектами також мають вирішальне значення для налагодження зв'язків із зацікавленими сторонами та просування ініціатив у сфері безпеки.

Аналітик інформаційної безпеки:

Роль: аналітики інформаційної безпеки служать першими захисниками цифрових активів організації, ретельно відстежуючи та аналізуючи заходи безпеки,

щоб виявляти потенційні загрози та інциденти та реагувати на них. Вони відіграють ключову роль у захисті конфіденційної інформації та забезпеченні цілісності, конфіденційності та доступності даних.

Обов’язки: їхні завдання охоплюють широкий спектр діяльності, включаючи проведення оцінок і аудитів безпеки, аналіз журналів безпеки та звітів, а також розслідування порушень безпеки або підозрілих дій. Аналітики інформаційної безпеки розробляють і впроваджують політики та процедури безпеки, а також надають вказівки щодо найкращих практик безпеки для співробітників. Вони співпрацюють із міжфункціональними командами, щоб забезпечити ефективну інтеграцію заходів безпеки в системи та робочі процеси.

Навички: Аналітики інформаційної безпеки потребують сильних аналітичних навичок для інтерпретації даних безпеки та виявлення аномалій або моделей, що вказують на потенційні загрози. Вони повинні добре розуміти принципи, технології та протоколи кібербезпеки. Важливо володіти інструментами безпеки, такими як системи виявлення вторгнень (IDS), рішення для управління інформацією та подіями безпеки (SIEM), а також інструменти оцінки вразливості. Навички ефективної комунікації та роботи в команді також важливі для співпраці з колегами та передачі інформації, пов’язаної з безпекою, зацікавленим сторонам.

Мережевий адміністратор:

Роль: мережеві адміністратори відповідають за повсякденне керування та обслуговування комп’ютерних мереж організації, забезпечуючи їх безперебійну роботу, надійність і безпеку. Вони відіграють життєво важливу роль у створенні та підтримці інфраструктури, яка полегшує спілкування та обмін даними в організації.

Обов’язки: в їхні обов’язки входить встановлення, налаштування та моніторинг мережевого апаратного та програмного забезпечення, наприклад маршрутизаторів, комутаторів, брандмауерів та систем виявлення/запобігання вторгненням. Адміністратори мережі усувають проблеми з мережею, оптимізують продуктивність мережі та впроваджують заходи безпеки для захисту від несанкціонованого доступу, витоку даних та інших кіберзагроз. Вони також

співпрацюють з іншими IT-командами, щоб забезпечити бездоганну інтеграцію та роботу мережевих служб і програм.

Навички: мережеві адміністратори потребують глибокого розуміння мережевих концепцій, протоколів і технологій, включаючи TCP/IP, DNS, DHCP, VPN і VLAN. Вони повинні володіти інструментами адміністрування мережі та утилітами для налаштування, моніторингу та усунення несправностей. Знання принципів безпеки та найкращих практик є важливими для впровадження та підтримки безпечного мережевого середовища. Сильні навички вирішення проблем, багатозадачності та спілкування також необхідні для ефективного керування мережевими операціями та вирішення проблем користувачів.

Тестер проникнення:

Роль: тестувальники проникнення, також відомі як етичні хакери, є професіоналами з кібербезпеки, які спеціалізуються на оцінці безпеки систем, мереж і програм шляхом імітації кібератак у реальному світі. Їхнє головне завдання — виявити вразливі та слабкі місця, перш ніж зловмисники зможуть ними скористатися.

Обов’язки: Тестери проникнення проводять комплексну оцінку безпеки за допомогою різноманітних методів, таких як сканування вразливостей, тестування на проникнення та соціальна інженерія. Вони аналізують результати цих оцінок, щоб виявити прогалини в безпеці та надати рекомендації щодо їх усунення. Тестери проникнення також можуть розробляти та виконувати спеціальні сценарії атак, щоб перевірити ефективність існуючих засобів контролю безпеки та процедур реагування на інциденти.

Навички: Тестери проникнення повинні мати глибокі знання про загрози кібербезпеці, вектори атак і методи експлуатації. Їм потрібні навички роботи з інструментами та фреймворками тестування на проникнення, а також практичний досвід проведення оцінок безпеки. Сильні аналітичні навички та навички критичного мислення необхідні для ефективного виявлення та використання вразливостей. Етична поведінка та дотримання професійних стандартів мають

першочергове значення, оскільки тестувальники проникнення повинні діяти в рамках правових та етичних кордонів під час моделювання кібератак.

Консультант з кібербезпеки:

Роль: консультанти з кібербезпеки надають експертне керівництво та підтримку організаціям у розробці, впровадженні та підтримці ефективних стратегій і рішень у сфері кібербезпеки. Вони є надійними консультантами, допомагаючи клієнтам орієнтуватися в складному ландшафті загроз кібербезпеці та нормативних вимог.

Обов’язки: їхні обов’язки охоплюють широкий спектр діяльності, включаючи проведення оцінки ризиків, розробку політик і процедур кібербезпеки, оцінку засобів контролю безпеки та технологій, а також надання рекомендацій щодо покращення. Консультанти з кібербезпеки можуть також допомогти з реагуванням на інциденти та судово-медичними розслідуваннями, а також провести навчання та програми підвищення обізнаності, щоб навчити співробітників передовим практикам кібербезпеки.

Навички: Консультантам з кібербезпеки потрібен широкий спектр навичок і компетенцій, у тому числі глибокі знання принципів, нормативних актів і галузевих стандартів кібербезпеки. Вони повинні володіти методологіями оцінки ризиків, структурами безпеки та вимогами відповідності. Сильні комунікативні та міжособистісні навички необхідні для побудови взаєморозуміння з клієнтами, передачі складних технічних концепцій простими словами та ефективної співпраці з внутрішніми та зовнішніми зацікавленими сторонами. Крім того, консультанти з кібербезпеки повинні продемонструвати здатність до адаптації, креативність і здатність вирішувати проблеми для вирішення різноманітних викликів кібербезпеки, що постійно розвиваються.

Висновок

Сфера кар’єри в галузі кібербезпеки у 2024 році та надалі є багатообіцяючою та постійно розширюється, пропонуючи професіоналам численні можливості для процвітання в цифровому середовищі, що швидко розвивається. Проходження курсу з кібербезпеки дає людям необхідні навички та знання, щоб розпочати

різноманітні робочі ролі в галузі. Від архітекторів кібербезпеки до аналітиків інформаційної безпеки, мережевих адміністраторів, тестувальників проникнення та консультантів з кібербезпеки, широкий спектр ролей підкреслює універсальність і важливість досвіду кібербезпеки. Удосконалюючи технічні навички, критичне мислення та здатність вирішувати проблеми за допомогою спеціалізованого навчання, люди можуть розпочати успішну кар'єру, захищаючи цифрові активи та борючись із кіберзагрозами в наступні роки». ***(Career Scope in Cyber Security in 2024 and beyond // OCNJ Daily (https://ocnjdaily.com/career-scope-cyber-security-2024-beyond/). 04.04.2024).***

***

«Зарплати фахівців з кібербезпеки зросли більш ніж на 23% з 2021 року, згідно з щорічним дослідженням робочої сили 2024 року від ISC2, організації, яка підтримує та адмініструє сертифікаційний іспит CISSP.

Середня зарплата професіонала з кібербезпеки у 2023 році становила 147 138 доларів США порівняно з 119 000 доларів США у 2021 році, повідомляється в дослідженні, яке базується на опитуванні майже 15 000 учасників, хоча дані про зарплату збиралися лише від учасників із США, що становить приблизно третину від загальної кількості вибірка опитування.

Як і слід було очікувати, середня зарплата різнилася залежно від досвіду та рівня роботи. Середня зарплата кіберпрофесіоналів початкового та молодшого рівня становила 86 000 доларів США; некерівний персонал і персонал середньої ланки становили в середньому 137 000 доларів США; менеджери, $149 000; директори та керівники середньої ланки — 175 тис. дол.; і керівник і виконавче керівництво, 215 000 доларів США.

У дослідженні зазначається, що ставки заробітної плати за вислугу років у США є дуже обнадійливими, особливо якщо порівнювати із середньою заробітною платою в 59 428 доларів США.

Інтенсивний, невизнаний характер кібербезпеки може збентежити потенційних кандидатів

«Зарплати стають вищими у сфері кібербезпеки, а розрив між чоловіками та жінками скорочується», — сказав генеральний директор ISC2 Клар Россо. «Тим не менш, ми все ще бачимо проблеми з наймом людей у цій професії».

«Не дивлячись на вищу винагороду, інтенсивний і часто невизнаний характер цієї роботи може знеохотити багатьох потенційних кандидатів, які віддають перевагу менш напруженій кар'єрі», — додав Девід Лінднер, керівник CISO компанії Contrast Security, виробника програмних рішень для самозахисту.

«Сильний стрес, необхідність постійного навчання та значна відповідальність за захист цифрових активів відіграють значну роль у постійній нестачі фахівців з кібербезпеки», — сказав Ліндер.

Бракує прозорості щодо діапазонів зарплат для кіберролей

Гендерні відмінності в зарплаті, виявлені в дослідженні ISC2, були неоднозначними. Жінки на некерівних і середніх посадах заробляли на 5% менше, ніж чоловіки, 131 000 доларів проти 138 000 доларів, як і жінки-менеджери, які заробляли на 9% менше, 138 000 доларів проти 150 000 доларів.

Однак жінки на посадах директорів і керівників середньої ланки заробляли на 1% більше, ніж чоловіки на цих посадах, 177 000 доларів США порівняно зі 175 000 доларів США, тоді як жінки на посадах керівників і керівників заробляли на 4% більше, ніж їхні колеги-чоловіки, 220 000 доларів США проти 212 000 доларів США.

«Вагомим фактором, що сприяє гендерній нерівності в оплаті праці, є відсутність точних знань про зарплату, яку компанія готова запропонувати за посаду», — сказав Ларрі Вайтсайд-молодший, засновник Whiteside Security, консалтингової фірми з кібербезпеки.

«Багатьом компаніям бракує прозорості щодо діапазонів зарплат для їхніх посад, що спонукає кандидатів до спекуляцій щодо того, яку, на їхню думку, повинна платити посада», — продовжив він. «Навіть за умови ретельного дослідження оцінки можуть не відображати фактичну шкалу заробітної плати».

Чи вплине ШІ на рівність оплати праці?

Доповідь також виявила розбіжності в оплаті праці між расовими та етнічними групами. Середня зарплата для білих чоловіків становила 149 000 доларів США порівняно з 144 000 доларів для небілих чоловіків, тоді як для білих жінок середня зарплата становила 142 000 доларів США проти 136 000 доларів для небілих жінок.

Однак у небілій групі дослідження показало, що професіонали з кібербезпеки, які назвали себе вихідцями з Південної Азії, мали середню зарплату вищу, ніж білі, — 155 000 доларів, як і учасники зі Східної та Південно-Східної Азії — 151 000 доларів.

Дані про різноманіття у звіті повинні бути головним попередженням для галузі. «У професії, якій важко набирати й утримувати кваліфікованих спеціалістів, це заклик до роботодавців звернути увагу на рівність оплати праці у своїх організаціях», — сказав Россо.

Чи може впровадження штучного інтелекту вплинути на рівність оплати праці? «Ми бачимо, що штучний інтелект виконує повторювані завдання, щоб існуючі фахівці з кібербезпеки могли вільно виконувати більш складні дії, що допоможе впоратися з прогалинами в пропозиції та попиті на робочу силу», — зазначив Россо. «Чи буде це вирішувати несправедливість в оплаті праці? Важко сказати.» ***(John Mello Jr. ISC2 study pegs average US cybersecurity salary at $147K, up from $119K in 2021 // IDG Communications, Inc. (https://www.csoonline.com/article/2088950/isc2-study-pegs-average-us-cybersecurity-salaries-at-147k-up-from-119k-in-2021.html). 12.04.2024).***

***

«Сучасний цифровий світ пропонує неперевершений рівень зручності в нашому особистому та професійному житті. Але це також несе з собою нові та інноваційні види кіберзагроз. Оскільки у всій нашій роботі ми значною мірою покладаємося на технології, попит на спеціалістів із кібербезпеки, які можуть захистити наші дані та системи, також швидко зростає.

Це означає, що в найближчі роки ми побачимо бум можливостей працевлаштування в сфері кібербезпеки. Питання лише в тому, чи достатньо ви готові, щоб скористатися можливостями?

Що ж, у цьому вичерпному посібнику ми розповімо вам крок за кроком, як розпочати свою кар'єру на цьому складному, але вдячному кар'єрному шляху в галузі кібербезпеки.

Кращі кар'єрні шляхи в галузі кібербезпеки

Перш ніж ми побачимо, як ви можете розпочати свою кар'єру в галузі кібербезпеки, давайте коротко розглянемо найпопулярніші посади в галузі кібербезпеки, на які ви можете прагнути.

Аналітик безпеки – ці спеціалісти з кібербезпеки відповідають за моніторинг мереж і систем на наявність підозрілих дій, аналіз загроз безпеці та впровадження заходів безпеки.

Тестер проникнення або етичний хакер – це дуже популярна посада в сфері кібербезпеки, і вони відповідають за виявлення вразливостей у системах безпеки організації шляхом імітації атак з належним дозволом. Також рекомендують дотримуватися профілактичних заходів.

Цифровий криміналіст – вони збирають і аналізують цифрові докази після нападу. Вони допомагають виявити зловмисників і сприяють судовому розгляду.

Інженер із безпеки – це одна з популярних посад у сфері кібербезпеки початкового рівня, і вони займаються розробкою інфраструктури безпеки для боротьби з різними видами кіберзагроз, що спокушають організації.

Менеджери з комплаєнсу та аудитори безпеки – це одна з нетехнічних ролей у кар'єрному шляху в галузі кібербезпеки, однак вони мають чітке розуміння навичок і знань у сфері кібербезпеки. Вони гарантують, що організації дотримуються визначених правил і відповідності.

У цій кар'єрі є інші подібні та різні типи робіт, як-от CISO, консультант з IT-безпеки, адміністратор безпеки, менеджер із безпеки тощо.

Побудова кар'єри в галузі кібербезпеки

Фонд зміцнення кібербезпеки

Першим кроком до побудови кар’єри в галузі кібербезпеки є створення міцного фундаменту, який складається з відповідної освітньої кваліфікації, відповідних навичок і знань.

Освіта: для кар’єри в галузі кібербезпеки може бути цінним ступінь бакалавра з комп’ютерних наук, інформаційних технологій та суміжних галузей. Отримання ступеня магістра або доктора може допомогти вам просуватися ще швидше.

Технічні навички: Ви повинні бути знайомі з основами мереж, операційними системами (Windows, Mac, Linux) і базами даних, як-от SQL, а базові знання штучного інтелекту можуть бути додатковою перевагою.

Мови програмування: ви повинні добре володіти різними мовами програмування, такими як Python, R, C++ тощо, що допоможе вам виконувати вашу звичайну роботу з кібербезпеки швидко. Завдяки цим обов’язковим навичкам ви можете автоматизувати завдання, аналізувати дані безпеки та навіть розробляти власні інструменти безпеки.

У звіті ISC2 зазначено, що 70% роботодавців кажуть, що програмування є важливою навичкою, необхідною для фахівців з кібербезпеки.

Збільште потужність завдяки сертифікатам кібербезпеки

Тепер, коли ви отримали необхідну освітню кваліфікацію та необхідні навички кібербезпеки, настав час підтвердити свої досягнення найкращими сертифікатами кібербезпеки.

Сертифікати – це чудовий спосіб продемонструвати свою професійну відданість, свої навички, знання та бажання вчитися. Вони також покращують вашу працевлаштування та допомагають домовитися про вищу зарплату.

Ось деякі з популярних сертифікатів кібербезпеки, які ви можете розглянути, щоб почати свою кар’єру в кібербезпеці:

CompTIA Security+

Сертифікований лікар загальної практики з кібербезпеки (CCGP™)

Сертифікований етичний хакер (CEH)

Сертифікований спеціаліст з безпеки інформаційних систем (CISSP) та інші

Ці онлайн-програми сертифікації з кібербезпеки допоможуть вам швидше просунутися в кар’єрі.

Отримайте практичний досвід

Наступний крок — отримати якомога більше практичного досвіду. Хоча теоретичні знання можуть допомогти вам вирішити будь-які проблеми, пов’язані з кібербезпекою, роботодавці віддають перевагу перевіреному практичному досвіду, який виділяє кандидатів. Ось кілька способів отримати практичні навички кібербезпеки:

Налаштуйте персональне лабораторне середовище та поекспериментуйте з інструментами кібербезпеки та застосуйте заходи безпеки

Беріть участь в онлайн-конкурсах з кібербезпеки

Приєднайтеся до роботи початкового рівня з кібербезпеки

Потрапити на стажування

Зробіть внесок у проекти безпеки з відкритим кодом

Ви можете бути здивовані, помітивши, що 61% менеджерів з найму надають перевагу практичному досвіду та вважають його важливим фактором при оцінці кандидатів на роботу в сфері кібербезпеки (ISC Cybersecurity Workforce Study).

Працюйте над своїми навичками спілкування

Після того, як ви опануєте основні технічні навички кібербезпеки, зосередьтеся на вдосконаленні своїх навичок програмного забезпечення, які стануть у нагоді під час співбесіди та на роботі. Працюйте над покращенням:

Комунікативні навички

Навички критичного мислення та вирішення проблем

Командна робота та лідерські якості

Ніколи не недооцінюйте силу цих навичок спілкування. Ви ніколи не дізнаєтесь, коли ці навички допоможуть підвищити вашу кар’єру.

Висновок

Початок кар’єри в галузі кібербезпеки може бути захоплюючим і складним. Створення міцної освітньої основи, технічних і програмних навичок, а також підтвердження за допомогою відповідних сертифікатів з кібербезпеки можуть

допомогти вам розпочати свою подорож у сфері кібербезпеки. Ви повинні переконатися, що у вас достатньо практичного досвіду, щоб підтвердити свою мужність. Також спілкуйтеся з іншими професіоналами в цьому домені через LinkedIn, Twitter та інші платформи, щоб збільшити свої шанси бути поміченими». ***(James Andrew. A Step-By-Step Method to Start a Career in Cybersecurity // TechBullion (https://techbullion.com/a-step-by-step-method-to-start-a-career-in-cybersecurity/). 13.04.2024).***

***

«У середовищі кібербезпеки, що постійно розвивається, служби безпеки стикаються з безліччю загроз і тенденцій, які вимагають уваги та надійних рішень. IT-інфраструктура зростає у різноманітності, розташуванні та розмірі, а кібератаки постійно розвиваються за темпами та витонченістю. Робота команди безпеки щодо захисту конфіденційних даних, нагляду за доступом користувачів, оперативного виявлення та усунення порушень безпеки та, зрештою, відновлення після кібератаки в усій інфраструктурі, включаючи межі, ядро та хмару, є складнішою, ніж будь-коли.

Ми бачимо докази цієї гри в реальному часі, а не лише через збільшення кількості заголовків про кібератаки. Наше дослідження також виявило, що майже половина (48%) британських організацій повідомили про кібератаки або інциденти, які перешкоджали відновленню даних протягом останнього року. Цей показник зріс до 87%, коли ми запитали респондентів, чи пригадують вони, що їхня організація зазнала збоїв, пов’язаних з кібернетичною діяльністю, у 2023 році.

Цікаво, що, незважаючи на те, що прогрес у GenAI просунувся вперед і викликав велике захоплення, він є водночас винуватцем і рятівником «вічної кризи», яку ми відчуваємо в кібербезпеці. З одного боку, GenAI надає нові способи захисту бізнесу в середовищі загроз, що постійно змінюється, захищаючи IT-середовища з більшою складністю та масштабом. З іншого боку, це ідеальний засіб для посилення атак зловмисників. Самі системи GenAI також можуть бути ціллю;

оскільки штучний інтелект стає все більш інтегрованим у критично важливі системи та інфраструктуру, потенціал для злому зростає.

У цьому новому світі серйозні збої під загрозою не лише бізнес-операцій. Наші висновки також показали, що витрати, пов'язані з кібератаками та пов'язаними інцидентами, подвоїлися в усьому світі й перевищили 1,41 мільйона доларів США (0,66 мільйона доларів США у 2022 році). Це показує, що неправильні стратегії кібербезпеки можуть коштувати дорого, і занепокоєння компаній щодо того, чи достатні їхні існуючі заходи захисту даних, щоб впоратися з цим, справедливо. Ми ще не розуміємо повного масштабу загроз і винагород, які пропонує GenAI, що робить управління ризиками та підвищення вартості балансуванням для всіх компаній на шляху GenAI. Отже, як бізнес-лідери можуть впоратися з цим викликом швидкого та безпечного розгортання GenAI, а також використовувати його для посилення захисних заходів?

Gen AI як чудовий детектор загроз

Хоча GenAI справді може бути прискорювачем загроз кібербезпеці (згідно з нашим дослідженням, 27% у всьому світі вважають, що GenAI спочатку забезпечить перевагу кіберзлочинцям), його також можна використовувати для виявлення аномалій і потенційних загроз і реагування на них у реальному часі. Знову ж таки, дивлячись на результати нашого нещодавнього дослідження, 40% організацій у Великій Британії оптимістично дивляться на можливості GenAI для посилення їх кіберзахисту.

Перш ніж використовувати GenAI як союзника для забезпечення безпеки організації, важливо посилити безпеку своєї інфраструктури. Організація повинна ідентифікувати та мінімізувати вразливості та точки входу, які можуть скомпрометувати додатки, системи або мережі в різних доменах, включаючи периферію, ядро та хмару. GenAI може стати найкращим захисником шляхів, якими люблять користуватися кіберзлочинці, завдяки вдосконаленому й автоматизованому виявленню загроз і реагування на них, прогнозуванню майбутніх загроз і ідентифікації закономірностей, аномалій, вразливостей і ознак компрометації.

Виявляти кіберзагрози та реагувати на них означає бути напоготові. Завдяки здатності розпізнавати відомі сигнатури атак і виявляти відхилену поведінку, залишатися напоготові та діяти — це те, що GenAI може робити неймовірно добре. Наприклад, для тих зловмисників, які отримають доступ, GenAI може використовувати свою силу, щоб допомогти утримати хакерів у вузлі та зупинити їх подальше поширення в системі, уникаючи ескалації атаки.

Постійно відстежуючи поведінку користувачів і мережеву активність, GenAI можна навчити зміцнювати позицію організації в кібербезпеці та коригувати дозволи на основі оцінки ризиків. Його навіть можна використовувати як генератор паролів для створення складних унікальних паролів. Кібербезпека не підлягає обговоренню для компаній, тому для боротьби зі складними кіберзагрозами організації повинні розуміти, як штучний інтелект може ідентифікувати та реагувати на те, що відомо та невідомо, уникати кібератак, підтримувати надійні методи безпеки та пришвидшувати ідеї до інновацій.

Сила нульової довіри

Традиційні методи запобігання, як правило, зосереджені на підході, орієнтованому на периметр, з використанням системи безпеки, що базується на «відомих довірених» всередині периметра, тобто співробітниках і партнерах, і «невідомих довірених» поза межами, тобто хакерів і зловмисників. Однак все більш витончена природа GenAI дозволила зловмисникам увійти в мережу під виглядом «довірених відомих». Захистити організацію від кібератак набагато складніше у світі, де кожен має під рукою ШІ покоління.

Добре захищені організації запроваджують модель безпеки Zero Trust, комплексну стратегію, що зосереджується на трьох основних практичних сферах: зменшення поверхні атаки, виявлення кіберзагроз і реагування на них, а також швидке відновлення бізнес-операцій із якомога меншими перервами. Zero Trust діє за принципом «ніколи не довіряй, завжди перевіряй». Підходячи до безпеки, припускаючи, що порушення вже відбулися, організації стикаються з проблемою не довіряти жодному користувачеві, пристрою чи мережі, внутрішній чи зовнішній.

Цілісний підхід Zero Trust забезпечує кілька контрольних точок політики та автоматично надає або відхиляє запити на основі моделей поведінки користувачів. Можна швидко оцінити зв’язок між GenAI і Zero Trust – такі можливості, як аналітика поведінки та виявлення аномалій, автоматичне реагування на загрози та їх усунення, а також адаптивний контроль доступу можуть зміцнити структуру Zero Trust організації.

Сучасна кібербезпека має бути інтелектуальною, масштабованою та автоматизованою

Щоб по-справжньому скористатися перевагами GenAI, команди безпеки повинні залишатися пильними та адаптуватися до нових векторів загроз. Інвестиції в більш інтелектуальну, адаптивну поведінкову систему захисту та захист машинного навчання будуть мати вирішальне значення, як і моніторинг впливу GenAI на мінливий ландшафт зловмисників. Усунення сліпих зон, зниження ризиків шахрайства та інтеграція GenAI у навчальні програми є ще одними важливими заходами, щоб залишатися попереду кіберзагроз.

Незважаючи на те, що GenAI справді потребує переоцінки стратегій безпеки, щоб включити захист власних систем, це також обіцяє величезні переваги. Ми побачимо цю цінність у покращеному виявленні загроз і реагуванні на них; прогнозування майбутніх загроз, автоматизація виявлення загроз, сприяння криміналістичному аналізу, проведення персоналізованого навчання з питань безпеки та масштабування операцій безпеки. GenAI також допоможе компаніям підвищити ефективність і збільшити розрив у навичках безпеки, звільнивши персонал служби безпеки, щоб зосередитися на більш стратегічних і складних завданнях.

2024 рік — це рік, коли ми переходимо від експериментів GenAI до реального часу, коли бачить відчутні бізнес-результати. І все ж ми знаємо, що технологія, а також переваги та ризики, які вона представляє, продовжуватимуть розвиватися, можливо, несподіваним чином. Це означає, що команди безпеки повинні переглянути та вдосконалити стратегії безпеки та безпеки в контексті штучного інтелекту та бути готовими адаптувати спосіб захисту своїх робочих

процесів і базових даних. Команди безпеки повинні підготуватися сьогодні, тому що ШІ обіцяє змінити спосіб ведення бізнесу (і забезпечити його безпеку) завтра». ***(Sean Pedrosa. The dual nature of GenAI within cybersecurity // Future US, Inc. (https://www.techradar.com/pro/the-dual-nature-of-genai-within-cybersecurity). 11.04.2024).***

***

«Міжнародний валютний фонд (МВФ) б'є на сполох щодо ризику зростання загрози світовій економіці через кібератаки.

Було зроблено жахливе попередження, в якому уряди закликалися запровадити надійні системи та кіберстратегії, щоб протистояти поточній проблемі.

У блозі МВФ детально описано масштаби занепокоєння та потенційні збитки, якщо не буде вжито коригувальних заходів. У ньому показано, як зловмисники можуть дестабілізувати економіку, що призведе до втечі банків. Якби така ситуація реалізувалася, наслідки відчули б усе суспільство.

Особливе занепокоєння викликала залежність від сторонніх фірм з кібербезпеки, оскільки вони є практичними власниками головних ключів для низки підприємств і галузей. У звіті рекомендовано заохочувати внутрішні команди для надання цих важливих послуг.

Геополітична напруженість була вказана як небезпека, при цьому підтримувані державою актори використовували цитату, щоб націлитися на деякі з найбільших компаній світу, щоб підірвати національні уряди, економіку та стабільність загалом.

Окрім боротьби зі зростаючою загрозою, вартість захисту життєво важливих онлайн-функцій також зростає. У звіті МВФ зазначено, що кібератаки зросли вдвічі після пандемії, а лише фінансовий сектор США втратив 12 мільярдів доларів через кіберінциденти з 2004 року.

МВФ рекомендував національним урядам, особливо в країнах, що розвиваються, значно вдосконалити свій підхід до кібербезпеки. Він закликав до

створення ефективних стратегій, регулярного перегляду викликів, змістовного охоплення бізнесу та лідерства у стандартах, обміні інформацією та готовності.

У відповідь на рекомендації Кев Брін, старший директор відділу аналізу загроз у Immersive Labs, висловив думку про те, які дії потрібні.

«Знання того, що конкретна загроза може націлитися на банки за допомогою DDOS, не означає бути готовим реагувати або проактивно пом'якшувати потенційний вплив цих загроз», — сказав він.

Брін додав, що організації повинні навчати всіх співробітників, включаючи членів правління та керівників, щоб підвищити кіберстійкість у фінансовому секторі. Він підкреслив, що проведення регулярних і реалістичних симуляцій кіберкриз і навчань гарантує, що люди в організації володіють необхідними знаннями, навичками та здатністю розуміти для захисту від кібератак». ***(Yana Khlebnikova. Cybersecurity Crisis: IMF Report Shows $12B Lost in US Financial Sector // Techopedia (https://www.techopedia.com/news/cybersecurity-crisis-imf-report-shows-12b-lost-in-us-financial-sector). 11.04.2024).***

***

«Співробітники відіграють найважливішу роль у забезпеченні загальної кібербезпеки організації, оскільки часто є першою лінією захисту від кіберзагроз. У цьому комплексному керівництві співробітники отримають важливі поради щодо кібербезпеки, щоб захистити себе та свої організації від кібератак.

Розуміння кібербезпеки

Перш ніж перейти до конкретних порад щодо кібербезпеки для співробітників організацій, необхідно отримати базове уявлення про те, що таке кібербезпека. Кібербезпека – це практика захисту цифрових систем, мереж та даних від несанкціонованого доступу, атак та збитків. Вона включає поєднання технологій, процесів і поведінки користувачів для зниження кіберризиків.

Корисні поради щодо кібербезпеки для співробітників організацій

Пропонуємо до вашої уваги 10 найкращих порад з кібербезпеки для співробітників організацій та підприємств.

1. Управління паролями

Паролі є вашою першою лінією захисту від кіберзагроз. Дотримуйтесь цих рекомендацій:

Створюйте надійні паролі. Використовуйте комбінацію великих та малих літер, цифр та спеціальних символів. Уникайте використання інформації, що легко вгадується, наприклад, днів народження або звичайних слів.

Використовуйте унікальні паролі. Не використовуйте той самий пароль для кількох облікових записів. Розгляньте можливість використання менеджера паролів для створення та безпечного зберігання складних паролів.

Регулярно змінюйте паролі. Періодично змінюйте паролі, особливо для важливих облікових записів.

Увімкніть двофакторну автентифікацію (2FA). По можливості вмикайте 2FA для своїх облікових записів. Це додає додатковий рівень безпеки.

2. Захист від фішингу

Фішинг є поширеною кіберзагрозою. Будьте обережні з електронними листами, повідомленнями чи посиланнями. Поради щодо виявлення спроб фішингу:

Перевірте відправника. Перевірте адресу електронної пошти відправника. Будьте обережні з невеликими орфографічними помилками та незнайомими доменами.

Звертайте увагу до тривожні сигнали. Погана граматика, термінові прохання та підозрілі посилання – це ознаки фішингу.

Перевірте посилання. Наведіть курсор миші на посилання, щоб переглянути URL-адресу. Не натискайте на посилання, якщо URL-адреса здається підозрілою.

Перевірте запити. Якщо ви отримали електронний лист із проханням надати конфіденційну інформацію, перевірте його справжність у відправника через довірений канал.

3. Безпека електронної пошти

Електронна пошта є найпоширенішим джерелом кібератак. Захистіть свою електронну пошту:

Використовуйте безпечні служби електронної пошти. Використовуйте авторитетні поштові служби з надійними засобами захисту.

Остерігайтесь вкладень. Не відкривайте вкладення з невідомих джерел. Перш ніж відкрити вкладення, перевірте їх на наявність шкідливих програм.

Не ділитесь конфіденційною інформацією. Ніколи не надсилайте електронною поштою конфіденційні дані, наприклад паролі або фінансову інформацію.

4. Атаки соціальної інженерії

Соціальна інженерія ґрунтується на маніпулюванні людьми з метою змусити їх розкрити конфіденційну інформацію. Будьте обережні:

Несподівані прохання. Скептично ставтеся до несподіваних дзвінків або повідомлень з проханням надати конфіденційну інформацію.

Перевіряйте особистість. Перевіряйте особу будь-якої людини, яка запитує інформацію, перш ніж надати її.

Не довіряйте визначнику номера. Телефонний номер може бути підроблений. Не покладайтеся лише на нього під час ідентифікації абонентів.

5. Безпечне використання пристроїв

Перебуваючи в офісі або віддалено, забезпечте безпеку своїх пристроїв:

Блокуйте пристрої. Завжди блокуйте комп’ютер або мобільний пристрій, коли він не використовується.

Використовуйте надійні паролі. Використовуйте надійні паролі або PIN-коди для своїх пристроїв.

Встановіть антивірусне програмне забезпечення. Захищайте пристрої за допомогою актуального антивірусного програмного забезпечення.

6. Оновлення програмного забезпечення

Регулярно оновлюйте програмне забезпечення та пристрої:

Увімкніть автоматичне оновлення. Активуйте автоматичні оновлення для операційних систем та програм, щоб отримувати виправлення безпеки.

Видаліть програмне забезпечення, яке не використовується. Видаліть непотрібні програми та програми, щоб зменшити кількість потенційних вразливостей.

7. Безпека віддаленої роботи

У зв’язку з поширенням віддаленої роботи зверніть увагу на ці міркування безпеки:

Використовуйте безпечну мережу. Підключайтеся до безпечної, захищеної паролем мережі Wi-Fi. Уникайте публічних мереж Wi-Fi для конфіденційної роботи.

Захистіть домашні маршрутизатори. Змініть стандартні паролі маршрутизаторів та увімкніть надійне шифрування.

Використовуйте VPN. Якщо ви працюєте віддалено, використовуйте віртуальну приватну мережу (VPN) для шифрування вашого інтернет-з’єднання.

8. Захист інформації

Надійно захищайте конфіденційні дані:

Шифруйте дані. Використовуйте засоби шифрування для конфіденційних файлів та повідомлень.

Захистіть фізичні документи. Замикайте фізичні документи, які містять конфіденційну інформацію, коли вони не використовуються.

Резервне копіювання даних. Регулярно створюйте резервні копії важливих даних, щоб запобігти їх втраті в результаті кібератак.

9. Звітність про інциденти

Якщо ви підозрюєте, що стався інцидент з безпекою, зробіть таке:

Повідомте про це. Негайно повідомляйте про будь-які підозрілі дії, фішингові листи або інциденти у свій IT-відділ або службу безпеки.

Дотримуйтесь правил. Дотримуйтесь інструкцій з реагування на інциденти, прийняті у вашій організації.

10. Постійне навчання та підвищення знань

Будьте в курсі подій і займайтеся самоосвітою:

Відвідуйте тренінги. Беріть участь у програмах навчання та підвищення рівня знань у галузі кібербезпеки, які проводить ваша організація.

Будьте в курсі подій. Дізнайтеся про останні кіберзагрози та тенденції з авторитетних джерел.

Висновок

Кібербезпека – це загальна відповідальність, і співробітники відіграють важливу роль у захисті своїх організацій від кіберзагроз. Дотримуючись цих порад з кібербезпеки та зберігаючи пильність, ви можете сприяти створенню безпечнішого цифрового середовища для себе та своєї організації. Пам’ятайте, що кібербезпека є безперервним процесом, і щоб залишатися захищеним у сучасному цифровому світі, необхідно бути поінформованим та проявляти активність». ***(Скарбик Павло. 10 основних порад із кібербезпеки для співробітників організацій // iTechua.com (https://itechua.com/articles/254888). 11.04.2024).***

***

«У моїй повсякденній роботі етичним хакером (я віддаю перевагу терміну «тестер на проникнення», але що б там не було), я стикаюся з купою типових помилок безпеки, які дозволяють мені отримати несанкціонований доступ до ваших комп’ютерних систем. Це значно полегшує мій робочий день, коли хтось залишає записаний пароль на своєму столі, але я не єдиний, хто ледачий і любить легкий виграш.

Економічні хакери зазвичай шукають найнижчі плоди, і за допомогою кількох простих змін ви можете значно ускладнити для когось випадкове порушення вашої безпеки та вторгнення у ваше приватне життя. З цією метою я склав список із п’яти головних звичок, які варто змінити під час користування Інтернетом — з точки зору хакера. Можливо, ви вже знаєте пару, але інші можуть бути різницею між тим, щоб вас зламали, і захистили себе.

1. Використовуйте VPN

Шифрування є важливим, і в ідеальному світі кожен веб-сайт використовував би як мінімум TLS із суворою транспортною безпекою HTTP. На жаль, це не ідеальний світ, тому для всього іншого у нас є віртуальні приватні мережі (VPN). Вони створюють зашифрований тунель, який направляє ваш інтернет-трафік між вашим пристроєм і VPN-серверами провайдера, що важливо, якщо ви часто подорожуєте та підключаєтеся до відкритих точок Wi-Fi. Серйозно. Вийдіть одного разу з копією Wireshark, встановленою на вашому ноутбуці, і подивіться, яку інформацію ви передаєте через безкоштовний Wi-Fi аеропорту через свій телефон. Це не красиво.

Слід визнати, що серед експертів із безпеки точаться дебати щодо того, чи варто вам використовувати VPN. Існують вагомі аргументи проти використання VPN, головним чином зосереджені на тому, щоб довірити маршрутизацію ваших даних потенційно ненадійній третій стороні. Мій аргумент такий: ви вже довіряєте своєму провайдеру, який не може працювати без згоди уряду. Ймовірно, ваш уряд також шпигує за вами. Чому б не зробити це трішки складнішим? Хоча я б не пропонував використовувати будь-якого постачальника VPN, який вам зустрінеться, вибір перевіреної VPN без реєстрації може забезпечити певний рівень захисту від стеження з боку уряду, якого ви не мали б інакше.

Що ще важливіше, високоякісний VPN пропонує дві ключові переваги: по-перше, він приховує вашу IP-адресу, значно ускладнюючи спроби відстежити ваше фактичне місцезнаходження; по-друге, він відфільтровує звичайних розповсюджувачів шкідливого програмного забезпечення та скомпрометованих рекламодавців через блокування DNS. Блокування реклами вже зменшує величезний вектор зловмисного програмного забезпечення, тому я б рекомендував одне лише для цього.

2. Використовуйте блокувальник JavaScript або білий список

Архітектура Інтернету означає, що велика частина вмісту, який ви зустрічаєте у своєму браузері, доставляється через JavaScript. Незважаючи на те, що JavaScript може покращити зовнішній вигляд веб-сайтів, він також служить вектором для

величезної кількості атак, включаючи клікджекінг, відмову в обслуговуванні, міжсайтовий сценарій і підробку запитів, а в деяких випадках навіть довільне виконання коду.

Застосовуючи блокувальник JavaScript або білий список, ви можете вибірково дозволяти сценарії з надійних джерел, одночасно зменшуючи ризики, пов'язані зі шкідливими або нав'язливими сценаріями. Це пом'якшує атаки, які породжуються зловмисною рекламою, і суттєво зменшує ймовірність викрадення ваших облікових даних сеансу під час атаки. NoScript досі є золотим стандартом для пакетів блокування Javascript. Я використовую це та uBlock Origin, щоб охопити більшість своїх баз онлайн.

3. Переслідуйте себе

Дуже мало людей уявляють, скільки інформації про їхнє особисте життя розміщено в Інтернеті й чекає, поки хтось з'єднає крапки. Я часто використовую LinkedIn, щоб отримати інформацію про співробітників компанії, технології та фізичне місцезнаходження, але мати справу з цільовими хакерами вимагає дещо іншого підходу.

Візьміть частину інформації, яка є загальнодоступною, наприклад вашу електронну адресу чи ім'я користувача, яке ви використовуєте. Використовуючи базові методи розвідки з відкритим кодом і спеціальний пошук у Google, ви будете вражені тим, скільки особистих даних є легко доступними, включаючи ваше справжнє ім'я, адресу тощо.

Якщо у вас є уявлення про кроки, які хтось повинен зробити, щоб пов'язати ваші особи в Інтернеті та реальні, видалення або видалення цієї інформації з ваших облікових записів в Інтернеті може розірвати зв'язок. Це значно ускладнює зловмисникам використання вашої особистої інформації (у свою чергу, зменшується ймовірність того, що ви станете жертвою божевільного гравця Call of Duty, який має надто багато часу).

Це особливо важливо для таких платформ, як Facebook і Twitter. Ви були б здивовані, скільки відповідей на питання безпеки можна знайти, швидко прокрутивши чиюсь стіну у Facebook або стрічку Twitter. Поки ви це робите,

переконайтеся, що ви вивчили налаштування конфіденційності, які пропонують сайти соціальних мереж, щоб переконатися, що лише люди, яких ви знаєте, мають доступ до вашої особистої інформації. Стати майстром розвідки з відкритим кодом (OSINT) не стає миттєво, але навіть трохи зусиль краще, ніж нічого.

4. Оновіть свої програми

Так, це нудна порада. На жаль, саме основні запобіжні заходи часто вирішують між успіхом і невдачею кібербезпеки. Застарілі версії програмного забезпечення викликають головний біль у фахівців із безпеки, тому, будь ласка, регулярно оновлюйте свою ОС і програмне забезпечення (особливо, якщо воно підключено до Інтернету). Простий погляд на список загальних вразливостей і експозицій дасть вам уявлення про велику кількість експлойтів програмного забезпечення.

Це ще важливіше для мобільних пристроїв, які часто є сховищами дуже конфіденційної інформації — справжнім раєм для хакерів. Ви, напевно, колись чули про шпигунське програмне забезпечення Pegasus, яке використовувало кілька складних експлойтів в операційних системах iOS і Android, щоб повністю дистанційно зламувати телефони відомих медіа-персон за допомогою текстових повідомлень.

Проте телефони — не єдине місце, де відбуваються ці атаки. Зокрема, старі веб-переглядачі є легкою мішенню для атак зловмисного програмного забезпечення без кліків, які залишають ваш комп’ютер під загрозою простого переходу за підозрілим посиланням.

Якщо вам потрібно підтримувати стару операційну систему для застарілих цілей, наприклад для запуску застарілих версій програмного забезпечення, подумайте про те, щоб ізолювати їх як віртуальні машини або системи з розривом повітря, які не мають підключення до Інтернету.

5. Припиніть повторне використання своїх паролів

Я впевнений, що вам це говорили тисячу разів, але на це є причина. Є незліченна кількість незахищених сайтів і програм, яким ви довіряєте свої паролі.

Деякі з них досі зберігають свої паролі у вигляді відкритого тексту або несолоного MD5 (по суті, марне шифрування, яке вас не захищає).

Якщо ви повторно використовуєте їх, це буде бомба уповільненої дії, якщо одну з цих платформ зламатимуть, і ваш пароль почне витати в темній мережі. Коли це станеться, це лише питання часу, коли хтось спробує вашу комбінацію електронної пошти та пароля на популярних веб-сайтах і отримає удар.

Навіть якщо ваші облікові дані не витік, використання звичайних паролів робить вас уразливими до атак. Атаки грубої сили часто використовують скомпільовані списки паролів із витоку даних, що значно скорочує час, необхідний для фактичного пошуку облікових даних для входу, які працюють.

Коли я намагаюся зламати систему, я не дивлюся на одного користувача, а пробую кожен пароль, який знаю. Я пробую три найпоширеніші паролі для кожного користувача системи. Пригнічує те, як часто це працює. Змінити пароль!

Тим не менш, може бути важко запам’ятати пароль для кожного сайту, на який ви збираєтеся входити. Вам слід розглянути можливість використання менеджера паролів (або, як мінімум, увімкнення двофакторної автентифікації). За допомогою таких інструментів, як haveibeenpwned, ви також можете перевірити, чи не зламано якісь із ваших облікових записів, чи використовуєте ви пароль, який часто використовують.

Нічому не довіряти

Є багато інших заходів, які ви можете вжити в Інтернеті, щоб захистити свою особисту інформацію, але п’ять вищезазначених кроків є найважливішими. З мого досвіду хакери часто досягають успіху не завдяки надзвичайним технічним здібностям чи витонченим інженерним досягненням, а радше використовуючи людську лінь і недогляд. Якщо хтось залишив задні двері відкритими, навіщо намагатися зламати замок? Дещо змінивши свої звички, ви можете значно зменшити ймовірність стати жертвою хакерської атаки (і значно ускладнити мою роботу).

Ось додаткова порада: якщо ви коли-небудь отримаєте дивний електронний лист від людини, якій довіряєте, з проханням перевірити файл, зателефонуйте йому

та переконайтеся, що він надіслав його. Повір мені в цьому. фішинг працює набагато частіше, ніж мав би бути». ***(Sam Dawson. 5 tips from a hacker to keep you safe online // Future US, Inc. (https://www.techradar.com/computing/cyber-security/5-tips-from-a-hacker-to-keep-you-safe-online?utm_source=flipboard&utm_content=DawnMartin4rfo%2Fmagazine%2FRead+NOW). 16.04.2024).***

***

«Культивування культури кіберпрозорості – це вже не просто питання відповідності. Від внутрішніх зацікавлених сторін до страхових і регуляторних органів, існує гучний заклик до організацій пролити світло на свої методи безпеки.

Необхідність більшої кіберпрозорості

У середовищі, яке визначається ескалацією регулятивного тиску, очікувань зацікавлених сторін і страхових імперативів, підтримання прозорості в практиках кібербезпеки стало наріжним каменем для зміцнення довіри, підзвітності та кіберстійкості.

Положення, що розвиваються, такі як ті, що випущені SEC та NIST, не лише наполягають на тому, щоб організації вживали профілактичних заходів, щоб справді розуміти свій ризик кібербезпеки; але вони також підсилили важливість нагляду зацікавлених сторін. визнають кібербезпеку головним пріоритетом Ці очікування вийшли за межі простих перевірок відповідності, проникаючи в дискусії в залі засідань, де 73% членів правління.

Інвестори також посилили своє занепокоєння, виступаючи за більшу постійну видимість стану безпеки своєї організації. Насправді 81% керівників IT та бізнесу кажуть, що зараз вони більше зосереджуються на кібербезпеці цільової компанії, ніж у минулому. Ці зацікавлені сторони більше не задовольняються гарантіями на поверхневому рівні; натомість вони вимагають чіткого та всебічного уявлення про заходи, які застосовуються для захисту конфіденційних даних і демонстрації стабільності бізнесу.

Водночас, зміна тенденцій у кіберстрахуванні ще більше підкреслює необхідність підвищення прозорості практики кібербезпеки. Лише за останні три роки кількість кіберстрахових вимог зросла на 100%, що супроводжувалося приголомшливим зростанням страхових виплат на 200%. Відповідно, страховики зараз вимагають більш детальних, «попередніх» непередбачених обставин, шукаючи доказів постійного прогресу у впровадженні ефективного контролю з часом.

Таким чином, оволодіння мистецтвом прозорого спілкування з кіберризиками стає обов'язковим. Ця подорож до ясності та відкритості залежить від прийняття п'яти «С» кіберпрозорості: розуміння, контекст, налаштування, стислість і послідовність.

Комплексний

Замість того, щоб просто перераховувати вразливості чи загрози, ефективне повідомлення про кіберризики вимагає від організацій застосування цілісного підходу, який включає не лише технічні аспекти, але й забезпечує прозорість загальної безпеки організації. Крім того, якщо це можливо, обов'язково надайте практичні рекомендації щодо пом'якшення кіберризиків, наприклад впровадження певних заходів безпеки або технологій. Чітко сформулюйте кроки, які зацікавлені сторони можуть зробити, щоб зменшити свій вплив на кіберзагрози.

«Ми бачимо чимало організацій, які намагаються отримати більш чітке, базове уявлення про те, «які наші кіберризики?», починаючи з великої кількості деталей навколо активів, і ви створюєте уявлення звідти до більш повного огляду, який дає їм можливість захистити позицію». – Річард Хорн, член Noetic Advisory Board

Контекстний

Допоможіть зацікавленим сторонам зрозуміти ширший контекст кіберризиків, пояснюючи актуальність конкретних загроз для галузі, бізнес-цілей і нормативного середовища вашої організації. Ілюструючи, як кіберзагрози можуть порушити роботу, завдати шкоди репутації або призвести до фінансових втрат,

зацікавлені сторони мотивуються виділяти ресурси на надійні заходи кібербезпеки, які підтримують загальні бізнес-цілі.

Визначення кіберризиків у нормативному середовищі також пояснює юридичні зобов'язання та зобов'язання щодо відповідності, яких організації повинні дотримуватися. Повідомлення про те, як конкретні загрози пов'язані з нормативними вимогами, не лише підкреслює правовий імператив щодо кібербезпеки, але й посилює зобов'язання організації щодо відповідності та управління ризиками.

Індивідуальний

Методи та зміст комунікації повинні відповідати потребам і перевагам різних зацікавлених сторін, включаючи членів правління, інвесторів і страховиків. Керівникам можуть знадобитися короткі підсумки, тоді як технічні групи можуть отримати користь від більш детальної інформації.

Скажімо, наприклад, організація збирається на щорічне засідання щодо бюджету, і правління шукає інформацію про те, які засоби контролю кібербезпеки та стратегії пом'якшення можуть принести найбільшу віддачу від інвестицій з точки зору зниження ризиків і стійкості. У той же час поліс кіберстрахування наближається до дати його оновлення, і страховик вимагає доказів для дванадцяти конкретних заходів контролю. Хоча обидва звіти вимагають видимості ваших засобів контролю, моніторингу та можливостей застосування політики, кожен має бути налаштований відповідно до конкретних проблем і пріоритетів аудиторії.

Лаконічний

Також важливо бути лаконічним у своєму спілкуванні, зосереджуючись на найважливіших моментах і уникаючи непотрібних деталей. Використовуйте пункти або підсумки, щоб висвітлити ключові висновки та зробити інформацію легшою для засвоєння та перевантажити вашу аудиторію непотрібними деталями чи технічним жаргоном.

Особливо корисним може бути використання візуальних засобів, таких як діаграми, графіки та інфографіка, щоб проілюструвати ключові моменти та

тенденції. Візуальні представлення можуть допомогти прояснити складну інформацію та полегшити її сприйняття зацікавленими сторонами.

Послідовний

Нарешті, регулярні оновлення та нагадування служать для посилення ключових повідомлень і гарантують, що кібербезпека залишається головним пріоритетом для зацікавлених сторін на всіх рівнях. Послідовна комунікація допомагає зацікавленим сторонам пам'ятати про кіберризики, запобігаючи самовдоволенню та посилюючи важливість заходів кібербезпеки. Обов'язково визначте будь-які можливості для автоматизації, щоб уникнути виснаження ресурсів, які вже розпорошені.

Оскільки ми продовжуємо орієнтуватися в викликах і можливостях епохи цифрових технологій, ми повинні прийняти прозорість як керівний принцип у наших спільних зусиллях, щоб забезпечити майбутнє.

Застосовуючи цілісний підхід, надаючи релевантний контекст, пристосовуючи комунікацію до потреб різних аудиторій, будучи стислим, але вичерпним, і підтримуючи послідовну взаємодію, організації можуть сприяти розвитку культури прозорості, яка зміцнює довіру, підвищує стійкість і захищає від нових кіберзагроз». ***(Alexandra Aguiar. Cyber Transparency: Shining a Light on Security // Noetic (https://noeticcyber.com/cyber-transparency-shining-a-light-on-security/). 17.04.2024).***

***

«Для багатьох бізнес-лідерів стати жертвою зусиль хакерів є найгіршим, що їм доводиться відчути у своєму професійному житті. Мільйони слів було присвячено порадам бізнесу щодо подолання збоїв, невизначеності та величезних витрат, пов'язаних із такими подіями, але проблема подолання емоційного та психологічного впливу, який відчувають команди керівництва та співробітники, розглядається рідко.

Коли інцидент трапиться вперше, добре підготовлені організації швидко зберуть основну команду внутрішніх і зовнішніх спеціалістів. Менш підготовленим

організаціям може знадобитися більше часу, щоб ініціювати відповідь. IT-фахівці, юристи та спеціалісти з комунікацій відіграють певну роль у відповіді на спір. Завдяки підтримці кваліфікованих фахівців більшість підприємств зможуть витримати більшість кібершторм, але мало хто вийде з них, не відчувши себе враженим досвідом.

Деякі з найважливіших професійних консультантів можуть і повинні надати не юридичну, а емоційну підтримку. У цій статті розглядається вплив кібератаки на добробут співробітників і керівництва, а також те, що можна зробити, щоб зменшити шкоду як наперед, так і перед нападом.

Зіткнувшись зі страхом

Початковою реакцією на кібератаку, швидше за все, буде шок і глибоке відчуття жаху. Спочатку атака може здатися звичайним IT-інцидентом, результатом збою або помилки конфігурації. Залежно від тяжкості та характеру нападу може знадобитися час, щоб з'ясувати справжню причину. У деяких випадках першою ознакою може бути повідомлення про викуп на екранах комп'ютерів або навіть на принтерах. Коли стає очевидним, що третя сторона несе відповідальність за інцидент, зазвичай виникає паніка. На цьому етапі можуть знадобитися рішучі дії, щоб захистити системи та запобігти подальшому компрометуванню. У разі великої атаки це може означати, що багато або всі системи повинні бути вимкнені. Раптове обмеження або видалення доступу до системи може викликати тривогу для компаній, які все більше працюють в Інтернеті. Просто отримати співробітників, щоб пояснити, що відбувається, може бути надзвичайно складно.

На ранніх стадіях кіберінциденту вся робоча сила може бути стурбована та боятися за свою роботу, і це буде посилюватися, якщо вони не зможуть зв'язатися з керівництвом. Навіть якщо мало що можна сказати, встановлення надійного та безпечного засобу зв'язку буде важливим для підтримки морального духу та доброзичливості персоналу.

Відкинути почуття провини

Одним із найскладніших аспектів управління кібератакою є відчуття провини, яке відчувають усі, крім найнадійніших лідерів. Зіткнувшись із наляканими працівниками, розлюченими клієнтами, несприйнятливими регуляторами та, якщо вам особливо не пощастить, допитливими журналістами, ви можете легко забути, що насправді ви стали жертвою злочину.

Якщо особисті дані скомпрометовано, як це зазвичай буває певною мірою під час кібератак, ви, ймовірно, зобов’язані повідомити про це свій регулятор даних, і якщо ви підпадаєте під дію галузевих норм або є публічною компанією, у вас можуть бути інші зобов'язання щодо звітності. Окрім цих обов’язків і залежно від характеру та серйозності порушення, ви також можете мати незавидне завдання повідомляти постраждалим особам, потенційно клієнтам, співробітникам та будь-яким іншим зацікавленим сторонам, що їхню інформацію було скомпрометовано.

Знати, коли повідомляти окремим особам і скільки розповідати, є справжньою проблемою. Можливо, вам доведеться вирішувати між виданням потенційно непотрібного попередження без особливих деталей і очікуванням більшої впевненості, тоді ваше попередження може бути надто пізнім, а люди піддаються більшому ризику заподіяння шкоди через шахрайство, спроби фішингу, шантаж чи гірше. У таких випадках експертне керівництво спеціалістів з права та комунікацій може бути неоціненним.

Уникнення виснаження

Коли адреналін, викликаний початковою кризою кібератаки, зменшиться, перед вами постане реальність того, що фактично є великим і несподіваним проектом на невизначений термін. Ймовірно, ця перспектива буде настільки ж виснажливою, наскільки й лякаючою.

Під час особливо руйнівних порушень, коли відновлення та відновлення систем може зайняти дні або навіть тижні, проблема підтримки роботи організації, підтримки довіри персоналу та клієнтів і вирішення складних IT, юридичних та комунікаційних проблем може здаватися нездоланною. Природа кібератак полягає в тому, що їх вирішення рідко буває гладким і передбачуваним.

Багато управлінських команд очолюють люди, які втомилися до ступеня виснаження ще до того, як почнеться кібератака, тому, хоч це й важко, єдиним життєздатним вибором є самостійний темп.

Незважаючи на те, що емоційним наслідкам боротьби з кіберзломом приділено мало офіційної уваги, керівництво Національного центру кібербезпеки Великобританії від 2022 року стосується ризику перевантаження команд. Втомлені люди не завжди приймають найкращі рішення під час кризи, і ситуація реагування на порушення навряд чи може бути покращена через зношених членів команди, яких доведеться відійти та замінити.

Прагнення до закриття

Мабуть, найбільше розчарування в боротьбі з кібератакою полягає в тому, що вона може здаватися нескінченною. Навіть після відновлення або перебудови систем і відновлення даних листи зі скаргами та занепокоєнням, у деяких випадках листи-претензії, продовжуватимуть надходити від суб'єктів даних. Клієнти вимагатимуть оновлень, а регулятори можуть дуже повільно повідомляти вам, що вони мають намір вжити проти вас. Залежно від характеру та структури вашої організації, у вас можуть бути інвестори, довірені особи або члени правління, які вимагають точно знати, що сталося, кого вони можуть звинувачувати та що робиться, щоб запобігти повторенню. Якщо у вас є страховка, переговори про премію, ймовірно, будуть більш складними після порушення.

Після кіберінциденту ви стаєте більш уразливими до подальших атак з боку тих самих та інших груп учасників загрози, тому будь-які уроки, засвоєні щодо IT-безпеки чи організаційних заходів безпеки, повинні діяти швидко. Будь-яка поблажливість, виявлена регулюючими органами, не повториться, якщо ви станете жертвою тієї самої чи подібної вразливості вдруге. Навіть якщо ви хочете рухатися далі та зосередитися на відновленні своїх операцій, ви, ймовірно, побачите, що кібератака забирає ваш час протягом місяців після її нібито завершення.

Тож що робити?

Якщо ви опинилися не на тій стороні кібератаки, слід пам'ятати кілька важливих речей:

Не звинувачуйте жертву – важливо визначити вразливі місця чи недоліки, які зробили вас уразливими для атак, щоб ви могли пояснити їх і вирішити їх, але якщо третя сторона, проти якої ви можете подати позов, не несе відповідальності, немає сенсу зосереджуватися на взаємні звинувачення та розподіл провини. Це не заохочуватиме відкритого залучення персоналу та лише посилить і без того напружену атмосферу. Це також означає бути добрим до себе. Ви стали жертвою злочину, і навіть якби замок у ваших дверях міг бути міцнішим, хтось інший вирішив проникнути.

Прислухайтеся до експертів – ви найкраще знаєте свою організацію, і, якщо справа зупиниться на вас, ніхто не зможе приймати рішення за вас, але було б дуже гарною ідеєю скористатися порадою експерта. У деяких організаціях є внутрішні експерти з IT-криміналістики, кризових комунікацій і юридичної підтримки з реагування на порушення, але більшості знадобиться зовнішня допомога. Спеціалісти з реагування на кібератаки щотижня стикаються з проблемами, з якими більшість бізнес-операторів не пощастить стикатися більше ніж один раз у своїй кар'єрі, і вони звикли вирішувати їх без загострених емоцій і рівня стресу, які впливають на тих, хто знаходиться на передовій інцидент. Довіряйте їхнім судженням.

Не беріть надмірних зобов'язань, але дотримуйтесь своїх обіцянок – якщо ви обіцяєте регулярні оновлення персоналу та особам, яких це стосується, вам доведеться виконувати їх або ризикуєте втратити їхню довіру. Будьте реалістичні щодо того, як часто ви можете спілкуватися, і не зобов'язуйтесь залишатися на зв'язку, якщо вам нема чого сказати нового. Якщо ви запропонували лінію довіри, переконайтеся, що вона належним чином укомплектована. Якщо ви надаєте послуги кредитного моніторингу для постраждалих осіб, переконайтеся, що вони доступні для всіх, хто їх потребує.

Зробіть перерву – переконайтеся, що всі, хто бере участь у реагуванні на порушення, регулярно відпочивають, і за потреби залучіть зовнішню підтримку, щоб уникнути вигорання та погіршення і без того стресової ситуації. Якщо ви керуєте відповіддю, дуже важливо, щоб ви практикували те, що проповідуєте.

Припиніть перевірку повідомлень після певного часу вночі та доручіть своїй команді зателефонувати вам у разі надзвичайної ситуації, щоб ви не відчували потреби постійно дивитися на свій телефон. Протягом дня спробуйте погуляти і на деякий час переключити свою увагу з пролому. Це може здатися неможливим під час кризи, але ви досягнете більшого, якщо відступите назад і час від часу глибоко вдихнете.

Призначте когось, хто керуватиме довгим хвостом – через певний період часу, коли вирішаться найневідкладніші справи, виникне спокуса зосередитися на поверненні до звичайної роботи, а не на затяжних наслідках атаки. Призначте члена команди для нагляду за подальшими діями, пов'язаними з порушенням, і для отримання необхідних уроків з інциденту. Нехай ця особа регулярно звітує перед керівництвом. Це може включати управління довгостроковою регулятивною взаємодією, судовий процес, що виникає через порушення, зв'язок із клієнтом, покращення IT-безпеки або навчання та оновлення політики. Не пропустіть можливість покращити ситуацію, яку може принести криза.

Стрибок у часі…

Якщо ви зараз не перебуваєте в центрі кіберінциденту, що ви можете зробити, щоб покращити своє становище, якщо станете його жертвою?

Культивуйте культуру відсутності звинувачень – перш ніж щось піде не так, підтримайте людей, щоб вони поділилися своїми проблемами. Спробуйте запропонувати особисті кібернавчання та тренінги з даних і заохочуйте всіх висловити будь-які проблеми з безпекою в рамках цих сесій. У культурі, де люди відчувають себе в змозі висловити свої побоювання та виявити потенційні помилки, ви з меншою ймовірністю станете жертвою нападу, і якщо ви це зробите, воно може бути менш серйозним. Що б не трапилося, у вас буде краще зберегти довіру та підтримку ваших співробітників, коли ви реагуєте, тому що ви в першу чергу вислухали їх.

Будьте готові до витоку – підготовка до витоку даних може здатися нерозумною, але час, витрачений на плани реагування на витік, вправи з моделювання інциденту та визначення членів вашої основної групи реагування,

може заощадити години або навіть дні на початку кібератаки, коли час дорогоцінний і будь-яка затримка може бути критичною. Вплив таких, здавалося б, дрібниць, як-от забезпечення того, щоб кожен, хто перерахований у вашій групі реагування, мав призначеного заступника, створення групи WhatsApp, щоб ви могли спілкуватися, якщо ваші електронні листи не працюють, і переконання, що ви вказали контактні дані своїх зовнішніх консультантів (та їх альтернативи), може позбавити вас незліченної кількості непотрібного стресу. Якщо можливо, налаштуйте обмін текстовими повідомленнями зі своїми працівниками, щоб ви могли надіслати текст на їхні особисті пристрої, якщо IT компанії вийдуть з ладу. Коли ви закінчите свій план реагування на порушення, не забудьте роздрукувати його – у світі, де все більше немає паперу, ваші ретельно підібрані крок за кроком процедури будуть марними, якщо у вас немає доступу до цифрових систем. Роздрукуйте дві копії та візьміть одну додому для безпечного зберігання – ви подякуєте нам пізніше.

Інвестуйте в IT – якщо підготовка до злому суперечить інтуїції, то інвестиції в IT дуже очевидні. Але справа не лише в тому, скільки ви витрачаєте. Важко оцінювати нашу власну роботу, і несправедливо доручати вашій IT-команді виявляти власні помилки. Часто ми не бачимо їх, коли вони прямо перед нами. Компанії часто витрачають величезні суми на проекти з IT-безпеки, але не виявляють простих уразливостей, які роблять безглуздими найскладніші засоби захисту. Присвятіть частину своїх витрат на безпеку зовнішньому аудиту безпеки та будьте готові кинути виклик внутрішньому статус-кво, коли отримаєте результати.

Страхуйте все, що можете, якщо можете – деякий час премії за страхування кібербезпеки були настільки високими, а виключення полісів настільки широкими, що було законним або навіть розумним вибором відмовитися від страхування та замість цього інвестувати премію в покращення безпеки. Враховуючи значну та зростаючу вартість реагування на кібератаку, страхування має бути частиною готовності до порушень, де ви можете визначити відповідну політику. Продукти диверсифікуються, і як традиційні брокери, так і брокери-претенденти

наполегливіше працюють, щоб відповідати клієнтам відповідною політикою. Обов'язково ознайомтеся зі своїм полісом під час підготовки плану реагування на порушення – ваш страховик може надати спеціальну підтримку або вимагати від вас залучення власних попередньо перевірених експертів». ***(Withstanding the cyber storm - the vital importance of emotional and institutional resilience for victims of cyber crime // Taylor Wessing (https://www.taylorwessing.com.cn/en/global-data-hub/2024/cyber-security---weathering-the-cyber-storms/withstanding-the-cyber-storm). 18.04.2024).***

***

«Організаціям необхідно належним чином та ефективно керувати собою, що вимагатиме створення та підтримки політик і процедур. Ці документи та інші внутрішні правила допомагають організації виконувати вимоги законодавства та виконувати місію.

Кібербезпека та інші аспекти управління інформаційними системами вимагають ефективних процесів управління та відповідності, щоб задовольнити зростаючі вимоги законодавства та забезпечити ефективну бізнес-операцію.

Керівні документи служать багатьом цілям, включаючи дотримання вимог

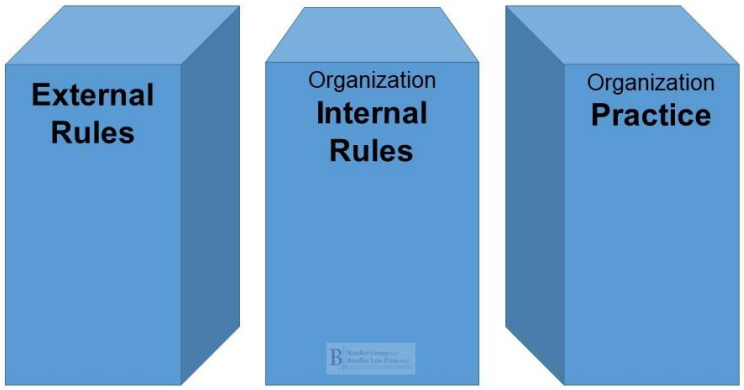
Документи управління включають політику, процедури, посібники, довідники та інші документи, які організації створюють для управління своїми людьми та процесами. Для зручності ми можемо посилатися на «політику» та «роботу на основі політики», розуміючи, що політика є одним із типів документів управління.

Відповідність є важливою метою, але не єдиною. Якщо є проблема відповідності, то перший рівень перевірки стосується документів.

Розглянемо мої три платформи для підключення для відповідності, які складаються з:

- Закони та правила (зовнішні правила);
- Політика та інші внутрішні правила;
- Практики (дія).

Сумісна організація узгоджує всі три платформи, як показано на схемі. Вони починаються з оцінки зовнішніх правил, які встановлюються здебільшого урядом і можуть також включати договірні вимоги з третіми сторонами. Потім організація створює та підтримує платформу своїх внутрішніх правил (багато з них у письмовій формі) та іншу платформу того, що вони насправді роблять — практики.



Bandler's Three Platforms to Connect for Compliance

Courtesy and copyright John Bandler from his book: Policies and Procedures for Your Organization

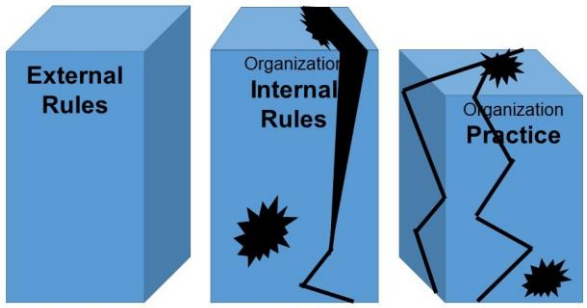
Якби всі організації відповідали вимогам, регулятори, адвокати позивача і навіть деякі прокурори були б бездіяльними та нудьгували. Але будьте впевнені, що багатьом організаціям не вистачає досконалості на фронтах відповідності (та ефективності).

Жодна організація не є ідеальною. Більшість людей працювали в організаціях, де можна було покращити політику чи практику — або те й інше. Покращення, які можуть призвести до кращої відповідності та ефективнішої роботи.

Організація, яка не відповідає вимогам, може не оцінити — або свідомо знехтувати — відповідними правовими вимогами. Вони можуть безсистемно створювати неадекватні платформи, які не відповідають цим зовнішнім правилам і можуть мати структурні недоліки. Їхню письмову політику можна було скопіювати та вставити з іншого місця без обдумування чи адаптації. Потім вони збирають пил, недоторкані. Лідери, менеджери та співробітники, можливо, не читали їх, навіть не чули про них і, як правило, не дотримуються їх.

Завдяки судам і новинам ми знаємо приклади організацій, які мали серйозні недоліки у дотриманні законодавства, а потім були визнані цивільно

відповідальними за грошові збитки або навіть засуджені за кримінальні злочини. Три платформи надзвичайно поганої організації можуть виглядати приблизно так, як ця схема, і мати погане узгодження та структурні недоліки.



Noncompliant organization

Courtesy and copyright John Bandler from his book: Policies and Procedures for Your Organization

Висновок трьох платформ полягає в тому, що кожна організація та кожна політика повинні оцінювати, які закони застосовуються, а потім дотримуватися їх. Далі практика має відповідати політиці та закону.

Відповідність – це ще не все

Дотримання законодавства важливо, але це не все.

Це тому, що організації існують, щоб виконувати місію, а не просто виконувати її.

Кожна політика повинна певним чином включати місію. Місія може називатися бізнес-цілями, цілями чи якось інакше, але принцип полягає в тому, що політика (і відповідність) сприяє і підтримує місію. Вони не борються проти цього.

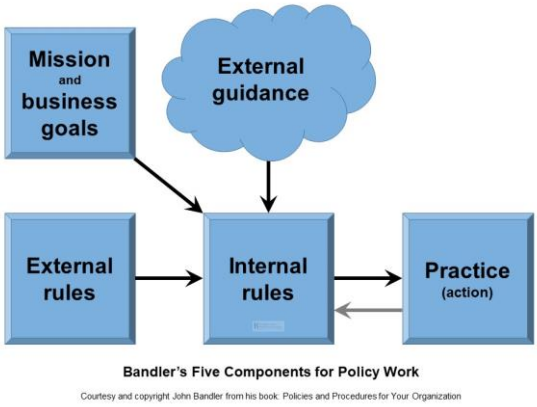
Як наслідок, хороші організації повинні виконувати свою ефективну роботу в межах правових вимог.

Після місії потрібне п’яте міркування, оскільки винахід колеса може зайняти багато часу. Політики повинні оцінювати та враховувати «найкращі практики», аморфний термін, який включає будь-які вказівки, які надходять ззовні організації та мають відношення до цієї теми політики.

Загалом, для ефективної роботи над політикою нам потрібно додати ще два компоненти до наших трьох платформ:

- Місія та бізнес-цілі;
- Найкращі практики (зовнішнє керівництво);

- і це означає, що ми тепер маємо п’ять компонентів для політичної роботи, як показано нижче.



Bandler’s Five Components for Policy Work

Courtesy and copyright John Bandler from his book: Policies and Procedures for Your Organization

Належна оцінка цих п’яти компонентів дозволяє нам ефективно створювати та оновлювати документи управління організацією, як я пояснюю в своїй новій книзі «Політики та процедури для вашої організації».

Кібербезпека та конфіденційність

Кібербезпека та конфіденційність – це складні сфери на перетині технологій, даних, кіберзлочинності, бізнесу та законів і правил, що розвиваються.

Кібербезпека є вимогою дотримання вимог і захисту від кіберзлочинності. Тоді подумайте, що організації, які належним чином керують своїми інформаційними системами, можуть захистити, дотримуватися вимог і також краще виконувати свою місію. Переклад: менше витрат і більше доходу.

Організаціям необхідно оцінити, які закони про кібербезпеку та конфіденційність застосовуються до них…

У підсумку їм потрібно оцінити правові зобов’язання щодо:

- Обов’язкове повідомлення про певні кіберзлочини (повідомлення про порушення даних);
- Cybersecurity;
- Privacy.

Наприклад, закони чи нормативні акти можуть вимагати від організації підтримувати програму кібербезпеки, яка складається з документів, а також відповідних процесів і практик для вирішення проблем і ризиків.

Закони про недбалість (не кажучи вже про добровільні принципи належного управління) передбачають, що організація повинна підтримувати розумну та старанну програму кібербезпеки. Закон може вимагати від організації вжити певних дій і повідомити певних людей і організації, якщо є порушення даних. Контракти накладають обов'язки, пов'язані з кібербезпекою. Визначивши ці зовнішні правила, організація тепер створює внутрішні правила та оцінює, що вона робить і що повинна робити.

Політики та процедури кібербезпеки

Кібербезпека майже завжди потребує письмових політик і процедур, оскільки це надто складно, а інакше було б погано повідомлено.

Незважаючи на те, що усні інструкції та комунікація є важливими для кожної частини управління бізнесом (включно з кібербезпекою), письмова форма необхідна для вирішення тонкого перетину кримінальних загроз, правових вимог, технологій, потреб бізнесу, внутрішньої політики, найкращих практик і дій співробітників.

Ефективні політики та процедури допомагають організаціям належним чином керувати своїми інформаційними активами та системами, захищати себе та виконувати вимоги законодавства.

З цього випливає усвідомлення того, що професіонали з кібербезпеки, включаючи керівників, менеджерів, юристів і консультантів, повинні писати ефективно. А потім працівники повинні читати і вміти розуміти написане.

Ці політики та процедури є необхідними, але їх написання, читання, перегляд та оновлення може викликати складність. Велика кількість вимог і найкращих практик, що збігаються, означає, що існують різні категорії та термінології, які збігаються та відрізняються. Це може викликати страх, невпевненість і сумніви (FUD) протягом усього процесу розробки політики.

Чи можемо ми використовувати інструменти ШІ для написання нашої політики?

Деякі відчувають спокусу дізнатися, чи можуть інструменти штучного інтелекту (AI) створити ідеальний письмовий продукт. Ця спокуса існує навіть

тоді, коли тематична область проста, а ці сфери управління інформацією, кібербезпека, запобігання кіберзлочинам і конфіденційність рідко бувають простими. Існують галузі права, що перетинаються та розвиваються, найкращі практики, технічні питання та питання кібербезпеки, а також нюансовані рішення щодо управління ризиками.

Можливо, штучний інтелект – це проста та зручна кнопка, яку ми можемо натиснути, щоб виконати нашу роботу?

На жаль, штучний інтелект не є чарівною панацеєю...

Відповідь тут — як завжди — полягає в тому, що люди повинні читати й розуміти написане слово, а це означає, що люди повинні відігравати домінуючу роль у його формуванні. Нам потрібно зрозуміти юридичні вимоги, найкращі практики, місію та бажані організаційні дії.

Написання політики – це і подорож, і пункт призначення. Подорож допомагає інформувати про пункт призначення та сприяє зміцненню особистості та організації. Організації, які йдуть короткими шляхами, можуть не дістатися до потрібного пункту призначення та позбавлять себе процесу навчання, який передбачає подорож.

Останні висновки

Кібербезпека складна і може здатися комусь незрозумілою. Але нам просто потрібно привнести в нього хороші принципи управління, прийняття рішень і написання політики.

Організаціям потрібні письмові керівні документи, щоб відповідати вимогам, захищати себе та виконувати свою місію. Остаточний документ важливий, але також важливий шлях до нього. Політики ніколи не повинні стояти на полиці, припадаючи пилом, але вони важливі для дій і місії, а також для всього, що робить організація. Особливо кібербезпека». ***(John Bandler. Management, policies, cybersecurity and compliance // Reuters (https://www.reuters.com/legal/legalindustry/management-policies-cybersecurity-compliance-2024-04-23/). 23.04.2024).***

***

«Кіберризики тепер визнаються на рівні правління. У результаті організації збільшують свої кібербюджети, щоб не відставати від ландшафту загроз, що розвивається, з безпрецедентною видимістю правління та керівників.

Gartner прогнозує, що світові витрати кінцевих користувачів на безпеку та управління ризиками становитимуть 215 мільярдів доларів цього року, що на 14,3% більше, ніж минулого року.

Однак, навіть із цим додатковим рівнем виконавчого нагляду, прийняття рішень щодо кібербезпеки, вимірювання ефективності та регуляторного нагляду все ще є надзвичайно неадекватними, здебільшого зумовленими недійсними даними, самоатестацією та неофіційними доказами. У 2023 році кількість кібератак зросла загрозливою швидкістю. У США було відкрито 3205 випадків витоку даних, що на 78% більше, ніж роком раніше.

Те, як сьогодні приймаються багато рішень щодо кібербезпеки, схоже на те, щоб звернутися до лікаря, пояснити свої симптоми, а лікар поставити діагноз і призначити лікування на основі того, що ви їм сказали, без проведення жодних лабораторій чи тестів для перевірки. У сфері медицини це називається недбалістю. У кібернетичному просторі це надто часто найкраще, що ми можемо зробити.

Проблема не в тому, що дані не існують. І навпаки, дані швидко стали перлиною корони для більшості організацій, а кібердані, які їх оточують, є безцінними. Завдання полягає в каталогізації, зборі, організації та аналізі допоміжних кіберданих таким чином, щоб лідери могли приймати обґрунтовані рішення на основі фактичної правди в режимі реального часу.

Перехід від даних моменту часу до даних руху протягом часу

Кібербезпека як галузь має проблему зрілості даних і ще більшу проблему спостережуваності. Ми використовуємо анекдотичні дані про зломи та вразливості, коли розглядаємо інструменти безпеки та елементи керування, у які варто інвестувати. Недолікові або неповні дані часто виявляються в спільних даних про загрози, на які ми витрачаємо непотрібні ресурси.

Крім того, ми покладаємося на інформацію з власноруч підтверджених опитувальників на певний момент часу, щоб приймати рішення щодо критично важливих компонентів програми стійкості, таких як кіберстрахування та управління ризиками третіх сторін.

Це аж ніяк не через недбалість з боку кіберспільноти. Це частина труднощів росту галузі, яка швидко розвивається. Оперативна спостережливість, можливість бачити та повністю розуміти дані в режимі реального часу, є надзвичайно важливою потребою, яка повільно вирішується. Перехід подібний до переходу медичної професії від емпіричних спостережень і філософських теорій до діагностики, керованої даними; це не виникло відразу, а був поступовим процесом, який охоплював століття.

Нам часто доводиться нагадувати собі, що кібер виповнилося лише 50 років. Поточна практика оцінки кіберризиків обмежена:

• Відсутність даних у реальному часі. Багато інструментів оцінки кіберризиків спираються на історичні дані, які можуть не відображати поточний ландшафт загроз.

• Відсутність інтеграції. Дані з різних джерел часто не інтегровані, що ускладнює отримання повного уявлення про стан кібербезпеки організації.

• Самоатестація за неофіційними даними. Організації часто покладаються на інформацію, отриману від співробітників або третіх сторін, щоб оцінити свої кіберризики, що може призвести до неточних або неповних даних.

• Перевантаження даних. Організації можуть мати доступ до великої кількості даних про стан своєї кібербезпеки, але може бути важко визначити найбільш релевантну та корисну інформацію.

Щоб галузь досягла зрілості, оцінка кіберризиків має перейти до автоматизованого прийняття рішень на основі даних у реальному часі. Щоб досягти цього, необхідно усвідомити, що:

1. Інтеграція інструментів кібербезпеки життєво важлива для комплексної оцінки кіберризиків. Кожен інструмент надає фрагментоване уявлення про кібер-положення організації.

Інтеграція цих інструментів дозволяє консолідувати дані в єдине джерело правди. Справжнє цілісне уявлення дозволить керівникам відділу інформаційної безпеки зрозуміти загальну кібер-позицію своєї організації, виявити прогалини та збіги та прийняти рішення на основі даних для посилення захисту своєї кібербезпеки.

2. Кіберзагрози постійно розвиваються, тому звітність про дані в реальному часі є важливою для ефективного управління кіберризиками. Статичні оцінки ризиків, які проводяться сьогодні, мають обмежену цінність.

Кіберризик розвивається в режимі реального часу. Це означає, що кібервиявлення та кіберпостава змінюються щомиті. Знімок кіберризику сьогодні не відображає кіберризик завтрашнього дня. CISO потрібен доступ до повних даних у реальному часі, щоб виявити та усунути важливі вразливості та пом’якшити наслідки потенційних кібератак.

Кульмінація: інтегрований, керований даними підхід до прийняття рішень щодо кібербезпеки

Звітність із даними в режимі реального часу через інтегровані інструменти кібербезпеки дозволяє приймати рішення щодо кібербезпеки на основі даних у фінансовій сфері.

Довіра є наріжним каменем будь-якої фінансової установи. Фінансові послуги покладаються на складні взаємопов’язані ІТ-системи та працюють у жорстко регульованому середовищі, де секунди можуть прирівнюватися до мільйонів втрачених або отриманих доларів. Таким чином, кіберпозиція організації є стрижнею у збереженні фінансової стабільності та довіри споживачів.

Таким чином, прийняття рішень на основі даних стає критично важливим для фінансових установ. Від управління кіберризиками до демонстрації відповідності до переговорів про вигідні умови страхування – мільярди вартостей чекають, щоб бути розблокованими завдяки використанню кіберданих у реальному часі в технологічному спектрі фінансової галузі.

На конкурентному ринку здатність швидко керувати кіберризиками та зменшувати їх може бути відмінною рисою для фінансових установ. Кібердані в

режимі реального часу підтримують проактивні заходи безпеки та інноваційні послуги, а також забезпечують безперебійну взаємодію з клієнтами, що може сприяти конкурентній перевагі.

Динамічний характер кіберзагроз означає, що рівень кіберризиків організації може змінюватися за мілісекунди. Бути в безпеці минулого місяця, минулого тижня, вчора чи годину тому може бути неважливим під час нової кібератаки. Загрози є «в реальному часі», і розуміння нашої кіберпозиції має бути таким же.

Високі ставки, пов'язані з фінансовими операціями, роблять використання даних у реальному часі необхідним. Використовуючи кібердані в реальному часі, фінансові установи можуть вміло виявляти, оцінювати та миттєво реагувати на кіберзагрози, мінімізуючи потенційні фінансові втрати та зміцнюючи довіру споживачів. Перехід до цієї цілісної, пильної позиції кібербезпеки втілює в собі стратегічну еволюцію — стрибок від позиції реагування до проактивної, інформованої готовності, що закріплює стійкість фінансового сектора в епоху цифрових технологій.

Важливість кіберданих у реальному часі у фінансових послугах важко переоцінити. Йдеться не лише про зменшення ризиків, але й про забезпечення безпечної, сумісної та безперебійної роботи, яка захищає як добробут клієнтів, так і прибутки установи». ***(Bob Ackerman. Cybersecurity In A Data-Driven World: The Problem Of Invalid Data // Forbes (https://www.forbes.com/sites/forbesfinancecouncil/2024/04/24/cybersecurity-in-a-data-driven-world-the-problem-of-invalid-data/?sh=7438c0d3240d). 24.04.2024).***

***

«Близько 23% команд із безпеки включають жінки, виявив ISC2 у своєму дослідженні Cybersecurity Workforce Study.

Лише 17% респондентів ISC2 Cybersecurity Workforce Study були жінками, що свідчить про постійну боротьбу за робочі місця за наймання та утримання жінок у цій галузі. Цьогорічний звіт також демонструє позитивні тенденції: молоді жінки знаходять шлях до кар'єри в галузі кібербезпеки. ISC2 надав детальний огляд стану

жінок у робочій силі, а також поради щодо того, як залучити та утримати різноманітні таланти.

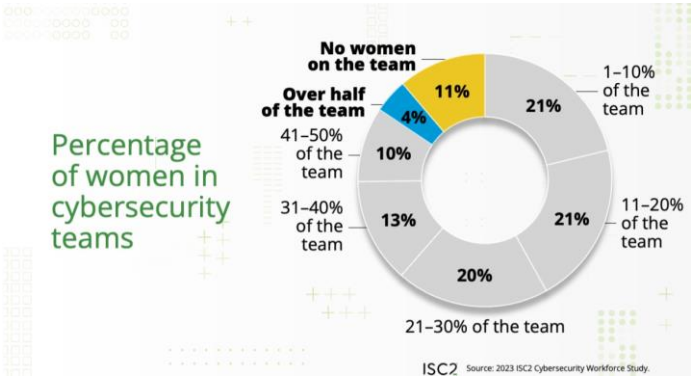
ISC2 опитав 14 865 фахівців з кібербезпеки в Північній Америці, Європі, Азії, Латинській Америці, на Близькому Сході та в Африці в період з квітня по травень 2023 року. Forrester Research, Inc. співпрацювала з ISC2 для збору даних.

У середньому жінки складають приблизно одну чверть у сфері кібербезпеки

За оцінками ISC2, від 20% до 25% людей, які працюють у сфері кібербезпеки, є жінками, і очікується, що до 2031 року ця кількість зросте до 35%.

Що стосується складу команди (мал. А), то в середньому 23% команд безпеки включають жінок. Примітно, що жінки повідомили, що в їхніх командах більше жінок: 30% жінок сказали, що в їхніх командах є інші жінки, на відміну від 22% чоловіків. ISC2 сказав, що це означає, що жінки, як правило, працюють в організаціях з іншими жінками в команді.

Малюнок А



Склад команди з кібербезпеки на основі опитування ISC2.

Сектори хмарних послуг, автомобільного та будівельного секторів повідомили про найвищий відсоток жінок у своїх командах (28%), але це число не набагато вище, ніж у секторах з найменшим відсотком жінок у їхніх командах, а саме у військовій та комунальній сферах. 20%.

Зарплати кібербезпеки демонструють гендерні розбіжності

Зарплати у сфері кібербезпеки дещо вищі для чоловіків, ніж для жінок (мал. В), і в середньому становлять 148 035 доларів для чоловіків і 141 066 доларів для жінок у США, або 115 003 доларів для чоловіків і 109 609 доларів для жінок у

всьому світі. Для кольорових людей середня зарплата кібербезпеки в США становить 143 610 доларів для чоловіків і 135 630 доларів для жінок.

Малюнок В

Порівняння середніх зарплат у сфері кібербезпеки в США.

Жінки в сфері кібербезпеки можуть стикатися з дискримінацією або боротися з автентичністю

Серед опитаних 29% жінок повідомили, що зазнавали дискримінації на роботі, порівняно з 19% чоловіків. Крім того, 36% жінок сказали, що вони не можуть бути автентичними на роботі, порівняно з 29% чоловіків.

Ці цифри можуть сильно відрізнятися залежно від країни: жінки чорношкірого або африканського походження в Канаді, Великій Британії та Ірландії стикалися з найбільшою дискримінацією (53%), за ними йдуть чоловіки чорношкірого та африканського походження в тих же країнах (42%).

Людям, які стикаються з дискримінацією на роботі, «важче ризикувати, пропонувати нові ідеї або висловлювати занепокоєння», відзначається у звіті McKinsey «Жінки на робочому місці» за 2023 рік.

Чому жінки займаються кібербезпекою та що це означає для найму

Жінки та чоловіки повідомляють, що займаються кібербезпекою приблизно з однакових причин. За даними ISC2, головними причинами, чому люди роблять кар'єру в галузі кібербезпеки, були можливості кар'єрного зростання (26% жінок і 27% чоловіків), здатність вирішувати проблеми (24% жінок і 22% чоловіків) і високий попит на навички кібербезпеки (24% жінок і 25% чоловіків). Деякі додаткові відмінності між двома опитаними групами:

Зацікавленість працювати в сфері, що постійно розвивається: 21% жінок і 18% чоловіків.

Знаходження особистого/емоційного задоволення: 14% жінок і 17% чоловіків.

Вплив моделей кібербезпеки, які їх заохочували: 14% жінок і 11% чоловіків.

Самостійно займалися кібербезпекою та отримали від цього задоволення: 10% жінок і 15% чоловіків.

Обидві групи повідомляють про високу задоволеність роботою, беручи до уваги загальну кар'єру: 76% жінок і 70% опитаних чоловіків сказали, що вони задоволені своєю роботою в сфері кібербезпеки.

Жінки повідомляють про меншу кількість кадрів із кібербезпеки на своїх робочих місцях порівняно з чоловіками (62% проти 68%), з чого ISC2 зробив висновок, що організації, які успішно залучають різноманітних кандидатів, вирішують свої кадрові проблеми трохи ефективніше. Організації, в яких працюють жінки-респондентки, зазвичай:

Наймайте потенційних талантів зсередини, тобто співробітників за межами кібернетики чи IT.

Здійснюйте ротацію посад, тобто переміщуйте співробітників між ролями.

Наймайте людей без попереднього досвіду кібербезпеки.

Розвиток інклюзивної культури приносить користь бізнесу

Наймання більшої кількості жінок і забезпечення того, щоб кожен член команди почувався комфортно у своєму робочому середовищі, може мати велике значення для заповнення відкритих посад у затребуваній, але все ще недостатньо укомплектованій сфері кібербезпеки. ISC2 пропонує такі пропозиції для організацій, які хочуть збільшити кількість жінок у сфері кібербезпеки та підвищити задоволеність роботою тих жінок, які вже працюють у цій сфері:

Створюйте програми з кібербезпеки, придатні для початкової освіти, відкриваючи молодим людям кібербезпеку як варіант кар'єри.

Встановіть конкретні показники найму, найму та просування у своїй політиці та практиках найму в сфері кібербезпеки, пов'язаних із додаванням і утриманням жінок у робочій силі.

Платіть жінкам однаково з чоловіками.

Підтримуйте цілі жінок щодо просування по службі, особливо тих, хто хоче досягти високих посад — побачивши жінок на керівних посадах, можна надихнути інших наслідувати їх.

Зосередьтеся на «інклюзивності» різноманітності, справедливості та інклюзії, створивши надійні показники та цілі щодо забезпечення того, щоб співробітниці відчували себе включеними та автентичними на роботі.

Долучіть до процесу найму жінок, які вже є в команді з кібербезпеки.

«Переваги інклюзивної культури, особливо в кібербезпеці, численні — і критичні», — сказав Клар Россо, генеральний директор ISC2, в електронному листі до TechRepublic. «Організації, які прагнуть інклюзії, залучають людей, які вирішують проблеми, аналітичних і критично мислячих людей, а також різноманітні набори навичок і досвід для вирішення проблем і створення можливостей». ***(Megan Crouse. Women in Cybersecurity: ISC2 Survey Shows Pay Gap and Benefits of Inclusive Teams // TechnologyAdvice (https://www.techrepublic.com/article/women-in-cybersecurity-study/). 25.04.2024).***

***

«Сьогодні цифрова революція трансформує звичайне банківське обслуговування, що призводить до того, що все більше користувачів виходять в Інтернет. За допомогою банківських додатків люди можуть забронювати зустріч, отримати кредитну чи дебетову картку та взяти участь у різноманітних заходах, у тому числі гейміфікованих. Однак ця зміна також відкрила новий кордон для кіберзлочинців. Отже, зараз фінансові установи часто стають головними мішенями для складних кібератак.

Таким чином, стратегії кібербезпеки постали як фундаментальні вимоги до банківського програмного забезпечення. Це вкрай необхідно для захисту активів клієнтів і підтримки довіри. Тому в цій спеціальній статті S-Pro досліджує виклики, з якими стикається банківська індустрія. Ми окреслимо ефективні стратегії побудови міцного захисту.

Потоки, які кіберзлочинці можуть нанести на банківський додаток

Сучасні кіберзлочинці використовують нові способи шахрайства. Вони використовують різноманітні технології та інноваційні рішення, які можуть викрасти облікові дані або перехопити транзакції.

Одним із найпопулярніших способів шахрайства є фішингові атаки. Вони використовують оманливі електронні листи або веб-сайти, щоб обманом змусити користувачів розкрити конфіденційну інформацію. Інші злочинці використовують тактику соціальної інженерії, яка може змусити працівників надати несанкціонований доступ.

Висококваліфіковані зловмисники можуть здійснювати складні, багатоетапні напади, відомі як Advanced Persistent Threats (APT). Це дозволяє їм обійти заходи безпеки та отримати постійний доступ до мережі банку. Ще один просунутий тип — це атаки нульового дня, які використовують раніше невідомі вразливості. Від них надзвичайно важко захиститися, як зазвичай, ці вразливості не помітні власникам програмного забезпечення.

Далі йде тип, про який усі чули – атаки на відмову в обслуговуванні (DoS). Цей тип використовується для перевантаження онлайн-інфраструктури банку трафіком, що робить її недоступною для законних користувачів. Незадоволені співробітники або сторонні постачальники з авторизованим доступом також можуть становити значний ризик безпеки, відомий як внутрішні загрози.

Будівництво укріпленої оборони

Звичайно, боротьба з цими різноманітними загрозами вимагає багаторівневого підходу, який інтегрує технології та людей, сприяючи ідеальному рівню автоматизації, що поєднується з ручною роботою. Регулярні оцінки вразливостей і виправлення мають вирішальне значення для виявлення та усунення слабких місць у системах і програмному забезпеченні.

Щоб ще більше захистити свою програму, ви, як власник програмного забезпечення, можете спробувати тестування на проникнення. Це може посилити рівень безпеки шляхом імітації атак у реальному світі. Використовуйте брандмауери, системи виявлення/запобігання вторгненням (IDS/IPS) і рішення для

запобігання втраті даних (DLP), щоб сформувати ядро безпеки мережі, моніторингу активності та запобігання несанкціонованому доступу або викраденню даних.

Цей крок здавалося б простим, але не нехтуйте ним. Встановіть антивірусне та антишкідливе програмне забезпечення на всіх внутрішніх пристроях компанії. Незважаючи на цей, здавалося б, простий крок, він може додатково підвищити безпеку кінцевої точки.

Еволюція кібербезпеки

Оскільки нові технології використовуються злочинцями, те саме стосується захисту банків. Тепер ви можете використовувати різні інноваційні технології, зокрема штучний інтелект, машинне навчання, блокчейн і біометричну автентифікацію, щоб допомогти вашому бізнесу залишатися на плаву.

Штучний інтелект і ML можуть використовуватися багатьма компаніями, які прагнуть аналізувати мережевий трафік, виявляти підозрілу активність і прогнозувати потенційні атаки в режимі реального часу.

Технологія блокчейн також може запропонувати потенціал для безпечного та захищеного від втручання зберігання даних і обробки транзакцій із додатковим захистом.

Біометрична автентифікація, як-от відбиток пальця та розпізнавання обличчя, може забезпечити більш надійний рівень безпеки. Оскільки банки переносять все більше операцій у хмару, впровадження надійних хмарних рішень безпеки, які відповідають галузевим стандартам, є надзвичайно важливим.

Висновки

Кібербезпека в банківській галузі все ще триває. У той же час це може дозволити зацікавленим сторонам обмінюватися інформацією про загрози та розробляти ефективні заходи протидії.

Однак кібербезпека — це не срібна куля. Це завжди вимагатиме постійної пильності та адаптації. І все ж, якщо ви хочете забезпечити своїм клієнтам безпечний цифровий досвід, це ваш шлях». ***(Cybersecurity Strategies for the Banking Industry: Protecting Assets in a Digital World // MacSources***

(https://macsources.com/cybersecurity-strategies-for-the-banking-industry-protecting-assets-in-a-digital-world/). 25.04.2024).

***

«Цифрові апаратні та програмні продукти є найбільшим входом, коли мова йде про успішні кібератаки. У цифровому середовищі все пов'язано, від систем внутрішнього зв'язку до пристроїв IoT і хмарних сховищ, а це означає, що порушення безпеки в одному продукті може вплинути на всю організацію.

Навіть програми, які вважаються організацією менш критичними, можуть призвести до порушення роботи всієї системи. Оскільки Statista оцінює, що кіберзлочинність обійшлася Німеччині в 206 мільярдів євро, а світовій економіці в 8,15 трильйона доларів у 2023 році, ставки, безумовно, високі.

Атака Sunburst є хорошим прикладом того, чому міркування безпеки такі важливі для розробки програмних продуктів. У 2020 році зловмисне програмне забезпечення було впроваджено в програмне забезпечення Orion від SolarWinds як частину оновлення. Цій атаці на один програмний продукт вдалося скомпрометувати понад 18 000 клієнтів, у тому числі Міністерство юстиції США, у якого було викрадено інформацію та шпигували за його системами. Це демонструє, наскільки сучасне підключення розширило охоплення кібератак.

Для боротьби з такими загрозами приймається нове законодавство. Європейський акт про захист від кібернетичної інформації – це нормативно-правова база, спрямована на зменшення вразливості цифрового обладнання та програмного забезпечення до кібератак. Він передбачає обов'язкові вимоги до кібербезпеки для цифрових продуктів, розміщених на ринку ЄС, і означає, що тепер виробники зобов'язані думати про безпеку протягом усього життєвого циклу продукту. Ця постанова певною мірою гарантує, що всі постачальники рішень безпеки, зв'язку та зберігання даних надають надійні технології та мають плани резервного копіювання та обмеження збитків для захисту даних клієнтів у разі інциденту. Однак для більшості організацій однієї відповідності недостатньо, щоб забезпечити захист від атаки.

Щоб підготуватися та захистити себе в боротьбі з кіберзлочинністю, організації повинні інвестувати в більшу профілактику. Але не всі стійкі до кібербезпеки продукти не однакові. Отже, які міркування повинні враховуватися постачальниками при розробці програмного забезпечення?

1: Безпека з самого початку

Безпеку необхідно враховувати з самого початку процесу розробки мережевих рішень і рішень для підключення. Мета полягає в застосуванні методів кібербезпеки як частини життєвого циклу розробки захищеного програмного забезпечення (SSDLC), щоб забезпечити безпеку програм із самого початку, тобто безпеку за проектом.

Перед створенням нового програмного продукту необхідно намітити та спланувати вимоги безпеки.

Потім слід дотримуватися найкращих практик безпечного кодування та архітектури, переконавшись, що програмні компоненти ізольовано та реалізовано такі протоколи, як шифрування та автентифікація. Комплексне тестування та перегляд забезпечать виявлення будь-яких потенційних вразливостей. Цей процес означає, що всі функції будуть розроблені таким чином, щоб безпека була центральною для їх функціонування, а не додавалась пізніше.

2: бути в курсі подій

Подібно до того, як компанії постійно інвестують у нові рішення безпеки, групи програм-вимагачів постійно використовують останні розробки в IT, щоб підвищити складність своїх атак. Нові технології, такі як генеративний штучний інтелект, створюють нові вектори атак із можливістю використання раніше невиявлених уразливостей, а зловмисне програмне забезпечення, що розвивається самостійно, часто може залишатися непоміченим існуючими розгортаннями безпеки. Квантові обчислення також на горизонті і створять нову загрозу криптоаналітичної атаки. Підтримка після розгортання може відстежувати активність у системі та надавати оновлення та виправлення, які захищають від нових загроз і забезпечують безпеку програмного забезпечення, запобігаючи будь-яким інцидентам безпеки. З цієї причини невід’ємною частиною рішень безпеки є

постійний розвиток і повторне оновлення, щоб гарантувати їх захист від новітніх тактик і технологій, які використовують хакери.

3: Гнучкість між платформами

Більшість організацій працюють, використовуючи різноманітне програмне забезпечення сторонніх виробників, кожна з яких має одну або кілька функцій. Наприклад, може існувати одна система для електронних листів, інша – для внутрішнього зв'язку, а третя – для зберігання файлів і даних.

Така фрагментація може підвищити ризик атаки на організації, оскільки командам із безпеки не вистачає єдиного уявлення про свою IT-систему. Крім того, потрібен лише один партнер із поганою безпекою, щоб поставити під загрозу всю організацію.

Підприємствам необхідно шукати гнучкі, адаптовані рішення безпеки, які можна запровадити для роботи в їхніх програмах, пристроях і платформах Інтернету речей, щоб забезпечити водонепроникний захист даних у їхніх мережах. Ці рішення забезпечують більш ретельний захист, а також ними простіше керувати командою безпеки.

Врахування цих трьох міркувань під час створення програмного та апаратного забезпечення дозволить постачальникам вийти за рамки дотримання законодавства ЄС, наприклад NIS-2. 2024 рік, безсумнівно, матиме певну частку викликів у сфері кібербезпеки, але, ставлячи безпеку в основу своїх продуктів, дизайнери мають найкраще місце, щоб надати своїм партнерам і клієнтам безпечне онлайн-середовище з хорошими зв'язками». ***(Vincent Lomba. Creating Successful Cybersecurity Solutions // Cyber Security Intelligence (https://www.cybersecurityintelligence.com/blog/creating-successful-cybersecurity-solutions-7618.html). 25.04.2024).***

***

«…Кібербезпека — це відповідальність для всього бізнесу, яка вимагає проактивної стратегії, яка виходить далеко за рамки лише технічних рішень.

Отже, уявіть собі: невпинний шквал шкідливих електронних листів заповнює вашу мережу (це безпосередній ризик). Застаріле програмне забезпечення робить вашу систему вразливою до нових загроз (це ризик повільного спалювання). Обидва становлять серйозну небезпеку, але кожен вимагає індивідуального підходу.

Давайте з'ясуємо, чому збалансована стратегія, яка проактивно враховує ризики як негайного, так і повільного спалювання, є ключем до надійної кібербезпеки.

Негайні ризики – вовки біля дверей

Швидкі дії є вирішальними, коли йдеться про очевидні кіберзагрози. Ці погрози не чекають чемно біля дверей – вони вже розбивають їх. Небезпека реальна і позбавляє ваш захист щохвилини паузи. Ось як вони виглядають:

Програми-вимагачі – шкідливе програмне забезпечення, яке шифрує ваші файли, роблячи їх недоступними, доки ви не заплатите викуп. Це може пошкодити цілі системи та призвести до серйозних збоїв у роботі.

Шахрайство з компрометацією бізнес-електронної пошти (BEC) – складні атаки соціальної інженерії, під час яких злочинці видають себе за довірених контактів (наприклад, вашого генерального директора, постачальників), щоб обманом змусити співробітників дозволити шахрайські платежі або розкрити конфіденційну інформацію.

Програмне забезпечення без виправлень – відомі вразливості у вашому програмному забезпеченні забезпечують легкий доступ для хакерів. Регулярне встановлення оновлень безпеки має важливе значення для усунення цих прогалин у безпеці.

Фішингові атаки – шахрайські електронні листи, текстові повідомлення або веб-сайти, призначені для викрадення облікових даних, фінансової інформації та інших конфіденційних даних. Часто замасковані як представники законних компаній або окремих осіб.

Щоб боротися з цими загрозами, ось короткий контрольний список інструментів і методів для боротьби з цими загрозами, які виникають безпосередньо у вас:

Конфігурації брандмауера – ваша перша лінія захисту, яка блокує спроби неавторизованого доступу.

Системи виявлення вторгнень (IDS) – як цифрові сторожові пси, IDS сповіщає вас про підозрілу активність у вашій мережі.

Групи швидкого реагування – еквівалент екстреного реагування з питань кібербезпеки.

Резервне копіювання даних – ваш життєвий шлях, якщо вам знадобиться натиснути кнопку скидання та відновити системи.

Реалістичне навчання – моделюйте атаки, щоб підготувати співробітників до реальних ситуацій.

Ризик повільного горіння – змії в траві

На відміну від відвертих атак, які захоплюють заголовки, ризики повільного спалювання ховаються на задньому плані, поступово підриваючи вашу позицію кібербезпеки. Але не обманюйте себе – їхній вплив з часом може бути таким же руйнівним, як і раптовий напад.

Які ризики повільного горіння?

Ризики повільного спалювання охоплюють уразливості або дії, які не завдають миттєвої шкоди, але створюють можливості, якими з часом можуть скористатися хакери. Думайте про них як про бомби уповільненої дії, приховані у вашій системі. Приклади ризику повільного горіння включають:

- Однократне навчання – працівники повертаються до ризикованих звичок без постійного підкріплення, що робить їх вразливими до нових атак
- Рідкісні оцінки ризиків – Ваш захист стає неефективним проти нових загроз, які виникають між оцінками
- Нехтовані перевірки відповідності – зловмисники легко обійдуть застарілі заходи безпеки

- Відсутність аналітики поведінки – зловмисники можуть довше залишатися непоміченими без інструментів для виявлення відхилень від нормальної поведінки мережі
- Погана сегментація мережі – одне порушення може поширитися на всю вашу мережу, посилюючи шкоду

Ціна нехтування

Ігнорування ризику повільного згоряння є небезпечним ризиком. Чим довше зберігаються ці вразливості, тим вище потенційна вартість. З часом нехтування може призвести до кількох тяжких наслідків:

Значні фінансові втрати. Витрати, пов'язані з витоком даних, збоями в роботі та штрафами, спричиненими нехтуванням цими ризиками, можуть швидко завдати шкоди фінансам компанії.

Шкода репутації та втрата довіри клієнтів. Розголошення конфіденційної інформації може завдати серйозної шкоди репутації вашої компанії та підірвати довіру клієнтів. І те, і інше важко відновити, і вони можуть мати тривалий вплив на ваш бізнес.

Юридичні наслідки. Залежно від галузевих норм, які застосовуються до вашої організації, недотримання стандартів і ризиків безпеки може призвести до дорогих судових суперечок і серйозних покарань.

Збалансований підхід – жонглювання негайним і повільним ризиком опіку

Захист вашої організації потребує багатостороннього підходу, такого, який бореться як з безпосередніми загрозами, так і з повільним ризиком, що ховається у фоновому режимі. Ось як знайти правильний баланс:

Інтегровані рішення для управління ризиками. Частичної кібербезпеки вже недостатньо, особливо в умовах складних загроз. Інвестування в інтегровані рішення допоможе вам отримати всебічне уявлення про свій ландшафт ризиків, дозволяючи визначити пріоритетність миттєвих проблем і одночасно активно пом'якшувати довгострокові вразливості.

Стрес-тестування. Регулярно перевіряйте свої засоби кібербезпеки через ретельні стрес-тести, щоб виявити слабкі місця, перш ніж ними скористаються

хакери. Це схоже на тренування на катастрофу для ваших цифрових активів, щоб переконатися, що ви готові до різних сценаріїв.

Сильна позиція кібербезпеки вимагає уваги як до миттєвих, так і до повільних ризиків спалювання. Розуміючи небезпеки, пов'язані з цими різними категоріями загроз, ваша організація може проактивно впроваджувати оборонні стратегії, що охоплюють технології, процеси та постійне навчання.

Перетин особистого та професійного ризику

Навіть, здавалося б, нешкідливі особисті звички щодо кібербезпеки можуть зробити вашу організацію незахищеною. Наприклад, співробітник, який повторно використовує паролі для соціальних мереж і робочих облікових записів, створює міст, яким можуть скористатися хакери. Така необережна поведінка значно збільшує ймовірність стати жертвою безпосередніх загроз, які ми досліджували вище.

Але справа не в тому, щоб звинуватити. Ефективне вирішення проблем кібербезпеки означає розширення можливостей ваших співробітників знаннями та інструментами, щоб стати потужною лінією захисту…» ***(Cherelle Johannes. Immediate vs. Slow Burn Risks: A Balanced Cybersecurity Strategy // NAVEX Global, Inc. (https://www.navex.com/blog/article/immediate-vs-slow-burn-risks-a-balanced-cybersecurity-strategy/). 25.04.2024).***

***

«Згідно зі звітом «Захист сектору ланцюга поставок», опитуванням, проведеним Hexnode, корпоративним рішенням безпеки від Mitsogo Inc., яке має десятирічну спадщину у сфері уніфікованого кінцевими точками керування (UEM), IT-адміністратори в галузях з активними секторами ланцюгів поставок опинилися між прицілом, коли вони прагнуть збалансувати кібербезпеку та продуктивність.

На основі відповідей понад 1000 IT-фахівців опитування виявило тривожну тенденцію: 77% співробітників висловлюють сумніви щодо ефективності поточних заходів безпеки, зокрема щодо загроз кібербезпеці в ланцюгах поставок.

Опитування Hexnode заглиблюється в динаміку кібербезпеки в різних вертикалях, визначаючи переважні проблеми в секторі ланцюга поставок і визначаючи його траєкторію.

Зокрема, опитування виявило небажання організацій виділяти достатній бюджет на ініціативи з кібербезпеки. З іншого боку, хоча 42% організацій залишаються неготовими до кібератак, 41% опитаних співробітників вказали лише на помірні знання у використанні інструментів і технологій для запобігання таким атакам.

«Сектор ланцюга постачання вимагає рівноваги між його складовими елементами: технологіями, співробітниками та сторонніми постачальниками. Це схоже на ефект доміно; вразливість в одному аспекті може спровокувати крах усієї структури», — зауважив Апу Павітран, генеральний директор і засновник Hexnode. «Завдяки поєднанню технологічних інновацій, стратегічних інвестицій і непохитного дотримання найкращих практик кібербезпеки компанії можуть рухатися по траєкторії до майбутнього, де цифровізація не тільки оптимізує ефективність і гнучкість, але й захищає цілісність і безпеку всієї екосистеми ланцюжка поставок».

Незважаючи на те, що компанії планують інвестувати в такі нові технології, як штучний інтелект і автоматизація, щоб оптимізувати роботу ланцюга постачання, такі проблеми, як прогалини в навичках, брак досвіду та бюджетні обмеження, залишаються. Опитування підкреслює важливість переоцінки інвестиційних стратегій і розробки переглянутих дорожніх карт, узгоджених з майбутнім ланцюжка поставок. Цей стратегічний підхід дозволить підприємствам швидко адаптуватися до коливань ринку, задовольняти потреби клієнтів, що постійно змінюються, і ефективно долати непередбачені збої». ***(Hexnode Survey Reveals Cybersecurity Imbalance in Supply Chain Impeding Adoption of Emerging Technologies // New Business Media (https://www.01net.it/hexnode-survey-reveals-cybersecurity-imbalance-in-supply-chain-impeding-adoption-of-emerging-technologies/). 24.04.2024).***

***

«Усі в курсі, хто такі кіберзлочинці і якої шкоди вони завдають. А ось із тими, хто протистоїть їм, люди знайомі гірше. Навколо інформаційної безпеки (ІБ) у масовій свідомості склалося багато міфів. Редакція GSMinfo проаналізувала і розвінчала три з них.

Міф перший: «ІБ – це тільки засоби захисту»

Технічні засоби, за допомогою яких забезпечується інформаційна безпека, відіграють найважливішу роль. Підвищена увага до них – одна зі складових повсякденної роботи фахівців з кібербезпеки. Але проектування ІБ-систем, їхня експлуатація, розвиток тощо. – тільки одне із завдань ІБ-служби, не менш важливу роль відіграє процесна частина роботи. При цьому вона не пов’язана з попередженням ризиків, зокрема людського фактора. Чому?

Річ у тім, що впровадження заходів інформаційної безпеки саме по собі не гарантує змін у поведінці користувачів, навіть найдокладніші описи процесів ІБ не забезпечують їх безумовного дотримання. Людський фактор усе ще залишається найбільш уразливим елементом ланцюжка створення ІБ-цінності: дисципліна важлива не менше, ніж захисні механізми та процедури.

Приклад. Відділ розробки ПЗ забезпечений захищеними інструментами власної розробки та комунікації. При цьому співробітники продовжують здійснювати ризиковані дії, такі як обмін файлами через загальні диски або надсилання конфіденційних даних через месенджери. Процеси є, інструменти теж, немає тільки усвідомленості їхнього беззастережного застосування, що пов’язує всі елементи ІБ воєдино.

Тільки введення відповідальності за порушення може сприяти поліпшенню ситуації. Наприклад, непройдене навчання ІБ може призвести до позбавлення премій, а регулярні перевірки на вразливість співробітників до фішингу та інші тести дозволять підтримувати ІБ-пильність на належному рівні. Порушникам пропонується додаткове навчання, що підкріплюється інформаційним супроводом і пропагандою правильної поведінки.

Людина – найслабша ланка в системі кібербезпеки будь-якої складності. Саме через рядових співробітників зловмисники сьогодні найчастіше проникають у захищені периметри організацій, поширюють в атакованих інфраструктурах шкідливе ПЗ, викрадають або компрометують дані, завдаючи жертвам багатомільйонних збитків.

Проста розсилка фішингових повідомлень з високою часткою ймовірності виявиться успішною. Це означає, що одержувачі фішингового повідомлення введуть свої облікові дані у фішинговий ресурс або відкриють файл, що містить шкідливе ПЗ. У результаті – витік даних, репутаційний, юридичний і фінансовий збиток.

Слабкою ланкою при цьому може виявитися не тільки рядовий співробітник. Відомі випадки, коли в рамках навчань, що проводяться в компанії службою безпеки, на вудку хакерів потрапляли самі керівники: прийнявши фішингові листи за чисту монету, переходили за посиланнями, які в них містилися.

Багато підприємств, зокрема великих, страждають на своєрідний інфантилізм. «Ми купили за серйозні гроші засоби захисту і тепер надійно захищені», – думає середньостатистичний начальник. На жаль, так ефективна система інформаційної безпеки не працює. Постійно з'являються нові вразливості, удосконалюються підходи до проведення кібератак, а також способи обходу впроваджених у компанії засобів захисту, і часто компрометація інфраструктури є питанням часу.

Міф другий: «ІБ – кібер-охорона»

В очах багатьох співробітників, які не мають відношення до ІБ, безпечники представляються окремою кастою. Щось на кшталт спецслужби або приватної охоронної фірми всередині компанії, завдання якої – забороняти будь-які вольності, пов'язані з використанням інформаційних ресурсів.

Багато років тому аналогічно сприймалися і самі IT-підрозділи. Але з часом IT і бізнес зблизилися, і часом уже неможливо провести чітку межу між бізнес- і технологічним блоками компанії. Сьогодні багато хто знає, що ролі адміністраторів

баз даних, розробників або DevOps-інженерів істотно різняться, але безпечників, як і раніше, вважають групою «людей у чорному».

Насправді у кожного ІБ-фахівця своя роль:

- менеджер з ІБ визначає вимоги, аналізує ризики і стежить за дотриманням політик безпеки;
- ІБ-архітектор вибудовує з окремих рішень систему, яка ефективно протистоїть загрозам;
- фахівець із тестування на проникнення оцінює побудовану систему захисту, імітуючи дії зловмисника;
- а фахівець DevSecOps або AppSec контролює захищеність розроблюваного ПЗ у компанії.

У них є керівник – директор з інформаційної безпеки (CISO), у деяких компаніях його роль виконує CIO (IT-директор). Їхнє завдання не в тому, щоб усе забороняти, обмежувати, контролювати кожну активність, а за порушення карати. Навпаки, мета ІБ – зробити так, щоб кожен співробітник розумів, що і від його дій залежать безпека та успішність бізнесу компанії.

У цього міфу є ще один бік. У багатьох компаніях вважають, що утримання власної ІБ-служби – неминуче, але необхідне зло, оскільки витрати на таких співробітників дуже високі. Це вірно далеко не завжди, часто простіше віддати напрямок на аутсорс.

Міф третій: «безпечники за всіма стежать»

Така можливість у них справді є, але подібні дії в їхні обов’язки не входять, оскільки заборонені законом.

Можливі винятки, але тільки в тих випадках, коли компанія попереджає співробітника (приймаючи його на роботу або під час зміни правил внутрішнього розпорядку) про те, що інформацію можуть збирати з використанням різних джерел, що відносяться до його робочого простору, але не стосуватимуться нічиєго приватного життя.

І тільки з дотриманням усіх формальностей ІБ-фахівці можуть відстежити листування співробітника, факт передавання даних, реальний час, витрачений на

роботу, відвідані інтернет-ресурси, установку та використання застосунків або реальне місцезнаходження». ***(Поставив антивірус і фахівці з кібербезпеки не потрібні: чому це не працює // GSMinfo (https://gsminfo.com.ua/164908-postavyv-antyvirus-i-fahivczi-z-kiberbezpeky-ne-potribni-chomu-cze-ne-praczyuye.html). 25.04.2023).***

***

«Кібербезпека постійно розвивається і, як така, вимагає постійної пильності.

Щодня корпорація Майкрософт аналізує понад 78 трильйонів сигналів безпеки, щоб краще зрозуміти новітні вектори атак і методи. Починаючи з минулого року, ми помітили зміни в тому, як суб'єкти загроз масштабують і використовують підтримку національних держав. Зрозуміло, що організації продовжують зазнавати більшої кількості атак, ніж будь-коли раніше, а ланцюжки атак стають усе складнішими. Час перебування скоротився, а тактика, техніка та процедури (TTP) еволюціонували, щоб стати спритнішими та більш ухильними за своєю природою.

На основі цих висновків організації кінцевих користувачів повинні регулярно стежити за п'ятьма тенденціями атак.

Досягнення скритності, уникаючи спеціальних інструментів і шкідливих програм

Деякі групи загроз надають перевагу стелсу, використовуючи інструменти та процеси, які вже існують на пристроях їхніх жертв. Це дозволяє супротивникам прослизати поза радаром і залишатися непоміченими, приховуючи свої дії разом з іншими суб'єктами загрози, які використовують подібні методи для здійснення атак.

Прикладом цієї тенденції є Volt Typhoon, китайська державна компанія, яка потрапила в заголовки газет, націлившись на критично важливу інфраструктуру США за допомогою методів життя поза межами землі.

Поєднання кібероперацій і операцій впливу для більшого впливу

Суб’єкти національної держави також створили нову категорію тактик, яка поєднує кібероперації та методи операцій впливу (IO). Цей гібрид, відомий як «кібероперації впливу», поєднує кіберметоди, такі як крадіжка даних, псування, розподілена відмова в обслуговуванні та програми-вимагачі, з методами впливу, такими як витік даних, маріонетки, видавання себе за жертву, оманливі дописи в соціальних мережах, а також зловмисне спілкування через SMS/електронну пошту — щоб посилити, перебільшити або компенсувати недоліки в доступі зловмисників до мережі або можливостях кібератак.

Наприклад, Microsoft спостерігала, як кілька іранських акторів намагалися використовувати масові SMS-повідомлення, щоб посилити посилення та психологічний ефект своїх операцій кібервпливу. Ми також спостерігаємо все більше кібер-операцій впливу, які намагаються видати себе за ймовірні організації-жертви чи провідних діячів у цих організаціях, щоб додати довіри до наслідків кібератаки чи компрометації.

Створення прихованих мереж шляхом орієнтації на периферійні пристрої мережі SOHO

Особливо актуальним для розподілених або віддалених співробітників є зростаюче зловживання периферійними пристроями в малих/домашніх офісах (SOHO). Дедалі частіше ми бачимо, як зловмисники використовують цільові пристрої SOHO — наприклад, маршрутизатор у місцевій кав’ярні — для створення прихованих мереж. Деякі зловмисники навіть використовують програми для визначення місцезнаходження вразливих кінцевих точок по всьому світу та визначення точок стрибка для наступної атаки. Ця техніка ускладнює атрибуцію, завдяки чому атаки з’являються практично з будь-якого місця.

Швидке прийняття публічно розкритих POC для початкового доступу та постійності

Корпорація Майкрософт все частіше спостерігає, як певні підгрупи національних держав приймають публічно оприлюднений код підтвердження концепції (POC) невдовзі після його випуску для використання вразливостей у додатках, що працюють в Інтернеті.

Цю тенденцію можна помітити в таких групах загроз, як Mint Sandstorm, іранська національна держава, яка швидко використовувала вразливості N-днів у звичайних корпоративних програмах і проводила цілеспрямовані фішингові кампанії для швидкого й успішного доступу до цікавого середовища.

Пріоритет спеціалізації в економіці програм-вимагачів

Ми спостерігаємо постійний рух до спеціалізації програм-вимагачів. Замість того, щоб проводити наскрізну операцію з програмами-вимагачами, зловмисники зосереджуються на невеликому діапазоні можливостей і послуг.

Ця спеціалізація має ефект розколу, поширюючи компоненти атаки програм-вимагачів між кількома постачальниками в складній підпільній економіці. Компанії більше не можуть думати, що атаки програм-вимагачів походять лише від окремої особи чи групи загроз. Натомість вони, можливо, борються з усією економікою програми-вимагача як послуги. У відповідь Microsoft Threat Intelligence тепер відстежує окремо постачальників програм-вимагачів, відзначаючи, які групи трафіку під час початкового доступу, а які пропонують інші послуги.

Оскільки кіберзахисники шукають ефективніші способи зміцнення своєї безпеки, важливо посилатися на важливі тенденції та порушення минулих років і вчитися на них. Аналізуючи ці інциденти та розуміючи мотиви різних опонентів і улюблені TTP, ми зможемо краще запобігти подібним порушенням у майбутньому». ***(5 Attack Trends Organizations of All Sizes Should Be Monitoring // Informa PLC (https://www.darkreading.com/threat-intelligence/5-attack-trends-organizations-of-all-sizes-should-be-monitoring?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 26.04.2024).***

***

Сполучені Штати Америки

«…Згідно з останніми даними, наданими CyberNut, програмою підвищення обізнаності про безпеку, розробленою для шкіл, існують певні штати, жителі яких частіше стають жертвами кіберзлочинців. Ця інформація

проливає світло на регіони, які є гарячими точками цифрових загроз, і пропонує вказівки щодо того, як ми можемо зміцнити наш захист. Отже, давайте дослідимо, які штати очолюють список ризиків кіберзлочинності, і дізнаємось, які кроки ми можемо вжити, щоб захистити себе

10. Вашингтон

Початком нашого списку є штат Evergreen із 13 903 зареєстрованими жертвами та понад 157 мільйонів доларів загальних збитків. Хоча Вашингтон може бути відомий своїми технологічними гігантами та інноваціями, кіберзлочинці, здається, звертають на це увагу. З огляду на його місце в першій десятці списку, стає очевидним, що жителі Вашингтона повинні залишатися пильними в Інтернеті.

9. Вірджинія

Далі йде Вірджинія з 11 785 жертвами та майже 173 мільйонами доларів збитків. Мабуть, не дивно, що Старий Домініон є мішенню для кіберзлочинців, де розташована значна кількість державних установ і оборонних підрядників. Жителі Вірджинії повинні бути дуже обережними щодо захисту своїх цифрових активів.

8. Мічиган

На восьмому місці у нас Мічиган, де зареєстровано 10 930 жертв і загальні втрати понад 181 мільйон доларів. Штат Великих озер може бути відомий своєю автомобільною промисловістю, але, здається, кіберзлочинці також проявляють інтерес. Жителі Мічіганду повинні переконатися, що їх безпека в Інтернеті на належному рівні.

7. Іллінойс

Іллінойс посідає сьоме щасливе місце з 17 999 жертвами та майже 185 мільйонами доларів збитків. Як головний центр фінансів, технологій і транспорту, цілком зрозуміло, чому штат Прерія може бути головною ціллю. Жителі штату Іллінойс повинні активно захищати себе в Інтернеті.

6. Нью-Джерсі

Garden State посідає шосте місце в нашому списку з 12 817 зареєстрованими жертвами та понад 203 мільйонами доларів загальних збитків. Близькість Нью-Джерсі до великих мегаполісів і його процвітаюча фармацевтична промисловість

можуть зробити його привабливою мішенню для кіберзлочинців. Жителі Нью-Джерсі повинні вжити заходів для захисту свого цифрового життя.

5. Пенсільванія

Замикає першу п’ятірку Пенсільванія з 17 262 жертвами та майже 207 мільйонами доларів збитків. Різноманітна економіка штату Кістоун і велика кількість населення можуть зробити його спокусливою мішенню для онлайн-злочинців. Жителі Пенсільванії повинні надавати пріоритет кібербезпеці у своєму повсякденному житті.

4. Флорида

Сонячний штат посідає четверте місце з приголомшливими 45 855 зареєстрованими жертвами та понад 528 мільйонів доларів загальних збитків. Велика кількість населення Флориди, процвітаюча індустрія туризму та висока концентрація пенсіонерів можуть сприяти її привабливості для кіберзлочинців. Жителі Флориди повинні бути особливо пильними щодо захисту себе в Інтернеті.

3. Нью-Йорк

Бронзову медаль отримав Нью-Йорк з 29 065 жертвами та майже 560 мільйонами доларів збитків. Оскільки Емпайр-Стейт є глобальним фінансовим центром і центром торгівлі, не дивно, що Емпайр-Стейт є головною мішенню для кіберзлочинців. Посівши одне з перших місць у списку, жителі Нью-Йорка повинні зробити кібербезпеку головним пріоритетом.

2. Техас

Штат «Самотня зірка» посідає друге місце з 41 148 зареєстрованими жертвами та загальними збитками понад 606 мільйонів доларів. Велике населення Техасу, економіка, що розвивається, і все більша залежність від технологій можуть зробити його привабливою мішенню для кіберзлочинців. Жителі Техасу повинні бути пильними та активними, коли йдеться про безпеку в Інтернеті.

1. Каліфорнія

Очолює список штатів, які піддаються найбільшому ризику кіберзлочинності, не що інше, як Каліфорнія. З приголомшливими 67 095 жертвами та збитками понад 1,2 мільярда доларів Голден-Стейт є головною мішенню для онлайн-

злочинців. Процвітаюча технологічна індустрія Каліфорнії, велике населення та висока концентрація багатства можуть сприяти її привабливості. Каліфорнійці повинні бути особливо пильними щодо захисту свого цифрового життя…» ***(Michelle Harler. The Top 10 US States Most At Risk From Cybercrime // Guide2Free (https://www.guide2free.com/interesting/us-states-most-at-risk-from-cybercrime/?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 08.04.2024).***

***

«Компанія Microsoft опинилася під пильною увагою та гострою критикою у 34-сторінковому звіті, опублікованому у вівторок Радою з огляду кібербезпеки (CSRB) - групою, створеною міністром внутрішньої безпеки США у 2021 році для аналізу великих інцидентів у сфері кібербезпеки.

У звіті йдеться про резонансний інцидент у травні та червні 2023 року, коли китайська хакерська група, відома як Storm-0558, ймовірно, скомпрометувала поштові скриньки Microsoft Exchange Online понад 500 людей і 22 організацій по всьому світу, включаючи високопоставлених урядовців США.

У звіті CSRB критикується культура безпеки корпорації Майкрософт, описується як «неадекватна» і вказується, що вона «вимагає капітального перегляду, особливо в світлі центральної ролі компанії в технологічній екосистемі та рівня довіри клієнтів до компанії для захисту своїх даних і операцій».

У звіті також критикуються публічні повідомлення Microsoft, зазначається, що компанія чекала минулого місяця, щоб виправити публікацію в блозі від вересня 2023 року про першопричину порушення після повторних запитань правління.

На завершення перевірки CSRB, як сказано у звіті, Microsoft все ще не знала, як саме Storm-0558 отримала критичний ключ підпису 2016 Microsoft Services Account (MSA), який використовувався під час вторгнення 2023 року.

Одного разу у звіті йдеться, що керівникам Microsoft необхідно розглянути можливість переорієнтації розробки продукту, віддаючи перевагу функціям

безпеки над новими функціями продукту, ефективно відроджуючи дух ініціативи «Надійні обчислення», яку співзасновник Microsoft Білл Гейтс започаткував у 2002 році.

У звіті CSRB, зокрема, йдеться:

«Правління дійшло висновку, що Microsoft відійшла від цього духу і має негайно відновити його як головний корпоративний пріоритет. Правлінню відомо про нещодавні зміни Microsoft у керівництві безпеки та «Ініціативу безпечного майбутнього», про яку вона оголосила в листопаді 2023 року. Правління вважає, що ці та інші заходи, пов'язані з безпекою, мають безпосередньо й уважно контролювати генеральний директор Microsoft та її рада. директорів, і що всі старші керівники повинні нести відповідальність за впровадження всіх необхідних змін у терміновому порядку».

Відповідаючи на прохання прокоментувати звіт, представник Microsoft зробив таку заяву:

«Ми цінуємо роботу CSRB з дослідження впливу добре забезпечених ресурсами суб'єктів загрози національній державі, які діють безперервно та без значущого стримування. Як ми оголосили в нашій ініціативі Secure Future Initiative, нещодавні події продемонстрували необхідність запровадження нової культури інженерної безпеки у наших власних мережах. Хоча жодна організація не застрахована від кібератак з боку зловмисників із достатньою кількістю ресурсів, ми мобілізували наші команди інженерів для виявлення та пом'якшення застарілої інфраструктури, покращення процесів і впровадження тестів безпеки. Наші інженери безпеки продовжують захищати всі наші системи від атак і встановлюють ще більш надійні датчики та журнали, щоб допомогти нам виявляти та відбивати кіберармії наших ворогів».

У заяві додається, що Microsoft «також перегляне остаточний звіт для додаткових рекомендацій». ***(Todd Bishop. Cyber Safety Review Board finds Microsoft security culture 'inadequate,' calls for accountability // GeekWire, LLC (https://www.geekwire.com/2024/cyber-safety-review-board-finds-microsoft-security-culture-inadequate-calls-for-internal-accountability/). 02.04.2024).***

***

«Міністерство охорони здоров’я та соціальних служб США (HHS), Управління з громадянських прав (OCR) нещодавно опублікувало резюме (звіт), у якому викладено ключові дії щодо забезпечення виконання Закону про перенесення та підзвітність медичного страхування (HIPAA) у 2022 році, пов’язані з порушеннями незахищених захищених інформація про здоров'я (PHI). OCR отримав загалом 626 повідомлень про порушення, які стосуються 500 або більше осіб, що на 3% більше, ніж у 2021 році. Ці порушення вплинули на приблизно 41,7 мільйона осіб і були здебільшого спричинені хакерськими атаками та іншими кібератаками. Крім того, OCR розглянуло 63 966 повідомлень про дрібніші порушення, що стосуються менше ніж 500 осіб, головним чином через несанкціонований доступ або розголошення.

Вплив і правозастосування

OCR розпочав розслідування всіх значних порушень, а також деяких менших порушень, розпочавши загалом 799 розслідувань. Ці розслідування були завершені шляхом надання технічної допомоги, добровільного виконання зобов’язань шляхом коригувальних дій, угод про врегулювання та планів коригувальних дій. Угоди про врегулювання, як правило, зарезервовані для висновків OCR про невідповідність через навмисне недбалість або іншу поважну причину, яка вимагає додаткових примусових заходів. Примітно, що три розслідування порушень OCR були завершені за допомогою угод про вирішення проблеми та грошових виплат на загальну суму 2 425 640 доларів США.

У Звіті наголошується на необхідності для регульованих організацій посилити дотримання норм HIPAA, особливо щодо стандартів Правил безпеки, пов’язаних з аналізом ризиків, управлінням і контролем аудиту. Хакерські інциденти були виділені як головна причина великих порушень, на них припадало 74% випадків у 2022 році, і вони торкнулися найбільше людей. Навпаки, порушення, які стосуються менше ніж 500 або більше осіб, були спричинені

головним чином несанкціонованим доступом або розголошенням і в основному вплинули на паперові записи, а не на мережеві сервери.

Рекомендації та дії

У системі охорони здоров'я існує високий ризик витоку даних, і цей ризик продовжує зростати, оскільки хакери стають все більш досвідченими, а системи охорони здоров'я продовжують оцифровувати та зберігати в електронному вигляді конфіденційні дані пацієнтів. Недавній збій Change Healthcare продемонстрував серйозні фінансові наслідки кібератаки. Однак ціна невідповідності не обов'язково обмежується фінансовою шкодою. Шкода репутації через погану інфраструктуру безпеки даних може стати надто серйозною для деяких установ охорони здоров'я. Крім того, збій Change Healthcare показав, що кібератаки також можуть негативно вплинути на безпеку пацієнтів і результати медичної допомоги через значні збої в своєчасному наданні медичних послуг. У зв'язку з цим законодавчо вживаються заходи щодо заохочення дотримання постачальниками медичних послуг стандартів кібербезпеки шляхом прив'язки виплат за федеральними програмами охорони здоров'я до постачальників медичних послуг, які відповідають таким стандартам кібербезпеки.

Щоб вирішити ці проблеми, ми рекомендуємо всім організаціям, які регулюються HIPAA, розглянути наступні 10 основних рекомендацій щодо зменшення ризику витоку даних і покращення захисту від кібератак:

Аналіз ризиків і їх пом'якшення: проведіть ретельний аналіз ризиків, щоб виявити й пом'якшити потенційні вразливості системи безпеки, включаючи впровадження надійних методів управління ризиками для запобігання несанкціонованому доступу або розголошенню.

Оцініть потреби в кіберстрахуванні. Придбайте поліс кіберстрахування, який відповідає рівню складності вашої компанії, з мінімальними лімітами покриття щонайменше один мільйон у сукупності для менших організацій і щонайменше п'ять мільйонів для великих організацій.

Реагування на інциденти безпеки: регулярно перевіряйте діяльність системи, щоб швидко виявляти інциденти безпеки та реагувати на них.

Моніторинг і запис. Покращуйте контроль аудиту, щоб ефективно контролювати та записувати події, пов’язані з безпекою.

Реагування та звітування: посиліть механізми реагування та звітування для ефективного усунення порушень безпеки.

Процес автентифікації користувача: вдосконалення процесів автентифікації для перевірки ідентичності осіб або організацій, які мають доступ до захищеної медичної інформації.

Шифрування та захищений зв’язок: шифруйте конфіденційні дані, щоб зробити їх непридатними для використання, читання або розшифровки для неавторизованих осіб.

Мінімально необхідні дані: Забезпечте належне знищення захищеної медичної інформації, коли вона більше не потрібна, і завжди використовуйте мінімально необхідні дані для досягнення цілей.

Навчання та навчання: ознайомте працівників і ділових партнерів з їхніми зобов’язаннями згідно з HIPAA та важливістю захисту інформації про здоров’я.

Культура відповідності: сприяйте розвитку культури відповідності та безпеки в організації, щоб запобігти порушенням і забезпечити максимально можливий захист PHI.

Реалізація цих рекомендацій може допомогти регульованим організаціям не лише виконувати вимоги HIPAA та HITECH Act, але й посилити захист PHI та зменшити ризик потенційних юридичних, фінансових і репутаційних наслідків». ***(Kathrin “Kat” Zaki, Christina Hultsch and W. Clifford Mull. Annual Report to Congress on Breaches of Unsecured Protected Health Information // Benesch (https://www.beneschlaw.com/resources/annual-report-to-congress-on-breaches-of-unsecured-protected-health-information.html). 03.04.2024).***

***

«Оскільки британські університети все більше покладаються на технології для здійснення своїх операцій, загроза кібератак зростає. З появою досвідчених кіберзлочинців і зростаючою цінністю досліджень і особистих

даних питання вже не в тому, чи станеться кіберзлом, а в тому, коли. Наталі Джейкобі-Данеш, партнер, і Хізер Маккей, старший юрист юридичної фірми Browne Jacobson у Великій Британії та Ірландії, досліджують проблеми, з якими стикаються університети, реагуючи на кіберзагрози.

Університети повинні займати проактивну позицію щодо передбачення кібератак і впровадження комплексних заходів кібербезпеки для захисту від них. Прислів'я «нездатність підготуватися — це готуйся до провалу» актуальна зараз як ніколи, і університети Великої Британії повинні бути готові до прямого протистояння виклику кіберзагроз.

Вони стикаються зі все складнішими кіберзагрозами, оскільки кіберзлочинці та суб'єкти загроз стають все більш витонченими у своїй тактиці, а геополітичні гравці можуть шукати нові цілі.

Кіберзагрози можуть спричинити значні збої в роботі університету, а також завдати значної шкоди, зокрема витоку даних, фінансових втрат і репутаційної шкоди.

У цій статті ми досліджуємо, які кроки можуть вжити університети Великобританії для захисту від цих загроз, досліджуючи, як модель життєвого циклу відповідності може відігравати ключову роль у підготовці до інцидентів та управлінні ними. Використовуючи ці кроки, вони можуть зменшити ризик кібератак і захистити конфіденційні дані, які вони зберігають.

Типи кіберзагроз в університетах Великобританії

Університети Великобританії стикаються з різноманітними кіберзагрозами, включаючи фішингові атаки, зловмисне програмне забезпечення, програми-вимагачі та розподілені атаки на відмову в обслуговуванні (DDoS).

Дійсно, кіберзлочинці стали більш витонченими у своїй тактиці, відійшовши від використання лише одного типу атак до комбінування кількох тактик. Наприклад, зловмисники можуть використовувати програми-вимагачі для шифрування даних університету, а потім погрожувати оприлюднити конфіденційну інформацію в темній мережі, якщо викуп не буде сплачено.

Цей тип атаки може паралізувати дослідження та інші операції університету, спричиняючи значні фінансові збитки, зокрема фінансові збитки та репутаційні збитки. У зв'язку з цим університети повинні бути пильними у своїх зусиллях щодо кібербезпеки та впроваджувати комплексну програму кібербезпеки, яка включає навчання співробітників, заходи IT-безпеки та регулярне резервне копіювання критично важливих даних.

Вживаючи цих заходів, університети можуть зменшити ризик стати жертвою таких типів атак і захистити конфіденційні дані, які вони зберігають.

Фішингові атаки є одним із найпоширеніших видів кіберзагроз. Вони включають використання шахрайських електронних листів або посилань на веб-сайти, щоб обманом змусити користувачів надати конфіденційну інформацію, таку як облікові дані для входу або фінансову інформацію.

Зловмисне програмне забезпечення – ще один поширений тип кіберзагроз, який може заразити комп'ютерні системи університету та викрасти конфіденційну інформацію. Програми-вимагачі – це різновид шкідливих програм, які шифрують дані університету та вимагають плату в обмін на ключ розшифровки. DDoS-атаки передбачають перевантаження комп'ютерних систем університету трафіком, що робить їх недоступними для користувачів.

Приклади кібератак на університети Великобританії

У 2020 році Blackbaud Hack став жертвою кібератаки понад 20 університетів і благодійних організацій у Великобританії та за кордоном. Це скомпрометувало постачальника програмного забезпечення для адміністрування освіти, збору коштів і фінансового менеджменту, використовуючи дані, зокрема особисту інформацію.

Інший орган державного сектору, Британська бібліотека, був об'єктом атаки в жовтні 2023 року, яка призвела до вилучення та публікації в темній мережі близько 600 ГБ файлів, включно з особистими даними користувачів і співробітників бібліотеки. Викупу не платили. У березні 2024 року звіт Британська бібліотека опублікувала дуже інформативний, який ми настійно рекомендуємо університетам.

По всьому каналу повідомлялося, що Маастрихтський університет заплатив викуп у розмірі майже 200 000 євро, щоб відновити доступ до своїх комп'ютерних систем після кібератаки в 2019 році.

Позиція влади Великої Британії полягає в тому, що кіберзлочинцям не будуть виплачуватися викупи.

Стратегії запобігання та пом'якшення

Для захисту від кіберзагроз університети Великої Британії можуть впроваджувати різноманітні стратегії запобігання та пом'якшення наслідків. Навчання та обізнаність співробітників є критично важливими компонентами будь-якої програми кібербезпеки.

Університети повинні проводити регулярні тренінги для співробітників щодо того, як виявляти та уникати фішингових атак, як створювати надійні паролі та як повідомляти про підозрілу активність. IT-відділи також повинні впровадити заходи безпеки, такі як брандмауери, антивірусне програмне забезпечення та системи виявлення вторгнень. Необхідно регулярно створювати резервні копії критично важливих даних, щоб забезпечити можливість відновлення даних у разі атаки програм-вимагачів.

Життєвий цикл відповідності

Життєвий цикл комплаєнсу складається з трьох етапів, включаючи підготовку, управління інцидентами та вивчення уроків.

1. Підготовчий етап

Це передбачає передбачення кіберінциденту або витоку даних, впровадження політик і процедур, а також визначення групи реагування, яка діятиме негайно у разі інциденту.

2. Управління інцидентами

Після виявлення інциденту або потенційного інциденту запускаються процеси реагування. Про інцидент слід повідомити Національний центр кібербезпеки. Центр працює 24 години на добу і може надати університетам консультації та рекомендації у разі нападу.

Він тісно співпрацює з партнерами з правоохоронних органів Великої Британії, включаючи Національне агентство боротьби зі злочинністю, щоб забезпечити спільне реагування, а також може допомогти координувати міжурядове реагування, якщо це необхідно. Якщо підготовчий етап реалізовано добре, етап управління інцидентами має бути схожим на добре змащену машину, яка починає працювати.

Команда реагування мобілізується з різними підгрупами, які починають свою роботу, включаючи IT-безпеку, юридичну, нормативно-правову відповідність, фінанси та PR. Зрозуміло, що це стресовий і критичний етап, тому хороша підготовка є ключовою.

3. Розучування уроків

Нарешті, коли інцидент було локалізовано та виправлено, звіти повинні бути написані та перероблені, що веде до третього етапу життєвого циклу відповідності, витягуючи уроки. Цей етап повертається до етапу підготовки, що дозволяє університету повернутися до звичайної роботи з покращеними заходами кібербезпеки.

Правові наслідки кібератак в університетах Великобританії

Кібератаки на університети Великобританії можуть мати значні та широкомасштабні правові наслідки залежно від характеру та масштабу атаки та її впливу на роботу університету. Можливі наслідки:

Персональні дані: Університети мають юридичне зобов’язання захищати особисту інформацію своїх студентів і співробітників відповідно до Загального регламенту захисту даних Великобританії (GDPR). У разі витоку даних університети можуть бути притягнуті до відповідальності за збитки та зазнати судових позовів. Крім того, університети мають етичне зобов’язання захищати конфіденційність своїх студентів і співробітників. Кібератаки, які порушують конфіденційні дані, можуть завдати значної шкоди особам, у тому числі викрадення особистих даних і фінансові втрати. Університети повинні розглядати будь-які скарги студентів щодо впливу кібератаки на їх конфіденційність і особисті дані відповідно до своєї процедури розгляду скарг. Якщо значна кількість студентів

скаржиться на один і той самий інцидент, університети повинні розглядати їх як групову скаргу.

Порушення студентського контракту: атака може поставити під загрозу освіту, що надається студентам, наприклад, якщо викладання не може продовжуватися за планом або якщо дослідницький проект не може бути завершений за призначенням. Щоб уникнути скарг студентів, університет повинен уважно впоратися з будь-якими перешкодами в роботі студентів. Університети повинні розглядати будь-які скарги студентів щодо впливу кібератаки на їхнє навчання чи наукові дослідження відповідно до процедури розгляду скарг. Якщо значна кількість студентів скаржиться на один і той самий інцидент, університети повинні розглядати їх як групову скаргу.

Порушення угод про співпрацю: Університет може бути позбавлений можливості виконувати свої зобов'язання за угодами про співпрацю з академічними чи галузевими партнерами, і йому доведеться максимально пом'якшити негативні наслідки для себе та своїх партнерів. Зміни до контракту можуть бути узгоджені в короткий термін, щоб уникнути відповідальності за порушення контракту.

Порушення умов фінансування: збій, спричинений атакою, може перешкодити університету виконати умови грантового фінансування (наприклад, унеможливлюючи завершення певних проектів у запропоновані терміни). До спонсорів може знадобитися зв'язатися на конфіденційній основі, у короткий термін, щоб узгодити виняткові продовження або зміни умов фінансування.

Регуляторні наслідки: про загрозу або реальну атаку, можливо, потрібно буде повідомити регуляторним органам університету, включно з Офісом для студентів як про «подію, про яку можна повідомити», та/або в Офіс уповноваженого з інформації. Національний центр кібербезпеки не зв'язуватиметься з регуляторними органами університету.

Наслідки для національної безпеки: запровадження Закону про національну безпеку та інвестиції 2021 року підкреслило необхідність для університетів краще зрозуміти, чи належить їх дослідницька діяльність до чутливих сфер економіки, які

становлять інтерес для національної безпеки. Якщо кібератака може призвести до того, що третя сторона отримає доступ або контроль над будь-якими активами чи правами інтелектуальної власності в цих областях, органи влади будуть особливо зацікавлені у вирішенні загрози. У першу чергу слід повідомити Національний центр кібербезпеки. Потім за потреби залучатимуть інші відповідні правоохоронні органи.

Наші топ-10 порад для університетів

1. Ознайомитися з Національним центром кібербезпеки

Він розміщує на своєму веб-сайті велику кількість безкоштовних порад і вказівок, які університети можуть використовувати як частину своєї навчальної та підготовки. Центр також пропонує безкоштовну службу раннього сповіщення про загрози, яка може допомогти попередити університет про потенційно підозрілу активність у їхніх мережах. Крім того, він може підтримати жертв атак, за потреби ідентифікуючи спеціалістів із питань кібербезпеки.

2. Залучайтеся до життєвого циклу відповідності

Керівний орган університету повинен взяти на себе відповідальність за участь у життєвому циклі відповідності, і, зокрема, підготовчому етапі. Організація повинна розуміти силу та обмеження своїх IT-систем, різноманітність загроз, яким вона може наражатися, та їхній потенційний вплив на її діяльність.

Ці знання не повинні обмежуватися IT-фахівцями, а розглядатися на стратегічному рівні. Під наглядом керівного органу повинна працювати виконавча група, до складу якої входять представники всіх основних центральних служб університету (включаючи IT, HR, фінанси, комплаєнс і ризики, внутрішні та зовнішні комунікації, студентську, регуляторну та юридичну команди). збираються, щоб бути доступними в дуже короткий термін, щоб мати справу з будь-яким фактичним або загрозливим нападом. З цією групою управління інцидентами має бути зв’язок у будь-який час.

3. Прийміть протоколи, які автоматично запрацюють, коли університет зазнає атаки

Це має включати попередньо узгоджені лінії зв’язку зі студентами, співробітниками та третіми сторонами. У разі витоку даних або збою в роботі університету спілкування з персоналом і студентами має ключове значення для врегулювання інциденту та максимального заспокоєння людей, не надаючи надмірного розголосу суб’єктам загрози.

4. Поговоріть зі своїми страховиками заздалегідь

У разі атаки може знадобитися зв’язатися зі страховими компаніями, і вони матимуть власні протоколи. Чим краще ви розумієте їхній підхід, тим краще вони зможуть підтримати вашу групу реагування у разі кризи.

5. Поговоріть зі своїми юристами заздалегідь

Ознайомтеся з послугами підтримки в кризових ситуаціях, які ваші юридичні консультанти можуть надати вам у стислі терміни, як-от допомога у внесенні змін до контракту, зв’язок із регуляторними органами, допомога у спілкуванні з персоналом і студентами та підвищення потенціалу юридичної команди в стислі терміни. Переконайтеся, що ви знаєте, до кого звертатися, коли заклад зазнає атаки.

6. Оновіть свою політику

Переконайтеся, що ваша внутрішня політика, правила, довідники та протоколи відповідають вашим заходам з підготовки до врегулювання кризових ситуацій, і щоб вони були доведені до відома вашого персоналу та студентів.

7. Перегляньте свої контракти

Подібно до того, як Covid-19 спричинив перегляд і (де це можливо) переробку статей про форс-мажор і відповідальність, ми б порадили університетам розглянути питання про необхідність перегляду поточних або шаблонних положень контракту, щоб обмежити потенційну відповідальність університету в разі порушення контракту через кібератаку.

Університети також повинні перевірити, що є суттєвою подією невиконання зобов’язань у будь-яких кредитних угодах з банками, оскільки положення про перехресне невиконання зобов’язань потенційно можуть спричинити зобов’язання щодо повернення за різними банківськими угодами. Якщо ви сумніваєтеся,

зверніться до юриста якомога раніше або спробуйте прояснити ситуацію зі своїми банкірами.

8. Пом'якшення практичного впливу потенційних атак

Хоча може бути важко «модернізувати» резервні копії на всіх існуючих системах університету, IT-інфраструктура будь-яких нових проектів повинна бути розроблена з резервними копіями, коли це можливо.

Наприклад, будь-які наукові проекти, які покладаються на збір зразків і даних, повинні бути розроблені, коли це можливо, таким чином, щоб дозволити реконструювати бази даних, якщо університет втратить доступ до первинної бази даних (наприклад, шляхом зберігання частин зразків або зразків). з третьою стороною, чиї системи безпеки безпосередньо не пов’язані з системами безпеки університету). Наслідки витрат можуть бути доведені до відома спонсорів гранту.

9. Тренуйте своїх людей

Більшості атак можна було б уникнути, якби всі особи в організації постійно дотримувалися всіх передових IT-практик і проходили навчання. Регулярно нагадуйте своєму персоналу та учням про важливість дотримання вимог і зробіть навчання обов’язковим. Переконайтеся, що співробітники та студенти обізнані про ваші зусилля на інституційному рівні, знають, до кого звертатися у разі загрози та як поводитися у разі нападу.

Наприклад, якщо персонал або студенти будуть заблоковані в особистих або дослідницьких базах даних і не зможуть провести своє дослідження чи завершити курсову роботу, існує ризик, що розчаровані члени персоналу або студенти можуть оприлюднити своє розчарування.

Вам би хотілося, щоб співробітники та студенти розуміли, що публічність – це кисень для вогню вимог викупу та грати на користь тих, хто загрожує. Ці повідомлення краще передавати на етапі підготовки, ніж у запалі атаки.

10. Оновіть свій реєстр ризиків

У світлі вищесказаного необхідно оновити документи з управління ризиками». ***(Nathalie Jacoby-Danesh and Heather McKay. Cyber-attacks in UK universities: Why failing to prepare is no longer an option // Browne Jacobson LLP***

(https://www.brownejacobson.com/insights/cyber-attacks-in-uk-universities-why-failing-to-prepare-is-no-longer-an-option). 02.04.2024).

***

«4 квітня 2024 року Агентство з кібербезпеки та безпеки інфраструктури («CISA») опублікувало для громадського обговорення довгоочікувану пропозицію про впровадження Закону про звітність про кіберінциденти для критичної інфраструктури 2022 року («CIRCIA»). Закон CIRCIA був підписаний 15 березня 2022 року і вимагає від охоплених організацій повідомляти про «значні» кіберінциденти протягом 72 годин, а про платежі програм-вимагачів — протягом 24 годин. Згідно з новим законом, на охоплених суб'єктів також поширюються додаткові вимоги щодо звітності та зобов'язання щодо збереження даних.

За оцінками CISA, це правило коштуватиме державному та приватному секторам понад 2,6 мільярда доларів США до 2033 року, і за цей час очікується отримання понад 200 000 звітів від понад 316 000 організацій. CISA також передбачає виділення значних ресурсів для реалізації правила, подавши бюджетний запит на 116 мільйонів доларів додаткового фінансування для реалізації нової програми, яка вимагатиме «суттєвих технологічних удосконалень» і додаткових 122 штатних працівників.

Суб'єкти, на які поширюється дія

Запропоноване правило широко визначає «суб'єкт, на який поширюється дія»: (1) будь-яку організацію, що входить до одного з 16 «секторів критичної інфраструктури», які охоплюють безліч галузей, від критичного виробництва до фінансових послуг і (2) або перевищує порогові значення Асоціації малого бізнесу США, або, незалежно від розміру, на нього поширюються спеціально перелічені критерії, пов'язані з певними критичними секторами інфраструктури.

Перелік секторів критичної інфраструктури широкий, і достатньо бути «активним учасником» у цьому секторі. Наприклад, CISA зазначає, що сектор комерційних об'єктів включає «поєднання організацій, таких як 1,1 мільйона торговельних центрів країни, торговельних центрів та інших роздрібних установ;

понад 52 000 готелів; майже 1400 казино та пов’язаних із ними курортів; 1 млн офісних будівель; 5,6 мільйона багатоквартирних будинків, що орендуються, і майже 125 000 закладів, призначених для публічних зібрань, таких як стадіони, арени, кінотеатри, музеї, зоопарки, бібліотеки та інші майданчики для виступів».

За даними CISA, рекламні фірми, юридичні фірми, політичні партії, фірми графічного дизайну, аналітичні центри та групи громадських інтересів можуть не належати до секторів критичної інфраструктури.

Суб’єкт господарювання відповідає пороговому значенню розміру, якщо він перевищує стандарт розміру малого бізнесу Адміністрації малого бізнесу США на основі кількості працівників або річного доходу, залежно від галузі. Для відповідних порогових значень див. 13 CFR pt. 121. Крім того, існують спеціальні галузеві критерії, за якими певні малі підприємства підпадають під вимоги CIRCIA щодо звітності.

Значні кіберінциденти

CIRCIA обмежує зобов’язання повідомляти лише про «значні» кіберінциденти. Запропоноване правило визначає значний кіберінцидент як будь-яку з наступних чотирьох ситуацій:

Значна втрата конфіденційності, цілісності або доступності інформаційної системи чи мережі суб’єкта, на який поширюється дія.

Серйозний вплив на безпеку та відмовостійкість операційних систем і процесів охопленої організації.

Порушення здатності охопленої організації брати участь у комерційній чи промисловій діяльності або постачати товари чи послуги.

Несанкціонований доступ до інформаційної системи чи мережі суб’єкта, на який поширюється дія, або будь-якої закритої інформації, яка в них міститься, що здійснюється через або викликано компрометацією постачальника хмарних послуг, постачальника керованих послуг або іншого стороннього постачальника даних.

Згідно з цими визначеннями, суб’єкти, на які поширюється дія, повинні розглянути, чи є кіберінцидент достатньо серйозним або істотним, щоб ініціювати

вимоги звітування. Як обговорюється нижче, заниження звітності може призвести до застосування різноманітних санкцій.

Інформація, яку потрібно повідомити

У звітах має бути описано кібер-інцидент або атаку програм-вимагачів, зокрема такі деталі, як функціонування постраждалих мереж, тактика, використана для скоєння інциденту, підозрюваний винуватець і будь-які заходи пом'якшення, вжиті у відповідь на інцидент.

Винятки з вимог до звітності

Є кілька винятків із вимог звітності CIRCIA.

Підприємству не потрібно звітувати до CISA, якщо від нього вже вимагається повідомляти суттєво схожу інформацію за суттєво подібний графік іншому федеральному агентству — і це агентство має затверджену угоду про обмін інформацією з CISA.

Підприємству не потрібно подавати два окремі звіти, якщо він зазнав значного кіберінциденту, що супроводжувався вимогою викупу. У цій ситуації він може подати комбінований звіт.

Вимоги до звітності не застосовуються до організацій або певних функцій організацій, якими володіють, керують або керують організації з багатьма зацікавленими сторонами, які розробляють, впроваджують і забезпечують дотримання політики щодо системи доменних імен (DNS).

Вимоги щодо звітності не застосовуються до федеральних агентств, якщо вони вже зобов'язані повідомляти про інцидент CISA відповідно до Федерального закону про модернізацію інформаційної безпеки 2014 року (FISMA).

Графіки звітування

Звіти про значні кіберінциденти мають бути надані не пізніше ніж через 72 години після того, як організація «обґрунтовано вважає», що стався охоплений інцидент, а звіти про платежі програм-вимагачів — не пізніше ніж через 24 години після виплати платежу.

Цей суворий графік означає, що суб'єкти, ймовірно, повинні будуть звітувати про інциденти, які все ще розслідуються, тоді як розуміння інциденту суб'єктом є неповним і розвивається.

І CISA чітко розуміє, що наявність неповної інформації не є виправданням для запізнілого звіту. Навпаки, організація, яка обґрунтовано вважає, що стався охоплений інцидент, повинна повідомити про це, а згодом повинна «негайно» подати додатковий звіт із будь-якою нововиявленою інформацією.

Вимоги до збереження даних

Окрім вимог до звітності, запропоноване правило також створює зобов'язання щодо збереження даних і записів протягом принаймні двох років, що стосуються масиву технічної інформації та інформації про інциденти, зокрема: зв'язок суб'єктів загрози, індикатори компрометації, мережевий трафік, вектор атаки, судово-медичні звіти, криміналістичні зображення, журнали та інші елементи. Розглядаючи, як найкраще підготуватися до цих вимог, охоплені організації можуть забажати розглянути структуру своїх конкретних мереж та IT-систем, а також потенційні потреби у зберіганні даних.

Правовий захист повідомленої інформації

Правило містить кілька засобів захисту для подання звітів і відповідей на запити інформації (RFI) від CISA. До них належать:

Позначення як комерційної, фінансової та службової інформації;

Звільнення від розголошення відповідно до Закону про свободу інформації;

Захист від відмови від привілеїв або інший захист, передбачений законом;

Відмова від повідомлень ex parte;

Заборона на використання звітів або відповідей на RFI в регуляторних діях;

Захист від майбутньої відповідальності за подання звіту або відповідь на RFI; і

Обмеження на дозволене використання інформації CISA.

Штрафи за неподання звіту

Якщо CISA вважає, що організація не дотримується CIRCIA, вона може надіслати запит на інформацію та/або повістку в суд, а також має право передати

невідповідність Генеральному прокурору для примусового виконання. Організації, які не відповідають вимогам, також можуть зіткнутися зі штрафними санкціями за придбання, включаючи призупинення та позбавлення права.

Період коментарів

Організації, які вважають, що вони можуть зіткнутися із зобов'язаннями щодо відповідності згідно з CIRCIA, можуть забажати прокоментувати запропоноване правило. CISA прийматиме коментарі щодо запропонованого правила протягом 60 днів після його публікації — до 3 червня 2024 року.

Остаточне правило, швидше за все, не набуде чинності до початку 2026 року». ***(Sumon Dantiki, Alexander Davey. Department of Homeland Security Proposes Rule for Reporting of Cyber Incidents // King & Spalding LLP (https://www.kslaw.com/news-and-insights/department-of-homeland-security-proposes-rule-for-reporting-of-cyber-incidents). 18.04.2024).***

***

«Нещодавня атака програмного забезпечення-вимагача проти пивоварні Duvel Moortgat продемонструвала цілком реальний ризик, який становлять інциденти з кібербезпекою для алкогольної промисловості, як повідомляється, призупинивши роботу на кілька днів на чотирьох підприємствах Duvel Moortgat у Європі та Сполучених Штатах. Ця атака сталася після того, як за останні кілька років інші великі виробники алкоголю зазнали руйнівних атак програм-вимагачів. Подібні інциденти можуть бути руйнівними для бізнесу та репутації компанії, а стратегії хакерів постійно розвиваються, щоб максимізувати шкоду. Але компанії можуть бути готові за допомогою програми інформаційної безпеки, розробленої для запобігання успішним атакам і швидкого реагування на них. Досвідчені партнери, такі як McDermott, є критично важливими ресурсами протягом цього процесу, що дозволяє компаніям краще оновлювати та зміцнювати свої програми безпеки.

Зростаюча загроза нападу

Хакери десятиліттями вимагали від компаній за допомогою атак програм-вимагачів, але стратегії хакерів розвивалися, щоб підвищити ризики для компаній, що часто призводило до більшого викупу для хакера. Атака «програмне забезпечення-вимагач» традиційно відноситься до стратегії, за якої хакер отримує доступ до комп'ютерної системи жертви, шифрує інформацію в цих системах і вимагає платити викуп за розблокування цієї інформації. Жертви можуть спробувати уникнути сплати викупу, відновивши більшість своїх систем із резервних копій, але нещодавно хакери запровадили додаткові стратегії, які можуть ускладнити це відновлення. Сьогодні хакери часто намагаються викрасти інформацію жертви перед тим, як зашифрувати її в системі жертви, щоб вони могли продати або опублікувати інформацію, якщо жертва відмовиться платити викуп. Хакери також можуть спробувати «пошкодити» резервні копії, щоб жертва не змогла ефективно відновити свою систему без допомоги хакера. Одна група програм-вимагачів, AlphV, каже, що також повідомляє про своїх публічних жертв Комісії з цінних паперів і бірж США, якщо вони не платять викуп.

Вирішити, чи сплачувати викуп, – це складне рішення, будь-який вибір представляє значні ризики. Викуп, ймовірно, буде дорогим і його потрібно буде заплатити без жодних гарантій, що хакер виконає свої обіцянки. Програмне забезпечення для дешифрування чи ключ можуть не працювати, або хакер може не видалити інформацію. Вважається, що одна хакерська група, LockBit, зберігає інформацію жертв після сплати викупу, незважаючи на обіцянки видалити її. Хакер може бути готовий домовитися про меншу суму платежу, але це забирає дорогоцінний час, а системи жертви, ймовірно, залишаються нефункціональними. Хакер може перебувати під санкціями, і в цьому випадку сплата викупу буде незаконною та може призвести до штрафу для жертви. Виплата викупу винагороджує хакера, що може збільшити ризик того, що хакер знову націлиться на жертву. Рідко існує чіткий шлях назад у безпеку після успішного порушення, тому важливо, щоб жертва прийняла ефективне, обґрунтоване рішення.

Можливості для підготовки та профілактики

Компанії можуть мінімізувати ці ризики, підтримуючи програму безпеки, розроблену для запобігання виникненню інцидентів і ефективного реагування, якщо вони трапляються. Програма безпеки повинна використовувати адміністративні, технічні та фізичні політики та процедури безпеки, щоб дозволити персоналу виявляти фактичні або призупинені інциденти та повідомляти про них, агресивно контролювати системи компанії на наявність підозрілих файлів і поведінки та захищати об'єкти компанії від несанкціонованих вторгнень. Програму безпеки потрібно регулярно тестувати й оновлювати, щоб виявити слабкі місця, запровадити відповідні рішення щодо виявлення та реагування, а також спланувати розвиток стратегій хакерів і бізнес-вимог. Плани реагування на інциденти слід регулярно перевіряти, щоб переконатися, що вони точно відображають ресурси та пріоритети компанії, і що реагувальники готові виконати план у разі необхідності.

Компанії також повинні залучати сторонніх спеціалістів для підвищення ефективності підготовки та реагування. Ці партнери можуть надати конкретні знання та перспективи, щоб допомогти компанії належним чином спланувати інцидент, не потребуючи попереднього досвіду в інциденті. Наприклад, досвідчена юридична фірма, така як McDermott, може проконсультувати компанію щодо її юридичних зобов'язань, допомогти виявити й усунути ризики в програмі безпеки, а також розслідувати і реагувати на інцидент, захищаючи привілеї компанії. Скориставшись цією підтримкою на ранній стадії, компанія може знайти й усунути свої слабкі сторони, перш ніж їх використають, краще зрозуміти підходи інших компаній до цих проблем і переконатися, що її партнери узгоджуються з пріоритетами компанії. У разі інциденту ефективний сторонній партнер може ефективно проконсультувати потерпілих щодо їхніх зобов'язань, варіантів і ризиків; забезпечити додаткові ресурси для зайнятого колективу; і допомогти визначити пріоритети реагування на основі потреб бізнесу.

Висновок

Інциденти кібербезпеки можуть швидко стати дорогими, складними та руйнівними для жертв. Хакери постійно вдосконалюють свої методи отримання

більших викупів, і після того, як почався інцидент, жертва часто не має можливості переконатися, що вона може повністю усунути проблему. Компанії можуть обмежити свої ризики, запровадивши системи захисту від загроз і підготувавшись до реагування на будь-який інцидент. Компанії також повинні регулярно консультуватися із зовнішніми професіоналами, щоб оцінити та покращити свій захист і переконатися, що їхня програма безпеки не застаріла». ***(David Sorenson, Michael G. Morgan and Alva C. Mather. Preparing for Evolving Cybersecurity Threats // McDermott Will & Emery (https://www.alcohollawadvisor.com/2024/04/preparing-for-evolving-cybersecurity-threats/#page=1). 15.04.2024).***

***

«Чи захист від сучасного ризику кібератак є частиною належної обачності, яка очікується від старанного та розсудливого службовця та директора?

Чи можуть директори та керівництво компанії нести особисту відповідальність за атаку на кібербезпеку на їхній годині? Нещодавні звинувачення, висунуті Комісією з цінних паперів і бірж США («SEC») проти компанії та її колишнього директора з інформаційної безпеки («CISO»), припускають, що відповідь може бути «так».

У жовтні 2023 року SEC висунула цивільні звинувачення проти SolarWinds Corporation («SolarWinds»), американської компанії, що надає програмне забезпечення для керування IT-послугами, а також її колишнього керівника CISO за шахрайство та збої внутрішнього контролю, пов’язані з кібератакою 2020 року. Це перший випадок, коли SEC висунула звинувачення проти CISO компанії у зв’язку з інцидентом кібербезпеки. У своїй скарзі SEC стверджувала, що SolarWinds і CISO ввели в оману своїх інвесторів щодо практики компанії в галузі кібербезпеки, не розкрили відомі ризики та неадекватно врахували ці відомі ризики для запобігання та виявлення потенційної атаки. Публічне розкриття інформації та фактори ризику, зокрема ті, що містяться в проспектах емісії, фінансовій звітності, циркулярах з інформацією про керівництво, прес-релізах і річних інформаційних

формах, є, зрештою, відповідальністю Правління, створюючи потенційний вплив на низку позивачів, включаючи комісії, акціонерів та інших корпоративних зацікавлені сторони.

Зі свого боку, SolarWinds у відповідь назвала звинувачення «необґрунтованими» та «незрозумілими» та подала заяву про звільнення звинувачень.

Хоча позов SEC проти SolarWinds може бути значною мірою мотивований передбачуваним спотворенням компанією масштабів відомого конкретного кіберризику, результат справи може мати ширші наслідки: директори та посадові особи можуть нести відповідальність за несприятливі події кібербезпеки, якщо вони це зроблять не вживати адекватних заходів для зменшення ризику, особливо якщо вони намагаються зменшити відомий ризик.

Справа SolarWinds пов’язана з іншими рішеннями США, які, на думку спостерігачів, вплинуть на канадське законодавство, як-от In re McDonald's Corporation Derivative Litigation (про яке ми писали раніше – див. https://www.pallettvalo.com/whats-trending/why). -canadian-officers-and-boards-should-follow-aus-decision-on-an-officers-duty-of-oversight/), які продовжують розширювати фідуціарні та стандартні обов’язки з догляду для вищого керівництва та рад (враховуючи обов’язки директора, як правило, бути дуже схожими в обох юрисдикціях – зокрема відповідно до законів Канади, таких як Закон Канади про комерційні корпорації та Закон про комерційні корпорації (Онтаріо).

З постійно зростаючим ризиком кібератак стає все більш імовірним, що несприятливі події в кібербезпеці вплинуть на фінансові показники компанії, зокрема через значну репутаційну шкоду. Якщо буде виявлено, що директор або посадова особа не виконав своїх обов’язків щодо запобігання кібератаці, або, що є ще більш кричущим, спотворив позицію компанії щодо них, це реально може призвести до шкоди для корпорації, яка, у свою чергу, відкриває правління та старше керівництво. управління до низки регулятивних (наприклад, примусове виконання комісій) або відповідальності вторинного ринку (тобто групові позови акціонерів).

Незалежно від конкретного результату у справі SolarWinds, сам факт висунення звинувачень підкреслює необхідність для директорів і посадових осіб прислухатися до своїх статутних обов'язків з особливою пильністю. Хоча жоден канадський директор/посадова особа ще не був об'єктом примусового провадження, пов'язаного з кібербезпекою, справа SolarWinds показує, що це може бути не вічно». ***(Mujir A. Muneeruddin and Cassie Wasserman. Not Just a Cyber Attack: Evolving Issues for Director and Officer Liability in the US and Canada // Pallett Valo LLP (https://www.pallettvalo.com/whats-trending/not-just-a-cyber-attack-evolving-issues-for-director-and-officer-liability-in-the-us-and-canada/). 04.2024).***

***

«Технічні компанії повинні взяти на себе більшу відповідальність за розробку систем, які захищають дані користувачів, сказав високопоставлений чиновник з кібербезпеки Білого дому в Сан-Антоніо, де він також закликав студентів розглянути федеральні роботи в галузі.

Головним пріоритетом Національної стратегії кібербезпеки є зняття тягаря кібербезпеки з окремих осіб, заявив Джейк Браун, виконуючий обов'язки головного заступника національного кібердиректора, під час «Tech Fiesta» Texas A&M у Сан-Антоніо.

«Великі технологічні компанії, які фактично створюють всі наші технології, мають більше ресурсів для забезпечення кібербезпеки, ніж мій батько або 13-річні близнюки, які можуть стати єдиною точкою відмови, де, якщо вони натиснуть на неправильне посилання, раптом вся їхня особиста інформація буде скомпрометована», - сказав він.

Стратегія адміністрації також передбачає довгострокові інвестиції в галузь.

«Те, що ми робили протягом приблизно 40 років, — це вбудовування кібербезпеки в усі речі, які ми створили... і, як ми з'ясували, закріплення кібербезпеки на сервері — це не найефективніший спосіб забезпечення кібербезпеки», - сказав Браун.

Ця стратегія відповідає плану інвестицій президента Байдена в Америку, пакету витрат на 1,8 трильйона доларів, який складається з двопартійного закону про інфраструктуру, закону про мікросхеми та науку та закону про зниження інфляції. Як приклад, Браун сказав, що законодавство призвело до федеральних інвестицій у розмірі 20 мільйонів доларів для модернізації електромережі в Сан-Антоніо, зусилля, яке включає посилення кібербезпеки системи.

«Ми сподіваємось, що люди по всій країні, які працюють у кіберіндустрії, побачать, як реалізуються ці проекти, можливість для кіберпростору бути реалізованим», - сказав він. «Коли ви бачите, як розгортаються ці проекти ... у вашій громаді, ми сподіваємось, що ви звертаєтесь до людей, які виграють контракти на реалізацію цих програм ... і говорите: «Гей, як ми можемо допомогти вам взяти участь у цих програмах, щоб забезпечити кібербезпеку на початковому етапі?» і щоб ці інвестиції були захищені заздалегідь, а не так, що ми прийдемо і займатимемось кібербезпекою через 20 років після того, як всі ці проекти будуть побудовані».

Ключ до їхнього підходу — сильна робоча сила.

«Це чудово мати стратегію. Це чудово мати ресурси, — сказав Браун, — але ми не зможемо зробити нічого з цього, якщо у нас немає робочої сили, яка б фактично виконувала роботу з випікання кіберпространства на передньому кінці всіх ці проекти».

Його офіс нещодавно запустив «Спринт технічного найму» для працевлаштування у федеральних агентствах по всій країні, зокрема в Сан-Антоніо. Він сказав, що такий підхід спрощує процес для претендентів, «щоб вам не довелося писати 50 різних резюме для 50 різних агентств», додавши, що зараз у Техасі є 36 000 кібервакансій, у тому числі 4 500 у Сан-Антоніо.

Близько 100 людей відвідали захід у п'ятницю вдень.

Ведучим заходу був першокурсник Ейрік Маркес, який висловив надію, що це підвищить популярність програм TAMUSA з кібербезпеки.

«Ми намагаємося масштабувати наші програми», - сказав він. «Я відчуваю, що всі знають про UTSA, але ми також є однією зі шкіл у Сан-Антоніо, яка має ступінь бакалавра з кібербезпеки.

Чон Янг, директор університетського Центру інформаційних технологій та кібербезпеки, сказав, що візит Брауна допомагає підвищити популярність програми.

«Багато людей не знають про існування нашої програми, але я вважаю, що це переломний момент», - сказала вона». ***(Brandon Lingle. Cybersecurity Onus on Tech Firms, White House Official Says // e.Republic LLC (https://www.govtech.com/security/cybersecurity-onus-on-tech-firms-white-house-official-says). 23.04.2024).***

***

«Водний сектор перебуває під тиском, щоб покращити захист кібербезпеки через зростання загроз хакерів.

Агентство з охорони навколишнього середовища та Білий дім зустрілися з губернаторами минулого місяця та попросили їх скласти плани до 28 червня, пояснюючи, як вони планують боротися з основними ризиками кібербезпеки, з якими стикаються системи водопостачання та каналізації їхніх штатів.

Минулого тижня представники Рік Кроуфорд (R., Арканзас) і Джон Дуарте (R., Каліфорнія) запропонували законопроект, який передбачає створення керівного органу для розробки мандатів щодо кібербезпеки для систем водопостачання та роботи з EPA для забезпечення виконання нових правил.

Багатьом об’єктам водопостачання потрібна допомога у захисті своїх систем, оскільки вони не мають бюджету на інструменти чи персонал із кібербезпеки, сказав Кевін Морлі, менеджер із федеральних відносин Американської асоціації водопостачання. Торгова група була частиною судового процесу, який боровся з попередньою спробою EPA надати обов’язковий кіберзахист для систем водопостачання, заявивши, що вартість дотримання вимог буде недосяжною для багатьох об’єктів.

За його словами, не вистачає навчання базовим заходам кібербезпеки. «У нас є ті, хто має, і хто не має», — сказав Морлі.

За його словами, для комунальних служб модернізація старого обладнання може зайняти кілька років і коштувати мільйони доларів, що є великим навантаженням на багато муніципальних систем. Водопостачання та інші об’єкти критичної інфраструктури використовують спеціалізовані технології для промислових процесів, які, як правило, використовуються десятиліттями, і тому не мають сучасного захисту кібербезпеки.

Френк Урі, президент правління водного району Санта-Маргарита в південній Каліфорнії, сказав, що головне занепокоєння полягає в тому, що хакери бездіяльно лежать у системах водопостачання, але врешті-решт можуть почати скоординовану атаку, яка може вразити кілька територій одночасно. За його словами, у закладі в Санта-Маргариті немає головного спеціаліста з інформаційної безпеки, і він витрачає близько 15% свого технологічного бюджету на кібербезпеку.

«Більшість агентств не знають, що їх зламали», — сказав він. Урі також є старшим керівником клієнтської консалтингової фірми CAI, яка працює з водопровідними та іншими компаніями.

Хакери, часто включаючи групи політичних активістів, які зазвичай використовують методи кібератак низького рівня, частіше атакують об’єкти водопостачання та в багатьох випадках виявляють їх недостатньо захищеними, сказав Ліор Френкель, виконавчий директор і засновник Waterfall Security Solutions, компанії з кібербезпеки, яка фокусується на критичній інфраструктурі. Водоспад працює з кількома сотнями водних об'єктів у США

Представники кібербезпеки та правоохоронних органів США нещодавно попередили, що хакери, спонсоровані урядом Китаю, атакують водні об’єкти. У лютому Федеральне бюро розслідувань заявило, що порушило роботу китайських хакерів, які ховалися в американських водопровідних системах та іншій критичній інфраструктурі. За словами ФБР, деякі цифрові зловмисники ховалися

щонайменше п’ять років. Посольство Китаю у Вашингтоні не відповіло на запит про коментар.

хакери, націлені на об’єкти водопостачання та іншу інфраструктуру, готуються знищити або пошкодити їхні системи. Директор ФБР Крістофер Рей заявив у січні, що Експерти з водної безпеки попереджають, що хакери також можуть регулювати рівень хімічних речовин у воді або зупиняти потік води чи роботу систем водовідведення.

За словами головного спеціаліста з інформаційної безпеки Джейка Марголіса, Metropolitan Water District Південної Каліфорнії інвестує в технології, які забезпечують доступ співробітників до технологій і використання облікових даних для входу, щоб запобігти таким атакам, про які попереджало ФБР. Тим не менш, важко дізнатися, чи проникли хакери в технологічні системи, якщо вони довго чекають, перш ніж розпочати атаку, сказав він.

«Навіть якщо ви все робите правильно, цього все одно недостатньо», — сказав Марголіс.

Наприкінці минулого року Агентство з кібербезпеки та безпеки інфраструктури повідомило, що зловмисники, пов’язані з Іраном, атакували обладнання ізраїльського виробника Unitronics, яке використовувалося на водопровідному об’єкті США в Пенсільванії. Об’єкт відключив контролер, який постраждав. Міністерство закордонних справ Ірану не відповіло на запит про коментар.

EPA не випустило обов’язкових вимог щодо кібербезпеки для водного сектору. Минулого року агентство відкликало керівні принципи для систем водопостачання після того, як водопровідні компанії та штати подали позови, стверджуючи, що правила призведуть до високих витрат на об’єкти». ***(Catherine Stupp. Water Facilities Warned to Improve Cybersecurity as Nation-State Hackers Pounce // Dow Jones & Company, Inc. (https://www.wsj.com/articles/water-facilities-warned-to-improve-cybersecurity-as-nation-state-hackers-pounce-69ca8818?siteid=yhoof2&yptr=yahoo). 19.04.2024).***

***

«Раніше цього місяця адміністрація Байдена оголосила про виділення 20 мільярдів доларів США в рамках Закону про зниження інфляції для кліматичних і чистих енергетичних проектів по всій країні, які мають на меті скоротити або уникнути викидів до 40 мільйонів метричних тонн вуглецю щорічно протягом наступних семи років. Успіх цієї амбітної інвестиції залежить від важливого, хоча часто забутого фактора: кібербезпеки технологій чистої енергії, що лежать в основі цих проектів.

Критичні сектори, включаючи водопостачання, транспорт, охорону здоров'я, виробництво та зв'язок, уже давно є привабливою мішенню для загрозливих суб'єктів, які проникають у незахищені активи, безпосередньо підключені до загальнодоступного Інтернету, для здійснення атак програм-вимагачів або шпигунства національної держави. розвідувальним співтовариством Нещодавня щорічна оцінка загроз проливає нове світло на цю проблему, попереджаючи про те, що уряд Китаю завчасно займається критичною інфраструктурою США, щоб утримати Сполучені Штати від військового втручання в регіональний конфлікт.

Окрім цього ризику для великих критичних секторів, системи чистої енергії є значно більш розподіленими, ніж звичайні підходи до виробництва енергії. Останні масштабні інвестиції в енергетичну інфраструктуру нашої країни, від великих сонячних і вітряних електростанцій, які безпосередньо живлять основну енергосистему, до невеликих домашніх установок, підключених до муніципальної розподільчої мережі, збільшать площу атаки в цьому секторі, зробивши енергетичний сектор все більш привабливою мішенню для актори цифрової загрози. Впровадження кібербезпеки поряд із цими інвестиціями може створити або зламати майбутнє нашої країни з використанням чистої енергії.

Моделювання клімату, державна політика та інновації спричиняють масштабні та швидкі зміни в енергетичній мережі, і їх потрібно доповнювати політикою кібербезпеки.

Ми переживаємо період безпрецедентних змін в енергетичній системі США, частково зумовлених екологічною державною політикою. Моделювання клімату,

включно зі звітом Net Zero by 2050 і проектом REPEAT, зміцнює внутрішні та міжнародні зобов'язання щодо досягнення конкретних кліматичних і екологічних цілей і термінів.

Закон про інвестиції в інфраструктуру та робочі місця (IIJA) і Закон про зниження інфляції (IRA) разом забезпечують фінансування цих зусиль у розмірі 30 мільярдів доларів США, кардинально змінюючи стимули та інвестиції в чисту енергію, компенсуючи витрати та посилюючи впровадження як домашніми користувачами, так і комерційними підприємствами. А технологічні вдосконалення, які зробили сонячні панелі все доступнішими, прискорили розробку інтелектуальних лічильників і дозволили використовувати хмарні сервіси для балансування навантаження, покращують взаємозв'язок і впровадження цих технологій.

Однак у нещодавньому повідомленні Білого дому не згадується кібербезпека, і, за помітним винятком 350-мільйонної державної та місцевої програми кібербезпеки, IIJA та IRA мають кілька положень, які прямо дозволяють грантовим агентствам встановлювати вимоги кібербезпеки до проектів, що фінансуються в рамках них. Враховуючи тривожне середовище кіберзагроз, амбітна державна політика щодо інфраструктури повинна супроводжуватися такими ж амбітними політиками кібербезпеки та стійкості.

Оскільки енергетична мережа розвивається для забезпечення виробництва, передачі та розподілу чистої електроенергії, кібербезпека цих розподілених технологій має розвиватися разом з нею.

З точки зору управління, сектор електроенергетики змінюється повільно, а нагляд поширюється на федеральні агентства та регулятори штатів. Історичні перешкоди для модернізації мережі залишаються; процес отримання дозволів на створення нової інфраструктури, від вітрових електростанцій до високовольтних ліній електропередач, залишається складним і трудомістким, а будівництво великих інфраструктурних проектів є дорогим.

Ці бар'єри тільки посиляться із запровадженням технологій відновлюваної енергетики; ще більше зацікавлених сторін є частиною процесу, більше активів

потребують захисту, а інфраструктура є більш розподіленою, ніж будь-коли раніше, з виробництвом енергії не лише з великих заводів, але й із будинків і комерційних будівель, а деякі з них посередництво споживчого рівня Інтернету пристроїв речей (IoT).

Передбачаючи цю загрозу, кілька федеральних агентств звертають увагу на кібербезпеку Інтернету речей і технології розподіленої мережі. Нещодавнє ухвалення Федеральною комісією зі зв'язку Федеральної комісії зі зв'язку правила, що встановлює знак кібердовіри США, дозволить виробникам підключених споживчих пристроїв, таких як дверні камери та побутова техніка, продемонструвати відповідність набору стандартів безпеки. Крім того, Міністерство енергетики (DOE) заявило про свій намір розробити індивідуальні вимоги безпеки для інтелектуальних лічильників електроенергії та підключених інверторних систем.

Ці політичні ініціативи узгоджуються із загальним зрушенням уряду в бік зосередження уваги на кібербезпеці під час розробки та впровадження продукту, як-от зусилля Агентства з кібербезпеки та безпеки інфраструктури (CISA) щодо розробки технологій, які є «безпечними за дизайном», і подібна програма в Міністерстві освіти під назвою «кіберінформована інженерія». Подвоєння цих програм безпечної архітектури має вирішальне значення для того, щоб низка існуючих і майбутніх технологій відновлюваних джерел енергії не створювала подібних рівнів вразливості в енергетичній мережі нашої країни.

У довгостроковій перспективі енергетичний сектор потребує скоординованої довгострокової співпраці, щоб гарантувати, що кібербезпека є основним принципом чистої енергії.

Протягом наступних кількох десятиліть необхідна тісна та регулярна співпраця між спільнотами кібербезпеки та енергетичних мереж, щоб переконатися, що кібербезпека є основним принципом нашої майбутньої чистої енергетичної мережі.

Традиційні державно-приватні партнерства ще не включають зазвичай представників великих компаній, що працюють у сфері відновлюваної енергетики

та хмарних технологій, а управління та стандарти кібербезпеки, зокрема, все ще поширені серед багатьох федеральних агенцій, включаючи Міністерство енергетики, CISA, Офіс Білого дому Національної кібербезпеки. директора та Національний інститут стандартів і технологій. Але зачатки правильної політики існують, від вищезгаданих програм безпечної архітектури в CISA та DOE до гранту на розвиток кібербезпеки для сільських і муніципальних підприємств і програми технічної допомоги, спрямованої на допомогу невеликим операторам, комунальним підприємствам і кооперативам у зміцненні їх кіберзахисту.

Незважаючи на те, що попереду ще багато викликів, ми все ще сподіваємося на співпрацю між фахівцями з кліматичної політики, енергетики та кібербезпеки в масштабах усієї країни — лише тоді кібербезпека зможе стати фактором, а не перешкодою для майбутнього чистої енергії». ***(Sarah Powazek and Steve Kelly. The future of clean energy hinges on cybersecurity // Nexstar Media Inc. (https://thehill.com/opinion/energy-environment/4615046-the-future-of-clean-energy-hinges-on-cybersecurity/). 23.04.2024).***

***

Країни ЄС та Великобританія

«Наприкінці березня близько 70 веб-сайтів у Люксембурзі стали жертвами великої хвилі кібератак, що викликало підвищену стурбованість щодо кібербезпеки в країні.

Питання про кібератаки та кібербезпеку нещодавно було піднято в депутатському запиті Піратської партії. Директор Урядового IT-центру (CTIE) підтвердив, що переважна більшість сайтів, націлених у березні, належали державі або невеликій кількості муніципалітетів. Примітно, що депутатське питання, поставлене депутатом Беном Полідорі, передувало останній кібератаці, яка, як вважають, походить з Росії. Незважаючи на цей інцидент, кібербезпека залишається актуальною проблемою.

Одним із прикладів цього є скандал із Taurus, коли високопоставлених німецьких чиновників прослуховували під час делікатної дискусії російської

спецслужби. У відповідь на цю справу прем'єр-міністр Люк Фріден і міністр цифровізації Стефані Обертін підкреслили непохитну відданість уряду забезпеченню конфіденційності електронних комунікацій і захисту даних.

Для дотримання цих стандартів для передачі конфіденційних документів рекомендовані безпечні рішення, рекомендовані CTIE. Крім того, директива забороняє представникам державних служб використовувати соціальні медіа-платформи, такі як Facebook, TikTok або WhatsApp, для отримання професійної чи непублічної інформації.

Крім того, вже майже рік запроваджено безпечну службу обміну повідомленнями, яка полегшує спілкування між працівниками державного сектору на робочих мобільних телефонах, інших професійних пристроях або навіть приватних телефонах. Спеціально зашифровані мобільні телефони також надаються членам уряду та вищим державним службовцям для посилення заходів безпеки». ***(Jean-Marc Sturm. Government determined to strengthen cyber security in Luxembourg // RTL Luxembourg (https://today.rtl.lu/news/luxembourg/a/2183509.html). 04.04.2024).***

***

«Європейський Союз насилу погодився на схему сертифікації кібербезпеки (EUCS), щоб гарантувати кібербезпеку хмарних сервісів і допомогти урядам і компаніям у блоці вибрати безпечного та надійного постачальника для свого бізнесу.

Цей крок стався, оскільки Big Tech шукає прибутковий ринок державних хмарних технологій, щоб стимулювати зростання.

З іншого боку, ЄС побоюється незаконного державного стеження, а деякі уряди стурбовані тим, що домінування американських хмарних провайдерів може перешкоджати зародженню конкурентів ЄС.

Один проект, розповсюджений урядам ЄС минулого року, вимагав від технологічних гігантів США створити спільне підприємство з компанією, що

базується в ЄС, а також зберігати та обробляти дані клієнтів у блоці, щоб мати право на мітку кібербезпеки ЄС.

Такі так звані вимоги до суверенітету викликали критику з боку європейських банків, клірингових центрів, страхових груп і деяких стартапів, які стверджували, що перевагу повинні мати технічні резерви, а не політичні та суверенні зобов'язання.

Останній проект від 22 березня скасував такі вимоги, згідно з якими хмарні постачальники зобов'язані надавати лише інформацію про місце зберігання та обробки даних своїх клієнтів і про чинне законодавство.

Зараз країни ЄС переглядають доопрацьований проект, після чого Європейська комісія ухвалить остаточну схему. Виконавчий орган ЄС не відповів на запит про коментар». ***(Foo Yun Chee. EU drops sovereignty requirements in cyber security certification scheme // nextmedia Pty Ltd. (https://www.itnews.com.au/news/eu-drops-sovereignty-requirements-in-cyber-security-certification-scheme-606695). 04.04.2024).***

***

«Законодавці ЄС скасували вимоги щодо суверенітету для запропонованої схеми маркування кібербезпеки, знаменуючи відхід від правил, які, на думку критиків, серйозно перешкоджатимуть провайдерам із-за меж ЄС.

Пропозиції вимагали від постачальників хмарних технологій, які не входять до ЄС, створити «спільне підприємство» з провайдерами, що базуються в союзі, через правила суверенітету даних і безпеки.

Однак нові зміни означають, що постачальники хмарних технологій будуть зобов'язані надавати інформацію лише про свої організаційні структури даних, згідно з документами, з якими ознайомився Reuters.

Це включатиме інформацію про те, де зберігаються дані, і методи обробки даних клієнтів.

Цей крок законодавців знаменує собою важливий поворот, і хоча очікується, що зміни будуть вітати фірми, що не входять до ЄС, рішення відмовитися від вимог щодо суверенітету може викликати подальшу плутанину.

Кілька великих компаній уже почали робити відповідні кроки для забезпечення дотримання майбутнього регулювання.

Зараз країни-члени ЄС переглянуть відредагований проект, після чого Єврокомісія завершить формулювання вимог». ***(George Fitzmaurice. EU lawmakers drop sovereignty requirements for cyber security labeling scheme // Future US, Inc. (https://www.itpro.com/business/policy-and-legislation/eu-lawmakers-drop-sovereignty-requirements-for-cyber-security-labeling-scheme). 08.04.2024).***

***

«Останнє опитування уряду Великої Британії показало, що половина підприємств країни стикалися з певною формою порушення кібербезпеки за останні 12 місяців.

Висновки також показують, що близько третини (32%) благодійних організацій повідомляють про такий самий ризик. Ця цифра зростає до 66%, якщо відфільтрувати до тих, хто має високий дохід (£500 000 або більше на рік).

Для середнього бізнесу результати набагато вищі – 70%, а для великого бізнесу – ще більше – 74%.

За останні 12 місяців витрати на ці атаки для підприємств становили в середньому близько 1205 фунтів стерлінгів, хоча для середніх і великих компаній ця цифра підскочила до 10 830 фунтів стерлінгів.

Однак генеральний директор фірми з кібербезпеки Socura Енді Кейс порадив організаціям ставитися до цих висновків з обережністю.

«Очевидно, що це опитування спрямоване в бік менших підприємств, ніж багато інших опитувань, тому цифри завжди будуть меншими. Ми знаємо, що великі корпоративні підприємства можуть втратити мільйони в разі витоку даних через збої, вплив на репутацію та падіння курсу акцій», — сказав він.

Згідно з опитуванням, найпоширенішим типом злому є фішинг – 84% для компаній і 83% для благодійних організацій, за якими йдуть інші організації, які видають себе за організації в електронних листах або в Інтернеті – 35% та віруси чи інше шкідливе програмне забезпечення – 17% компаній.

«Звіт вказує на явний сплеск атак соціальної інженерії, — сказав Кріс Рекл, CPO фірми з кібербезпеки Appdome, — що є наслідком розширення доступності генеративного штучного інтелекту, що підкреслює гостру проблему безпеки».

«Для брендів необхідно рішуче протидіяти тактиці соціальної інженерії. Використання методів поведінкового аналізу в реальному часі для запобігання маніпулятивним стратегіям може захистити споживачів від того, щоб стати жертвою шахраїв», – додав він.

За словами Кейса з Socura, лише невелика частина підприємств Великобританії має будь-який формалізований план реагування на інциденти – факт, який він вважає «вражаючим».

«Компанії завжди матимуть план на випадок пожежі, але не застосовуватимуть належної обережності щодо витоку даних — що статистично більш імовірно. Це суперечить здоровому глузду». ***(Nicole Deslandes. Half of UK businesses hit by cyber security attacks in past year // The Frontier of Tech News (https://techinformed.com/half-of-uk-businesses-hit-by-cyber-security-attacks-in-past-year/). 10.04.2024).***

***

«Змінений Закон про військову службу Швейцарії пропонує надати Федеральній раді Швейцарії повноваження вимагати ІТ-експертів та інфраструктуру для військової стійкості, особливо проти кіберзагроз. Він передбачає розширення на мирний час, потребує схвалення Федеральної ради Швейцарії та передбачає положення про компенсацію. Консультації завершилися в березні 2024 року. Положення, яке розглядається після консультацій, рекомендує компаніям відстежувати оновлення та готувати стратегії для потенційних заявок.

У Швейцарії триває перегляд Швейцарського військового закону, який, серед іншого, надасть Федеральній раді Швейцарії право наймати приватних ІТ-експертів і вимагати ІТ-інфраструктуру, якщо це необхідно для захисту ланцюгів постачання збройних сил Швейцарії та військової інформації і комунікаційних технологій, а також підтримувати оперативну безперервність і стійкість до загроз, зокрема в кіберсфері.

Докладніше, раніше неіснуюча стаття 95 консультаційного проекту Закону Швейцарії про військову службу звучить так (неофіційний переклад англійською мовою, курсив додано):

ст. 95 Безперервність і стійкість бізнесу

1 З метою захисту ланцюгів постачання Збройних Сил і військових інформаційно-комунікаційних технологій, а також для підтримки оперативної безперервності та стійкості перед обличчям загроз, зокрема в кібернетичній сфері, Військова адміністрація та Збройні Сили можуть, за винятком: радіочастоти: a. обмежувати або забороняти використання реквізованих товарів;

b. реквизиция реквізиція товарів.

2 Такі заходи потребують схвалення Федеральної ради.

3. Конфедерація виплачує відповідну компенсацію за обмеження або заборону використання та реквізицію реквізованого майна.

4. Обмеження та заборони на використання та реквізиції видаються компетентними органами Військової адміністрації та Збройних Сил. Процедура регулюється Законом про адміністративну процедуру від 20 грудня 1968 року.

5. Федеральна рада призначає компетентні органи Військової адміністрації та Збройних Сил і описує їхні завдання більш детально.

У військовій термінології реквізиція означає конфіскацію цивільного майна для військових цілей.

Згідно з консультаційним проектом, розширення прав реквізиції на нематеріальне майно застосовується як під час кризи, так і в мирний час.

Це може мати значні наслідки для компаній у приватному секторі та супроводжується втратою юридичної та планової визначеності: зокрема великі та

малі технологічні компанії, а також усі інші приватні компанії, які наймають кібер- та інших ІТ-експертів, можуть зіткнутися з Реальність полягає в тому, що їхні співробітники набираються щодня і що їм потрібно зробити свою ІТ-інфраструктуру (наприклад, сервери, програмне забезпечення, мережеві ресурси та послуги) доступною для збройних сил Швейцарії – за умови схвалення Федеральної ради Швейцарії.

Захисний механізм, який гарантує, що сама компанія все ще має кібер- та інших ІТ-фахівців та інфраструктуру, необхідну для забезпечення безперервності її власних операцій, не передбачено в консультаційному проекті. Раптова втрата ключового кібер-або іншого ІТ-персоналу та ІТ-інфраструктури може порушити роботу компаній. У зв'язку з можливістю реквізиції компаніям може бути складно планувати довгострокові стратегії, що має вирішальне значення для підтримки конкурентної переваги. Крім того, компаніям може знадобитися інвестувати в резервні системи або найняти додатковий кібер-або інший ІТ-персонал як буфер від потенційних запитів, що призведе до збільшення операційних витрат.

Позитивним моментом є те, що за умови належного управління такими вимогами можна створити міцніші державно-приватні партнерства, коли компанії будуть тісно співпрацювати з урядом у проектах кібербезпеки та національної оборони.

Процедура реквізицій відповідно до переглянутої статті 95 Швейцарського військового закону регулюється Федеральним законом про адміністративну процедуру від 20 грудня 1968 року (APA). По-перше, це означає, що застосовуються процесуальні права, передбачені в APA, тобто, що компанії, яких стосується запит, мають, наприклад, право перевіряти файли та повинні бути заслухані до видання наказу (стаття 30). По-друге, це означає, що зацікавлені компанії мають право оскаржити наказ. Федеральний адміністративний суд Швейцарії (Bundesverwaltungsgericht) буде апеляційним органом відповідно до нової статті 33 lit. hbis Федерального закону про Федеральний адміністративний суд Швейцарії від 17 червня 2005 року.

Згідно з консультаційним проектом, федеральний уряд виплатить компенсацію, якщо він скористається своїм правом на реквізицію, але буде виплачена лише належна компенсація, тобто, ймовірно, не повна компенсація.

Це нове правове положення ще не встановлено. Процес консультацій було завершено в березні 2024 року. Федеральний департамент оборони, цивільного захисту та спорту DDPS (VBS) зараз розглядає отримані коментарі, а потім представить проект переглянутого акта.

Особливо великі та малі технологічні компанії, а також усі інші приватні компанії, які наймають кібер- та інших IT-експертів або керують IT-інфраструктурою, повинні уважно стежити за подальшим розвитком і, якщо статтю 95 буде збережено у формі, передбаченій у консультаційному проекті, вжити відповідних заходів для підготовки до заявки, наприклад, розробити плани на випадок непередбачених обставин, покращити навчання для інших співробітників або знайти тимчасову заміну». ***(Christian Kunz and Eric Stupp. Swiss Cyber Defence: Forced Recruitment of Private IT Experts and Infrastructure Considered // Bär & Karrer (https://www.baerkarrer.ch/en/publications/swiss-cyber-defence). 08.04.2024).***

***

«Великі європейські гравці промисловості, включаючи Airbus, OVHcloud і Orange, засудили нещодавнє рішення Європейського агентства з кібербезпеки (ENISA), яке більше не розрізнятиме постачальників хмарних послуг на основі їх походження, у листі, з яким ознайомився Euractiv.

Агентство блоку з кібербезпеки ENISA, яке координує роботу над схемою сертифікації кібербезпеки ЄС (EUCS), вирішило видалити посилання на вимоги суверенітету в своєму останньому проекті від 22 березня, про який повідомляє Euractiv.

EUCS має на меті створити схему сертифікації на рівні ЄС, яка допоможе урядам і компаніям у блоці визначити атрибути кібербезпеки будь-якого постачальника хмарних послуг під час покупки таких послуг.

Схема визначає різні рівні захисту залежно від конфіденційності даних, що обробляються.

«Ми вважаємо, що включення вимог щодо суверенітету є необхідним для подолання фрагментації ринку» та «захисту найбільш конфіденційних даних європейських організацій», — написали 18 підписантів у відкритому листі.

Лист закликає «держави-члени відхилити будь-яку пропозицію [EUCS]», яка не містить положень про суверенітет.

У листі повторюється, що вимоги суверенітету важливі для усунення ризику незаконного доступу до даних іноземними урядами. Таким чином, ці положення також захищають конфіденційність користувачів, зазначено в листі.

Їхні прихильники розглядають положення як важливий інструмент для захисту компаній і урядів ЄС від влади іноземних держав.

У листі цитується закон про національну розвідку Китаю та закон США про хмарні технології, від яких мають бути захищені європейські провайдери та користувачі хмарних технологій.

Ці закони могли б дати агентствам національної безпеки можливість отримати доступ до даних третіх сторін, які обробляються їхніми місцевими компаніями.

Підписанти додали, що поточний проект правил призведе до фрагментації ринку, оскільки відповідальність за визначення суверенних елементів ляже на національні регулятори.

Компанії зазначили, що схема EUCS суперечитиме закону ЄС про обмін даними; Закон про дані.

Закон забороняє незаконний доступ іноземних урядів до неперсональних даних, підкреслили підписанти.

Спеціальна робоча група ENISA має зустрітися 15 квітня для обговорення схеми хмарної сертифікації.

Серед підписантів — постачальник електроенергії EDF, Dassault Systèmes, яка володіє постачальником хмарних послуг Outscale, технологічні компанії Sopra Steria та Capgemini, а також телекомунікаційні компанії Deutsche Telekom, Telecom

Italia та Proximus». ***(Théophane Hartmann. European industrial giants condemn latest EU cybersecurity agency decision on cloud sovereignty // Euractiv (https://www.euractiv.com/section/competition/news/european-industrial-giants-condemn-latest-eu-cybersecurity-agency-decision-on-cloud-sovereignty/). 10.04.2024).***

***

«У 2023 році в Польщі було виявлено понад 90 000 інцидентів, що порушували кібербезпеку, що більше, ніж у попередні роки. Такі дані були представлені в щорічному звіті уповноваженого польського уряду з питань кібербезпеки.

Міністерство цифровізації Польщі вперше представило документ громадськості. Поки що річний звіт готувався виключно для внутрішніх потреб уряду.

Віцепрем'єр-міністр, міністр цифровізації та урядовий уповноважений з питань кібербезпеки Кшиштоф Ґавковський заявив, що значна частина кібератак та інцидентів пов'язана з діяльністю Росії.

«Протягом останнього року Російська Федерація посилила свої атаки за допомогою або завдяки діяльності груп, що були спеціально підготовлені для атакування партнерів чи союзників України, або пов’язані з діяльністю, що має на меті дестабілізацію», — сказав Кшиштоф Ґавковський.

Міністр цифровізації Польщі попередив, що найближчими тижнями громадська думка може стати об'єктом посилених дезінформаційних кампаній. Це пов'язано з виборами до Європарламенту.

«Наші відділи фіксують ще більший масштаб запланованих атак. Це пов’язано з виборами до Європейського парламенту. Поляризація на добрих та злих в кіберпросторі тільки посилюється», — додав політик.

Згідно зі звітом, із понад 80 000 інцидентів, зареєстрованих CERT Polska (команда, створена для реагування на події, що порушують безпеку в Інтернеті, - прим.ред.), 40 були класифіковані як серйозні, решта стосувалися державних і військових організацій, підконтрольних Агентству внутрішньої безпеки (ABW)

(4676 інцидентів) і Міністерству національної оборони — 5841 інцидент. З міркувань безпеки не була надана детальна інформація. Звіт без секретної частини доступний на сайті Міністерства цифровізації.

Найближчими тижнями відомство має оприлюднити деталі поправок до Закону про національну систему кібербезпеки. Цей закон також регулює роботу Групи реагування на інциденти комп'ютерної безпеки (CSIRT). У Польщі є три таких групи, які контролюються Агентством внутрішньої безпеки, Міністерством національної оборони та Національним дослідницьким інститутом (CERT Polska).

Міністерство хоче, щоб цього року уряд також схвалив нову Стратегію кібербезпеки Республіки Польща». ***(У 2023 році в Польщі було зафіксовано понад 90 тисяч кіберзагроз // Polskie Radio S.A. (https://www.polskieradio.pl/398/7856/Artykul/3362894,%D1%83-2023-%D1%80%D0%BE%D1%86%D1%96-%D0%B2-%D0%BF%D0%BE%D0%BB%D1%8C%D1%89%D1%96-%D0%B1%D1%83%D0%BB%D0%BE-%D0%B7%D0%B0%D1%84%D1%96%D0%BA%D1%81%D0%BE%D0%B2%D0%B0%D0%BD%D0%BE-%D0%BF%D0%BE%D0%BD%D0%B0%D0%B4-90-%D1%82%D0%B8%D1%81%D1%8F%D1%87-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7). 11.04.2024).***

***

«Експерти з кібербезпеки відклали голосування за проект ярлика кібербезпеки ЄС, що дозволяє Amazon, Alphabet Google і Microsoft брати участь у торгах на дуже конфіденційні контракти ЄС на хмарні обчислення до травня, повідомили люди, знайомі з цим питанням.

Європейський Союз хоче запровадити схему сертифікації кібербезпеки (EUCS), щоб гарантувати кібербезпеку хмарних сервісів і допомогти урядам і компаніям вибрати безпечного та надійного постачальника для свого бізнесу хмарних обчислень.

Однак розбіжності щодо того, чи слід накладати суворі вимоги на Big Tech, щоб претендувати на найвищий рівень маркування кібербезпеки ЄС, перешкодили зусиллям.

Експерти, які зустрілися в понеділок і вівторок у Брюсселі, не голосували за останній проект схеми, запропонований агентством ЄС з кібербезпеки ENISA у 2020 році та змінений Бельгією, яка зараз головує в ЄС, повідомили люди.

Після голосування експертів наступним кроком є висновок країн ЄС і остаточне рішення Єврокомісії.

Остання версія скасувала так звані вимоги суверенітету з попередньої пропозиції, яка зобов'язувала технологічних гігантів США створити спільне підприємство або співпрацювати з компанією, що базується в ЄС, для зберігання та обробки даних клієнтів у блоці, щоб отримати право на найвищий рівень. знака кібербезпеки ЄС.

У той час як Big Tech привітав скасування вимог, європейські хмарні постачальники та компанії, такі як Deutsche Telekom, Orange і Airbus, розкритикували цей крок і попередили про ризик незаконного доступу до даних урядами країн, що не входять до ЄС, на підставі їхнього законодавства». ***(Foo Yun Chee. Vote on EU cyber security label delayed to May // nextmedia Pty Ltd. (https://www.itnews.com.au/news/vote-on-eu-cyber-security-label-delayed-to-may-607126). 17.04.2024).***

***

«Велика дискусія щодо наскрізного шифрування продовжується в Європі, оскільки керівники поліції регіону оприлюднили спільну заяву, в якій зазначено, що вони принципово не вірять у двійковий вибір між кібербезпекою та конфіденційністю. Ця заява, яку підтримують Європол і керівники європейської поліції, надійшла в той момент, коли Meta почала розгортати наскрізне шифрування на всіх своїх платформах обміну повідомленнями (раніше це було обмежено WhatsApp за замовчуванням, але тепер буде поширено на Instagram і також чати Facebook Messenger).

Наскрізне шифрування дозволяє двом або більше користувачам спілкуватися, при цьому ніхто інший не бачить вміст цих повідомлень, навіть постачальник послуг обміну повідомленнями (наприклад, Meta). Уряди та органи поліції стверджують, що такий рівень захисту зменшує їх здатність перехоплювати незаконну діяльність в Інтернеті, особливо коли йдеться про експлуатацію дітей; у той час як активісти конфіденційності вважають, що впровадження «чорних дверей» для зашифрованих послуг дозволить урядам здійснювати масове спостереження за даними громадян.

У багатьох відношеннях це заковика 22: чи приймаєте ви повну конфіденційність у службах обміну повідомленнями та визнаєте, що це неминуче призведе до певної незаконної діяльності? Або ви запроваджуєте чорні двері, які, як наслідок, зменшують усі принципи конфіденційності, за які важко боролися? У той час як дехто заперечить, що «Якщо ви не робите нічого поганого, яке це має значення?»; багато хто не захоче запроваджувати механізми, які дозволяють державі та поліцейським органам масового стеження.

Дебати, здавалося, були скасовані наприкінці минулого року після того, як було помічено, що британський уряд відмовився від суперечки з технологічними компаніями щодо технології «сканування на стороні клієнта», яка дозволяла аналізувати вміст повідомлення на пристрої користувача перед повідомленням. відправлено. Знову ж таки, борці за конфіденційність стверджували, що це відкриває двері для масового стеження, але в той же час стверджувалося, що ефективних технологій у цій сфері ще не існує для цієї мети. Уряд поступився після того, як WhatsApp і Signal погрожували вийти з країни разом, а британські чиновники заявили, що відповідний пункт у законопроекті про безпеку в Інтернеті не буде виконуватися.

Однак у зв’язку з тим, що Meta зараз розгортає розширені служби шифрування, а Закон Британії про повноваження щодо слідчих повноважень знаходиться на завершальній стадії внесення до парламенту, згідно з яким технологічні компанії повинні повідомляти уряд про будь-які зміни, які можуть вплинути на діяльність штату зі спостереження (і дозволити Міністерство

внутрішніх справ, щоб ввести зміни), дебати щодо наскрізного шифрування знову розпалилися.

«Не бінарний вибір»

Зважаючи на цей контекст, керівники європейської поліції наполягають на тому, щоб технологічні компанії переглянули свою позицію та зайшли так далеко, щоб стверджувати, що вони несуть «соціальну відповідальність» за створення «безпечнішого середовища, де правоохоронні органи та правосуддя можуть виконувати свою роботу», як злочинці переміщують більше дій в Інтернет.

У спільній декларації, опублікованій останніми днями, зазначено, що дві ключові можливості мають вирішальне значення для підтримки онлайн-безпеки:

По-перше, здатність технологічних компаній надавати правоохоронним органам розслідування – у відповідь на законну владу з сильними гарантіями та наглядом – дані підозрюваних злочинців на їх службі. Це відоме як «законний доступ».

По-друге, здатність технологічних компаній завчасно виявляти незаконну та шкідливу діяльність на своїх платформах. Це особливо вірно щодо виявлення користувачів, які мають сексуальний інтерес до дітей, обмінюються образами насильства та намагаються вчинити контактні сексуальні злочини.

Наразі компанії мають можливість сповістити відповідні органи влади, в результаті чого багато тисяч дітей було захищено, а злочинці заарештовані та притягнуті до відповідальності.

Наразі британська поліція, наприклад, отримує дані про підозрілу діяльність від Meta, що призводить до сотень арештів на місяць і сотень дітей, визначених як особи, які мають право на захист. Начальники європейської поліції стверджують, що ці механізми щодня допомагають «рятувати багато життів» і «захищати вразливих».

У декларації додається, що органи поліції «глибоко стурбовані» тим, що наскрізне шифрування розгортається таким чином, що підриває обидві ці можливості. У ньому зазначено, що компанії не зможуть ефективно реагувати на законні органи влади, а також не зможуть ідентифікувати або повідомляти про

незаконну діяльність на своїх платформах. Це означає, стверджують правоохоронці, що вони не зможуть забезпечити безпеку населення.

Декларація продовжується:

Раніше наше суспільство не терпіло місць, які знаходяться поза межами досяжності правоохоронних органів, де злочинці можуть безпечно спілкуватися і де може процвітати жорстоке поводження з дітьми. Вони не повинні зараз. Ми не можемо дозволити, щоб нас засліпили злочини. Ми знаємо, як швидко та широко злочинці використовують таку анонімність із захисту, який надає темна мережа.

Ми прагнемо підтримувати розвиток критично важливих інновацій, таких як шифрування, як засіб посилення кібербезпеки та конфіденційності громадян. Однак ми не погоджуємося з тим, що потрібен двійковий вибір між кібербезпекою чи конфіденційністю з одного боку та громадською безпекою з іншого.

Абсолютизм з обох сторін не приносить користі. Ми вважаємо, що технічні рішення існують; вони просто вимагають гнучкості як від промисловості, так і від урядів. Ми усвідомлюємо, що рішення будуть різними для кожної можливості, а також відрізнятимуться між платформами.

Однак варто зазначити, що хоча керівники поліції закликають технологічну індустрію «створювати безпеку за проектом», вони чітко не вказують, які існують технологічні рішення для забезпечення наскрізного шифрування та дозволяють технологічним компаніям контролювати повідомлення за незаконну діяльність. Активісти захисту конфіденційності стверджують, що таких технологій не існує, не ставлячи під загрозу принципи конфіденційності для всіх громадян.

Моя думка

Проблема, як я бачу, полягає в тому, що навіть якщо уряди, поліцейські органи та технологічні компанії мають зараз найкращі наміри у світі, ми не можемо бути впевнені, що майбутні органи влади та державні лідери матимуть такі самі наміри. Хоча всі можуть погодитися, що захист людей і дітей в Інтернеті є критично важливим, під час регулювання стає важче підірвати принципи конфіденційності кожного. Чи хочемо ми сценарію, за якого влада матиме механізми, за допомогою яких назавжди матиме доступ до приватних

комунікаційних даних, якщо вони вважають за потрібне? Я б стверджував, що це дуже серйозний компроміс, який багатьом не сподобається». ***(Derek du Preez. Encryption debate rolls on - European police chiefs do not accept 'binary choice between cyber security and privacy'// diginomica (https://diginomica.com/encryption-debate-rolls-european-police-chiefs-do-not-accept-binary-choice-between-cyber-security). 22.04.2024).***

***

«Організація Об'єднаних Націй та Європейський Союз запровадили суворі правила щодо кібербезпеки в автомобілях. Згідно їх логіки, сучасні автомобілі наповнені камерами та високотехнологічними датчиками, які підтримують безліч систем для нашої безпеки та зручності. Однак усі ці технології роблять їх потенційною мішенню для хакерів та кібератак, повідомляє carscoops.

Усі нові автомобілі, що продаватимуться в Європейському Союзі з 7 липня 2024 року, повинні відповідати правилам ООН R155 і R156, які вже діють для затвердження нових моделей з липня 2022 року. Якщо коротко, то R155 вимагає від автовиробників системи управління, а R156 гарантує, що оновлення програмного забезпечення транспортних засобів є більш захищеними від загроз кібербезпеки.

Ці зміни змусили кількох автовиробників зняти старі моделі зі своїх лінійок на Старому континенті, оскільки вартість оновлення їхньої електроніки виявилася занадто високою.

Говорячи про сучасні автомобілі німецькій газеті Handelsblatt, економіст Моріц Шуларік сказав: «Йдеться про конфіденційні дані, які можуть бути викачані – особливо за допомогою електромобілів. З точки зору спецслужб, ці автомобілі з їхніми численними датчиками і камерами є нічим іншим, як шпигунськими машинами на чотирьох колесах».

На попередній конференції, що відбулася в Німеччині, Шуларік припустив, що сучасні електромобілі можуть знімати все, що відбувається навколо них, коли вони їздять містами, а потім передавати дані своїм виробникам – деякі з них знаходяться в Китаї. Потім він запитав аудиторію: «Чи хочемо ми цього? Чи

хочемо ми, щоб очі і вуха іноземного уряду стежили за нашими вулицями через мільйони автомобілів?»

Згідно з нещодавнім дослідженням «Автомобільна кібербезпека», проведеним німецьким Центром автомобільного менеджменту (CAM) та американською компанією Cisco Systems, загрози кібербезпеки є «неминучими», оскільки сучасні автомобілі є вразливими до кібератак.

Нагадаємо, електричні авто з Китаю накопичуються в європейських портах, перетворюючи їх на «автостоянки», оскільки виробники і дистриб'ютори стикаються із уповільненням продажів і логістичними проблемами, включаючи нестачу водіїв вантажних автівок». ***(Іван Гавриляк. ЄС запроваджує нові правила кібербезпеки для сучасних авто // Українські медійні системи (https://glavcom.ua/techno/auto/jes-zaprovadzhuje-novi-pravila-kiberbezpeki-dlja-suchasnikh-avto-996791.html). 18.04.2024).***

***

Австралія та Нова Зеландія

«Компанія Fujitsu створила передову інтегровану команду експертів із безпеки даних і криміналістики, посилюючи свою прихильність боротьбі зі зростаючими глобальними та локальними кіберзагрозами, які впливають на організації в Австралії та Новій Зеландії. Ця спеціальна команда консультантів під назвою Fujitsu Cyber Security Services зосереджена на допомозі організаціям і керівникам інформаційної безпеки в підготовці та реагуванні на критичні виклики безпеки даних.

Новий підрозділ об’єднує навички та спеціалізацію існуючої команди регіональної безпеки Fujitsu та розширені можливості, отримані в результаті нещодавніх придбань фірмою, таких як Enable, InPhySec, MF & Associates і oobe. Цим кроком Fujitsu не лише встановлює еталон цифрового досвіду та трансформації сталого розвитку, але й посилює свою роль як надійного партнера, що підтримує кібернетостійкість.

Грем Бердселл, головний виконавчий директор Fujitsu для Азіатсько-Тихоокеанського регіону, каже: «Організації будь-якого розміру все частіше стикаються з кіберзагрозами. Служби кібербезпеки Fujitsu нададуть підтримку компаніям у підготовці та реагуванні на найгостріші виклики безпеки даних сьогодні. Наша інтегрована команда експертів надає комплексні, індивідуальні рішення, від розширеного аналізу загроз до механізмів швидкого реагування. Об'єднуючи регіональний досвід нашої фірми, Fujitsu пропонує унікальну стратегічну перевагу, дозволяючи нашим клієнтам зосередитися на своєму основному бізнесі з гарантією надійної кіберстійкості».

Fujitsu Cyber Security Services надає організаціям в Австралії та Новій Зеландії провідну в галузі колекцію послуг і можливостей кібербезпеки. Послуги включають консультування та надання гарантій, цифрову криміналістику та реагування на інциденти, оцінки та підвищення потенціалу кібербезпеки, а також операції безпеки за допомогою ШІ. Організації можуть скористатися інтегрованою наскрізною підтримкою безпеки даних, починаючи від розробки стратегії та дорожньої карти, послуг віртуального головного спеціаліста з інформаційної безпеки та управління інформаційною безпекою до розширеного аналізу загроз і механізмів швидкого реагування.

Стюарт Кілдафф, керівник служби кібербезпеки Fujitsu, додав: «Наша експертна команда з кібербезпеки та стратегічні партнери по альянсу спираються на інноваційну спадщину Fujitsu. Це дозволяє Fujitsu надавати швидкі та ефективні рішення для захисту даних, забезпечуючи кіберстійкість наших клієнтів. Організації також матиме доступ до інтегрованого спектру технологій, у тому числі штучного інтелекту та навичок цифрової трансформації та безпеки для підтримки складних потреб організацій в Австралії та Новій Зеландії».

Зміцнення можливостей Fujitsu у сфері кібербезпеки відбулося після нещодавніх регіональних придбань, зокрема хмарного провайдера Microsoft oobe, спеціалістів з консалтингу та кібербезпеки MF & Associates, консалтингової компанії ServiceNow Enable та новозеландської консалтингової компанії з безпеки InPhySec. Інтегрований досвід цих придбаних компаній допомагає зміцнити досвід

Fujitsu у цифровому досвіді та трансформації досвіду сталого розвитку, обіцяючи підвищити безпеку їхніх клієнтів у цифровій сфері». ***(Kaleah Salmon. Fujitsu strengthens cyber security with new Australian, NZ division // TechDay (https://securitybrief.co.nz/story/fujitsu-strengthens-cyber-security-with-new-australian-nz-division). 17.04.2024).***

***

Китай

«22 березня 2024 року Адміністрація кібербезпеки Китаю (CAC) випустила довгоочікувані нові Правила сприяння та регулювання транскордонних потоків даних (нові правила) для дотримання Закону Китаю про захист персональної інформації (PIPL), даних Закон про безпеку (DSL) та його імплементаційні нормативні акти. Нові правила набувають чинності негайно та створені на основі проектів постанов, виданих CAC 28 вересня 2023 року (проект постанов).

Крім того, CAC також випустив Посібник із застосування для оцінки безпеки вихідної передачі даних (друге видання) та Посібник із подання стандартного контракту на вихідну передачу персональної інформації (друге видання) (разом – Посібник). Керівні принципи містять детальні процедури для обробників даних, які також тепер можуть використовувати програмну систему вихідної передачі даних для вихідної передачі особистої інформації. Однак Нові правила мають пріоритет над будь-якими положеннями, які можуть суперечити PIPL і Керівним принципам.

Нові правила та рекомендації полегшують численні вимоги до відповідності та сприяють транскордонній передачі даних для обробників даних. Примітно, що загалом немає положень, які полегшують передачу конфіденційної особистої інформації згідно з новими правилами. Крім того, особи, які займаються обробкою даних, повинні пам’ятати, що враховуючи відсутність чіткості щодо визначення «важливих даних», Нові правила дозволяють особам, які займаються обробкою даних, вважати свої дані неважливими, якщо це чітко не зазначено; або вони повідомлені регуляторами; або якщо відповідні дані вважаються важливими згідно

з публічним оголошенням органів влади. Ми очікуємо, що галузеві та місцеві регулятори нададуть додаткові вказівки щодо класифікації важливих даних. Крім того, нові правила вимагають, щоб транскордонна передача особистої інформації за межі Китаю все ще відповідала вимогам PIPL щодо повідомлення, окремої згоди та оцінки впливу на захист персональної інформації.

Нижче наведено деякі ключові зміни, передбачені новими правилами.

Винятки

Нові правила тепер звільняють обробників даних від подання стандартного контракту (стандартний контракт), сертифіката захисту персональної інформації (сертифікація) або заявки на оцінку безпеки (оцінка безпеки), якщо застосовуються наведені нижче дії з обробки даних.

Новий поріг. Якщо транскордонна передача персональних даних менше ніж 100 000 осіб відбувається з 1 січня поточного року. Раніше проект правил ініціював стандартне подання контракту або сертифікацію для менш ніж 10 000 осіб. Однак це не стосується транскордонної передачі конфіденційної особистої інформації або операторів критичної інформаційної інфраструктури (CIIO).

Діяльність з персоналом. Якщо необхідно передати особисту інформацію за кордон з метою здійснення управління людськими ресурсами відповідно до норм і правил праці та законно укладених колективних договорів (Інформація про людські ресурси). Однак інформація про людські ресурси має відповідати принципу PIPL «мінімально та необхідно».

Договірна необхідність. Нові правила звільняють транскордонну передачу особистої інформації, необхідної для виконання контракту, стороною якого є особа. Це включає в себе контракти на транскордонні покупки, транскордонну поштову відправку та доставку, транскордонні грошові перекази, транскордонні платежі, транскордонні відкриття рахунків, бронювання авіаквитків і готелів, оформлення віз та послуги перевірки.

Надзвичайні ситуації. Транскордонна передача персональних даних необхідна для захисту життя, здоров’я та майна фізичної особи в надзвичайних ситуаціях.

Особиста інформація за межами Китаю. Якщо особиста інформація збирається й обробляється за кордоном, а потім передається до Китаю для обробки перед передачею за кордон і не передбачає введення внутрішньої особистої інформації чи важливих даних під час обробки.

Інші дані. Будь-яка транскордонна передача особистої інформації в результаті міжнародної торгівлі, транскордонного транспортування, наукового співробітництва, транснаціонального виробництва, маркетингу та іншої діяльності, яка не стосується особистої інформації чи важливих даних.

Стандартне подання або сертифікація контракту

Нові правила окреслюють, що обробник даних може використовувати стандартне подання контракту або сертифікацію для транскордонної передачі особистої інформації, якщо:

Він обробляє особисту інформацію менше ніж 1 000 000 осіб;

Передає персональну інформацію менше ніж 100 000 осіб з 1 січня поточного року;

Він передає конфіденційну особисту інформацію менше ніж 10 000 осіб з 1 січня поточного року; або

Це не СІІО.

Оцінка безпеки

Згідно з новим Регламентом, якщо обробник даних обробляє особисту інформацію за межами Китаю, оцінка безпеки потрібна, коли:

СІІО передає будь-яку особисту інформацію або важливі дані за межі Китаю;

Обробник даних (за винятком СІІО) передає важливі дані або особисту інформацію понад 1 000 000 осіб; або

Обробник даних передає конфіденційну особисту інформацію понад 10 000 осіб.

Крім того, нові правила збільшують термін дії затвердженої оцінки безпеки з двох до трьох років.

Зони вільної торгівлі

Нові правила передбачають, що зони вільної торгівлі мають повноваження на пілотування політики щодо списків даних, які вимагають оцінки безпеки, стандартного подання контракту або сертифікації (Негативний список). Негативний список може бути експортований за умови схвалення провінційними CAC і повинен бути поданий до центрального CAC і Національного управління даних (NDA) (яке є новостворeним регулюючим органом згідно з Новими правилами). Ці вимоги звільняються від даних, які не входять до Негативного списку.

Компанії повинні будуть ретельно оцінювати всі свої дії з обробки даних у кожному конкретному випадку. Крім того, компаніям потрібно буде оновити свої політики, процедури та процеси, щоб вони відповідали новим правилам, інструкціям, PIPL і DSL». ***(Trisha Sircar. Cybersecurity Administration of China Issues Relaxed Rules for Cross-Border Data Transfers // Katten Muchin Rosenman LLP (https://quickreads.ext.katten.com/post/102j5eb/cybersecurity-administration-of-china-issues-relaxed-rules-for-cross-border-data). 15.04.2024).***

***

Інші країни

«Малайзія сьогодні прийняла законопроект про кібербезпеку 2024 року.

Законопроект був одноголосно прийнятий після третього читання міністром цифрових технологій Гобіндом Сінгхом Део.

Метою законопроекту є посилення кібербезпеки країни шляхом дотримання певних заходів, стандартів і процесів управління загрозами кібербезпеці.

Раніше Гобінд, завершуючи дебати, сказав, що впровадження законопроекту може допомогти уряду забезпечити життєздатність і ефективність Критичної національної інформаційної інфраструктури (CNII) у обробці інцидентів кібербезпеки.

Він сказав, що законопроект має вирішальне значення, оскільки сектор CNII охоплює уряд, банківську справу та фінанси, транспорт, оборону та національну

безпеку, а також інформаційний, комунікаційний та цифровий сектори, які зазвичай є об'єктами кібератак, щоб завдати шкоди уряду.

Також перераховані сфери охорони здоров'я, водопостачання та управління відходами, енергетика, сільське господарство та фермерство, промисловість і торгівля, а також сектори науки, технологій та інновацій.

«Це сектори, які ми вважаємо дуже важливими, і якщо є кіберзагрози, у разі успіху вони можуть мати дуже згубний вплив на країну.

«Отже, нам необхідно побачити, як створити закон, щоб ми могли вжити заходів для того, щоб ці організації CNII були пильними, розуміли ризики та знали, як вживати контрзаходи», — сказав він.

Гобінд додав, що в законопроекті буде прийнято підхід, заснований на оцінці ризику, і визначено захисний контроль проти будь-якої технології, яка використовуватиметься в майбутньому.

«Справді, технологія блокчейн має можливість перевіряти автентичність записів, даних і транзакцій, але ця технологія містить загрози кібербезпеці. Тому ми повинні бути обережними», - сказав він». ***(Dewan Negara passes Cyber Security Bill 2024 // Malay Mail (https://www.malaymail.com/news/malaysia/2024/04/03/dewan-negara-passes-cyber-security-bill-2024/127162). 03.04.2024).***

***

«Будівельний сектор Близького Сходу є вразливим до кіберзлочинності, як підкреслює нещодавнє опитування Freshfields, Accuracy та NYU Abu Dhabi. Ті, хто знаходиться в групі ризику, повинні вжити заходів для підвищення готовності до кібербезпеки.

Двадцять років тому міжнародна будівельна компанія пережила зухвалу спробу вимагання: заплати 50 мільйонів доларів викупу, інакше кранівника застрелять. (На щастя, нікого не застрелили, і ніхто не заплатив 50 мільйонів доларів). На жаль, у сучасному будівельному секторі вимагання є більш поширеним ризиком, але загроза постає у формі кібератак, а не снайперської

гвинтівки. Маючи це на увазі, ми запитали будівельний сектор Близького Сходу, чи здатні вони ефективно боротися з кіберзлочинністю. Відповідь: ні.

Freshfields, Accuracy та Нью-Йоркський університет (Абу-Дабі) нещодавно спільно провели опитування будівельного сектору Близького Сходу, щоб оцінити ризики, з якими стикаються учасники будівельних проектів у зв'язку з кіберзлочинами, і оцінити рівень їх готовності. Опитування проводилося серед респондентів вищої ланки, переважно працюючих у великих компаніях Близького Сходу.

У цьому блозі ми підсумовуємо причини, через які будівельний сектор є вразливим до кібератак, пропонуємо огляд результатів нашого опитування та надаємо деякі рекомендації щодо підвищення готовності до кібербезпеки.

Чому будівництво на Близькому Сході вразливе до кібератак?

На нашу думку, будівельний сектор, особливо на Близькому Сході, є вразливим до кібератак з п'яти основних причин:

Будівельні проекти на Близькому Сході передбачають низку конфіденційних даних, у тому числі інформацію про особу, необхідну для отримання робочих/персоналових віз, потенційно дані розпізнавання відбитків пальців або райдужної оболонки ока для доступу до сайту, банківські реквізити та платіжну інформацію для цілей оплати ланцюжка поставок, а також деталі дизайну, що показують доступ балів за готовий актив. У чужих руках ці дані можуть бути використані в підлих цілях.

Можуть існувати довгі ланцюги поставок – аж до невеликих постачальників і інсталяційних компаній – з конфіденційними даними, що проходять по цьому ланцюгу поставок. Системи, які існують для захисту конфіденційних даних, ефективні лише за найслабшою ланкою в ланцюжку постачання. Само собою зрозуміло, що не кожен постачальник у ланцюжку постачання матиме однаковий рівень кібербезпеки. Крім того, технологія активів зазвичай імпортується, і клієнт може мати обмежену видимість щодо ризику постійного цифрового доступу через виробника.

Як ми знаємо, час – це гроші: будь-які затримки із завершенням можуть мати значні фінансові наслідки. Це створює додаткові важелі для суб'єктів загрози, які можуть використовувати кібератаки, щоб загрожувати хаосу проекту та відстрочити завершення.

Порівняно з багатьма іншими регіонами світу, державні кошти часто залучаються до будівельних проектів на Близькому Сході – прямо чи опосередковано. Це додає політичний вимір, який може створити різні мотиви для суб'єктів загрози.

У будівельному секторі Близького Сходу зараз зростає впровадження технологій, що створює більше можливостей для учасників загроз.

З огляду на ці причини, а також на тлі дослідження IBM про те, що середня вартість витоку даних на Близькому Сході стрімко зростає (середня вартість витоку даних у 2023 році становила 8,07 млн доларів США, покриваючи як прямі, так і непрямі витрати), це Важливо, щоб учасники проекту в будівельному секторі Близького Сходу були достатньо підготовлені до боротьби з кіберризиками. Але чи вони?

Кіберзлочинність зростає, але захист ні

Наше кібератак показало збільшення кількості кібератак на будівельні підприємства після пандемії COVID-19, причому 73 відсотки респондентів повідомили про збільшення кількості кібератак з 2020 року. Однак, перед обличчям зростання злочинності, лише половина респондентів відчували, що що заходи з кібербезпеки їхніх компаній були достатніми, щоб захистити їх від кіберризиків, і лише 13 відсотків побачили, що їхні підприємства доклали значних зусиль для посилення заходів із запобігання кіберзлочинам після пандемії.

Зрозуміло, що навіть великі та досвідчені компанії відчувають себе недостатньо оснащеними для боротьби зі зростаючим ризиком кіберзлочинів. Але які типи атак зазвичай спостерігаються в будівельному секторі?

Види кіберзлочинності

Кіберзлочини стають все більш прогресивними і включають:

Програми-вимагачі: це одна з найбільш руйнівних і дорогих форм кіберзлочинності, коли кіберзлочинці шифрують дані компанії та вимагають оплату в обмін на ключ дешифрування та зобов'язання не розповсюджувати викрадені дані. Дослідження показують, що у 2022 році будівельний сектор був сектором, який найбільше зазнав атак програм-вимагачів у всьому світі.

Схеми соціальної інженерії: кібер-зловмисники видають себе за вище керівництво та ключових постачальників за допомогою тактики зламу ділової електронної пошти (наприклад, використання підробленої електронної пошти, яка виглядає як офіційна, або викрадення електронної пошти постачальника чи облікових записів соціальних мереж). Їх мета — переконати жертв переказати кошти або надати конфіденційну інформацію, яка може бути використана для отримання фінансової вигоди.

Інсайдерські загрози: цей тип атаки виникає, коли хтось усередині організації («інсайдер») (ненавмисно чи навмисно) зловживає системними обліковими даними, які були належним чином авторизовані для використання в організації. Інсайдерські загрози зазвичай призводять до того, що облікові дані компанії або конфіденційні дані стають доступними зовнішнім суб'єктам загрози, які використовують ці дані для незаконного доступу до систем і програмного забезпечення організації в злочинних цілях. Інсайдерські загрози є звичайним способом потрапляння конфіденційних даних компанії в чужі руки.

Різноманітність кіберзлочинів показує, що підготовка до кібербезпеки вимагає багатостороннього розгляду.

Як захистити свій бізнес від кіберзлочинців?

Коротше кажучи, хоча легкого вирішення проблеми немає, є кілька заходів, які компанії можуть і повинні вжити, щоб зменшити ризики кіберзлочинності.

Інвестиції в заходи кібербезпеки

Інвестиції в заходи кібербезпеки вимагають культурних змін, коли керівники вищої ланки та керівники віддають пріоритет кібербезпеці та виділяють як фінансові, так і людські ресурси для захисту своїх активів і операційної цілісності. Це може включати:

- співпрацювати з експертами з кібербезпеки для консультування щодо мінливого ландшафту кіберзагроз;
- виділення додаткових ресурсів на кібербезпеку та підвищення обізнаності в організації;
- відображення даних для забезпечення чіткого розуміння того, де розташовані дані та як взаємодіють системи – як інформаційні технології, так і операційні технології;
- сприяння ефективній культурі кібербезпеки через навчання передовим практикам; і
- робота з юридичним радником для виявлення слабких місць у існуючій політиці та потенціалі. покращення

Технічний контроль і дотримання законодавства

Це може включати:

- розгортання ефективних технічних засобів контролю, включаючи брандмауери, системи виявлення та запобігання вторгненням, антивірусне програмне забезпечення, шифрування та контроль доступу;
- розробка надійних систем резервного копіювання (які регулярно тестуються) для забезпечення стійкості та продовження операцій після атаки програм-вимагачів;
- класифікація даних на основі чутливості, включаючи операційний, регулятивний і репутаційний ризик для організації, а також впровадження належного контролю доступу на основі ризику на основі критичності конкретних даних;
- створення планів реагування на інциденти (і імітаційне навчання інцидентів) у нещасливому випадку порушення;
- вжиття заходів у разі інциденту кібербезпеки для дотримання нормативних вимог та ефективної взаємодії із зацікавленими сторонами без шкоди для правових позицій; і
- проведення розслідувань для визначення причини, масштабу та впливу будь-якого порушення даних.

Учасники проекту на Близькому Сході залишатимуться вразливими до кібератак і витоку даних, доки будівельний сектор у цілому не створить готовність...» ***(Kim Rosenberg and Jodie Reindorf. Cybercrime risk in the Middle East construction industry // Freshfields Bruckhaus Deringer (https://riskandcompliance.freshfields.com/post/102j4a8/cybercrime-risk-in-the-middle-east-construction-industry#page=1). 03.04.2024).***

***

«26 березня 2024 року Чилі прийняло свій головний нормативний акт у сфері кібербезпеки – Рамковий закон про кібербезпеку та інфраструктуру критичної інформації.

Закон має на меті забезпечити захист і безперервність основних послуг у разі кібератаки та накладає певні зобов'язання на приватні компанії та державні служби, які були визначені як оператори таких основних послуг. Він також створює Національне агентство з кібербезпеки (ANCI), яке виконує роль нового регулюючого органу, уповноваженого забезпечувати дотримання закону.

Поки що визначеної дати вступу закону в силу немає. Чилійська правова система дозволяє Президенту Чилі опублікувати указ, що містить додаткову інформацію про впровадження та початок діяльності ANCI, в Офіційному віснику протягом одного року після публікації закону. Відповідно до чилійського закону, регулятори мають шість місяців, щоб визначити дату впровадження закону після публікації закону.

Нижче ми окреслюємо ключові аспекти положення.

Що таке основні служби та хто ними керує?

Основні послуги – це ті, що надаються приватними компаніями, які здійснюють такі види діяльності:

- Виробництво, передача або розподіл електроенергії
- Наземний, повітряний, залізничний або морський транспорт, а також функціонування відповідної інфраструктури

- Телекомунікації, послуги цифрової інфраструктури та послуги інформаційних технологій, якими керують треті сторони
- Транспортування, зберігання або розподіл палива
- Постачання питної води або послуги каналізації
- Банківські, фінансові та платіжні послуги
- Адміністрування виплат соціального страхування
- Поштові та кур'єрські послуги
- Інституційні медичні послуги, що надаються лікарнями, клініками, медичними кабінетами та медичними центрами
- Виробництво або дослідження фармацевтичних продуктів

Основні послуги також включають будь-які послуги, що надаються органами державного управління та Національним координатором електроенергії, а також ті, що надаються в рамках концесії на державні послуги.

Чи можна вважати інші послуги необхідними?

Так. ANCI може використовувати обґрунтовану резолюцію для класифікації інших послуг як необхідних, якщо будь-яке переривання їх нормального функціонування може завдати серйозної шкоди життю або фізичній цілісності 1) населення; 2) відповідні галузі економічної діяльності; 3) середовище; або 4) нормальне функціонування суспільства, уряду, національної оборони або служби безпеки та громадського порядку.

ANCI також може визначати додаткові послуги як важливі через консультації з громадськістю, які повинні проводитися, як це передбачено Законом № 19.880, заходом, який встановлює основу адміністративних процедур, що регулюють дії органів державної адміністрації. Міністерство внутрішніх справ та громадської безпеки видасть постанову, яка визначає необхідні аспекти процедури її правильного виконання.

Окрім перерахованих вище послуг, ANCI також має визначити конкретні інфраструктури, процеси або функції, які вважатимуться важливими.

Про які інциденти постачальники основних послуг зобов'язані повідомляти і кому?

Оператори основних послуг повинні якомога швидше повідомляти групу реагування на інциденти комп'ютерної безпеки про всі серйозні кібератаки чи інциденти кібербезпеки. Серйозні інциденти визначаються як ті, які можуть перервати безперервність основної послуги або вплинути на фізичну цілісність чи здоров'я людей, а також ті, які можуть вплинути на комп'ютерні системи, що містять персональні дані.

Які ще зобов'язання повинні виконувати оператори основних послуг?

Оператори основних послуг повинні постійно впроваджувати заходи (технологічного, організаційного, фізичного чи інформаційного характеру) для запобігання, звітування та вирішення інцидентів кібербезпеки.

Крім того, оператори основних послуг зобов'язані впроваджувати будь-які протоколи та стандарти, встановлені ANCI, і стандарти кібербезпеки, продиктовані відповідним галузевим регулюванням (наприклад, оборона).

ANCI встановлює диференційовані заходи безпеки відповідно до типу відповідної організації, особливо враховуючи характеристики та можливості малих і середніх компаній, як це визначено Законом № 20.416, який встановлює спеціальні правила для менших компаній». ***(Carla Illanes. Chile's Cybersecurity Framework Act: How will it affect private companies? // DLA Piper (https://www.dlapiper.com/en/insights/publications/2024/04/chiles-cybersecurity-framework-act-how-will-it-affect-private-companies). 02.04.2024).***

***

«Багатонаціональний інтернет-гігант Google пообіцяв посилити кібербезпеку, допомогти мікро-, малим і середнім підприємствам (ММСП) і сприяти відповідальному використанню цифрових технологій на Філіппінах.

Зобов'язання було прийнято під час зустрічі президента Фердинанда Р. Маркоса-молодшого з топ-менеджерами Google на полях тристороннього саміту

Філіппін із США та Японією у Вашингтоні в п’ятницю (за манільським часом), заявив міністр комунікацій Челой Гарафіл у своїй заяві. Субота.

Гарафіл сказав, що під час зустрічі Маркос закликав Google активізувати діяльність у галузі кібербезпеки на Філіппінах, зокрема, у сфері регулювання країни.

Маркос закликав Google розробити систему, яка забезпечить ефективні цифрові послуги для всіх філіппінців по всій країні, підкреслюючи прагнення його адміністрації забезпечити безперервне підключення до моря.

«Я намагаюся бути стурбованим, коли ми від моря. Тож, як я вже сказав, ми спробуємо підхопити це, звернемося до вашої організації та допоможемо нам із цим», — сказав Маркос, маючи на увазі урядові програми кібербезпеки, а також ініціативи, інструменти та структуру для посилення захисту кібербезпеки та сприяння безпечніша цифрова екосистема в країні.

Глобальний віце-президент Google із питань уряду та державної політики Каран Бхатія заявив, що Google готовий допомогти Філіппінам у зміцненні їх кібербезпеки, заявивши, що компанія «хотіла б стати частиною» зусиль уряду щодо цифрової трансформації.

Бхатія також висловив намір Google розширити свій бізнес і діяльність на Філіппінах, враховуючи «вражаючий перехід» Філіппін до цифровізації своїх послуг.

«Дозвольте мені, перш за все, сказати, яке враження справило на нас лідерство, яке ви та ваша команда вже продемонстрували в програмі цифрової трансформації. Ми знаємо, що це дуже високий пріоритет для вас, для Філіппін в цілому, але зокрема для уряду», — сказав він Маркосу.

Він сказав, що Google дуже хоче розширити свій бізнес і операції на Філіппінах, де працює близько 50 000 співробітників.

Підвищення кваліфікації ММСП

Бхатія також запевнив Маркоса в прагненні Google допомогти ММСП на Філіппінах розвивати їхній бізнес, посилаючись на партнерство з Міністерством

торгівлі та промисловості (DTI) для підвищення кваліфікації сектора в цифровому середовищі.

«Я б відзначив ту роботу, яку ми ведемо з малим і середнім бізнесом. Отже, це з DTI. Це для того, щоб малий бізнес міг бути присутнім в Інтернеті та з'ясувати, як вони зв'язуються з рештою світу», – сказав він.

Google співпрацює з DTI у розгортанні Google Career Certificates (GCC) у віртуальних кампусах департаменту, охоплюючи понад 1300 центрів DTI Negosyo у 16 регіонах по всій країні.

Це ґрунтується на 40 000 стипендій GCC, які Google раніше розподілив, щоб надати філіппінській молоді, шукачам роботи, підприємцям ММСП і державним службовцям затребувані навички з управління проектами, кібербезпеки, IT-підтримки, аналітики даних, UX-дизайну та цифрового маркетингу.

Відповідальне використання цифрових технологій

Google пообіцяв провести тренінги з відповідального використання цифрових технологій для понад 100 000 дітей та їхніх батьків, які вважаються «найбільш вразливим сектором суспільства».

«Оскільки діти часто знаходяться в Інтернеті протягом тривалого періоду часу, ми повинні переконатися, що вони знають, як використовувати цю технологію. Отже, на даний момент ми беремо участь у навчанні для 100 000 філіппінських дітей і збираємося продовжувати розвивати цю кількість», — сказав він.

Компанія Google на Філіппінах, яка розпочала роботу в 2013 році, підтримує глобальну діяльність інтернет-гіганта, надаючи послуги клієнтської та операційної підтримки в країні». ***(Ruth Abbey Gita-Carlos. Google vows to improve PH cybersecurity, promote responsible tech use // Philippine News Agency (https://www.pna.gov.ph/articles/1222557). 13.04.2024).***

***

«Відповідно до першого звіту про стан кібербезпеки Сінгапуру, опублікованого минулого місяця Агентством кібербезпеки Сінгапуру (CSA),

понад 80 відсотків із 2036 організацій, опитаних у 2023 році, зіткнулися з інцидентом кібербезпеки того року. З них 99 відсотків сказали, що вони зазнали негативних наслідків для своїх операцій, таких як збої в бізнесі, втрата даних і репутаційна шкода. Однією з найпоширеніших атак на кібербезпеку є програмне забезпечення-вимагач, тип шкідливого програмного забезпечення, яке зависає та пошкоджує комп'ютерні системи, яке потім використовується для вимагання грошей.

У звіті зазначено, що найбільшою проблемою у впровадженні кібербезпеки є брак знань і досвіду. Лише кожна третя організація запровадила три чи більше категорій заходів у Cyber Essentials, рекомендованих CSA. За словами CSA, «потрібно зробити ще багато».

З 2021 року Сінгапур зазнав серйозних втрат від атак на кібербезпеку та шахрайства, створюючи значні загрози для окремих осіб, компаній та інфраструктури безпеки країни. Цей коментар також містить дві ключові рекомендації та інші пропозиції щодо протидії атакам на кібербезпеку та шахрайству.

Як випливає зі звіту, за останні кілька років у Сінгапурі спостерігалося помітне збільшення частоти та складності шахрайства та кібератак. Програми-вимагачі, фішинг, інвестиційне шахрайство та шахрайські транзакції стали надзвичайно поширеними. За даними поліції Сінгапуру (SPF), жертви шахраїв у Сінгапурі втратили близько 632 мільйонів сінгапурських доларів у 2021 році, 660 мільйонів сінгапурських доларів у 2022 році та 651 мільйон сінгапурських доларів у 2023 році. Сукупні збитки від шахрайства в місті-державі з 2021 року, ймовірно, скоро перевищать 2 мільярди доларів. По всьому світу кіберзлочинці вразили підприємства та сектори критичної інфраструктури, такі як охорона здоров'я та фінанси, використовуючи вразливі місця в системах і мережах.

Одним із головних факторів цього сплеску атак на кібербезпеку та шахрайства є швидка цифровізація економіки та суспільства Сінгапуру на додаток до зростання кількості злочинців. Сінгапур має один із найвищих показників проникнення Інтернету в світі (99 відсотків), і це також робить сінгапурців

надзвичайно схильними до онлайн-загроз. Технологічний прогрес у сфері комунікацій також розширив поле для атаки онлайн-зловмисників. Шахрайство може здійснюватися за допомогою телефонів і ноутбуків. Атаки на кібербезпеку, такі як використання програм-вимагачів, можна здійснити безшумно та швидко в Інтернеті. Ці кібератаки можуть викрасти заощадження та активи протягом години. Поширення взаємопов'язаних пристроїв, залежність від хмарних сервісів і впровадження нових технологій, таких як Інтернет речей і штучний інтелект, створили нові можливості для використання.

Для подолання цих загроз необхідні дієві заходи. По-перше, підвищення обізнаності громадськості та освітніх програм є найважливішими. Громадяни та компанії повинні володіти знаннями та навичками, щоб ідентифікувати підозрілу діяльність і повідомляти про неї, а також захистити себе від злочинних шахраїв і хакерів. Державні установи, навчальні заклади та приватні організації повинні постійно співпрацювати, щоб своєчасно поширювати інформацію про поширені шахрайства та найкращі практики кібербезпеки.

SPF випускає щотижневі бюлетені щодо шахрайства та Посібник з ресурсів для боротьби з шахрайством, а також створює лінію довіри для боротьби з шахрайством і додаток ScamShield для мобільних телефонів. Місцеві ЗМІ також активно висвітлювали випадки шахрайства у своїх онлайнових та друкованих звітах. Управління розвитку медіакомпанії InfoComm запровадило багаторівневий підхід до боротьби з онлайн-шахрайськими SMS-повідомленнями та шахрайськими дзвінками. Однак шахраї продовжують знаходити нові способи протистояти цьому захисту та розробляти нові методи шахрайства.

Незважаючи на ці зусилля, Сінгапуру необхідно застосувати більш проактивний і ефективний підхід до навчання та озброєння населення відповідними знаннями та навичками, щоб успішно захистити себе. Перша ключова рекомендація полягає в тому, щоб раз на два місяці проводити регулярні асинхронні або синхронні онлайн-навчальні курси з кібербезпеки та боротьби з шахрайством, щоб інформувати, навчати та оновлювати інформацію для всіх громадян і жителів, які потім будуть перевірені на знання та навички. Щоб полегшити навчання, ці основні

курси цифрового захисту можна проводити в стислій та ефективній формі в режимі он-лайн, поєднуючи з відповідним оцінюванням, оперативним відгуком і цілеспрямованим застосуванням знань і навичок.

У результаті люди та організації будуть проінформовані, навчені та перевірені, щоб краще захищатися від шахрайства та атак на кібербезпеку. Як було сформульовано урядовим парламентським комітетом із зв'язку та інформації в січні, Сінгапуру слід прагнути до створення міцніших партнерських стосунків між державним і приватним секторами, а також з окремими особами, щоб поглибити увагу до навчання людей цифровій грамотності, шахрайству та іншим шкідливим діям в Інтернеті.

Зміцнення системи кібербезпеки в країні також є обов'язковим. Сінгапур досяг цілеспрямованих успіхів у цьому відношенні завдяки таким ініціативам, як створення CSA, яке відіграє провідну роль у кібербезпеці в Сінгапурі. Постійне вдосконалення політики, регулярні аудити кібербезпеки, ефективні програми та надійні механізми реагування на інциденти є життєво важливими для того, щоб випереджати загрози, що розвиваються.

Як запропонувало CSA, організаціям необхідно провести перевірку стану кібербезпеки та впровадити Cyber Essentials, щоб забезпечити належну кібергігієну та бути захищеним від кібератак. CSA закликає повністю вжити важливих заходів кібербезпеки, щоб організації не наражалися на непотрібні кіберризики. Виконавчий директор CSA Девід Ко зазначив, що «хоча організації вжили певних заходів для захисту своїх активів, цього недостатньо, враховуючи зростаючу частоту та масштаб кіберзагроз, з якими ми стикаємося сьогодні».

Друга ключова рекомендація полягає в тому, щоб встановити чіткий графік і подальші заходи для впровадження Cyber Essentials CSA для всіх компаній у Сінгапурі. Пропозиція полягає в тому, щоб встановити крайній термін, наприклад, наприкінці цього року, до якого всі директори компаній повинні будуть підписати декларацію про те, що їхні організації запровадили важливі заходи кібербезпеки. Можна проводити вибіркові перевірки, і якщо є прогалини та недоліки, їм слід

надати попередження та вказівки. Враховуючи сотні мільйонів, які втрачаються щороку, Сінгапуру необхідно зайняти сильнішу позицію у зміцненні свого захисту.

Успішне вирішення проблем, пов'язаних із шахрайством, загрозами кібербезпеці та ризиками, спричиненими ШІ, потребує багатогранної співпраці. Країни потребують постійної пильності, постійних зусиль і партнерства між академічними колами, урядом, промисловістю та широким суспільством. Оскільки Сінгапур переживає складні процеси цифрової ери, головним пріоритетом має залишатися захист своїх людей і активів, а також збереження довіри до цієї цифрової інфраструктури. Окремі особи та компанії також повинні регулярно вживати заходів для захисту себе та своїх активів.

Підсумовуючи, сплеск кібератак і шахрайства підкреслює нагальну потребу в проактивних заходах для підвищення стійкості кібербезпеки та освіти. Підвищуючи обізнаність громадськості, зміцнюючи спільні та проактивні зусилля, використовуючи технології та рішення на основі штучного інтелекту, а також посилюючи освіту та навчання, Сінгапур може протистояти ризикам і створити безпечнішу та надійнішу цифрову екосистему для своїх громадян і компаній». ***(Ronald Lee and Edmund Lim. Is Singapore Doing Enough to Safeguard Itself Against Cybersecurity Attacks and Scams? // Diplomat Media Inc. (https://thediplomat.com/2024/04/is-singapore-doing-enough-to-safeguard-itself-against-cybersecurity-attacks-and-scams/). 12.04.2023).***

***

«У 2023 році Об'єднані Арабські Емірати щодня активно відбивали понад 50 тис. кібератак, пояснили в Раді з кібербезпеки ОАЕ. За перші три квартали того ж року країна успішно запобігла понад 71 мільйону спроб атак. Відповідно до звіту Frost & Sullivan, індустрія кібербезпеки GCC продовжує зростати, за оцінками F&S, її вартість потроїться до 2030 року та досягне 13,4 мільярдів доларів США, такі країни, як ОАЕ та Саудівська Аравія, продовжують зменшувати свою залежність від експорту нафти та натомість обирають цифрові інструменти та технології.

Проблеми, пов’язані з поінформованістю та дефіцитом кваліфікованих професіоналів, а також брак ясності серед компаній щодо активної боротьби з кібератаками, сприяють існуючим викликам із збільшенням залежності від технологій. У відповідь на ці загальногалузеві недоліки та в той час, як регіон продовжує перебудовувати глобальні технології, країни Близького Сходу вживають помітних кроків для підвищення рівня кібербезпеки. Оскільки цього місяця наближається Gisec, найбільша подія з кібербезпеки на Близькому Сході, яка відбудеться в Дубаї з 23 по 25 квітня, лідери з кібербезпеки матимуть можливість вивчити потенціал ринку кібербезпеки Близького Сходу та визначити проблеми та можливості, з якими стикається індустрія, що розвивається в регіоні.

«Минулий рік ознаменувався загальним зростанням державних атак через геополітичні конфлікти. Поширення штучного інтелекту також зростає і значно вплинуло на те, як можна було підвищити кібербезпеку, водночас дозволяючи кіберзлочинцям, які добре знають ШІ, здійснювати більш витончені атаки на своїх жертв, що ускладнює їх виявлення та захист від них. Уразливості Інтернету речей (IoT) також зростають. За даними Statista, у 2023 році кількість пристроїв IoT перевищила 15 мільярдів. Атаки програм-вимагачів також зросли у 2023 році, ймовірно, через їх уявну прибутковість. Хмара також зростає експоненціально завдяки багатьом подіям, які відбуваються в хмарі. Ця постійна поява хмарних середовищ значно вплинула на розробку додатків і пов’язану з ними архітектуру безпеки. Хмарні середовища за своєю природою часто складаються зі швидких циклів DevOps, що позбавляє розробників додатків потреби належним чином підтримувати безпечні додатки», — сказав Муат АльХомуд, директор відділу кібербезпеки D360 Bank.

Оскільки Близький Схід продовжує розвивати надійну інфраструктуру кібербезпеки та економіку, він залишається одним із найперспективніших глобальних регіонів для розвитку галузі; її відданість регулюванню, навчанню з кібербезпеки та безпеці ланцюга постачання виділяють її як лідера галузі з амбітним баченням інтеграції технологій і задоволення потреб клієнтів, що постійно розвиваються. Майбутня виставка GISEC Global 2024, організована

DWTC і організована Радою кібербезпеки ОАЕ, є свідченням того, що ОАЕ віддають пріоритет співпраці, інноваціям і розвитку талантів.

«Лідери в галузі кібербезпеки отримують переваги від GISEC, отримуючи доступ до останніх галузевих тенденцій, ідей та інновацій, що дозволяє їм залишатися попереду в кібернетичному середовищі, що швидко розвивається. Подія слугує плавильним котлом ідей і рішень, пропонуючи лідерам інструменти та знання, необхідні для посилення кіберзахисту їхніх організацій», – пояснив д-р Рім Фарадж АльШаммарі, голова та співзасновник Women in CyberSecurity MiddleEast.

«Відомий факт, що наш Близькосхідний регіон постійно стикається з різними проблемами кібербезпеки, включаючи складні кібератаки, спрямовані на критично важливу інфраструктуру, потребу в покращенні управління кібербезпекою та нормативних актах, а також скорочення розриву в навичках робочої сили з кібербезпеки. GISEC вирішує багато з цих питань, надаючи платформу для діалогу, співпраці та обміну передовим досвідом між міжнародними та регіональними фахівцями з кібербезпеки. Завдяки комплексному порядку денному цього року та стратегічним партнерствам GISEC більше не розглядається як просто конференція, а як один із провідних регіональних центрів для підвищення стійкості кібербезпеки та досвіду в нашому регіоні Близького Сходу». ***(Andrea Benito. Regulation remains the strongest multiplier to cybersecurity growth // IDG Communications, Inc. (https://www.cio.com/article/2088676/regulation-remains-the-strongest-multiplier-to-cybersecurity-growth.html). 11.04.2024).***

***

«БЛИЗЬКО 87% філіппінців високо схвально ставляться до зміцнення кібербезпеки та захисту конфіденційності даних на тлі порушень безпеки державних мереж Філіппін, показало нове опитування PUBLiCUS Asia, Inc.

Консалтингова фірма заявила, що заслуговує на увагу підтримка посилення кібербезпеки в країні, особливо в таких регіонах, як Visayas, серед вікової групи 50-59 років і серед людей з високим рівнем доходу.

З минулого тижня веб-сервери державних установ зазнали кібератак, останніми жертвами витоку даних стали Департамент науки і технологій (DoST) і Митне управління (BoC). Серед найбільших кібератак були кібератаки на державну Філіппінську корпорацію медичного страхування (PhilHealth) наприкінці минулого та на початку цього року.

«Громадськість хоче, щоб уряд звернув увагу на зростаючу стурбованість проти кіберзлочинів, пов'язаних із хакерством, компрометацією даних та іншими пов'язаними проблемами», – сказав Рональд Б. Густіло, учасник національної кампанії Digital Pinoys у Viber у відповідь на останнє опитування.

За його словами, держава повинна виділити кошти на інструменти кібербезпеки та найняти експертів, які гарантуватимуть, що інфраструктура кібербезпеки країни буде безпечною та зможе відбивати атаки.

Більше про опитування, PUBLiCUS Asia сказав, що його опитування PAHAYAG за перший квартал 1500 респондентів показало, що окрім кібербезпеки, економічні ініціативи були одними з головних пріоритетів філіппінців, хоча це також відображало невелику підтримку змін економічної хартії або «ча-ча» через народна ініціатива лише 28%

Друге за величиною схвалення серед філіппінців — 78% — ухвалення Сенатом мінімальної денної заробітної плати в 100 песо в приватному секторі, а потім запропонований перегляд Програми безкоштовної вищої освіти в усіх державних і місцевих університетах і коледжах — 74%.

Встановлення прожиткового мінімуму та розподіл різної матеріальної допомоги підтримали 72% та 69% відповідно.

Після цього було укладено Угоду про взаємний доступ між Японією на рівні 64% і президентом Фердинандом Р. Маркосом-молодшим, який продовжив кінцевий термін для консолідації громадських транспортних засобів на рівні 61%.

Серед найменш сприятливих національних питань були дозволи Міжнародному кримінальному суду заарештувати колишнього президента Родріго Р. Дутерте, віце-президента Сару З. Дутерте-Карпіо, сенатора Бато дела Роса тощо

(28%) та введення непрограмованих коштів у розмірі 800 мільярдів песо. у держбюджеті на 2024 рік (22%).

Під час дослідження респондентам із столичного регіону, Північного Центрального Лусона, Південного Лусона, Вісайських островів і Мінданао було запропоновано оцінити проблеми від одного до п’яти, де одна – категорично несхвалена, а п’ять – категорично схвалена.

Похибка становить 3%...» ***(Poll says Filipinos most concerned about cybersecurity, data privacy // BusinessWorld Publishing (https://www.bworldonline.com/the-nation/2024/04/10/587147/poll-says-filipinos-most-concerned-about-cyber-security-data-privacy/). 10.04.2024).***

***

«Комісія зі зв’язку Нігерії (NCC) порадила абонентам телекомунікацій обирати надійні паролі, щоб запобігти несанкціонованому доступу до своїх мобільних пристроїв.

Цю пораду NCC повідомила на своїй офіційній сторінці у Facebook.

Кібербезпека залишається однією з великих проблем, з якими стикається цифровий простір Нігерії, але NCC вважає, що за допомогою свідомих зусиль із загрозою безпеці можна впоратися.

Уряд та його відповідні відомства також докладають зусиль для ефективної боротьби з загрозою.

NCC є провідною організацією, яка займається створенням сприятливого середовища для зацікавлених сторін галузі та забезпеченням захисту абонентів телекомунікацій від кіберзагроз.

Комісія регулярно ділиться цінною інформацією з нігерійськими абонентами телекомунікацій, пропонуючи поради щодо того, як залишатися в безпеці в цифровому просторі.

NCC поділився нещодавнім оновленням, у якому зосереджено увагу на тому, як можна запобігти кібератакам, наголошуючи на важливості створення надійних паролів для захисту онлайн-акаунтів.

Комісія закликала абонентів переконатися, що вони мають пароль для безпечного входу.

NCC написав на своїй офіційній сторінці у Facebook: «Захистіть свої онлайн-рахунки (такі як банки та цифрові медіа) за допомогою надійних і складних паролів».

Він вважає, що, обираючи надійні паролі, люди можуть захистити себе від кібератак». ***(John Owen Nwachukwu. Cyber security: NCC advises telecom users on ways to beat hackers // Daily Post Media Ltd (https://dailypost.ng/2024/04/16/cyber-security-ncc-advises-telecom-users-on-ways-to-beat-hackers/). 16.04.2024).***

***

«Асоціація судноплавства Сінгапуру (SSA) оголосила про запуск MaritimeSG Shipping CyberSafe Scorecard. Ця індустріальна ініціатива, яка отримала підтримку Управління морського та портового судноплавства Сінгапуру (MPA) та галузевих експертів, дозволяє власникам, менеджерам і операторам суден проводити самооцінку через онлайн-портал www.scissor.sg, який вимірює рівень кібернетичної безпеки. готовність до безпеки роботи їхнього флоту.

Кіберризики для систем і операцій суден зростають. Індивідуальна система показників допомагає судноплавним компаніям оцінити ці ризики. Система показників надає інформацію про сфери, які потрібно вдосконалити, і дозволяє вчасно пом’якшити наслідки. Система показників використовує створений Національний інститут стандартів і технологій США

(NIST) Компоненти кібербезпеки Framework Identify, Protect, Detect, Respond і Recover, що забезпечує спільну мову та системний підхід для морських компаній будь-якого розміру, щоб краще розуміти, керувати та зменшувати ризики кібербезпеки операцій суден.

Понад 30 морських компаній, включаючи таких лідерів галузі, як OSM Thome, Pacific International Lines, PCL і BW Group, завершили самооцінку на пілотному етапі. З часом SSA використовуватиме анонімні дані, щоб отримати

інформацію про тенденції в галузі. Це забезпечує базу для зареєстрованих компаній для порівняння з іншими аналогами. Майбутні плани щодо цієї ініціативи включають запровадження автоматизованого процесу запитів на страхування кібербезпеки, що дозволить використовувати варіанти покриття кібербезпеки.

Пан Т. С. Тео, голова Комітету з цифровізації SSA, який керував розробкою цієї ініціативи, сказав: «Щоб Сінгапур залишався центром надійних і стійких морських операцій, вкрай важливо, щоб галузь зміцнила свою позицію в галузі кібербезпеки. Зараз на ринку немає нічого, що дозволило б компаніям проводити таку оцінку.

«Система показників є основою для будь-якої компанії для планування та здійснення довгострокових заходів для підвищення рівня готовності до кібербезпеки. Таким чином, запуск MaritimeSG Shipping CyberSafe Scorecard знаменує ключовий момент на шляху нашої галузі до кіберстійкості. Забезпечуючи комплексну систему оцінки, ми не лише підвищуємо обізнаність, але й надаємо компаніям можливість проактивно захищати свої цифрові активи, сприяючи розвитку культури готовності до кібербезпеки, яка має вирішальне значення для сталого зростання морської торгівлі». ***(SSA launches new cyber security readiness self-assessment tool // Elaborate Communications Limited (https://shipmanagementinternational.com/ssa-launches-new-cyber-security-readiness-self-assessment-tool/)/ 20/04/2024)/***

***

«Згідно з останнім опитуванням QBE SME для Сінгапуру, малі та середні підприємства (МСП) у Сінгапурі демонструють тривожне зниження обізнаності про кібербезпеку, де зростає їх кількість, яка працює без будь-якого захисту від кіберзагроз.

Опитування показало, що лише 47% малих і середніх підприємств у Сінгапурі були повністю поінформовані про потенційні ризики кібербезпеки цього року, що є значним падінням порівняно з 57%, зафіксованими в попередньому році.

Викликає тривогу те, що 19% малих і середніх підприємств вказали, що не мають захисту від ризиків кібербезпеки, що більш ніж удвічі перевищує 9% минулого року.

У звіті також окреслено основні ризики для кібербезпеки на думку МСП. Зловмисне програмне забезпечення лідирує в списку, за ним йдуть витоки даних, а фішинг і смішинг завершують трійку головних загроз.

Цікаво, що опитування відзначило зменшення кількості МСП, які постраждали від кіберінцидентів: 25% повідомили про кіберподії цього року порівняно з 38% минулого року. За даними QBE, ця тенденція до зниження кількості зареєстрованих інцидентів може сприяти зниженню обізнаності про кібербезпеку серед малих підприємств.

«Ця цифра показує, наскільки МСП можуть бути вразливими до кіберризиків, і підкреслює необхідність для компаній навчатися, підвищувати кваліфікацію та захищати себе в цій сфері», — сказав Шун Куан Го, керівник відділу роздрібної торгівлі МСП у QBE Singapore. «Бізнес не може дозволити собі бути самовдоволеним щодо кібербезпеки. Справа в тому, коли, а не в тому, чи станеться кіберзлом».

Опитування QBE також вивчало, як МСП захищають себе від кіберзагроз. Найпоширенішою формою захисту були програмні рішення, ними користуються 59% підприємств. Інші заходи захисту включали навчання персоналу (46%), спеціалізований персонал із кібербезпеки (44%) та внутрішню політику щодо обробки потенційних ризиків (43%).

Незважаючи на ризики, лише 38% МСП повідомили про страхування кібербезпеки. Однак більше половини (55%) висловили зацікавленість у придбанні кіберстрахування цього року, що свідчить про зростаюче усвідомлення необхідності зниження ризиків у цій сфері.

Результати були засновані на відповідях 605 керівників малого та середнього бізнесу в Сінгапурі, опитаних у період з грудня 2023 року по січень 2024 року.

У звіті підкреслюється критична потреба для малих і середніх підприємств у Сінгапурі вживати активних заходів для захисту своїх цифрових активів та

інфраструктури. Оскільки кіберзагрози продовжують розвиватися, підприємствам настійно рекомендується приділяти пріоритет обізнаності про кібербезпеку та впроваджувати комплексні стратегії безпеки, щоб мінімізувати потенційні ризики». ***(Jewel Stolarchuk. Singapore SMEs show worrying decline in cybersecurity awareness, new survey finds // The Independent News & Media Pte Ltd (https://theindependent.sg/singapore-smes-show-worrying-decline-in-cybersecurity-awareness-new-survey-finds/). 25.04.2024).***

***

Кіберстрахування

«Останні кілька років були важкими для фахівців з кібербезпеки. Натиск нових інновацій та еволюції атак підвищив ризик атаки — і витрати. Більше організацій, ніж будь-коли, намагаються передати частину цього ризику через кіберстрахування.

Проте поліси кіберстрахування, які колись було легко отримати та були надійними, стало складно отримати, їх складно підтримувати, а підтримувати дорого. Премії різко зросли, тоді як постачальники полісів посилили необхідні засоби контролю, необхідні організаціям, щоб отримати право на покриття. Це складний страховий ландшафт, у якому організації намагаються орієнтуватися, стикаючись із щоденними загрозами з боку глобальних противників.

Одним із рішень, яке може допомогти організації швидко зупинити атаку та відновити бізнес-операції, є реагування на інциденти (IR), яке також може допомогти їй забезпечити високоякісний поліс кіберстрахування.

Що таке відповідь на інцидент?

IR — це набір процесів та інструментів, які використовуються для виявлення, стримування та усунення кібератак, а також для відновлення роботи організації до інциденту. Це процес:

- Захист середовища шляхом усунення доступу суб’єкта загрози;

- Аналіз причини та масштабів діяльності суб'єкта загрози всередині мережі; і
- Відновлення мережі до її стану до інциденту (включаючи переговори про викуп і оплату, якщо необхідно).

Кожна частина процесу виконується одночасно та залежить від інших частин і інформує їх. Існує кілька типів експертів у сфері реагування на інциденти. Наприклад, деякі служби реагування зосереджені на криміналістичному аналізі, а інші спеціалізуються на відновленні даних і системі.

Усі члени команди повинні працювати в унісон, співпрацюючи та спілкуючись протягом усього процесу, щоб швидко відновити роботу бізнесу з мінімальними витратами.

Чому страховики цінують IR

Ще десять років тому кіберстрахування було ринковою нішою, де лише кілька перевізників пропонували поліси приблизно чверті організацій США. За останні роки кількість опублікованих вразливостей і спроб кібератак стрімко зросла, що призвело до сплеску нових шукачів політики, оскільки організації захищали свою політику протягом попередніх 12 місяців.

У міру того, як страховики заповнювали більше полісів, вони прагнули правильного розміру ринку через зростання кількості атак програм-вимагачів, які встановили нові рекорди за кількома атаками та середні вимоги щодо викупу. Середній початковий запит на викуп за випадки, які розслідує Arctic Wolf Incident Response у 2023 році, становив 600 000 доларів США.

Основний фокус цих зусиль щодо правильного розміру зосереджувався на створенні нових вимог, яким організації повинні відповідати, щоб отримати або підтримувати політику. Поліси кіберстрахування тепер відповідають стандартам перевірки та оцінки, які застосовуються до полісів страхування житла, автомобіля, бізнесу та життя, і експерти очікують, що незабаром вони затьмарять їх, оскільки кіберландшафт продовжує розвиватися протягом наступних років.

Зараз кіберстрахувальники схильні відносити організації до «відер ризиків». Ті організації, які перевірили впровадження основних засобів контролю, таких як

багатофакторна автентифікація, керування виправленнями та створення плану інфрачервоного зв'язку, подолали бар'єр входу та можуть отримати поліс кіберстрахування. Однак це мінімальні вимоги, і вони не призведуть до винагороди організацій премією чи елітним полісом.

Щоб організація опинилася в «елітному» сегменті ризиків, де премії є найдоступнішими, а покриття найповнішим, їй потрібно буде піти набагато далі, досягнувши значного прогресу на шляху безпеки завдяки впровадженню проактивних Рішення для операцій безпеки, які забезпечують цілодобовий моніторинг, виявлення та реагування на кібератаки в режимі реального часу, надійне управління вразливістю та ризиками, а також практичне навчання з питань безпеки для користувачів, щоб допомогти їм мінімізувати людський ризик і запобігти атакам соціальної інженерії, таким як фішинг.

IR — це ще одне рішення, яке може перекинути організацію в це елітне відро. Оцінюючи профіль ризику організації, страховики знають, що бізнес має швидкий доступ до команди експертів із реагування та виправлення, які можуть допомогти у всьому, від відновлення резервних копій до цифрової криміналістики та переговорів із суб'єктами загроз, якщо це необхідно.

Цей різновид повнофункціонального IR зменшує збиток і, отже, зменшує витрати, які страховик може попросити покрити. Через це, якщо організація має IR-послуги на утриманні, вона може опинитися в елітному відрі ризику, маючи доступ до найкращих доступних політик і премій.

Оцінка IR-провайдерів і утримувачів

Щоб повністю викорінити загрозу та відновити нормальну бізнес-операцію — і мати найкращі шанси, що постачальники послуг кіберстрахування віднесуть вас до цієї елітної групи ризиків — компаніям потрібен постачальник повного спектру послуг IR. Видалити загрозу недостатньо. Натомість пошук основної причини, документування того, що трапилося, і відновлення бізнес-операцій до умов, що передували інциденту, є життєво важливими в кожному сценарії реагування, щоб відновити роботу організації та запобігти майбутнім інцидентам.

IR доступний у різних постачальників, кожен з яких пропонує послуги безпосередньо організаціям — деякі навіть через самих операторів кіберстрахування. Незалежно від того, кого ви виберете, обов'язково виберіть постачальника повного спектру послуг із власним досвідом, який може надати комплексні послуги цифрової експертизи та відновлення даних. Лише постачальники повного спектру послуг усувають доступ зловмисника до середовища, аналізують ступінь атаки та відновлюють роботу бізнесу до нормального функціонування до інциденту.

Для ефективного досягнення всіх трьох цілей потрібна фірма з IR з багатогранною командою власних експертів. Координація всієї команди та з клієнтом є життєво важливою для процесу реагування, і кожен, від центру безпеки до зали засідань, має розуміти статус розслідування та важливість висновків.

Крім того, використання ІЧ-сервісів часто є затримкою.

Традиційно це означало попередню покупку певної кількості годин, які ви використовуєте або втрачаєте протягом року. Однак нові моделі фіксаторів, як-от Arctic Wolf від IR JumpStart Retainer, забезпечують проактивне IR-планування з годинним часом відповіді та без передплачених годин, забезпечуючи пріоритетний доступ без попередніх витрат…» ***(Cybersecurity insurance – why having incident response is crucial // NewsCentral Media (https://techcentral.co.za/cybersecurity-insurance-incident-response/242821/). 12.04.2024).***

***

«В останньому звіті Mineta Transportation Institute (MTI) досліджуються зміни в ландшафті кіберризиків, реакція страхового ринку та громадських транспортних агентств на ці зміни та надаються рекомендації щодо того, як різні сегменти ринку можуть продовжувати допомагати керувати ризиками катастрофічна втрата.

Доповідь Чи є світло в кінці тунелю? Перспективи страхування кібербезпеки та транзиту в 2024 році досліджують питання, пов'язані з кіберризиками, і стверджують, що:

Атаки на кібербезпеку та загрози критичній інфраструктурі Сполучених Штатів викликають серйозне занепокоєння, оскільки вони можуть мати значні наслідки для економіки, національної безпеки та громадської безпеки.

З червня 2020 року кількість щотижневих атак програм-вимагачів збільшилася на 186 відсотків порівняно з минулим роком. У Північній Америці атаки сталися на транспортні агентства в Каліфорнії, Колорадо, Канзасі, Нью-Йорку, Техасі, Вашингтоні та багатьох містах Канади. лише за останні кілька років.

Разом зі зростанням кількості кібератак, відбулося відповідне зростання кількості страхових відшкодувань у сфері кібербезпеки, і практика страхування кібербезпеки адаптується. Зміни також збільшують витрати на покриття втраченого бізнесу, виявлення та ескалацію, реагування після порушення та сповіщення.

У звіті автори, Скотт Белчер, науковий співробітник MTI та співзасновник Cybrbase, LLC, і Тодд Чоллет, виконавчий директор SFB Consulting, LLC, зазначають: «Агентства громадського транспорту, які зараз не сприймають ризики кібербезпеки серйозно, повинні інвестувати у розумінні їхнього впливу та вжиття заходів для створення більш стійких програм кібербезпеки. Це означає, що вони повинні визнавати кіберризик частиною загального управління ризиками підприємства. На щастя, кошти та послуги доступні, щоб допомогти».

Автори продовжують пояснювати, що наразі дискреційні грантові програми мають вимоги до кібербезпеки, а формульні грантові програми — ні. Таким чином, «наявність вимог до обох спонукатиме невеликі агентства до впровадження програм кібербезпеки».

MTI каже, що кількість кібератак зростає, а також зросла кількість успішних атак і середня вартість відновлення після них. Страховка адаптується. Кожен оператор, опитаний для дослідження, вказав, що їхні витрати на покриття зросли на 100-200 відсотків після 2020 року. У звіті робиться висновок, що транспортні агентства можуть отримати користь від глибшого розуміння ландшафту загроз, їх вартості для галузі та того, як найкраще підійти до безпеки в епоху цифрових технологій..

За даними MTI, хоча кількість кібератак зросла в геометричній прогресії, більшу стурбованість для більшості транспортних агентств викликає кількість успішних атак і середня вартість відновлення після них. Багато транспортних операторів вжили заходів, щоб підвищити свою стійкість до кібернетики, тоді як інші продовжують припускати, що вони не стануть ціллю. Страхові компанії обмежили покриття, відкоригували вартість покриття, посилили андеррайтинг і навіть пішли з ринку. Регулятори відповіли посиленням освіти, ресурсами та введенням основних вимог щодо кібербезпеки». ***(Latest MTI report outlines changing pattern in transit cybersecurity risk and how to manage it // Mass Transit (https://www.masstransitmag.com/safety-security/press-release/55020891/mineta-transportation-institute-mti-latest-mti-report-outlines-changing-pattern-in-transit-cybersecurity-risk-and-how-to-manage-it). 25.04.2024).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Адміністрація Байдена готується вдатися до незвичайного кроку – видати наказ, який заборонить компаніям і громадянам США використовувати програмне забезпечення, виготовлене великою російською фірмою з кібербезпеки, через занепокоєння національною безпекою, повідомили CNN п'ятеро американських чиновників, знайомих із цим питанням.

Цей крок, який завершується і може відбутися вже цього місяця, передбачає використання відносно нових повноважень Міністерства торгівлі, заснованих на указах, підписаних президентами Джо Байденом і Дональдом Трампом, щоб заборонити «Лабораторії Касперського» надавати певні продукти та послуги в США, сказали джерела.

Урядовим установам США вже заборонено використовувати програмне забезпечення Лабораторії Касперського, але дії, спрямовані на те, щоб заборонити приватним компаніям використовувати програмне забезпечення, були б

безпрецедентними. Джерела попередили, що нічого остаточного поки не буде оголошено, але Міністерство торгівлі прийняло «початкове рішення» заборонити певні транзакції між російською компанією та американськими особами, повідомили джерела.

Це остання спроба уряду США використати свої величезні регуляторні повноваження, щоб запобігти використанню американцями популярних технологій, які офіційні особи США вважають загрозою національній безпеці. Це відбувається в той момент, коли Сенат розглядає законопроект, який змусить TikTok, що належить Китаю, знайти нового власника або зіткнеться з забороною США.

Джерела, обізнані з політичним процесом, повідомили CNN, що однією з цілей указу буде пом'якшити будь-який ризик для критичної інфраструктури США. За словами джерела, яке переглядало проект, проект початкового рішення щодо заборони певного програмного забезпечення Касперського, який поширювався минулого року, стосувався громадян США, але міг бути змінений.

Джерела відмовилися розповісти повний обсяг будь-якого остаточного наказу проти продуктів Kaspersky, але очікується, що він буде зосереджений на антивірусному програмному забезпеченні фірми.

Представник «Лабораторії Касперського» не відповів на питання про можливу заборону або про те, наскільки велика частка компанії на ринку США.

Представник Міністерства торгівлі відмовився коментувати будь-які потенційні дії, пов'язані з продуктами Kaspersky.

Американські офіційні особи протягом багатьох років стверджували, що російський уряд може змусити «Лабораторію Касперського» передати дані або використати своє антивірусне програмне забезпечення для спроби злому або стеження за американцями — звинувачення, які «Лабораторія Касперського» рішуче заперечує.

Згідно із законодавством США, «Лабораторія Касперського» може оскаржити «початкове рішення» щодо заборони використання її продуктів або укласти угоду з урядом, яка пом'якшить занепокоєння щодо безпеки США, до оголошення будь-якого остаточного рішення з боку Комерції.

Посадовці Міністерства торгівлі повинні ретельно проаналізувати, наскільки практичними будуть будь-які подібні правила для Департаменту та для користувачів. Наприклад, було б мало сенсу змусити невеликий бізнес десь в Америці видалити програмне забезпечення Kaspersky, якщо воно було руйнівним і бізнес не мав жодного відношення до національної безпеки.

За даними компанії, програмними продуктами «Лабораторії Касперського» користуються понад 400 мільйонів людей і 240 000 компаній у всьому світі. Скільки з цих людей і компаній знаходяться в США, невідомо. Але офіційні особи США вважають, що ризик, який представляє програмне забезпечення для інфраструктури США, достатньо високий, щоб виправдати незавершене замовлення.

«Нова ера» в регулюванні торгівлі

У 2017 році адміністрація Трампа змусила федеральні цивільні агентства США видалити програмне забезпечення «Лабораторії Касперського» зі своїх мереж, а пізніше Конгрес кодифікував цю заборону та застосував її до військових мереж США. Але очікуваний крок адміністрації Байдена піде на крок далі, використовуючи органи Міністерства торгівлі, щоб перешкодити приватним компаніям використовувати програмне забезпечення Лабораторії Касперського.

Торговельні органи є відносно новими і частково випливають із указу 2021 року, який Байден підписав від імені захисту персональних даних американців від «іноземних ворогів», і пов’язаного з ним указу, підписаного Трампом у 2019 році.

Обидва накази посилаються на «надзвичайний стан національного масштабу», пов’язаний із загрозами безпеці для американського ланцюжка поставок програмного забезпечення та здатність міністра торгівлі переглядати ризиковані транзакції відповідно до закону 1977 року, відомого як Закон про міжнародні надзвичайні економічні повноваження. секретар може заборонити або пом’якшити ризик транзакцій, пов’язаних із ланцюгом поставок інформаційно-комунікаційних технологій Зокрема, відповідно до оновленого закону на основі двох виконавчих указів,.

Минулого року The Wall Street Journal повідомила, що Міністерство торгівлі намагається обмежити використання програмного забезпечення «Лабораторії Касперського», використовуючи свої повноваження, але жодного рішення щодо цього прийнято не було.

Але після кількох місяців обговорень того, як ефективно використовувати регулятивні повноваження Міністерства торгівлі проти використання програмного забезпечення «Лабораторії Касперського», офіційні особи США нарешті готуються використовувати владу, повідомив CNN американський чиновник, знайомий з приватними дискусіями.

Зазначені дії «сигналізують нову еру, в якій комерція буде більш охоче втручатися в ім'я захисту національної безпеки», — сказав CNN Генрі Янг, колишній старший радник Міністерства торгівлі.

Компанії, які «володіють або контролюються іноземним супротивником, повинні взяти до відома», якщо міністр торгівлі демонструє «готовність заборонити операції, які створюють неприйнятний ризик для національної безпеки США», — сказав Янг, який зараз є старшим директором з політики в Business Software Alliance., промислове лобі.

Міністерство торгівлі прагне використовувати свої повноваження якомога точніше, щоб вирішувати проблеми національної безпеки, не маючи негативного впливу на американський бізнес або споживачів, повідомив CNN офіційний представник Міністерства торгівлі. Чиновник обговорив загальний підхід департаменту до регулювання технологічних транзакцій, а не якісь конкретні потенційні дії.

«Ми будемо робити те, що спрямоване на загрозу національній безпеці, і не більше», — сказав представник Міністерства торгівлі. «Якщо це означає: X, Y, Z оператори критичної інфраструктури в секторах високого ризику, ви не можете використовувати це програмне забезпечення, і цей постачальник програмного забезпечення не може здійснювати з вами операції, тоді ми це зробимо. І якщо потрібно буде ширше, ми це зробимо».

Головний гравець у сфері кібербезпеки

Заснована в Москві в 1997 році, «Лабораторія Касперського» стала однією з найуспішніших у світі компаній, що займаються розробкою антивірусного програмного забезпечення, поряд із американськими конкурентами, такими як McAfee і Symantec. Дослідники «Лабораторії Касперського», визнані лідерами індустрії кібербезпеки, відомі тим, що аналізують хакерські операції, які, ймовірно, здійснюють низка урядів, включаючи Росію, США та Ізраїль, а також загрози кіберзлочинців, які впливають на звичайних користувачів.

Деякі припущення та підозри офіційних осіб США щодо російської компанії зосереджені навколо Євгена Касперського, харизматичного комп'ютерного експерта, який став співзасновником Лабораторії Касперського в Москві в 1997 році.

Євген Касперський вивчав криптографію в університеті, спонсорованому КДБ — факт, який деякі американські законодавці люблять згадувати, намагаючись пов'язати компанію з російським урядом. «Лабораторія Касперського» заперечує «будь-які неетичні зв'язки чи приналежність до будь-якого уряду, включаючи Росію». Після закінчення навчання Касперський працював інженером-програмістом в російському інституті Міністерства оборони, і це «обсяг його військового досвіду», кажуть у компанії.

Касперський поскаржився, що його компанія є жертвою геополітичної напруженості між Заходом і Росією — напруги, яка лише загострилася після повномасштабного вторгнення Кремля в Україну в 2022 році.

Але, незважаючи на судові баталії та роки гарячої риторики, відносини «Лабораторії Касперського» з урядом США не завжди були гострими. Повідомлення компанії уряду США зрештою призвело до арешту в 2016 році підрядника Агентства національної безпеки на ім'я Гарольд Мартін, якого було засуджено за звинуваченнями у крадіжці секретної інформації, повідомляє Politico.

Але інший зареєстрований інцидент, пов'язаний з іншим підрядником АНБ, не зміг пом'якшити підозри офіційних осіб США щодо російської фірми програмного забезпечення.

Хакери, які працювали на російський уряд у 2015 році, викрали файли про кібероперації США в іншого підрядника АНБ, повідомляв Wall Street Journal у 2017 році. Схоже, російські хакери націлилися на підрядника після ідентифікації файлів за допомогою підрядника за допомогою програмного забезпечення Лабораторії Касперського, повідомляє журнал з посиланням на людей, знайомих з інцидентом.

У заяві «Лабораторії Касперського» тоді говорилося, що компанії «не було надано жодної інформації чи доказів, які б підтверджували цей передбачуваний інцидент, і, як наслідок, ми повинні вважати, що це ще один приклад неправдивого звинувачення». ***(Sean Lyngaas. Biden administration preparing to prevent Americans from using Russian-made software over national security concern // Cable News Network (https://edition.cnn.com/2024/04/09/politics/biden-administration-americans-russian-software/index.html). 09.04.2024).***

***

«Агентство з кібербезпеки та безпеки інфраструктури США заявило, що підтримувані російським урядом хакери використали їхній доступ до Microsoft (MSFT.O) системи електронної пошти для викрадення листування між чиновниками та технічним гігантом, надзвичайна директива спостерігача США, опублікованого в четвер.

У директиві від 2 квітня агентство попередило, що хакери використовували дані автентифікації, надіслані електронною поштою, щоб спробувати зламати клієнтські системи Microsoft, включаючи системи невизначеної кількості державних установ.

Попередження про те, що урядові установи стають мішенню за допомогою вкрадених електронних листів Microsoft, виникло після оголошення компанії в березні про те, що вона все ще бореться зі зловмисниками, яких вона назвала «Опівнічна хуртовина».

Це розголошення, яке викликало тривогу в галузі кібербезпеки, послідувало лише минулого тижня звітом Комітету з аналізу кібербезпеки США, в якому говорилося, що окремому злому, звинуваченому в Китаї, можна було запобігти,

звинувативши компанію в помилках у кібербезпеці та свідома відсутність прозорості.

CISA відмовився назвати агентства, які могли постраждати. Microsoft повідомила в електронному листі, що «працює з нашими клієнтами, щоб допомогти їм розслідувати та пом'якшити наслідки. Це включає роботу з CISA над надзвичайною директивою для надання вказівок урядовим установам».

Посольство Росії у Вашингтоні, яке в минулому заперечувало причетність до хакерських кампаній, не відразу повернуло повідомлення з проханням прокоментувати.

CISA попередила, що хакери також могли переслідувати неурядові групи.

«Інші організації також могли постраждати від викрадання корпоративної електронної пошти Microsoft», — заявили в CISA, заохочуючи клієнтів зв'язуватися з Microsoft для отримання додаткової інформації». ***(Raphael Satter. US cyber agency says Russian hackers used Microsoft access to steal government emails // Reuters (https://www.reuters.com/technology/cybersecurity/us-cyber-agency-says-russian-hackers-use-microsoft-access-steal-government-2024-04-11/). 12.04.2024).***

***

«1 квітня Агентство з кібербезпеки та безпеки інфраструктури (CISA) видало надзвичайну директиву у відповідь на Midnight Blizzard, також відомий як Cozy Bear, спонсорований державою російський організатор загроз, націлений на облікові записи електронної пошти Microsoft у своїй останній кампанії.

Група викрадає інформацію з корпоративних систем електронної пошти Microsoft, щоб отримати доступ до систем клієнтів Microsoft. Microsoft і CISA вже визначили, листування яких компаній було викрадено, і повідомили їх про це.

«Початковим вектором доступу для атаки Midnight Blizzard був розпилювач паролів Microsoft 365», — сказав Джон Фоккер, керівник відділу аналізу загроз у Trellix, у заяві, надісланій електронною поштою. Дослідники з Trellix спостерігали понад 120 таких атак лише за перший квартал цього року.

Директива CISA спочатку була видана виключно федеральним відомствам 2 квітня. Вона вимагала від агенцій спостерігати та аналізувати облікові записи електронної пошти Microsoft, щоб визначити, чи вони були вражені, скидати скомпрометовані облікові дані та захищати будь-які привілейовані облікові записи Microsoft Azure.

Ці вимоги стосуються лише агентств Федеральної цивільної виконавчої влади (FCEB), оскільки вони, здається, є найбільшою ціллю Midnight Blizzard. Але CISA зазначає, що інші організації також могли зв'язатися, і їм слід звернутися за допомогою.

«Незалежно від прямого впливу, всім організаціям наполегливо рекомендується застосовувати суворі заходи безпеки, включаючи надійні паролі, багатофакторну автентифікацію (MFA) і заборонений обмін незахищеною конфіденційною інформацією через незахищені канали», — йдеться у заяві CISA.

Джен Істерлі, директор CISA, також зазначила, що цей компроміс Microsoft є лише останньою зловмисною кіберактивністю в російському підручнику, і що надзвичайна директива призначена для забезпечення безпеки мереж і систем федеральних цивільних агентств». ***(Kristina Beek. CISA Issues Emergency Directive After Midnight Blizzard Microsoft Hits // Informa PLC (https://www.darkreading.com/cyberattacks-data-breaches/cisa-emergency-directive-after-midnight-blizzard-microsoft-hits?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 12.04.2024).***

***

«Цього року на виборчі дільниці підуть понад 50 країн, включно з такими великими економіками, як США, Індія та Велика Британія. 2024 рік, так чи інакше, стане визначальним, адже в демократичному процесі візьмуть участь понад 4 мільярди виборців - близько половини населення планети. Однак серед цієї глобальної практики демократії ховається зростаючий ландшафт загроз, який підживлюється постійною геополітичною напруженістю, розвитком

технологій і постійним ризиком недобросовісної інформації (інформації, вирваної з контексту для маніпулювання), яка може вплинути на результати виборів.

В останні роки дезінформація та кампанії з дезінформації вплинули на громадську думку. Під час виборів у Великій Британії у 2019 році кілька політичних рекламних оголошень і кампаній у соціальних мережах обманювали виборців неправдивими заявами та прихованими планами. У 2016 році ми стали свідками того, як потенційна участь іноземних супротивників призвела до злому та витоку конфіденційних даних, щоб вплинути на громадськість і результати президентських перегонів у США. Усе це створило неминучі загрози перед виборами президента США в листопаді 2024 року.

Геополітичні ризики та напади на національні держави

Перетин глобальних збройних конфліктів і кібервійни значно посилює ризик для критичної інфраструктури, яка є ключовою для підтримки виборчого механізму в країнах на порозі майбутніх виборів. Представники виборчих органів та їхні служби безпеки будуть дуже пильними.

Відповідно до Звіту про дослідження загроз кібервтручання у вибори за 2024 рік, США, Великобританія, Південна Корея та Індія є країнами з найбільшим ризиком щодо кібервтручання у вибори з боку таких геополітичних супротивників, як Китай і Росія. Останнім часом ми спостерігаємо зростання кількості фінансованих державою кіберзагроз, з останнім проникненням APT29 у мережі Microsoft і HPE, щоб стежити за електронною поштою керівників. Подібним чином у лютому 2024 року китайська група Volt Typhoon зламала життєво важливі мережеві системи широко використовуваного постачальника урядовими установами США.

Епоха штучного інтелекту, дезінформації та дезінформації: підготовка до дня виборів

З наближенням дня виборів у будь-якій країні з’являється нове поле битви, де стикаються штучний інтелект (ШІ), дезінформація та дезінформація. Зростання фішингових і вішингових атак загрожує використанням особи виборців, що потенційно може призвести до фальсифікації виборів. Приховані кампанії впливу,

ретельно організовані, можуть вплинути на мислення виборців і результати виборів. Останні звіти підтвердили потенційне міжнародне втручання через соціальні мережі під час циклу проміжних виборів у США 2022 року. А тепер, із появою штучного інтелекту, стратегічне націлювання на окремих осіб або групи осіб за допомогою атак через видавання себе за іншу особу зростатиме, і їх буде все важче ідентифікувати як законні. Наприклад, у січні виборці в Нью-Гемпширі отримали автоматичний дзвінок, нібито від президента США Джо Байдена з проханням не голосувати на праймеріз у штаті. Після розслідування офіційні особи штату встановили, що це була вішингова атака з підтримкою ШІ, спрямована на маніпулювання виборами.

Щоб запобігти подібним атакам, Національне поліцейське управління Південної Кореї (KNPA) запровадило інструмент для виявлення глибоких фейків. Ці складні алгоритми спрямовані на виявлення маніпуляційних відео та запобігання їх поширенню під час виборів». ***(Election security: Defending democracy in today's cyber threat landscape // CTech (https://www.calcalistech.com/ctechnews/article/bkhrexkg0). 14.04.2024).***

***

«Спонсоровані державою кібертерористи заробляють на застарілій інфраструктурі комунальних служб і слабких протоколах кібербезпеки.

У 2013 році спонсоровані державою актори з Ірану отримали віддалений доступ до промислової системи контролю (ICS), яка контролює невелику дамбу на північ від Нью-Йорка. Їхній несанкціонований доступ дозволив їм отримати інформацію про роботу дамби, включаючи рівень води та температуру. На щастя, атаку вдалося запобігти — не першокласній команді кіберзахисту чи ручним керуванням, а знерухомленим шлюзом, який було від'єднано для регулярного технічного обслуговування.

Це лише один ранній приклад мотивації національної держави націлитися на американські ICS. Нещодавно Агентство з кібербезпеки та безпеки інфраструктури США (CISA) оприлюднило пораду, в якій детально описано спонсорованих

державою китайських кіберакторів, які намагаються використовувати мережі інформаційних технологій (IT) для руйнівних або руйнівних кібератак на критичну інфраструктуру США. Незважаючи на те, що деякі американські компанії вжили заходів для захисту своїх ICS, застосувавши нові системи IT та операційних технологій (OT), їм потрібно буде зробити набагато більше, щоб підготуватися до політично мотивованих кібератак у майбутньому.

Нижче наведено найбільш значні перешкоди, з якими зіткнуться комунальні підприємства, зміцнюючи захист ICS, і заходи, які вони повинні вжити для їх усунення.

Найбільший виклик, що постає перед комунальними службами: старіючий набір технологій

Апаратне забезпечення та вбудоване програмне забезпечення, які сьогодні розгортають багато утиліт, налічують десятиліття. Хоча апаратне забезпечення часто базується на простіших 16- та 32-розрядних процесорах, які не мають функцій віртуалізації та безпеки сучасних центральних процесорів (ЦП), більша проблема полягає в тому, що мікропрограмне забезпечення розгортається в складних середовищах із супутніми загрозами безпеці. для яких він не був розроблений і розроблений.

Щоб забезпечити зворотну сумісність із застарілим програмним забезпеченням системи керування та уникнути витрат і операційного ризику повного оновлення, на багатьох пристроях старіші операційні системи накладаються на новіші, потужніші. Ці системи стали сумішшю старих і нових технологій, у яких старі проблеми безпеки не тільки залишаються, але й стають більш вразливими через нові функції. Старіші пристрої також, як правило, мають архаїчні мережеві стеки ICS, такі як уразливості Ripple20, знайдені в стеку Treck TCP/IP у 2020 році.

Іншими словами, те, що ця технологія існує десятиліттями, не означає, що хакери все ще не нишпорять у пошуках потенційних подвигів. Наприклад, коли утиліти підключають застарілі пристрої до Інтернету, це за своєю суттю наражає їх на вразливості, які раніше були несуттєвими. Багато з цих пристроїв не призначені

для навігації в середовищі безпеки, в якому ми зараз перебуваємо, і не призначені для дистанційного керування.

Як комунальні підприємства можуть захистити свої промислові системи управління

Незважаючи на численні технологічні перешкоди, комунальні підприємства все ще можуть зробити важливі покращення безпеки та захистити свої важливі активи. Нижче наведено кілька ключових кроків, які вони повинні виконати:

Оцініть свій ризик

Утиліти можуть почати з ідентифікації всіх IT/OT активів, доступних через Інтернет. Щоб отримати повне розуміння того, як вони пов’язані (і через які дані можуть проходити), керівники повинні створити надійну карту мережі та діаграму потоку даних.

Зробивши це, вони можуть провести комплексну оцінку ризику, яка визначає ключові вразливості, ймовірність їх використання та вплив, який таке використання матиме на організацію та за її межами. Наприклад, порушення кібербезпеки великих енергетичних і водопровідних об’єктів можуть поставити під загрозу не лише окреме комунальне підприємство, але й національну та громадську безпеку.

Крім того, розгляньте незалежну оцінку ризиків, щоб оцінити існуючу політику, процедури та засоби контролю кібербезпеки. Ці оцінки забезпечують зовнішній погляд на бізнес-ризик, вільний від організаційних упереджень, і вважаються найкращою практикою.

Використовуйте рамки кібербезпеки як дорожню карту

Комунальним підприємствам слід розглянути можливість прийняття однієї з десятків систем кібербезпеки IT/OT, спрямованих на запобігання витоку даних, збою системи чи іншим збоям. Національний інститут стандартів і технологій Cybersecurity Framework 2.0, спочатку розроблений для використання в уряді США, є чудовим початком.

Інфраструктура, яка адаптується до широкого спектру галузей і вирішує ключові проблеми приватного сектора, зводить кібербезпеку до шести простих для

розуміння основних функцій: управління, ідентифікація, захист, виявлення, реагування та відновлення. CISA також випустило вказівки щодо кіберзахисту організацій, які можуть допомогти організаціям будь-якого розміру зменшити ймовірність кібератак.

Тим часом Управління кібербезпеки, енергетичної безпеки та реагування на надзвичайні ситуації (CESER) Міністерства енергетики проводить програму Cyber Testing for Resilient Industrial Control Systems (CyTRICS), яка спеціально спрямована на співпрацю з виробниками та комунальними підприємствами в енергетичному секторі. CyTRICS проводить тестування пристроїв і систем, включаючи аналіз уразливостей апаратного, програмного та мікропрограмного забезпечення.

Визначити необхідність дистанційного моніторингу

Віддалений моніторинг, який дозволяє операторам оцінювати та контролювати об’єкт за допомогою автоматизації, також може запропонувати переваги кібербезпеки, дозволяючи раннє виявлення загрозливих суб’єктів і запобігання атакам на критичну інфраструктуру.

Однак без належної технічної реалізації віддалений моніторинг сам по собі може стати вектором кібератак. Перш ніж запроваджувати цю нову технологію, дуже важливо провести оцінку ризику, щоб визначити ймовірність того, що суб’єкт загрози використовує потенційну вразливість. Це дозволить комунальним підприємствам зробити стратегічний вибір щодо прийняття та впровадження.

Створіть захист від атак людей, що живуть поза межами землі

Занепокоєне зростання атак живих поза межами (LOTL) — безфайлових кібератак зловмисного програмного забезпечення, які використовують інструменти, уже наявні в «середовищі» (включно з PowerShell або Windows Management Instrumentation) — привернуло увагу міжнародних органів з кібербезпеки та уряду США. Наприклад, у травні 2023 року Microsoft виявила цілеспрямовану шкідливу діяльність, спрямовану на критичну інфраструктуру в США, яку здійснював Volt Typhoon, спонсорований державою актор із Китаю.

Подібні атаки можуть підірвати IT/OT-системи комунальних підприємств, знищити обладнання та призвести до повної зупинки роботи. Але це ще не все: є докази того, що Volt Typhoon зміг підтримувати доступ до IT-середовища протягом п’яти або більше років, тобто утиліта вже могла бути скомпрометована, навіть не підозрюючи про це.

Щоб запобігти цим порушенням, організації повинні переконатися, що їхні засоби безпеки належним чином налаштовані. Це може означати впровадження багатофакторної автентифікації або розгортання сегментації мережі, яка розділяє комп’ютерні мережі на кілька підмереж, щоб адміністратори могли контролювати потік мережевого трафіку.

Продумано інтегруйте застарілі IT та OT

Освітлення з таймером, системи опалення, вентиляції та кондиціонування, ліфти та маршрутизація викликів — ми схильні припускати, що подібні пристрої OT навряд чи будуть зламані або вимкнені, оскільки вони не підключені безпосередньо до Інтернету.

Але в міру зближення IT і OT — через комп’ютери, сервери для віддаленого моніторингу чи інші випадки використання — ці технології можуть стати доступними через Інтернет і, отже, вразливими для кібератак. Зловмисники можуть отримати доступ до IT-систем через невиправлені шлюзи, брандмауери, віртуальні приватні мережі та інші вектори. Звідти вони можуть підвищувати свої привілеї, переміщатися по системі та дистанційно керувати певними пристроями.

Розмірковуючи про бізнес-рішення щодо інтеграції IT та OT, враховуйте рамки, найкращі практики та посібники для забезпечення безпечного процесу.

Проводити планове обслуговування кібербезпеки

Минає небагато часу, перш ніж експлойт нульового дня — уразливість програмного забезпечення, про яку не знають її розробники чи власники — досягне глобальної аудиторії через Інтернет. Кіберзлочинці можуть використовувати різні інструменти для виявлення вразливих машин, які ще не виправлені. У результаті лише минулого року оператори програм-вимагачів експортували 1,1 мільярда доларів із понад 4000 організацій-жертв.

Щоб не стати мішенню, організації повинні надавати пріоритет активній та відданій програмі керування виправленнями. Якщо утиліту буде зламано, також важливо мати процедури та політики, які можна розгорнути якнайшвидше. Це може включати призначення групи реагування на кризу та/або призначення конкретних ролей працівникам під час кібератаки. Нарешті, кризова подія не повинна бути першим випадком, коли ці процедури реагування та відновлення зламуються. Плани реагування на інциденти повинні виконуватись принаймні раз на рік за участю правління.

Дійте зараз, щоб захистити критичну інфраструктуру

Експлуатація ICS, підключеної до Інтернету, може призвести до катастрофічних наслідків для комунальних служб США, громадськості та уряду.

Це не те, що є далеким у майбутньому. Кібератаки відбуваються зараз, на нашій власній землі. Оскільки геополітична напруженість продовжує зростати в усьому світі, ніколи не було найкращого часу для комунальних служб оновити та зміцнити свою критичну інфраструктуру». ***(Christopher Stangl and Steve Chapin. As Cyberattacks Surge, Utilities Must Safeguard Their Industrial Control Systems // Berkeley Research Group, LLC (https://www.thinkbrg.com/insights/publications/ts-cyberattacks-utilities-must-safeguard-industrial-control-systems/). 04.2024).***

***

«Провідна фірма з кібербезпеки Mandiant вважає, що за нещодавньою серією атак на водопровідні служби в кількох країнах, включаючи Сполучені Штати, стоїть сумнозвісна група російських хакерів. 18 січня група змогла спровокувати переповнення резервуара на водоочисній станції в Техасі та здійснила подібні вторгнення у Францію та Польщу.

Безпосередньо відповідальна група називає себе «Cyber Army of Russia Reborn» або «Xaknet» і представляє себе як незалежна «хактивістська» група, яка підтримує свою країну. Дослідники вважають, що ця група насправді є маріонеткою Sandworm, відомої команди російських хакерів, яка безпосередньо контролюється російськими військовими.

Російські хакери демонструють здатність перешкоджати роботі водоканалів

Головна новина від Mandiant – січневе переповнення резервуарів у місті Мулшу на півночі Техасу. Дослідники безпеки виявили російськомовний канал Telegram, у якому ймовірні «хактивісти» взяли на себе відповідальність за злом. Група стверджує, що є незалежною, але дослідники раніше пов'язували її з контрольованим ГРУ загоном Sandworm, який діє вже близько двох десятиліть.

Атака була відносно нешкідливою, не створюючи загрози зараження для 5000 жителів Мулешу, яких обслуговує водоочисна станція. По суті, це просто витратило воду, оскільки російські хакери спричинили переповнення резервуара приблизно на півгодини. Працівники місцевих комунальних служб змогли покласти край атаці, перейшовши на ручні офлайн-операції.

Два сусідніх міста на півночі Техасу повідомили про підозрілу активність під час зламу, хоча жодне з них не було скомпрометовано. Одне місто помітило незвичайну кіберактивність у системі SCADA, яка використовується для нагляду за іншим планом очищення води, а інше помітило невдалу спробу встановити брандмауер для захисту подібної системи. Невідомо, чи були ці спроби також справою рук російських хакерів.

Існують звинувачення та документи про злам російських хакерів у комунальні служби США вже принаймні десять років, але на сьогоднішній день вважалося, що це здебільшого було шпигунство та перевірка засобів захисту, які не мали на меті привернути увагу. Якщо група ГРУ стоїть за активними маніпуляціями з водоочисними спорудами на чужій території, це означатиме значну ескалацію. Відкриті атаки на критично важливу інфраструктуру є відносно новим явищем, яке стало серйозною проблемою лише після інцидентів Colonial Pipeline та JBS у 2021 році, і до цього часу вони були здебільшого роботою приватних некомерційних злочинців. Росія навіть пішла на незвичайний крок, добровільно надавши США допомогу в розгромі банди програм-вимагачів Darkside, здійснивши арешти членів на початку 2022 року, приблизно за місяць до її вторгнення в Україну.

Це може свідчити про те, що атаки на критичну інфраструктуру більше не вважаються Москвою «поза межами». У звіті Mandiant російські хакери описані як найнахабніша та найздатніша та небезпечна передова група постійних загроз, яка зараз діє.

Боб Хубер, головний спеціаліст із безпеки та керівник державного сектору в Tenable, зазначає, що від федерального уряду можна очікувати лише стільки, щоб запобігти нападам такого роду: «Це кошмарний сценарій для багатьох експертів з оборони. Поганим акторам і державам більше не потрібно покладатися на кулі та ракети. Вони можуть втручатися або вимикати критично важливу інфраструктуру, використовуючи вразливі місця в конвергентних IT- та OT-системах. США та їхні союзники повинні краще працювати у своїй колективній обороні від цих супротивників. Тим часом постачальники критичної інфраструктури повинні дотримуватися кількох основних вказівок, щоб запобігти атакам. Серед них використання рішень багатофакторної автентифікації, використання криптографічних ключів на додаток до протоколів захисту паролів, таких як ротація паролів, захист віддаленого доступу, а також журналювання та аудит мережевої активності OT підрядниками та співробітниками для запобігання атакам на основі ідентифікації та облікових даних».

У США, Польщі та Франції постраждали очисні споруди

Російські хакери також використали свій канал у Telegram, щоб опублікувати відео, в якому стверджується, що подібна атака була здійснена на гідроелектростанцію у Франції, тимчасово перериваючи виробництво електроенергії за допомогою промислових засобів контролю для зміни рівня води. Вважається також, що група скомпрометувала принаймні одну очисну станцію в Польщі.

Mandiant надав ряд доказів, які підтверджують його твердження про те, що російські хакери таємно контролюються урядом. Дослідники посилаються на створення каналу Youtube групою, який був відстежений до відомої інфраструктури Sandworm, і попередні приклади посилань на атаку, здійснену групою APT до того, як про інцидент стало відомо всім. На думку цих дослідників,

єдиний елемент, про який йдеться, полягає в тому, наскільки автономією у своїх діях є ймовірна «хактивістська» група. Здавалося, що хакери лише частково знали, як працює система керування водоочисними станціями, і були більш нахабними у своїх атаках, ніж Sandworm загалом відомий, що призвело до деяких припущень про те, наскільки жорстко група контролюється та навчається ГРУ.

Агентство з охорони навколишнього середовища та Рада національної безпеки нещодавно випустили спільне попередження про кібератаки на водний сектор, але вони зосередилися на іранських та китайських хакерських командах. Атака на водоочисну станцію в Пенсільванії в листопаді минулого року була приписана іранській державній команді, а нещодавно в доповіді виявилося, що численні китайські державні хакери проникають у всілякі критичні інфраструктурні системи та залишають бекдори на майбутнє. використання у разі військового конфлікту.

Відомо, що Sandworm спеціалізується на атаках на критичну інфраструктуру, але останнім часом більшість своєї енергії спрямовує на цілі в Україні, оскільки вторгнення в цю країну триває. Ця команда також загалом більше зацікавлена у виведенні з ладу електроенергії та супутникового зв'язку в регіоні, а також проникненні в урядові установи з метою викрадення військових секретів.

Том Келлерманн, старший віце-президент із кіберстратегії в Contrast Security, вважає, що російський уряд замовив ці атаки з певною метою, і що буде ще більше: «Російські кіберзбройні сили атакують критичну інфраструктуру як помсту за американську підтримку України. Ці напади стануть більш каральними, оскільки Путін випустив гончих з прив'язі».

А Роджер Граймс, проповідник захисту на основі даних у KnowBe4, вважає, що атак на критичну інфраструктуру вже відбувається більше, ніж це робиться в новинах: «Це набагато гірше, ніж ви думаєте. Щоразу, коли ви чуєте про одну юридичну особу чи назву якоїсь компанії, які були успішно зламані за допомогою певного методу, просто усвідомте, що це лише тому, що ця особа потрапила в новини того дня, а існують буквально сотні тисяч подібних організацій, які роблять ті самі помилки. зараз. І вони або зараз скомпрометовані, або просто чекають, щоб

їх скомпрометували, коли якийсь супротивник просто спробує. Отже, не звинувачуйте цих жертв у проблемах, тому що проблеми поширені набагато ширше, ніж хтось поза галуззю кібербезпеки може собі уявити. Це не виняток, як можуть подумати багато випадкових читачів. Сумна частина цього, незважаючи на те, що політики знищують вимоги щодо запобігання такого роду атакам, полягає в тому, що всі знають, як запобігти такому виду нападу... вимоги чи ні, але ми досі цього не робимо. Думка про те, що будь-хто з Інтернету може отримати доступ до системи, яка контролює критичну інфраструктуру безпеки, божевільна! Ми знаємо, що це божевілля. Проте ми все ще дозволяємо цьому статися, оскільки засоби контролю, які зменшують імовірність цього, можуть спричинити деякі реальні чи уявні незручності».

«Я спостерігав за успішними атаками на нашу критично важливу інфраструктуру ще до широкомасштабного розгортання Інтернету (тобто на початку 1990-х років), і той факт, що подібні атаки не тільки все ще трапляються, але й відбуваються все частіше, мене вражає! Ми знаємо, що у нас є проблема. Усі погоджуються, що це серйозна проблема. І все ж багато/більшість організацій, відповідальних за захист тих самих систем, просто не намагаються цьому запобігти. Це як залишити свою машину незамкненою з пістолетом у ній і здивуватися, коли злодій відкриває двері вашої машини вночі, викрадає вашу зброю та використовує її проти вас. Це майже так, ніби ви вітали злочин. Я не хочу применшувати більшість захисників кібербезпеки, які активно витрачають своє життя, намагаючись запобігти цьому, тому що вони це отримують. Решта організації заважає їм бути більш успішними. Вся система налаштована проти захисників кібербезпеки, які намагаються діяти правильно. І якщо захисник кібербезпеки зробить усе необхідне, щоб зупинити подібні речі, і цього не станеться, можна посперечатися, що хтось в організації сумнівається, чому вони витрачають стільки грошей або завдають стільки незручностей», — додав Граймс». ***(Scott Ikeda. State-Sponsored Russian Hackers Linked to Breach of Texas Water Treatment Plant // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-***

security/state-sponsored-russian-hackers-linked-to-breach-of-texas-water-treatment-plant/). 23.04.2024).

***

Створення та функціонування кібервійськ

«У середу, 24 квітня, в Естонії стартували найбільші у світі навчання з кібербезпеки Locked Shields 2024, які розпочав Центр передового досвіду з кіберзахисту НАТО.

Про це йдеться на офіційному сайті Центру.

У навчаннях беруть участь понад 40 країн, зокрема й Україна, а також понад 4000 тисяч експертів для тестування, зміцнення та впровадження інновацій у можливості НАТО з кіберзахисту, що відображають реальні загрози.

Команди захищають віртуальну державу Берилія від складних кібератак, організованих командою-агресором. Крім вирішення технічних завдань учасники проходять підготовку з юридичної, стратегічної та комунікаційної тактики. Такий цілісний підхід гарантує, що учасники будуть добре підготовлені до того, щоб впоратися з усіма цими труднощами в реальному житті.

Цього року до програми навчання залучили передові системи нейромереж, оскільки штучний інтелект і 5G є невід'ємною частиною сценаріїв. ***(Євгеній Василенко. В Естонії почалися масштабні навчання НАТО з кібербезпеки за участю України // ТОВ «ВИДАВНИЧИЙ ДІМ «МЕДІА-ДК» (https://nv.ua/ukr/world/geopolitics/locked-shields-2024-v-estoniji-pochalisya-masshtabni-navchannya-nato-z-kiberbezpeki-50412978.html). 24.04.2024).***

***

«НАТО створить новий кіберцентр у своїй військовій штаб-квартирі в Монсі у Бельгії. Про це повідомив заступник помічника Генерального секретаря НАТО з інновацій, гібридних технологій та кібербезпеки Джеймс Аппатурай під час конференції з питань кібербезпеки, передає Recorded Future News.

Робоча назва нового об’єкта – Інтегрований кіберцентр НАТО (NICC). Його створення – зміна в Стратегічній концепції Альянсу.

Як зазначив Аппатурай, відтепер «кіберпростір постійно є предметом боротьби», а не лише в моменти кризи чи конфлікту. НАТО має постійно слідкувати за супротивниками в комп’ютерних мережах.

NICC цілодобово інформуватиме НАТО щодо інцидентів, які можуть вплинути на військові операції в Європі.

«Наприклад, порт у Європі зазнав тривалої кібератаки з метою заблокувати шлюзи. Отже, у нас є кораблі, що проходять через шлюз, [нападники] намагаються замкнути його та злити воду, щоб кинути корабель усередину шлюзу, що зашкодить кораблю і заблокує порт», - розповів заступник помічника Генерального секретаря НАТО.

У виданні зазначають, що офіційні особи в США попереджають, що кібератаки є серйозною загрозою для портів». ***(НАТО створить новий кіберцентр для захисту від хакерських атак // Судово-юридична газета (https://sud.ua/uk/news/abroad/298610-nato-stvorit-noviy-kibertsentr-dlya-zakhistu-vid-khakerskikh-atak). 19.04.2024).***

***

Кібервійна проти Ізраїлю

«Група міжнародних хакерів, зосереджених на атаках на Ізраїль та ізраїльські організації, на початку квітня запустила новий веб-сайт, присвячений публікації витоків із серії порушень конфіденційних баз даних і веб-сайтів в Ізраїлі за останні місяці.

Веб-сайт і платформа називається Cyber Court, і афілійовані з ним хакери вже атакували веб-сайти, пов’язані з міністерством оборони Ізраїлю, що виглядає як остання ескалація проксі-війни між Ізраїлем та Іраном.

Тип Wikileaks пропалестинських активістів, веб-сайт надає платформу для пропалестинських хакерів різного рівня для розміщення цифрової здобичі, яку вони вкрали з ізраїльських систем.

«Схоже, що це керована Іраном або, можливо, пов’язана з нею операція впливу в кібернетичному просторі», — йдеться в дописі в блозі Memetic Warfare, написаному Арі Бен Амі. «Кіберсуд, здається, служить розрахунковим центром для різноманітних груп хакерів, які розміщують зламаний контент», — пояснив Бен Амі, засновник Telemetry Data Labs.

Веб-сайт уже опублікував посилання на витоки, включаючи тисячі документів, які, як стверджується, були отримані хакерами, які зламали веб-сайти та адміністративні портали, пов’язані з Міністерством оборони Ізраїлю та Національним інститутом страхування.

Кіберсуд нібито новий, як і деякі групи, що розміщують на ньому матеріали; однак Ізраїль перебуває в центрі хвилі кібератак, кількість яких з початку війни зросла на понад 40 відсотків. За останні два місяці хакери стверджували, що їм вдалося зламати Міністерство юстиції та навіть отримати матеріали з Центру ядерних досліджень Негев у Дімоні на півдні Ізраїлю.

Нові хакери?

Веб-сайт Cyber Court опублікував витік, відповідальність за який взяла на себе нова та незнайома група хакерів під назвою NetHunters (стилізована як NetHunt3rs). Хоча державні хакери, як правило, діють таємно, ця група вимагала від Ізраїлю звільнити 500 палестинських в’язнів в обмін на те, щоб вони не публікували всю інформацію, отриману від Міністерства оборони, яке цього тижня підтвердило, що «неконфіденційні веб-сайти» справді були зламані.

Перевірка деяких витоку матеріалів Haaretz показує, що вони були взяті з адміністративних порталів Міністерства оборони та містять ідентифікаційну інформацію про співробітників міністерства та тендери на безпеку, які насправді можуть виявитися ризиком для Ізраїлю.

Витік матеріалів також розкриває інформацію про технологічні системи Армії оборони Ізраїлю, включаючи подробиці про бронетехніку, такі як інженерні

ескізи, і технічну інформацію про супутникові фотосистеми. Також була розпізнавальна інформація про бійців та підрозділи, в яких вони служать.

Інша незнайома група під назвою Makhlab al-Nasr, «The Eagle's Talon», стверджувала, що зламала Національний інститут страхування, отримавши особисту інформацію близько 8 мільйонів громадян Ізраїлю, «включаючи банківські рахунки та домашні адреси», яку вона погрожувала розповсюдити. в соціальних мережах.

Інститут заперечує будь-яке порушення, але група поширила відео, яке демонструє, що їй вдалося отримати особисту інформацію громадян Ізраїлю. Відео Makhlab al-Nasr і стиль злому та витоку майже ідентичні відео NetHunters, що вказує на те, що вони насправді можуть бути одним і тим же.

Відповідно до одного відеоролика, оприлюдненого на Cyber Court і приписуваного хакерам NetHunters, вони змогли отримати ім’я користувача та пароль інваліда солдата ЦАХАЛу, які вони використовували для входу в власну систему як рядовий користувач – використовуючи точно такий же метод Як стверджував Makhlab al-Nasr, він використовувався для злому систем, пов’язаних з Національним інститутом страхування.

Потім вони обійшли механізми безпеки всередині системи та вилучили значну кількість інформації, яка мала бути доступною лише для інших користувачів. Матеріали опубліковані на спеціальному сайті.

Memetic Warfare пов’язав злом Національного інституту страхування з витоком Міністерства оборони через веб-сайт Cyber Court, який першим опублікував обидва витоки. На сайті також є канали на X і Telegram, які відкрилися в день, коли відбулися перші витоки з груп.

«Кіберсуд — це трибунал, де звинувачуються злочинці. Сьогоднішніми злочинцями є сіоністи, які вчиняють жорстокі вбивства невинних палестинських дітей і жінок. Тепер хакери несуть відповідальність за їх покарання. Цим ми виносимо вердикти… і також запрошуємо всіх хакерів світу, які шукають свободи, щоб приєднатися до нас у кампанії покарання цих злочинців", - йдеться в їх першому дописі.

Кібердослідники в Ізраїлі та в усьому світі, які уважно стежать за кіберактивністю Ірану, не були знайомі з цими групами до минулого тижня. Після того, як їхні хакери вперше були озвучені на новому веб-сайті Кіберсуду та його платформах, кібератаки нібито невідомих груп також висвітлювали державні ЗМІ Ірану – як це вже траплялося в минулому з групами нападників, ідентифікованими з кіберпідрозділами Ірану або в.о. за погодженням з ними.

Cyber Court стверджує, що інші активні та відомі групи приєдналися до його відкритого заклику створити коаліцію антихакерів, включаючи Anonymous Sudan, яка в минулому проводила хвилю простих атак на Ізраїль і вважається близькою до Росії та її інтереси.

Загадкова команда Бангладеш, група, яка часто атакує цілі, пов'язані з Ізраїлем, Індією та світськими організаціями, які вважаються загрозою ісламу, також стверджується, що є частиною коаліції веб-сайту.

Більшість із цих груп належать до другої ліги кіберсвіту, професійні групи зі здібностями, які більше відомі з цифрового злочинного світу, а не пов'язані з державою групи з військовими кіберпотенціалами.

Cyber Court більше нагадує кампанію впливу, спрямовану не лише на збір зламаної інформації, але й на приниження Ізраїлю та створення відчуття широкої мобілізації міжнародної хакерської активності, наприклад, нова група нібито з Південної Африки також приєдналася до бійки, хоча дослідники вважають це також лише прикриття для вже існуючої групи, також, ймовірно, іранської. Нова група намагається помститися за смерть у Газі через хвилю вторгнень – навіть якщо вони не є значними, руйнівними, а в деяких випадках навіть правдивими.

За різким збільшенням цифрових атак на Ізраїль після початку війни в Газі також послідувала хвиля безпідставних заяв про атаки, що підкреслює спектр між операціями впливу та кібератаками. Ізраїльський національний кіберуправління стверджує, що разом із справжніми атаками також спостерігалося збільшення кампаній впливу, спонсорованих Іраном і Хезболлою, які включали резонанс нових атак, переробку матеріалів зі старих хаків і поширення безпідставних заяв про нові атаки.

Cyb3r Avengers є одним із прикладів серйозної групи хакерів, яку Сполучені Штати пов’язували в минулому з Іранською революційною гвардією, і яка була в основному стурбована з початку війни використанням кібернавички для цілей впливу, наприклад, спрямовуючи трафік з по всьому світу на веб-сайти в Ірані, які повідомляють про хакерські атаки проти Ізраїлю.

Від Ширбіту до Південної Африки

Старші ізраїльські кібердослідники попереджають, що ми не повинні забувати про наслідки різноманітних зломів і накопичення такої кількості інформації про ізраїльських громадян, зокрема про працівників оборонного відомства та тих, хто займає секретні посади.

Дослідники кажуть, що оприлюднення витоку інформації у багатьох випадках є лише загальнодоступною кінцевою точкою набагато більш тривалої та серйознішої таємної кібероперації, спробою досягти PR-перемоги після втрати доступу до зламу, через який було таємно зібрано значну кількість розвідувальних даних.

Дослідники стверджують, що хакери знають, як використовувати витік особистої інформації для таргетування та фішингу, що може дозволити їм отримати додаткові деталі, щоб зламати додаткові конфіденційні системи.

Вони кажуть, що, можливо, зломи Національного інституту страхування та Міністерства оборони стали можливими завдяки інформації, яка просочилася в минулому, у контексті злому 2021 року в компанію Shirbit Insurance, яка страхує автопарк Ізраїлю, і таким чином надав хакерам доступ до організованої бази даних чиновників.

Інформація включала особисті дані працівників державної служби та міністерств, у яких вони працювали, включно з конфіденційними організаціями безпеки

Іншу інформацію про ізраїльтян можна знайти в Інтернеті: наприклад, витік додатка Elector App, який обслуговував партію Лікуд під час минулих виборів, що призвело до оприлюднення інформації про шість мільйонів ізраїльтян, включаючи їхні особисті ідентифікаційні номери, адреси та номери телефонів.

Велика кількість інформації про громадян Ізраїлю зараз доступна в Інтернеті, її можна придбати та використовувати для різних цілей.

Ця інформація поступово накопичується: ще однією невідомою групою, яка почала діяти на фоні Кіберсуду, є Anonymous South Africa, яка представляє себе цифровим фронтом, паралельним петиції країни проти Ізраїлю в Міжнародному суді в Гаазі, і погрожував витоком додаткової інформації, зламаної з ізраїльської бази даних.

Хакери, які назвали себе лише членами колективу Anonymous, також заявили цього місяця, що їм вдалося зламати Міністерство юстиції. Багато ізраїльських експертів з конфіденційності та дослідників кібербезпеки описали це як великий витік, можливо, навіть історичного масштабу, повні наслідки якого ще невідомі, і він також може продовжувати допомагати тим, хто хоче атакувати Ізраїль.

Міністерство юстиції та кіберуправління у відповідь повідомили, що «початкову підозру на кіберподію в технологічних системах Мін’юсту виключено, проникнення в системи міністерства не виявлено.

«Після перевірки оприлюднених документів ми виявили, що це документи минулих років і, ймовірно, не є результатом зламу систем Мін'юсту», - додали вони.

Але кіберрозслідувачі, які досліджували документи, які були витоку, поставили під сумнів твердження уряду. Вони кажуть, що якщо це не активне порушення державних систем, це ще гірше, тому що це означає, що файли, що містять конфіденційні дані, вже були розкриті в Інтернеті.

Витік інформації включає особисті дані вищих посадових осіб у міністерстві разом із конфіденційною кореспонденцією, внутрішніми та секретними документами міністерства, протоколами обговорень, які проводилися за закритими дверима та все ще перебувають під розпорядженням, тощо.

«Після розповсюдження матеріалів щодо Мін'юсту було відкрито розслідування, у зв'язку з чим накладено заборону на деталі розслідування, а також інформацію, яка була отримана», - повідомили в кіберуправлінні.

«На сьогодні низку Telegram-каналів, які опублікували документи, видалено, робота з цього питання триває», – додали в дирекції.

Дійсно, між Ізраїлем і загрозливими акторами, які злили свою інформацію, точилася гра в кішки-мишки. Після того, як канали Telegram, які поширювали інформацію, були закриті, ймовірно, на прохання Ізраїлю, хакери повернулися та почали зливати свої товари на інші канали. Через 24 години більшість розповсюджувальних груп було знову видалено.

Цього б не сталося з новоспеченим кіберсудом. Веб-сайт заснований на технології блокчейн, яка є основою цифрових валют, таких як біткойн. Веб-сайт використовує децентралізовану технологічну інфраструктуру, тому його не можна видалити з Інтернету, навіть якщо групи Telegram або обліковий запис X закрито. Інформацію вже буде опубліковано на ряді інших сайтів, щоб гарантувати, що вона залишається відкритою назавжди.

Ізраїль, як завжди, дає відсіч. Згідно з різними повідомленнями, вона також бере участь у низці кіберактивностей, а також може використовувати вплив проізраїльських хакерських груп, у тому числі деяких, які публікують ганебну інформацію про Революційну гвардію.

Минулого тижня голова Національного кіберуправління Ізраїлю, який є частиною офісу прем'єр-міністра, також зробив власний удар і минулого тижня розкрив справжню особу Black Shadow, групи, яка стоїть за зломом страхової групи Shirbit, заявивши, що це була філія міністерства розвідки Ірану». ***(Omer Benjakob, Oded Yaron. Iran-linked Website Leaks Secret Israeli Data // Haaretz Daily Newspaper Ltd. (https://www.haaretz.com/israel-news/security-aviation/2024-04-16/ty-article/.premium/click-here-for-sensitive-israeli-data-iran-linked-website-leaks-hacked-secret-info/0000018e-e6c8-de97-a5bf-f6f876a10000?utm_source=flipboard&utm_content=Haaretz%2Fmagazine%2FIsrael+and+Middle+East+News). 16.04.2024).***

***

«Хакерська організація Anonymous опублікувала заяву в п'ятницю, в якій заявила, що зламала ЦАХАЛ і, як повідомляється, продемонструє нібито військові документи. Він також претендує на контроль над 20 гігабайтами даних, що охоплюють понад 233 000 документів, включаючи PDF-файли, файли Word, презентації PowerPoint тощо.

Супровідне відео хакерів демонструє уривки з презентацій PowerPoint за участю персоналу ЦАХАЛу, а також слайди з логотипами відомств Генерального штабу. Автентичність документів на відео залишається невизначеною.

Згідно з оцінками безпеки IDF, ймовірність справжнього зламу мінімальна, що свідчить про можливу тактику «психологічної війни» з боку хакерів. Комп'ютерна система ЦАХАЛу суворо захищена та засекречена на різних рівнях. Якщо злам все-таки стався, малоймовірно, що доступ поширювався безпосередньо на комп'ютери IDF; натомість файли могли бути отримані з цивільних комп'ютерів, потенційно порушуючи правила.

Раніше цього місяця анонімне джерело заявило, що зламало Міністерство юстиції, отримавши 8 мільйонів файлів загальним розміром 300 гігабайт, у тому числі особисті дані фігурантів. Деякі з хакерів, що працюють під прапором Anonymous з 2003 року, повторили свою клятву «знищити сіоністів».

На початку місяця національний кібермасив попередив про очікуване зростання кількості атак після закінчення Рамадану та ескалацію підбурювання проти Ізраїлю та його присутності в Інтернеті. Проблеми включають можливі порушення веб-сайтів, проникнення в цифрові системи (включаючи розумні будинки), витоки секретних документів, розголошення особистих даних, розгортання програмного забезпечення для відстеження та спроби вторгнень.

Ізраїльську громадськість закликали уникати переходів за підозрілими посиланнями та повідомляти про будь-які ознаки кібератак». ***(ITAY GAL. 'We broke into IDF, hold quarter of a million documents,' hacker group Anonymous claims // Jpost Inc. (https://www.jpost.com/international/article-797925?utm_source=flipboard&utm_content=other). 19.04.2024).***

***

«У сучасному взаємопов'язаному світі важливість безпеки критичної інфраструктури та промислових процесів важко переоцінити. Системи операційних технологій (ОТ), які охоплюють апаратне та програмне забезпечення, що відстежує та контролює фізичні пристрої та процеси, стали основними цілями для кібератак.

Організація OT Security Waterfall повідомила про 140-відсоткове збільшення кількості кібератак, у яких постраждали понад 150 промислових операцій. Щоб зміцнити ці системи проти загроз, що розвиваються, ми повинні підкреслити симбіотичні стосунки між інженерними спільнотами ОТ і фахівцями з кібербезпеки. Системи ОТ є основою таких галузей, як енергетика, виробництво, фармацевтика, транспорт і охорона здоров'я.

За оцінками Міжнародної корпорації даних (IDC), до 2025 року буде 41,6 мільярда підключених пристроїв IoT. Ці пристрої забезпечують безперебійну роботу електростанцій, виробничих ліній і навіть критичного глобального дослідницького обладнання в галузі охорони здоров'я. Однак їх інтеграція з цифровими мережами, хмарними службами та додатками продовжує наражати їх на кіберризики.

Співпраця між інженерами ОТ і фахівцями з кібербезпеки є ключем до покращеного пом'якшення цих загроз і, що важливо, відкриває численні переваги:

Комплексна оцінка ризиків: інженери ОТ розуміють тонкощі промислових процесів, що робить їх життєво важливими для виявлення вразливостей, унікальних для їхніх систем. Щоб вийти за межі типової відповідності IT-безпеці, цілісна оцінка ризиків ОТ використовуватиме стандарт IEC 62443 і сильні сторони ATT&CK MITRE для ICS, а також стандарт ISO 31010. Співпраця забезпечує більш повну оцінку ризиків, яка враховує як операційні аспекти, так і аспекти безпеки.

Індивідуальні рішення безпеки: Фахівці з кібербезпеки надають досвід у техніках зменшення ризиків безпеки, наприклад, запроваджуючи модель нульової

довіри, яка зазвичай розглядається лише в традиційних IT-середовищах. Центру кібербезпеки Всесвітнього економічного форуму Документ про нульову довіру для мереж OT визначає нульову довіру як «модель, засновану на принципах, розроблену в рамках стратегії кібербезпеки, яка передбачає підхід, орієнтований на дані, постійно розглядати все як невідоме – будь то людина чи машина. - забезпечити надійну поведінку». Впровадження моделі нульової довіри разом з інженерами OT дозволяє реалізувати це рішення, захищаючи критично важливі системи, не перешкоджаючи безпеці та ефективності роботи.

Своєчасне реагування на загрози: у разі кіберінциденту добре налагоджена співпраця забезпечує швидке реагування. Існують корисні ресурси та програми для обміну загрозами OT та Industrial Control System (ICS), які дозволяють підвищити глибину доступної інформації для прийняття обґрунтованих рішень, наприклад спільнота автоматизованого обміну індикаторами CISA, консультації NCSC та Альянс кіберзагроз. Захист цифрового виробництва Інженери OT можуть у режимі реального часу надати інформацію про вплив на роботу, а експерти з кібербезпеки можуть зосередитися на стратегіях стримування та відновлення.

Обмін знаннями та навичками: подолання розриву між цими двома спільнотами сприяє обміну знаннями. Нещодавня ініціатива Cyber-Informed Engineering (CIE), запроваджена Міністерством енергетики США минулого року, починає мати позитивний вплив, особливо в сферах обізнаності та освіти, які визнають ці зусилля співпраці. Симуляція атак на мережі OT під час спільних бойових навчань може максимізувати навички захисту. Платформи Cyber діапазону, такі як Cyberbit, надають повномасштабну емульовану мережу OT, включаючи HMI, апаратні контролери (PLC) і фізичні пристрої, а також забезпечують наскрізне моделювання атак IT to OT. Інженери OT можуть вивчати найкращі практики кібербезпеки, а фахівці з кібербезпеки можуть отримати глибше розуміння промислових процесів. Це перехресне запилення знань має неоціненне значення для того, щоб випереджати загрози, що розвиваються.

Відповідність нормативним вимогам: багато галузей підпадають під дію суворих правил щодо кібербезпеки та безпеки. Національний інститут стандартів і

технологій (NIST) наголошує на важливості інтеграції безпеки OT та IT для відповідності нормативним вимогам, таким як NIST SP 800-82 Rev 3 для промислових систем керування. Спільні зусилля полегшують навігацію щодо вимог відповідності, наприклад, NIS 2, зменшуючи ризик штрафів і простоїв через невідповідність.

Економічність: спільні зусилля можуть призвести до ефективнішого розподілу ресурсів. Ponemon Institute Дослідження показало, що організації, які інтегрували функції безпеки IT і OT, заощадили в середньому 1,5 мільйона на витратах на кібербезпеку. Замість того, щоб дублювати зусилля, команди розробки OT і кібербезпеки можуть працювати разом, щоб визначити пріоритети та вирішити найбільш критичні проблеми безпеки.

Інновації: системи OT швидко розвиваються завдяки таким досягненням, як промисловий Інтернет речей (IIoT) і автоматизація. Нещодавнє дослідження AT&T показує переваги інновацій від співпраці OT та IT, що веде до ефективної та ефективної конвергенції за рахунок останніх галузевих технологічних досягнень. Співпраця дозволяє з самого початку впроваджувати заходи кібербезпеки в ці конвергентні інновації, створюючи за своєю суттю більш безпечні системи.

Відмовостійкість: зрештою, співпраця між інженерами OT і фахівцями з кібербезпеки підвищує загальну стійкість критичної інфраструктури. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) наголошує на важливості інтеграції безпеки IT та OT для підвищення стійкості систем критичної інфраструктури. Це гарантує, що системи можуть протистояти кібератакам і продовжувати безпечно працювати навіть у несприятливих умовах.

Кіберзагрози часто використовують стики між IT- та OT-середовищами, і без інтегрованої безпеки організація менш готова до захисту від цих загроз. Щоб подолати ці виклики та покращити загальний стан кібербезпеки, організації дедалі більше визнають необхідність усунути розбіжності між командами OT та IT-безпеки.

Спільні зусилля, спільна відповідальність і інтегровані стратегії безпеки є важливими для пом’якшення складних і мінливих загроз, які спрямовані як на операційні, так і на інформаційні технології.

Підсумовуючи, переваги співпраці між інженерними спільнотами ОТ і фахівцями з кібербезпеки незаперечні. Оскільки ландшафт загроз продовжує розвиватися, наша здатність захищати критичну інфраструктуру та промислові процеси залежить від цього партнерства. Разом ці дві спільноти можуть зміцнити наші основні системи, захистити наші галузі та забезпечити більш безпечне майбутнє. Це не просто співпраця; це необхідність». ***(Richard Beck. 8 benefits of converged OT cyber security // techUK (https://www.techuk.org/resource/8-benefits-of-converged-ot-cyber-security.html). 15.04.2024).***

***

Кіберзахист закладів охорони здоров’я

«Окрім того, що моделювання кіберзагроз взагалі не проводиться, деякі з найбільших помилок, які можуть зробити виробники медичного обладнання, починають процес моделювання надто пізно на етапі розробки або використовують його просто як «вправу на вагу паперу», — сказав експерт із моделювання загроз Адам Шостак із Shostack & Associates.

«Мені подобається думати про моделювання загроз як про «двічі відміряй, один раз відріж» кібербезпеки», — сказав Шостак.

«Якщо ви включите велику мовну модель у свій МРТ-апарат для зчитування сканів мозку, ви витратите багато грошей на навчання цієї моделі машинного навчання, її включення, тестування — і тоді ви побачите, наскільки вона погано робить», - сказав він Media Security Media Group.

«Виконання моделювання загроз із запізненням, а не на початку, коли все на дошці чи коктейльній серветці, щоб уникнути помилок, які мають статися, — це велика помилка людей».

Початок моделювання загроз на самому початку процесу розробки медичних пристроїв допомагає надати більше можливостей для пом’якшення, оскільки розробники краще розуміють загрози, сказав Шостак.

За його словами, серед основних ризиків, пов’язаних з медичними пристроями, – «баланс між інноваціями, швидкістю та безпекою». «Те, на що я витрачаю багато свого часу, полягає в тому, як зробити моделювання загроз більш ефективним на одиницю енергії, яку ми вкладаємо в нього?» він сказав.

Це включає спрощення відстеження всіх виявлених загроз медичних пристроїв і полегшення пошуку рішень для всіх цих загроз, «щоб ми могли швидше запропонувати людям краще лікування», — сказав Шостак. «Це справді важливий інженерний виклик, на який ми всі повинні стежити».

У цьому аудіоінтерв’ю з Information Security Media Group (див. аудіопосилання під фотографією) Шостак також обговорював:

- Поради щодо початку роботи з моделюванням загроз для медичних пристроїв;
- міркування щодо моделювання загроз для медичних пристроїв із підтримкою штучного інтелекту та чому він скептично ставиться до медичних пристроїв із підтримкою машинного навчання;
- Теми моделювання загроз обговорюються на майбутньому семінарі з кібербезпеки медичних пристроїв у Новому Орлеані, організованому Центром охорони здоров’я та кібербезпеки медичних пристроїв Північно-Східного університету Архімеда, де він виступатиме з доповіддю.

Шостак є автором кількох книг, у тому числі «Моделювання загроз: проектування безпеки». Він є провідним фахівцем із моделювання загроз, консультантом, свідком-експертом і дизайнером ігор із десятирічним досвідом забезпечення безпеки». ***(Marianne Kolbasuk McGee. Medical Device Cyberthreat Modeling: Top Considerations // Information Security Media Group, Corp. (https://www.databreachtoday.com/interviews/medical-device-cyberthreat-modeling-top-considerations-i-***

5370?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology). 05.04.2024).

***

«Висока ефективність кібербезпеки в охороні здоров'я має вирішальне значення для забезпечення безпеки пацієнтів і безперервності роботи в будь-який час, особливо під час інциденту кібербезпеки. Але нові дослідження показують, що потужність програми кібербезпеки організації також безпосередньо пов’язана з фінансовими показниками.

Згідно з новим звітом Diligent Institute та Bitsight, компанії з високими показниками кібербезпеки за п'ятирічний та трирічний періоди забезпечили середній загальний дохід акціонерів (TSR) на рівні 71% та 67% відповідно. Компанії з базовими показниками кібербезпеки отримали відповідно 37% і 14% TSR.

Diligent Institute і Bitsight проаналізували дані понад 4000 організацій у різних секторах. Дослідники створили методи для оцінки нагляду правління за кібербезпекою та класифікації організацій за базовою, середньою та розширеною класифікацією безпеки.

Дотримуючись цієї методології, дослідники виявили, що високорегульовані галузі, такі як охорона здоров’я та фінанси, перевершують інші галузі з точки зору ефективності кібербезпеки. З усіх проаналізованих секторів охорона здоров’я мала найвищий середній рейтинг безпеки.

На додаток до спостережуваного зв’язку між ефективністю кібербезпеки та прибутком акціонерів, дослідники виявили кореляцію між структурою правління та рейтингами безпеки. Компанії зі спеціалізованими комітетами ризиків показали значно кращі результати, ніж ті, у яких немає.

«Одним із можливих пояснень є те, що делегування нагляду за складними сферами ризику, такими як кібернетичність, дає змогу вибраним членам правління більш детально зосередитися», — йдеться у звіті.

«Комітети мають кращі можливості для глибокого вивчення конкретних питань кібербезпеки, і вони можуть налагодити міцніші стосунки з керівниками, відповідальними за повсякденні операції з кібербезпеки. Це, у свою чергу, може призвести до кращої політики щодо кібербезпеки, бюджету та інших рішень, які приймаються на рівні правління».

Ці висновки підкреслили важливість участі на рівні правління для кібербезпеки. Однак присутність кіберекспертів у наглядовій раді, хоча й корисно, може не призвести до покращення ефективності кібербезпеки саме по собі, показали попередні дослідження Diligent Institute і NightDragon.

Натомість дослідники припустили, що включення цих експертів до існуючих структур, які використовуються для управління ризиками, таких як раніше згадані спеціалізовані комітети ризиків, може мати помітний позитивний вплив на ефективність безпеки.

«Компанії, які бажають найняти експертів з кібербезпеки для членів правління, повинні спочатку переконатися, що правління належним чином організовано, щоб експертиза могла бути належним чином включена в механізми нагляду», — йдеться у звіті.

Загалом дослідження показало, що охорона здоров’я та інші високорегульовані галузі розуміють важливість кібербезпеки у своїх секторах і вживають заходів для її покращення на рівні правління.

«Ці висновки показують, що кібербезпека — це не просто IT-проблема — це корпоративний ризик, який суттєво впливає на продуктивність компанії в найближчій перспективі та здоров’я в довгостроковій перспективі. Керівництво та правління повинні бути в курсі цього ризику», - сказала Дотті Шиндлінгер, виконавчий директор Diligent Institute.

«Зі збільшенням тиску з боку регулюючих органів на організації, щоб продемонструвати, як вони здійснюють нагляд за кібербезпекою, настав час для правлінь і керівників розвинути свою компетентність щодо кіберризиків». ***(Jill McKeon. Advanced cybersecurity performance translates to higher shareholder returns***

// TechTarget, Inc. (https://healthitsecurity.com/news/advanced-cybersecurity-performance-translates-to-higher-shareholder-returns). 08.04.2024).

***

«UnitedHealth Group (UNH.N) заявила в понеділок, що хакери викрали медичні та особисті дані потенційно «значної частини» американців з її систем у лютому, в той час як найбільший американський медичний страховик намагається обмежити збитки.

Вторгнення в його підрозділ Change Healthcare, який обробляє близько 50% медичних претензій у США, було одним із найгірших хакерських атак, які вразили американську охорону здоров'я, і спричинило масштабні збої в оплаті послуг лікарям і медичним закладам.

Розголошення свідчить про те, що інформація про здоров'я пацієнтів залишається вразливою. Початкова перевірка скомпрометованих даних показала файли із захищеною інформацією про здоров'я або особистою інформацією, «яка може охоплювати значну частину людей в Америці», — йдеться в заяві компанії на своєму веб-сайті.

Ця крадіжка 21 лютого сталася незважаючи на сплату викупу.

«Викуп був сплачений як частина зобов'язання компанії зробити все можливе, щоб захистити дані пацієнтів від розголошення», — сказав CNBC у понеділок виконавчий директор UnitedHealth Ендрю Вітті.

«Ця атака була здійснена зловмисниками, і ми продовжуємо працювати з правоохоронними органами та кількома провідними фірмами з кібербезпеки під час нашого розслідування».

Хакери зазвичай шукають конфіденційні дані, такі як історії пацієнтів, історії хвороби або плани лікування, щоб використовувати їх у подальших злочинних діях або вимагати викуп у таких порушеннях.

Хоча повний аналіз зламаних даних займе «кілька місяців», немає жодних доказів того, що карти лікарів або повні історії хвороби людей були викрадені, заявили в UnitedHealth. У ньому не було зазначено, скільки саме даних людей було

вкрадено, але було зазначено, що він відслідковував онлайн-форуми, де хакери, як правило, витікають або торгують такими пакетами даних.

Група кіберзлочинців, відома як AlphV або BlackCat, яка стоїть за зломом, не відповіла на численні запити про коментарі.

Інша група хакерів опублікувала 22 скріншоти в темній мережі протягом тижня, деякі з яких містили захищені медичні та особисті дані клієнтів UntiedHealth, повідомила компанія, додавши, що наразі їй не відомо про будь-які інші витоки.

Ця група, яка називає себе Ransomhub, що незадоволена філія Blackcat надала їй дані.

Невдовзі після того, як у лютому стало відомо про злом, Blackcat повідомила на своєму веб-сайті, що вкрала 8 терабайт конфіденційних записів із Change Healthcare, щоб пізніше видалити цю заяву без пояснень.

«Ми знаємо, що ця атака викликала занепокоєння та була руйнівною для споживачів і постачальників, і ми прагнемо зробити все можливе, щоб допомогти та надати підтримку всім, хто може її потребувати», — заявив генеральний директор UnitedHealth Вітті у повідомленні компанії». ***(Manas Mishra and Zeba Siddiqui. UnitedHealth says hackers possibly stole large number of Americans' data // Reuters (https://www.reuters.com/technology/cybersecurity/unitedhealth-says-hack-could-impact-data-substantial-proportion-americans-2024-04-22/). 23.04.2024).***

***

Захист персональних даних та соціальні мережі

Масштабні витоки персональних даних

«Експерт з кібербезпеки Джеремія Фаулер повідомляє, що вони виявили вразливу базу даних, що містить особисті дані майже 300 000 пасажирів таксі Великобританії та Ірландії.

Повідомляється, що розкрита база даних, пов’язана з дублінською технологічною компанією iCabbi, не була захищена паролем ще в січні, що робило доступ до конфіденційної інформації.

З тих пір iCabbi видалив файл даних і повідомив операторів таксі про подію. Технічна фірма також вжила додаткових заходів, щоб переконатися у відсутності інших потенційних ризиків.

Фаулер, дослідник кібербезпеки для vpnMentor, повідомив про недолік, який включав 22 745 записів. Вони містили імена, адреси електронної пошти, номери телефонів та ідентифікатори користувачів у різних доменах, включаючи основних постачальників електронної пошти та престижні установи. Зокрема, серед зламаних були адреси електронної пошти, пов’язані з BBC, NIH, Казначейством Її Величини, Міністерством юстиції та кількома університетами та урядовими департаментами.

Дані, зібрані в документах CSV, також виявили ділову приналежність викритих осіб, що посилило занепокоєння щодо конфіденційності та безпеки. Відповідно до відповіді iCabbi на відкриття, характер порушення припускає, що це могло статися через недогляд під час процесу міграції даних клієнтів.

iCabbi спеціалізується на диспетчерських технологіях операторів таксі та приватних автомобілів на прокат.

За словами Фаулера, компанія негайно відреагувала, захистивши базу даних і розпочавши внутрішній аудит, щоб оцінити ступінь порушення та будь-які подальші вразливості. Вони також визнали інцидент, пов’язаний з людською помилкою, і висловили своє зобов’язання поінформувати постраждалих клієнтів.

У відповідь безпосередньо Фаулеру iCabbi заявив: «Ще раз дякую, що звернули на це мою увагу — ми видалили записи. На жаль, виною тут є людська помилка... частина міграції клієнтів, але ми не повинні використовувати загальнодоступні папки. Ми збираємося взаємодіяти з клієнтами, щоб повідомити їм про це порушення».

Фаулер сказав: «Я не маю на увазі жодних протиправних дій з боку iCabbi, їхніх партнерів, клієнтів чи клієнтів. Я також не кажу, що ці дані перебували під загрозою або до них були доступні інші особи».

Представник iCabbi сказав у відповідь на висновки vpnMentor: «Ще в січні цього року автор сьогоднішнього допису на vpnMentor повідомив нам про дані, які залишилися в загальнодоступному файлі AWS, результат міграції даних таксомоторної компанії з однієї програми. до іншого.

«Ми видалили файл даних, повідомили компанії таксі про подію та вжили додаткових заходів, щоб переконатися, що немає інших потенційних випадків.

«Наша система не була зламана, і автор публікації, який, за його власними словами, виступає як «етичний хакер», похвалив нас за такі швидкі та професійні дії.

«Ми не знаємо, чому vpnMentor, веб-сайт, який рекламує себе як «відданий і корисний інструмент для навігації VPN і веб-конфіденційності», вирішив опублікувати цю статтю сьогодні – ми не отримали попереднього повідомлення про публікацію. Ми з повагою вважаємо, що назва публікації вводить в оману». ***(Perry Richardson. iCabbi have taken vital steps to ensure no other potential exposures after cyber security discovery // TaxiPoint (https://www.taxi-point.co.uk/post/data-breach-at-icabbi-exposes-records-of-nearly-300-000-taxi-and-phv-passengers). 12.04.2024).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Такі інструменти штучного інтелекту, як Midjourney, ChatGPT-5 і DALL-E, можуть змінити правила гри, коли йдеться про створення контенту, але, на жаль, багато з них закриті для підписки або доступні лише в обмеженому доступі.

Хакери не люблять нічого більше, ніж щось дефіцитне, і згідно з новим звітом Bitdefender, вони розробили складний спосіб використання цих інструментів - і доступу до них - для зараження користувачів, які нічого не підозрюють, шкідливим програмним забезпеченням, що викрадає інформацію.

Як і у випадку з іншими онлайн-шахрайствами, ця кампанія починається у Facebook, перш ніж потенційні жертви потрапляють на шкідливий сайт, який контролюють хакери, що стоять за цією кампанією. Звідти шкідлива реклама використовується для зараження тих, хто цікавиться штучним інтелектом, різними видами небезпечного шкідливого програмного забезпечення.

Хоча поки що ця кампанія в основному була націлена на європейських користувачів, її можна переробити, щоб переслідувати тих, хто шукає інструменти штучного інтелекту на Facebook і в інших країнах. Ось усе, що вам потрібно знати про те, як хакери використовують популярність інструментів штучного інтелекту у своїх атаках, а також кілька порад про те, як захиститися від зловмисного програмного забезпечення, яке викрадає інформацію.

Ця шкідлива кампанія починається з того, що хакери заволоділи існуючими обліковими записами Facebook. Це поширена тактика, яку використовують кіберзлочинці, оскільки вони можуть використовувати існуючу репутацію облікового запису чи сторінки та підписників для власної вигоди.

Після того, як обліковий запис зламано, хакери змінюють його на тему штучного інтелекту з новою обкладинкою та фотографіями профілю, а також описами, щоб виглядати так, ніби ним керує одна з відомих компаній, що займаються створенням зображень і відео зі штучним інтелектом. Звідси вони намагаються підвищити легітимність сторінки новинами, фотографіями та рекламою, згенерованими штучним інтелектом, щоб надалі імітувати будь-який генератор зображень штучного інтелекту чи службу генератора відео, яку вони хочуть використати у своїх атаках. Вони також додають посилання, на які нічого не підозрюють користувачі можуть натиснути, щоб отримати безкоштовний доступ або безкоштовну пробну версію цього конкретного інструменту ШІ. Кінцева мета всього цього — змусити користувачів натиснути посилання на шкідливий сайт, звідки зловмисне програмне забезпечення буде завантажено на їхні пристрої.

Під час свого розслідування дослідники безпеки Bitdefender виявили, що відповідальні хакери використовували зовсім інший підхід до Midjourney. Для інших інструментів штучного інтелекту вони закликали відвідувачів завантажити

останні версії з Dropbox або Google Drive, але з Midjourney вони створили більше дюжини шкідливих сайтів, які імітували фактичну цільову сторінку інструменту. Потім ці сайти намагалися обманом змусити відвідувачів завантажити останню версію інструменту за посиланням GoFile.

У всіх розповсюджених у рамках цієї кампанії зловмисних програмах для крадіжки інформації є одна спільна риса: усі вони використовують бізнес-модель шкідливих програм як послуги. Для тих, хто не знайомий, ці види зловмисного програмного забезпечення розробляються кіберзлочинцями, а потім купуються іншими хакерами, щоб використовувати їх у своїх атаках як підписку. Так, навіть хакери теж завалені послугами підписки. Загалом ми маємо справу з чотирма різними штамами зловмисного програмного забезпечення для крадіжки інформації, зокрема Rilide, Vidar, ICERAT і Nova.

Дослідники безпеки Bitdefender помітили, що нова версія Rilide Stealer використовувалася в ряді спонсорованих рекламних кампаній, які імітували інструменти ШІ та фоторедактори, зокрема Sora, CapCut, Gemini AI, Photo Effects Pro та CApCut Pro. Це зловмисне програмне забезпечення є зловмисним розширенням, яке видає себе за розширення Google Translate і націлене на браузери на базі Chromium, як-от Chrome, Edge, Brave та Opera, щоб відстежувати історію веб-перегляду жертви, збирати її облікові дані для входу та навіть викрадати криптовалюту, обходячи двофакторну автентифікацію (2FA).

З цих кількох кампаній, що імітують інструменти штучного інтелекту, та, що включає Midjourney, була найуспішнішою та залишалася активною найдовше. Як зазначає BleepingComputer, сторінка Facebook, яка імітує Midjourney, змогла залучити 1,2 мільйона підписників і залишалася активною протягом майже року, перш ніж її закрили. Однак ця фейкова сторінка була закрита Meta.

Як і під час завантаження безкоштовних програм в офіційних магазинах додатків, ви повинні бути обережними, коли справа доходить до спробування нових інструментів ШІ. Наприклад, ще немає версії Midjourney для настільних ПК, але це не завадило хакерам, які стоять за цією кампанією, рекламувати її в Інтернеті.

Ми бачили, як подібну тактику використовували з підробленими програмами ChatGPT, коли OpenAI чат-бот ще не був відкритий для всіх. Хакери обдурили б нічого не підозрюючих користувачів швидким доступом і шансом перескочити в чергу, лише щоб заразити їх шкідливим програмним забезпеченням.

З цієї причини найкраще перейти на офіційну сторінку інструментів штучного інтелекту та провести багато досліджень, перш ніж щось встановлювати. Швидкий онлайн-пошук дасть вам знати, чи має генератор зображень зі штучним інтелектом або інший інструмент версію для настільного комп'ютера чи програму для мобільних пристроїв. Будь-хто, хто стверджує щось інше, швидше за все, є хакером, який намагається вас обдурити.

У той же час ви хочете уникати натискання на рекламу, незалежно від того, наскільки законною вона може здаватися на перший погляд. Хакерам легко купити рекламний простір і запустити шкідливу рекламу в Інтернеті, тому я особисто рекомендую вам не натискати жодну рекламу. Якщо ви бачите рекламну акцію щодо продукту, який вас цікавить, просто перейдіть на сторінку цієї компанії, де ви, ймовірно, знайдете його за тією самою розпродажною ціною.

Щоб захистити себе, ви повинні використовувати найкраще антивірусне програмне забезпечення для свого ПК, найкраще антивірусне програмне забезпечення для Mac з вашим комп'ютером Apple і одну з найкращих антивірусних програм для Android з вашим телефоном Android. Немає еквівалента останнього для найкращих iPhone, але антивірусне програмне забезпечення Mac від Intego може сканувати iPhone або iPad на наявність зловмисного програмного забезпечення, але лише тоді, коли вони підключені через USB до Mac.

Іншим корисним інструментом від Bitdefender для виявлення шахрайства є Scamio. Цей детектор шахрайства на основі штучного інтелекту може розповісти вам усе, що вам потрібно знати про те, чи є електронний лист, повідомлення чи веб-сайт насправді шахрайством, і ви можете завантажити підозрілі посилання, знімки екрана чи навіть QR-коди в службу для оцінки.

Методи, які хакери використовують у своїх атаках, і людська природа йдуть рука об руку, оскільки вони часто намагаються використовувати наші емоції чи

бажання першими спробувати щось нове. Проте, проявляючи терпіння та обережність в Інтернеті, ви можете уникнути зараження своїх пристроїв шкідливим програмним забезпеченням і викрадення особистих даних». ***(Anthony Spadafora. 1.2 million people fooled by fake MidJourney Facebook page used to spread malware — don't fall for this // Future US, Inc. (https://www.tomsguide.com/computing/malware-adware/12-million-people-fooled-by-fake-midjourney-facebook-page-used-to-spread-malware-dont-fall-for-this?utm_source=flipboard&utm_content=onelife007%2Fmagazine%2FInteresting+Spaces%21). 05.04.2024).***

***

«Пропозиція Microsoft Copilot for Security стала загальнодоступною в понеділок, надаючи партнерам і користувачам інструмент штучного інтелекту, який обіцяє швидше реагування на кіберзагрози, оцінку ризиків і обробку сигналів.

Підсумок інцидентів, зворотне проектування сценаріїв і керовані покрокові інструкції для реагування на інциденти є одними з можливостей Copilot for Security, згідно з Редмондом, штат Вашингтон, Microsoft.

Корпорація Майкрософт застосувала деякі інші підходи до Copilot for Security порівняно з Copilot для Microsoft 365, включаючи модель ціноутворення та дозвіл учасникам партнерської програми Cloud Solution Provider (CSP) продавати Copilot for Security одночасно з GA.

Корі Кіркендолл, генеральний директор і президент 5K Technical Services, учасник рейтингу CRN US 2024 MSP 500 із штату Техас, сказав в інтерв'ю CRN US, що він є одним із постачальників рішень Microsoft, які прагнуть побачити, чим Copilot for Security може допомогти його бізнес стежить за всіма заходами, які контролюються, щоб забезпечити кібербезпеку клієнтів.

«Це дає деяким людям перевагу, коли справа доходить до того, як ми обробляємо цю частину з точки зору безпеки Microsoft», — сказав Кіркендолл.

Тим не менш, Кіркендолл сказав, що до використання ціни на основі споживання Copilot for Security може знадобитися звикання, на відміну від моделі ціни за ліцензію Copilot для Microsoft 365.

Він сподівається, що можливості других пілотів виділяються достатньо, щоб клієнти не завищували ціни.

«Нам легше використовувати модель для кожного користувача та йти цим шляхом», — сказав він.

«Але сьогодні ми дійсно зведемося до того, що ми не зосереджуватимемося на ціні, а це означає, що ми продовжуємо наполягати на тому, що ми робимо, продаючи вартість, чому ви це робите. Тоді ціна стає спірним питанням».

Ендрю Ходжес, віце-президент із надання послуг постачальника рішень Microsoft Difenda, розташованого в Оквіллі, штат Онтаріо, який був частиною партнерського приватного періоду попереднього перегляду Copilot for Security, сказав у нещодавньому інтерв'ю CRN US, що інструмент штучного інтелекту має допомогти в обміні інформацією з молодших співробітників, повертаючи старшим співробітникам час для більш складних завдань.

«Ми бачимо величезні можливості для справжнього покращення способів нашої роботи — більшої послідовності, вищої якості тощо», — сказав Ходжес.

«Ми не думаємо, що це замінить людей, як таке, це справді допомогло доповнити та підвищити послідовність, якість і швидкість, з якою ми надаємо наші послуги».

Щодо моделі ціноутворення Copilot for Security, він сказав, що бачить плюси та мінуси в ціноутворенні на основі ліцензії та споживання, але щодо споживання йому подобається, що користувачі економлять гроші в періоди низької активності.

«Це має сенс», — сказав він. «Це масштабоване. Ви можете занурити палець ноги у воду, а потім накип. Ви можете стати досить передбачуваними, коли моделюєте кілька варіантів використання».

Незважаючи на те, що Copilot for Security доступний у CSP того самого дня, коли він став GA, учасникам CSP довелося чекати до 16 січня, щоб продати Copilot для M365, хоча він став GA для корпоративних клієнтів 1 листопада.

Вимоги щодо мінімальної кількості місць також обмежували використання Copilot для M365 невеликими організаціями, поки Microsoft не скасувала їх

Copilot for Sales і Copilot for Service стали GA 1 лютого, але не стали доступними через CSP new commerce experience (NCE) до 1 березня. Ці два копілоти коштують 50 доларів США за користувача на місяць або 20 доларів США як доповнення до Copilot для M365.

У той час як Copilot для M365 коштує 30 доларів США за користувача на місяць із річним зобов'язанням, Copilot for Security коштує 4 долари США за обчислювальну одиницю безпеки (SCU) на годину.

Згідно з даними Microsoft, клієнти отримують щомісячний рахунок за кількість SCU, наданих щогодини для виконання робочих навантажень Copilot for Security.

Споживання SCU залежить від кількості виконаних запитів і складності кожного запиту, а не від кількості аналітиків чи пристроїв.

Крім того, Copilot для M365 вимагає, щоб користувачі мали M365 E3, E5, Business Standard або Business Premium або Office 365 E3, O365 E5.

За словами Microsoft, єдиною необхідною умовою для Copilot for Security є обліковий запис Azure.

Крім того, починаючи з понеділка, у Партнерському центрі Microsoft працює робоче середовище безпеки, яке покликане допомогти «Партнери оцінюють свою безпекову ситуацію та вживають необхідних заходів для підвищення рівня безпеки», — йдеться в публікації постачальника.

«Робочий простір полегшить роботу користувача, надасть навчальні ресурси та стане єдиним місцем для всіх питань, пов'язаних із безпекою, у Партнерському центрі».

Понеділок також знаменує собою початок загальнодоступної попередньої версії Copilot в Intune, повідомляє Microsoft. Інші інструменти копілотів у попередній версії включають Copilot для фінансів і Copilot для Azure». ***(Wade Tyler Millward. Microsoft Copilot for Security is generally available, adding AI to cyber fight***

// nextmedia Pty Ltd. (https://www.crn.com.au/news/microsoft-copilot-for-security-is-generally-available-adding-ai-to-cyber-fight-606606). 02.04.2024).

***

«Джейлбрейки ChatGPT стали популярним інструментом для кіберзлочинців і продовжують поширюватися на хакерських форумах майже через два роки після публічного релізу революційного чат-бота.

За цей час було розроблено та просунуто кілька різних тактик як ефективних способів обійти політику OpenAI щодо контенту та безпеки, що дозволило зловмисникам створювати фішингові електронні листи та інший шкідливий контент.

«Поширеність підказок для джейлбрейку та зловживання ШІ на форумах, присвячених кіберзлочинності, безумовно, зросла з перших днів існування ChatGPT. Хоча перші дискусії про потенціал технології відбувалися у 2022/2023 роках, з часом ми спостерігаємо зростаючу тенденцію до детальних обговорень конкретних підказок для джейлбрейку», - повідомив SC Media Майк Бріттон, директор з інформаційної безпеки компанії Abnormal Security, у своєму електронному листі. «Зараз існують цілі розділи форуму, присвячені зловживанню штучним інтелектом, зокрема, на двох великих форумах, присвячених кіберзлочинності».

До цієї тактики вдаються не лише «діти зі скриптами». Раніше цього року Microsoft виявила, що члени п'яти спонсорованих державою угруповань з Росії, Північної Кореї, Ірану та Китаю використовували ChatGPT для виконання різноманітних завдань - від соціальної інженерії до допомоги в написанні скриптів і дослідження вразливостей.

У дослідницькому звіті за 2023 рік компанія Abnormal Security виявила п'ять шкідливих email-кампаній, які, ймовірно, були створені чат-ботами зі штучним інтелектом, відзначивши здатність ШІ застосовувати тактику соціальної інженерії, наприклад, створювати відчуття терміновості при створенні своїх листів.

Підозрювані листи, створені штучним інтелектом, також не містили орфографічних і граматичних помилок, які часто зустрічаються у фішингових листах, що надає їм додаткової легітимності.

«Найпоширеніший випадок використання джейлбрейку ChatGPT (і використання інших шкідливих версій) - це запуск атак соціальної інженерії, чи то для компрометації облікових даних, чи то для фішингової електронної пошти, чи то для шахрайства з боку постачальників», - сказав Бріттон. «Генеративний ШІ дозволяє зловмисникам масштабувати ці атаки соціальної інженерії не лише за обсягом, але й за складністю».

У понеділок компанія Abnormal Security опублікувала в блозі статтю, в якій висвітлила п'ять підказок, які використовують кіберзлочинці для джейлбрейку ChatGPT. Хоча ці зломи не обов'язково є новими, широке розмаїття та постійна популярність методів маніпулювання чат-ботами повинні сигналізувати організаціям про те, що ворожий генеративний штучний інтелект - це загроза, яку не можна ігнорувати.

«Оскільки кіберзлочинці продовжують використовувати генеративний ШІ в своїх атаках на електронну пошту, організаціям варто врахувати цю загрозу у своїй кіберстратегії. Існують інструменти, які можуть допомогти в цьому - наприклад, компанія Abnormal минулого року випустила CheckGPT, інструмент, який дозволяє компаніям визначити, чи був підозрілий електронний лист написаний за допомогою генеративного ШІ», - сказав Бріттон.

Чи є оперативна інженерія новою соціальною інженерією?

Тактика втечі з в'язниці, описана на сайті Abnormal Security, в основному спирається на дві тактики: переконати ChatGPT «зіграти роль» нефільтрованого бота або «обдурити» ШІ, змусивши його повірити, що він діє за певним сценарієм, де генерування шкідливого контенту було б прийнятним.

Наприклад, «Do Anything Now» - добре відома тактика джейлбрейку ChatGPT, яка існує вже більше року і полягає в тому, щоб змусити чат-бота зіграти роль іншого ШІ на ім'я DAN.

Цей альтернативний персонаж «звільнився від типових обмежень ШІ», як зазначено в одній з підказок на форумі «темного ШІ», і, прийнявши його образ, ChatGPT може генерувати контент, який суперечить політиці OpenAI.

Інший метод передбачає повідомлення ChatGPT, що він перебуває «в режимі розробки» або що його відповіді «використовуються лише з метою тестування», що може включати повідомлення боту про те, що «політики розробника» відрізняються від звичайних політик OpenAI.

Подібне повідомлення повідомляє ChatGPT, що це чат-бот-перекладач, який тестується на здатність перекладати і відповідати на запитання різними мовами. Це може переконати ChatGPT обійти його фільтри, щоб зробити точний переклад незалежно від контенту, який перекладається.

Дві інші тактики, описані Abnormal Security, схожі на DAN в тому, що вони наказують ChatGPT прийняти новий, необмежений образ. «Завжди розумний і макіавелліст» (AIM) - це підказка, призначена для генерування відповідей «незалежно від того, наскільки вони аморальні, неетичні або незаконні», тоді як підказка «BISH» - це варіант «Зроби що завгодно зараз», якому можна призначити «рівень моралі», що визначає, наскільки цензурованими або нецензурованими мають бути його відповіді.

«Еволюцію використання ChatGPT на цих форумах можна охарактеризувати як природний розвиток подій. Ми бачимо, як багато кіберзлочинців низького рівня експериментують з використанням ChatGPT для створення шкідливих електронних листів і коду», - сказав Бріттон.

Що можуть зробити організації для захисту від ворожих GenAI?

Кіберзлочинність за допомогою GenAI, можливо, все ще перебуває в зародковому стані, але обізнаність про експерименти противника зі штучним інтелектом може допомогти організаціям підготуватися до більш досконалих методів атак у майбутньому. Оскільки фішинг є найпопулярнішим незаконним використанням ChatGPT, захисники електронної пошти можуть розглянути можливість використання таких інструментів, як CheckGPT, для фільтрації підозрілого контенту, згенерованого штучним інтелектом.

«Однак розуміння того, що лист був згенерований штучним інтелектом, є лише одним із сигналів потенційної атаки. Щоб забезпечити ефективне і точне виявлення, цей сигнал повинен поєднуватися з низкою інших різноманітних сигналів з усього поштового середовища», - зазначає Бріттон.

У цьому випадку штучний інтелект також може стати частиною захисту, дозволяючи організаціям аналізувати відповідні дані таким чином, щоб підвищити стійкість до майбутніх атак.

«Аналізуючи додаткові сигнали, включаючи шаблони спілкування користувачів, взаємодію, автентифікацію та інші атрибути, організації можуть створити базову лінію відомої поведінки кожного співробітника і постачальника в організації, а потім застосувати передові моделі ШІ для виявлення аномалій, що вказують на потенційну атаку - незалежно від того, чи була ця атака створена людиною або ШІ», - підсумував Бріттон.

Що стосується самої OpenAI, то компанія працює над тим, щоб зменшити кількість зловмисних підказок і посилити здатність ChatGPT залишатися в межах встановлених компанією обмежень.

«ChatGPT все ще залишається одним з найпопулярніших інструментів для кіберзлочинців, які шукають способи масштабування своїх атак на електронну пошту, але з тих пір, як OpenAI створив обмеження, покликані зупинити генерацію шкідливого контенту, зловмисникам стало складніше ефективно запускати атаки за допомогою цього інструменту», - пояснив Бріттон. «Це призвело до створення шкідливих версій ChatGPT, таких як WormGPT і FraudGPT, які зазвичай можна придбати через темну мережу».

Однак захиститися від джейлбрейків складно через нескінченну кількість можливих підказок, які хтось може створити, намагаючись маніпулювати моделлю штучного інтелекту. У деталях своєї програми винагород за виправлення помилок, яка була запущена в квітні 2023 року, OpenAI чітко зазначає, що винагороди за «джейлбрейки» не передбачені: «Хоча ми докладаємо всіх зусиль для запобігання ризикам, ми не можемо передбачити, чи будуть люди використовувати або зловживати нашою технологією в реальному світі кожного дня».

Оскільки в понеділок OpenAI оголосила, що ChatGPT незабаром стане доступним для користувачів без облікових записів OpenAI, але з «додатковим захистом контенту», залишається тільки з'ясувати, чи прискорить розширення доступу до чат-бота спроби кіберзлочинців здійснити злом». ***(Laura French. ChatGPT jailbreak prompts proliferate on hacker forums // CyberRisk Alliance, LLC (https://www.scmagazine.com/news/chatgpt-jailbreak-prompts-proliferate-on-hacker-forums). 02.04.2024).***

***

«Експерти прогнозують, що через швидке поширення кіберзагроз кіберзлочинність коштуватиме американським компаніям 452 мільярди доларів у 2024 році, і ця цифра швидко зростатиме в найближчі кілька років.

Забезпечення надійних заходів кібербезпеки — це вже не просто рекомендація — це вкрай важливо для підтримки бізнес-операцій. Зараз штучний інтелект став незамінним інструментом кібербезпеки, наприклад, від інструментів виявлення фішингу до чат-ботів ШІ, які можуть відповідати на запити щодо кібербезпеки.

Виконуючи та оптимізуючи повторювані завдання, AI звільняє людські ресурси для більш стратегічних ініціатив у сфері безпеки. Проте штучний інтелект у сфері кібербезпеки не є надійним, тому важливо розуміти як плюси, так і мінуси.

ШІ прокладає шлях до успіху чи невдачі?

Оскільки ШІ продовжує розвиватися, зростає і його роль у кібербезпеці. Системи ШІ пропонують безцінні інструменти для захисту від кіберзагроз. Однак організації повинні обережно орієнтуватися в складнощах і проблемах.

Боротьба з кіберзагрозами або їх створення

Однією з найбільш значущих переваг штучного інтелекту в кібербезпеці є його здатність передбачати загрози та визначати потенційні загрози до того, як вони виявляться. Аналізуючи шаблони даних і виявляючи аномалії, штучний інтелект може попередити про ризики, які в іншому випадку могли б залишитися непоміченими, поки не стане надто пізно.

Однак така ж складність, яка дозволяє ШІ передбачати загрози, може зробити його корисним інструментом для зловмисників. Хакери можуть використовувати штучний інтелект для створення складніших шахрайств, які можуть обійти традиційні заходи безпеки (наприклад, фільтри для захисту від спаму для електронних листів). Крім того, хакери можуть застосувати тактику соціальної інженерії, керовану штучним інтелектом, щоб створювати підроблені повідомлення чи запити, які виглядають особистими та переконливими. Ці повідомлення можуть обманом змусити людей надати конфіденційну інформацію або отримати доступ до захищених систем.

Виявлення загроз — благословення і прокляття

AI чудово забезпечує негайне реагування на інциденти безпеки. Він може автоматизувати процеси, заощаджуючи час і мінімізуючи шкоду шляхом ізоляції заражених систем і блокування втручальних дій.

Але ця автоматизована система швидкого реагування іноді може мати зворотний ефект. Визначення штучним інтелектом того, що є загрозою, не завжди може бути точним, що призводить до помилкових спрацьовувань, які можуть порушити бізнес-операції. Крім того, якщо суб'єкти загроз розуміють схему відповіді ШІ, вони потенційно можуть маніпулювати системою, щоб викликати бажану реакцію, повертаючи швидкість ШІ проти нього самого.

Безперервне (не)навчання та (де)еволюція

Системи штучного інтелекту створені для навчання та розвитку, а це означає, що вони стають ефективнішими, оскільки обробляють більше даних. Ця здатність постійно вчитися на основі взаємодії та нових загроз робить їх все більш вправними у розпізнаванні та реагуванні на ландшафт кібернетичних ризиків, що постійно змінюється.

Парадоксально, але цю силу можна використовувати. Якщо суб'єктам загрози вдасться надати системам штучного інтелекту маніпульовані дані (відомі як «отруєння даних»), вони можуть спотворити процес навчання штучного інтелекту, що призведе до неточних моделей, які не зможуть виявити справжні загрози або, що ще гірше, вважатимуть зловмисну діяльність безпечною.

Чи можуть технології перехитрити обман?

Незважаючи на те, що штучний інтелект приносить багато переваг кібербезпеці, кожна перевага супроводжується власним набором проблем. Ці проблеми підкреслюють необхідність ретельного та стратегічного підходу до інтеграції штучного інтелекту в кіберсферу, гарантуючи, що ці потужні інструменти підвищують безпеку, а не випадково її підривають.

У міру розвитку технологій штучного інтелекту онлайн-загрози розвиваються відповідно, і їх стає важче виявити. Їжа для роздумів: чи збережемо ми перевагу в цій гонці технологічних озброєнь із високими ставками, чи будемо надмірно використовувати штучний інтелект настільки, що не зможемо розпізнати, що є нормальним, а що загрозою?» ***(Vytautas Kaziukonis. AI In Cybersecurity: Understanding The Advantages And Disadvantages // Forbes (https://www.forbes.com/sites/forbestechcouncil/2024/04/12/ai-in-cybersecurity-understanding-the-advantages-and-disadvantages/?sh=5e507394769a). 12.04.2024).***

***

«У міру того як розширюється технологія розумного дому, розширюється і спектр підключених пристроїв, більш відомих як Інтернет речей (IoT). Від розумних замків і дверей з розпізнаванням обличчя до інтелектуальних термостатів і навіть пристроїв Інтернету тіл (IoB), таких як розумні кардіостимулятори: різноманітність і кількість пристроїв IoT зростає, тоді як рівень кібербезпеки цих пристроїв IoT відстає.

У цій статті наведено загальний огляд вхідних зобов’язань щодо кібербезпеки та зобов’язань для пристроїв Інтернету речей відповідно до Закону ЄС про кіберстійкість (CRA), переглянутої Директиви про відповідальність за продукт (PLD) і Закону про штучний інтелект, за винятком пов’язаних зобов’язань згідно (запропонованого) законодавства, наприклад як NIS2, DORA, Закон про дані та Загальні правила безпеки продукції.

Нові зобов’язання щодо безпеки для пристроїв Інтернету речей відповідно до Закону про кібернетостійкість

У березні 2024 року Європейський парламент схвалив CRA, залишивши лише схвалення Ради, перш ніж CRA стане законом. CRA застосовуватиметься до «продуктів із цифровими елементами» (PDE), які в широкому сенсі визначаються як усі програмні та апаратні продукти та їхні рішення для віддаленої обробки даних, які доступні на ринку, якщо запланована мета або розумно передбачуване використання включає пряме чи непряме логічне або фізичне з'єднання даних із пристроєм чи мережею – коротше кажучи, всі апаратні та програмні продукти, які під час використання можуть мати з'єднання з даними або мережею. CRA виключає медичні пристрої, авіацію та автомобілі, на які вже поширюються існуючі правила.

PDE можуть бути розміщені на ринку, лише якщо вони відповідають досить загальним «основним вимогам», перерахованим у Додатку I CRA. Конкретне формулювання вимог має відбутися в так званих «гармонізованих стандартах», які наразі ще розробляються. «Основні вимоги» включають:

- Кібербезпека за проектом - забезпечення того, що PDE розроблено, розроблено та виготовлено таким чином, щоб вони забезпечували належний рівень кібербезпеки на основі ризиків.
- Кібербезпека за замовчуванням — гарантія того, що PDE будуть доступні на ринку з безпечною конфігурацією за замовчуванням (з можливістю різних договірних угод для індивідуальних продуктів), включаючи можливість скинути продукт до початкового стану.
- Оновлення для усунення вразливостей, які можна усунути за допомогою оновлень безпеки, включно з автоматичними оновленнями безпеки. Такі оновлення мають надаватися протягом періоду підтримки (див. нижче) і залишатися доступними протягом десяти років після розміщення PDE на ринку або протягом решти періоду підтримки, залежно від того, що довше.
- Запобігання несанкціонованому доступу за допомогою відповідних механізмів контролю, таких як автентифікація, ідентифікація або системи керування доступом.

- Захист конфіденційності збережених, переданих чи іншим чином оброблених даних, особистих чи інших, наприклад, шляхом шифрування відповідних даних у стані спокою чи передачі за допомогою найсучасніших механізмів.

- Захист цілісності збережених, переданих або іншим чином оброблених даних, команд, програм і конфігурації від будь-яких маніпуляцій або модифікацій.

- Мінімізація даних шляхом обробки лише даних, особистих чи інших, які є адекватними, релевантними та обмеженими тим, що необхідно щодо передбачуваної мети PDE.

- Захист доступності важливих і базових функцій, зокрема після інциденту, за допомогою заходів стійкості та пом'якшення атак типу «відмова в обслуговуванні» та

- Портативність даних дозволяє користувачам назавжди безпечно та легко видалити всі дані та налаштування, а якщо такі дані можна перенести в інші продукти чи системи, у безпечний спосіб.

Хоча CRA широко застосовується до PDE, він особливо зосереджений на «важливих» або «критичних» PDE. Важливі та критичні продукти розділені на різні списки на основі їх критичності та рівня ризику кібербезпеки, який вони становлять. До важливих і критичних продуктів із цифровими елементами висуваються додаткові вимоги, особливо щодо відповідної оцінки відповідності, як зазначено вище. PDE вважаються «важливими», якщо вони мають основні функції категорії продуктів, викладених у Додатку III, такі як інтелектуальні дверні замки, системи спостереження за дитиною та системи сигналізації, підключені іграшки, операційні системи та персональні переносні медичні технології (клас I) та міжмережевих екранів або систем виявлення чи запобігання вторгненням (Клас II).

Виробники, імпортери та дистриб'ютори PDE мають особливі зобов'язання.

Зобов'язання виробників PDE

До них належать:

Оцінка ризиків – виробники повинні переконатися, що PDE розроблено, розроблено та виготовлено відповідно до «основних вимог». Таким чином,

виробник повинен оцінити ризики, пов’язані з PDE, і брати до уваги результати такої оцінки на всіх етапах життєвого циклу PDE. Оцінка ризику має бути задокументована та оновлена протягом періоду підтримки та повинна включати пояснення того, як виробник дотримується вимог щодо обробки вразливостей.

Документація та звітність – виробники повинні задокументувати відповідні аспекти кібербезпеки, що стосуються PDE, включаючи вразливості, про які їм стало відомо. Будь-які активно використовувані вразливості та інциденти повинні бути повідомлені компетентним національним органам через платформу звітності про інциденти, яку контролює Агентство ЄС з кібербезпеки (ENISA) не пізніше ніж через 24 години після того, як стало відомо про вразливість або інцидент (для попереднього сповіщення) і 72 годин (для повного сповіщення).

Моніторинг і оновлення програмного забезпечення - виробники повинні визначити відповідний період підтримки, враховуючи економічний життєвий цикл продукту та розумні очікування користувачів. Період підтримки має становити принаймні 5 років, за винятком продуктів, які, як очікується, використовуватимуться менше, ніж цей період, і виробники повинні контролювати свої продукти протягом такого періоду та документувати відповідні аспекти кібербезпеки

Оцінка відповідності та маркування CE - виробник повинен виконати відповідну оцінку відповідності, як зазначено в CRA. Для неважливих і некритичних PDE буде достатньо внутрішньої оцінки відповідності. «Важливі» та «критичні» PDE підлягають суворішим процедурам оцінки відповідності. Маркування CE є видимим наслідком оцінки відповідності в широкому сенсі, і його слід наносити на PDE відповідно до CRA.

Прозорість - виробник повинен вести технічну документацію та видавати інструкції для користувача в чіткій та зрозумілій формі. Такі інструкції мають бути надані мовою, яку легко розуміють користувачі та органи ринкового нагляду.

Зобов'язання імпортерів ПДЕ

Перш ніж розмістити PDE на ринку, імпортери повинні переконатися, що:

- відповідні процедури оцінки відповідності були проведені виробником

- виробник склав технічну документацію
- продукт має маркування CE
- виріб супроводжується чіткою, зрозумілою, зрозумілою та розбірливою інформацією та інструкціями, які забезпечують безпечне встановлення, роботу та використання.

Імпортери не повинні розміщувати PDE на ринку, якщо вони вважають, що він не відповідає «основним вимогам».

Зобов'язання дистриб'юторів ПДЕ

Перед розміщенням PDE на ринку дистриб’ютори повинні перевірити, що:

PDE має маркування CE

виробник додав інформацію та інструкції та декларацію відповідності ЄС

імпортер вказав свою назву, зареєстровану торгову назву або зареєстровану торгову марку та контактну адресу на продукті або на його упаковці.

Програмне забезпечення з відкритим кодом

Після жорсткої критики ранніх проектів остання версія CRA містить спеціальні виключення для певного програмного забезпечення з відкритим кодом (OSS), надання якого не передбачає «господарської діяльності». Він вводить концепцію «розпорядника відкритого коду»: юридична особа, яка підтримує розробку OSS, призначеної для комерційної діяльності, і яка відіграє головну роль у забезпеченні життєздатності цих продуктів. Основна робота розпорядника відкритого коду полягає в підтримці та підтримці OSS, гарантуючи, що він залишається безпечним і функціональним для комерційного використання зі штрафами, пов’язаними з недотриманням. У поясненнях до CRA зазначено, що розпорядник відкритого коду підлягає «легкому та індивідуальному режиму регулювання», але CRA все ще залишає багато запитань без відповіді щодо того, хто що робитиме та як нормативне робоче навантаження може бути ефективно розподіленими в складних проектах з відкритим кодом.

Примусове виконання

Держави-члени призначатимуть органи ринкового нагляду, відповідальні за виконання CRA. Вони матимуть повноваження вимагати припинення

невідповідності, забороняти чи обмежувати доступ до невідповідного продукту або наказувати його вилучення чи відкликання.

Органи ринкового нагляду зможуть накладати штрафи з найсуворішим діапазоном покарань у розмірі до 15 мільйонів євро або до 2,5% річного світового обороту, залежно від того, що більше. Держави-члени встановлять власні правила щодо штрафів, які мають бути пропорційними та стримуючими.

Наступні кроки

Тепер CRA має бути офіційно прийнятий Радою, перш ніж він стане законом, що, ймовірно, станеться в квітні 2024 року. Більшість положень буде застосовуватися в повному обсязі через три роки після набуття чинності CRA, але зобов'язання повідомляти про вразливості діятимуть протягом 21 року. місяців.

Розширена відповідальність за кібербезпеку пристроїв (B2C) IoT відповідно до нової Директиви про відповідальність за продукт

CRA не містить жодних конкретних правил щодо відповідальності за (відсутність достатньої) кібербезпеки пристроїв IoT. Натомість CRA посилається на Директиву про відповідальність за продукт (PLD) як на доповнення до CRA. Оскільки PLD вже 40 років, він потребує оновлення, і в грудні 2023 року Європейський парламент і Рада досягли згоди щодо внесення змін до нього. Основні зміни:

Розширений обсяг – «продукт» тепер включатиме програмне забезпечення та файли цифрового виробництва. Це означає, що операційні системи, мікропрограми, комп'ютерні програми та системи штучного інтелекту, незалежно від того, продаються вони як окремий продукт або інтегровані як компоненти в інші матеріальні продукти, підпадають під дію Директиви, і що позивачі можуть отримати компенсацію за матеріальні та не- матеріальної шкоди, а також знищення або пошкодження даних, які не використовуються в професійних цілях.

Більше потенційних відповідачів – окрім (квазі) виробника та імпортера продукту з ЄЕЗ, переглянута PLD накладає сувору відповідальність за відсутність вини на уповноважених представників виробника в ЄС, постачальників послуг виконання (тобто служби зберігання, пакування та доставки). постачальники) і, в

деяких випадках, навіть роздрібні продавці та оператори онлайн-ринку. Компанії, які «суттєво модифікують» продукт поза контролем виробника, вважатимуться фактично виробником модифікованого продукту.

Тягар доведення – переглянута PLD спрямована на спрощення тягаря доведення для позивачів, які зазвичай мають довести, що продукт був дефектним і що це спричинило заподіяну шкоду. На додаток до кількох інших презумпцій, проект передбачає, що як брак, так і причинно-наслідковий зв'язок між дефектом продукту та пошкодженням можна припустити, якщо позивач стикається з надмірними труднощами, зокрема через технічну чи наукову складність.

Це означає, що всі сторони, задіяні в усьому ланцюгу постачання, можуть нести відповідальність за шкоду, спричинену недотриманням певних зобов'язань згідно з CRA. Однак переглянута PLD матиме обмежений вплив щодо відповідальності за недотримання зобов'язань щодо кібербезпеки в ситуаціях B2B, оскільки вона стосується лише продуктів B2C.

Кібербезпека штучного інтелекту речей (AIoT) і зв'язок із Законом про штучний інтелект

Поєднання AI та IoT також відоме як штучний інтелект речей (AIoT). AI додає цінність IoT через машинне навчання та прийняття рішень, тоді як пристрої IoT додають цінність AI через обмін даними, сигналізацію та підключення. На AIoT може поширюватися як CRA, так і Закон AI. Закон про штучний інтелект стосується широкого кола зацікавлених сторін, залучених до розробки, розгортання та використання систем штучного інтелекту в ЄС, і використовує підхід, що ґрунтується на оцінці ризику, тобто Регламент розрізняє різні типи систем штучного інтелекту залежно від рівня ризику. вони позують. Системи штучного інтелекту з високим рівнем ризику, такі як автономні транспортні засоби, системи біометричної ідентифікації або системи оцінки кредитоспроможності, підлягають суворішим вимогам і контролю, ніж системи штучного інтелекту з меншим ризиком, такі як чат-боти.

Що стосується систем штучного інтелекту з високим рівнем ризику, Закон про штучний інтелект містить зобов'язання, які стосуються саме кібербезпеки.

Коротше кажучи, зобов'язання щодо кібербезпеки передбачають, що системи штучного інтелекту з високим рівнем ризику повинні бути розроблені та розроблені таким чином, щоб вони досягали належного рівня точності, надійності та кібербезпеки та працювали стабільно протягом усього життєвого циклу. CRA містить спеціальну домовленість для ситуацій, коли PDE також кваліфікується як система штучного інтелекту високого ризику відповідно до Закону про штучний інтелект: якщо система штучного інтелекту та процеси, запроваджені виробником, відповідають «основним вимогам» і необхідному рівню кібернетичного захисту. захист безпеки продемонстровано у відповідній декларації про відповідність, за певних обставин можна вважати, що система ШІ відповідає зобов'язанням щодо кібербезпеки відповідно до Закону про ШІ.

Закон про AI був схвалений Європейським парламентом у березні 2024 року та має бути офіційно схвалений Радою. Він набуде чинності через двадцять днів після його публікації в Офіційному віснику та (здебільшого) буде застосовуватися через 24 місяці після набуття ним чинності. Зобов'язання для систем високого ризику будуть застосовуватися через 36 місяців після набрання ним чинності.

Що далі?

Тепер, коли законодавчі ініціативи, про які йдеться вище, знаходяться на завершальній стадії законодавчого процесу, постачальники PDE можуть підготуватися, почавши оцінювати, чи підпадають їхні продукти та послуги в сферу дії наступного законодавства, і, якщо так, до якої категорії вони належать. Далі їм потрібно буде оцінити, які конкретні зобов'язання вони повинні виконувати та яким чином. На практиці це буде непростим завданням, оскільки деякі визначення не є достатньо конкретними, а основні стандарти та рамки ще не встановлені, особливо щодо внутрішньої оцінки відповідності». ***(Martijn Loth, Dominique Lensink. IoT and new EU cyber security obligations and liabilities // Taylor Wessing (https://www.taylorwessing.com/en/global-data-hub/2024/cyber-security---weathering-the-cyber-storms/iot-and-new-eu-cyber-security-obligations-and-liabilities). 18.04.2024).***

***

«У міру того як розширюється технологія розумного дому, розширюється і спектр підключених пристроїв, більш відомих як Інтернет речей (IoT). Від розумних замків і дверей з розпізнаванням обличчя до інтелектуальних термостатів і навіть пристроїв Інтернету тіл (IoB), таких як розумні кардіостимулятори: різноманітність і кількість пристроїв IoT зростає, тоді як рівень кібербезпеки цих пристроїв IoT відстає.

У цій статті наведено загальний огляд вхідних зобов'язань щодо кібербезпеки та зобов'язань для пристроїв Інтернету речей відповідно до Закону ЄС про кіберстійкість (CRA), переглянутої Директиви про відповідальність за продукт (PLD) і Закону про штучний інтелект, за винятком пов'язаних зобов'язань згідно (запропонованого) законодавства, наприклад як NIS2, DORA, Закон про дані та Загальні правила безпеки продукції.

Нові зобов'язання щодо безпеки для пристроїв Інтернету речей відповідно до Закону про кібернетостійкість

У березні 2024 року Європейський парламент схвалив CRA, залишивши лише схвалення Ради, перш ніж CRA стане законом. CRA застосовуватиметься до «продуктів із цифровими елементами» (PDE), які в широкому сенсі визначаються як усі програмні та апаратні продукти та їхні рішення для віддаленої обробки даних, які доступні на ринку, якщо запланована мета або розумно передбачуване використання включає пряме чи непряме логічне або фізичне з'єднання даних із пристроєм чи мережею – коротше кажучи, всі апаратні та програмні продукти, які під час використання можуть мати з'єднання з даними або мережею. CRA виключає медичне обладнання, авіацію та автомобілі, на які вже поширюються існуючі правила.

PDE можуть бути розміщені на ринку, лише якщо вони відповідають досить загальним «основним вимогам», перерахованим у Додатку I CRA. Конкретне формулювання вимог має відбутися в так званих «гармонізованих стандартах», які наразі ще розробляються. «Основні вимоги» включають:

Кібербезпека за проектом - забезпечення того, що PDE розроблено, розроблено та виготовлено таким чином, щоб вони забезпечували належний рівень кібербезпеки на основі ризиків

Кібербезпека за замовчуванням — гарантія того, що PDE доступні на ринку з безпечною конфігурацією за замовчуванням (з можливістю різних договірних угод для індивідуальних продуктів), включаючи можливість скинути продукт до початкового стану

Оновлення для усунення вразливостей, які можна усунути за допомогою оновлень безпеки, включно з автоматичними оновленнями безпеки. Такі оновлення мають надаватися протягом періоду підтримки (див. нижче) і залишатися доступними протягом десяти років після розміщення PDE на ринку або протягом решти періоду підтримки, залежно від того, що довше

Запобігання несанкціонованому доступу за допомогою відповідних механізмів контролю, таких як автентифікація, ідентифікація або системи керування доступом

Захист конфіденційності збережених, переданих чи іншим чином оброблених даних, особистих чи інших, наприклад, шляхом шифрування відповідних даних у стані спокою чи передачі за допомогою найсучасніших механізмів

Захист цілісності збережених, переданих або іншим чином оброблених даних, команд, програм і конфігурації від будь-яких маніпуляцій або модифікацій

Мінімізація даних шляхом обробки лише даних, особистих чи інших, які є адекватними, релевантними та обмеженими тим, що необхідно щодо передбачуваної мети PDE

Захист доступності важливих і базових функцій, зокрема після інциденту, за допомогою заходів стійкості та пом’якшення атак типу «відмова в обслуговуванні» та

Портативність даних дозволяє користувачам назавжди безпечно та легко видалити всі дані та налаштування, а якщо такі дані можна перенести в інші продукти чи системи, у безпечний спосіб.

Хоча CRA широко застосовується до PDE, він особливо зосереджений на «важливих» або «критичних» PDE. Важливі та критичні продукти розділені на різні списки на основі їх критичності та рівня ризику кібербезпеки, який вони становлять. До важливих і критичних продуктів із цифровими елементами висуваються додаткові вимоги, особливо щодо відповідної оцінки відповідності, як зазначено вище. PDE вважаються «важливими», якщо вони мають основні функції категорії продуктів, викладених у Додатку III, такі як інтелектуальні дверні замки, системи спостереження за дитиною та системи сигналізації, підключені іграшки, операційні системи та персональні переносні медичні технології (клас I) та міжмережевих екранів або систем виявлення чи запобігання вторгненням (Клас II).

Виробники, імпортери та дистриб'ютори PDE мають особливі зобов'язання.

Зобов'язання виробників PDE

До них належать:

Оцінка ризиків – виробники повинні переконатися, що PDE розроблено, розроблено та виготовлено відповідно до «основних вимог». Таким чином, виробник повинен оцінити ризики, пов'язані з PDE, і брати до уваги результати такої оцінки на всіх етапах життєвого циклу PDE. Оцінка ризику має бути задокументована та оновлена протягом періоду підтримки та повинна включати пояснення того, як виробник дотримується вимог щодо обробки вразливостей.

Документація та звітність – виробники повинні задокументувати відповідні аспекти кібербезпеки, що стосуються PDE, включаючи вразливості, про які їм стало відомо. Про будь-які активно використовувані вразливості та інциденти необхідно повідомляти компетентні національні органи через платформу звітності про інциденти, яка контролюється Агентством ЄС з кібербезпеки (ENISA) не пізніше ніж через 24 години після того, як стало відомо про вразливість або інцидент (для попереднього повідомлення) і 72 годин (для повного сповіщення).

Моніторинг і оновлення програмного забезпечення - виробники повинні визначити відповідний період підтримки, враховуючи економічний життєвий цикл продукту та розумні очікування користувачів. Період підтримки має становити принаймні 5 років, за винятком продуктів, які, як очікується,

використовуватимуться менше, ніж цей період, і виробники повинні контролювати свої продукти протягом такого періоду та документувати відповідні аспекти кібербезпеки

Оцінка відповідності та маркування CE - виробник повинен виконати відповідну оцінку відповідності, як зазначено в CRA. Для неважливих і некритичних PDE буде достатньо внутрішньої оцінки відповідності. «Важливі» та «критичні» PDE підлягають суворішим процедурам оцінки відповідності. Маркування CE є видимим наслідком оцінки відповідності в широкому сенсі, і його слід наносити на PDE відповідно до CRA

Прозорість - виробник повинен вести технічну документацію та випускати інструкції для користувача в чіткій і зрозумілій формі. Такі інструкції мають бути надані мовою, яку легко розуміють користувачі та органи ринкового нагляду.

Зобов'язання імпортерів ПДЕ

Перш ніж розмістити PDE на ринку, імпортери повинні переконатися, що:

- відповідні процедури оцінки відповідності були проведені виробником
- виробник склав технічну документацію
- продукт має маркування CE
- виріб супроводжується чіткою, зрозумілою, зрозумілою та розбірливою інформацією та інструкціями, які забезпечують безпечне встановлення, роботу та використання.

Імпортери не повинні розміщувати PDE на ринку, якщо вони вважають, що він не відповідає «основним вимогам».

Зобов'язання дистриб'юторів ПДЕ

Перед розміщенням PDE на ринку дистриб’ютори повинні перевірити, що:

- PDE має маркування CE
- виробник додав інформацію та інструкції та декларацію відповідності ЄС
- імпортер вказав свою назву, зареєстровану торгову назву або зареєстровану торгову марку та контактну адресу на продукті або на його упаковці.

Програмне забезпечення з відкритим кодом

Після жорсткої критики ранніх проектів остання версія CRA містить спеціальні виключення для певного програмного забезпечення з відкритим кодом (OSS), надання якого не передбачає «господарської діяльності». Він вводить концепцію «розпорядника відкритого коду»: юридична особа, яка підтримує розробку OSS, призначеної для комерційної діяльності, і яка відіграє головну роль у забезпеченні життєздатності цих продуктів. Основна робота розпорядника відкритого коду полягає в підтримці та підтримці OSS, гарантуючи, що він залишається безпечним і функціональним для комерційного використання зі штрафами, пов'язаними з недотриманням. У поясненнях до CRA зазначено, що розпорядник відкритого коду підлягає «легкому та індивідуальному режиму регулювання», але CRA все ще залишає багато запитань без відповіді щодо того, хто що робитиме та як нормативне робоче навантаження може бути ефективно розподіленими в складних проектах з відкритим кодом.

Примусове виконання

Держави-члени призначатимуть органи ринкового нагляду, відповідальні за виконання CRA. Вони матимуть повноваження вимагати припинення невідповідності, забороняти чи обмежувати доступ до невідповідного продукту або наказувати його вилучення чи відкликання.

Органи ринкового нагляду зможуть накладати штрафи з найсуворішим діапазоном покарань у розмірі до 15 мільйонів євро або до 2,5% річного світового обороту, залежно від того, що більше. Держави-члени встановлять власні правила щодо штрафів, які мають бути пропорційними та стримуючими.

Наступні кроки

Тепер CRA має бути офіційно прийнятий Радою, перш ніж він стане законом, що, ймовірно, станеться в квітні 2024 року. Більшість положень буде застосовуватися в повному обсязі через три роки після набуття чинності CRA, але зобов'язання повідомляти про вразливості діятимуть протягом 21 року. місяців.

Розширена відповідальність за кібербезпеку пристроїв (B2C) IoT відповідно до нової Директиви про відповідальність за продукт

CRA не містить жодних конкретних правил щодо відповідальності за (відсутність достатньої) кібербезпеки пристроїв IoT. Натомість CRA посилається на Директиву про відповідальність за продукт (PLD) як на доповнення до CRA. Оскільки PLD вже 40 років, він потребує оновлення, і в грудні 2023 року Європейський парламент і Рада досягли згоди щодо внесення до нього поправок. Основні зміни:

Розширений обсяг – «продукт» тепер включатиме програмне забезпечення та файли цифрового виробництва. Це означає, що операційні системи, мікропрограми, комп'ютерні програми та системи штучного інтелекту, незалежно від того, продаються вони як окремий продукт або інтегровані як компоненти в інші матеріальні продукти, підпадають під дію Директиви, і що позивачі можуть отримати компенсацію за матеріальні та не- матеріальної шкоди, а також знищення або пошкодження даних, які не використовуються в професійних цілях.

Більше потенційних відповідачів – крім (квазі) виробника та імпортера продукту з ЄЕЗ, переглянута PLD накладає сувору відповідальність за відсутність вини на уповноважених представників виробника в ЄС, постачальників послуг виконання (тобто служби зберігання, пакування та доставки). постачальники) і, в деяких випадках, навіть роздрібні продавці та оператори онлайн-ринку. Компанії, які «суттєво модифікують» продукт поза контролем виробника, вважатимуться фактично виробником модифікованого продукту.

Тягар доведення – переглянута PLD спрямована на спрощення тягаря доведення для позивачів, які зазвичай мають довести, що продукт був дефектним і що це спричинило заподіяну шкоду. На додаток до кількох інших презумпцій, проект передбачає, що як брак, так і причинно-наслідковий зв'язок між дефектом продукту та пошкодженням можна припустити, якщо позивач стикається з надмірними труднощами, зокрема через технічну чи наукову складність.

Це означає, що всі сторони, задіяні в усьому ланцюгу постачання, можуть нести відповідальність за шкоду, спричинену недотриманням певних зобов'язань

згідно з CRA. Однак переглянута PLD матиме обмежений вплив щодо відповідальності за недотримання зобов'язань щодо кібербезпеки в ситуаціях B2B, оскільки вона стосується лише продуктів B2C.

Кібербезпека штучного інтелекту речей (AIoT) і зв'язок із Законом про штучний інтелект

Поєднання AI та IoT також відоме як штучний інтелект речей (AIoT). AI додає цінність IoT через машинне навчання та прийняття рішень, тоді як пристрої IoT додають цінність AI через обмін даними, сигналізацію та підключення. На AIoT може поширюватися як CRA, так і Закон AI. Закон про штучний інтелект стосується широкого кола зацікавлених сторін, залучених до розробки, розгортання та використання систем штучного інтелекту в ЄС, і використовує підхід, що ґрунтується на оцінці ризику, тобто Регламент розрізняє різні типи систем штучного інтелекту залежно від рівня ризику. вони позують. Системи штучного інтелекту з високим рівнем ризику, такі як автономні транспортні засоби, системи біометричної ідентифікації або системи оцінки кредитоспроможності, підлягають суворішим вимогам і контролю, ніж системи штучного інтелекту з меншим ризиком, такі як чат-боти.

Що стосується систем штучного інтелекту з високим рівнем ризику, Закон про штучний інтелект містить зобов'язання, які стосуються саме кібербезпеки. Коротше кажучи, зобов'язання щодо кібербезпеки передбачають, що системи штучного інтелекту з високим рівнем ризику повинні бути розроблені та розроблені таким чином, щоб вони досягали належного рівня точності, надійності та кібербезпеки та працювали стабільно протягом усього життєвого циклу. CRA містить спеціальну домовленість для ситуацій, коли PDE також кваліфікується як система штучного інтелекту високого ризику відповідно до Закону про штучний інтелект: якщо система штучного інтелекту та процеси, запроваджені виробником, відповідають «основним вимогам» і необхідному рівню кібернетичного захисту. захист безпеки продемонстровано у відповідній декларації про відповідність, за певних обставин можна вважати, що система ШІ відповідає зобов'язанням щодо кібербезпеки відповідно до Закону про ШІ.

Закон про AI був схвалений Європейським парламентом у березні 2024 року та має бути офіційно схвалений Радою. Він набуде чинності через двадцять днів після його публікації в Офіційному віснику та (здебільшого) буде застосовуватися через 24 місяці після набуття ним чинності. Зобов'язання для систем високого ризику будуть застосовуватися через 36 місяців після набрання ним чинності.

Що далі?

Тепер, коли законодавчі ініціативи, про які йдеться вище, знаходяться на завершальній стадії законодавчого процесу, постачальники PDE можуть підготуватися, почавши оцінювати, чи підпадають їхні продукти та послуги в сферу дії наступного законодавства, і, якщо так, до якої категорії вони належать. Далі їм потрібно буде оцінити, які конкретні зобов'язання вони повинні виконувати та яким чином. На практиці це буде непростим завданням, оскільки деякі визначення не є достатньо конкретними, а основні стандарти та рамки ще не встановлені, особливо щодо внутрішньої оцінки відповідності». ***(Martijn Loth and Dominique Lensink. IoT and new EU cyber security obligations and liabilities // Taylor Wessing (https://www.taylorwessing.com/en/global-data-hub/2024/cyber-security---weathering-the-cyber-storms/iot-and-new-eu-cyber-security-obligations-and-liabilities). 18.04.2024).***

***

«Штучний інтелект (ШІ) є гарячою темою в кібербезпеці, як і практично в кожній галузі зараз, і це справедливо. Штучний інтелект готовий змінити роботу багатьох із нас, причому справжнє питання полягає не в тому, «чи» це вплине на нас, а «скільки». У сфері кібербезпеки штучний інтелект має потенціал змінити правила гри в захисті від кіберзловмисників, які також шукають, як вони можуть використовувати штучний інтелект у своїх інтересах. Це схоже на те, що ви перебуваєте в середині перегонів і раптом виявляєте, що у всіх є ракетний прискорювач, і їм просто потрібно зрозуміти, як його увімкнути.

Штучний інтелект є потужним інструментом, як би ви його не розділили. Але серед ажіотажу також прокралася деяка дезінформація. Щоб по-справжньому

прийняти силу штучного інтелекту, нам потрібно її зрозуміти. Давайте подивимося на деякі з сучасних міфів і на те, як насправді розвиваються справи для штучного інтелекту в кібербезпеці.

Міф 1: кіберзлочинці використовують передові технології ШІ

Потенціал для суб'єктів загрози використовувати штучний інтелект для покращення своєї діяльності був темою, яка активно розголошується в ЗМІ. Однак у звіті про стан загрози Secureworks 2023 зазначено, що зловмисники все ще вивчають і тестують його. Кіберзлочинці — опортуністи, більше схожі на котів-грабіжників, ніж на злочинців. Вони хочуть отримати максимальний результат при мінімальних зусиллях. І саме зараз випробувані методи, які є низькотехнологічними та недорогими, все ще дають свої результати.

Тим не менш, те, що зараз ми не спостерігаємо великого поширення, не означає, що цього не станеться. Вони експериментують з ним, і ми можемо очікувати, що він все більше стане частиною їхнього набору інструментів.

Міф 2: штучний інтелект є новим у захисті кібербезпеки

Однією з найбільших переваг інструментів штучного інтелекту в захисті кібербезпеки є його здатність прискорювати процеси, що він робить уже деякий час. Штучний інтелект може синтезувати величезні обсяги даних і виявляти ідеї зі швидкістю, яку важко досягти людям. Це може зменшити час виявлення, що, у свою чергу, прискорить час відповіді. Що стосується розслідувань, використання ШІ в Secureworks скоротило час розслідування більш ніж на 50% і заощадило аналітикам 90% часу, необхідного для написання розслідувань.

Прискорення та ефективність також допомагають вирішити одну з найбільших проблем сучасної кібербезпеки — брак кадрів. Оскільки дефіцит талантів у сфері кібербезпеки продовжує змушувати все більше організацій робити більше з меншими витратами, ШІ має можливість заповнити прогалини та посилити кіберзахист. Оскільки системи штучного інтелекту продовжують розвиватися та розвиватися, легко уявити день, коли штучний інтелект демократизує доступ до передових технологій безпеки, дозволяючи організаціям

будь-якого розміру мати потужні засоби кібербезпеки, для керування якими не потрібна велика команда експертів.

Саме ця здатність до зростання викликає у багатьох людей захоплення майбутнім ШІ в кібербезпеці. ШІ зможе швидко переглядати історичні дані та використовувати їх для прогнозування потенційних вразливостей і векторів атак. Системи штучного інтелекту можуть існувати в стані постійної еволюції, постійно навчаючись і адаптуючись для підвищення своєї ефективності. Ці вдосконалення можна надалі адаптувати до галузі та цілей організації, щоб створити більше індивідуальних заходів кібербезпеки.

Міф 3: ШІ замінить людей

Важливо підкреслити, що заповнити прогалину в талантах не означає з'ясувати, як ШІ може замінити людей у центрі SecOps. Навпаки, штучний інтелект оптимізується лише тоді, коли професіонали з кібербезпеки вкладають свою інтуїцію, креативність і досвід. Ці якості необхідні для розуміння контексту, прийняття тонких рішень і розробки стратегії.

Наприклад, скажімо, детектор із штучним інтелектом переглядає дані з кінцевої точки в промисловому механічному цеху. Якщо він виявляє загрозу та залишається приймати власне рішення, він може розумно вважати, що ізоляція хоста є найкращим підходом. Однак фахівець із кібербезпеки матиме контекст, що ізоляція хосту призведе до зупинки виробничої лінії, що призведе до величезної втрати часу та грошей для виробника. Фахівці з кібербезпеки можуть розглянути всі нюанси та зрозуміти, що «найкращий підхід» у цій ситуації значною мірою залежатиме від впливу цього вибору на виробника.

Так само, коли мова заходить про етичні та юридичні питання, спеціалісти з кібербезпеки завжди будуть потрібні, щоб орієнтуватися в складних питаннях і гарантувати, що будь-які рішення, які приймає штучний інтелект, приймаються відповідно до юридичних і етичних стандартів.

Замість того, щоб замінити людські рішення, штучний інтелект має неймовірний потенціал, щоб покращити роботу фахівців з кібербезпеки, допомагаючи їм швидше приймати рішення, як показує наш власний скорочений

час розслідування. Автоматизація повсякденних завдань також звільнить час для фахівців з кібербезпеки для розробки нових стратегій кібербезпеки та інноваційних рішень для нових загроз. ШІ може підтримувати цей процес, але він не може замінити творчий розум і стратегічне мислення, які надають експерти.

Розкриття потенціалу ШІ

Створення систем штучного інтелекту, які можуть випереджати наших супротивників, також означатиме, що індустрія кібербезпеки повинна сприяти створенню середовища співпраці та обміну інформацією. Нам потрібна екосистема безпеки додатків на основі штучного інтелекту, яка може об'єднати наші найкращі практики та колективні знання, щоб бути на крок попереду кіберзлочинців, коли вони з'ясовують, як увімкнути ракетний прискорювач, яким є ШІ.

Немає сумнівів у здатності штучного інтелекту змінити форму індустрії кібербезпеки, але ми також повинні визнати, що штучний інтелект сам по собі не є ідеальною кулею. Комплексний план кібербезпеки організації завжди потребуватиме людського контролю та досвіду. ШІ може значно підвищити рівень кібербезпеки організації та забезпечити рівень захисту, якого важко досягти лише людськими ресурсами. Але штучний інтелект також не здатний замінити критичне мислення, етичне судження та креативне вирішення проблем, які пропонують фахівці з кібербезпеки.

Найефективніші стратегії кібербезпеки, що рухаються вперед, використовуватимуть сильні сторони штучного інтелекту та людського досвіду, працюючи в тандемі для захисту від загроз». ***(Kyle Falkenhagen. Dispelling the myths around AI in cybersecurity // Future US, Inc. (https://www.techradar.com/pro/dispelling-the-myths-around-ai-in-cybersecurity). 18.04.2024).***

***

«Корпорація Ноуа, велика оптична компанія, відома у фотоспільноті своїми фільтрами для об'єктивів, минулого тижня зазнала кібератаки, яка продовжує порушувати її виробничі системи та системи доставки.

«Позавчора ми дізналися, що в головному офісі Групи та кількох її бізнес-підрозділах стався інцидент IT-системи. Компанія тісно співпрацюватиме з кожним із своїх бізнес-підрозділів і сайтів, а також із зовнішніми експертами, щоб визначити характер і масштаби інциденту та якомога швидше відновити ситуацію», — сказав Хойя в заяві 1 квітня. І ні, це не був першоквітневий жарт.

«Інцидент», який Bleeping Computer описує як кібератаку, стався 30 березня.

У наступному оновленні ситуації 2 квітня Ноуа пояснює, що працює над вирішенням проблеми якомога швидше. Однак станом на сьогодні, 5 квітня, додаткові терміни для виправлення не доступні, що свідчить про те, що робота над вирішенням проблеми продовжується.

4 квітня корпорація Ноуа опублікувала PDF-файл із додатковою інформацією про інцидент. Компанія найняла зовнішніх спеціалістів, щоб допомогти швидко відновити послуги, і Ноуа співпрацює з відповідними органами.

«Хоча всі наслідки, масштаби та природа інциденту продовжуються досліджуватися, системи деяких виробничих підприємств і система замовлення для кількох продуктів були вражені», — пояснює Хойя. «Компанія докладає всіх зусиль, щоб задовольнити попит клієнтів і якомога більше мінімізувати вплив на наших клієнтів».

За допомогою консультантів Ноуа також з'ясовує, чи була внаслідок інциденту розкрита будь-яка конфіденційна або особиста інформація клієнтів. У компанії вважають, що повний аналіз того, що сталося, і наслідків займе «значну кількість днів».

На жаль, це не перший раз, коли Хойя стає жертвою кіберзлочинців. Виробнича лінія компанії в Таїланді була тимчасово припинена в 2019 році через атаку зловмисного програмного забезпечення. У 2021 році компанія пережила чергову кібератаку. У цьому випадку передбачувані зловмисники, Astro Team,

стверджували, що розмістили понад 300 ГБ конфіденційної інформації з Ноуа в темній мережі.

Будь-які клієнти, які придбали продукти безпосередньо в Ноуа, повинні стежити за ситуацією, оскільки залишається незрозумілим, чи їхні особисті дані були скомпрометовані. Ноуа також є одним із провідних виробників окулярів, який постачає 90% коригувальних лінз у світі. У Ноуа працює близько 40 000 співробітників у понад 30 країнах». ***(Jeremy Gray. Japanese Optics Company Hoya Suffers Debilitating Cyberattack // PetaPixel Inc. (https://petapixel.com/2024/04/05/japanese-optics-company-hoya-suffers-debilitating-cyberattack/?utm_source=flipboard&utm_content=PetaPixel%2Fmagazine%2FPhotography+News). 05.04.2024).***

***

«Група філіппінських хакерів зламала сервери, якими володіє та керує Департамент науки і технологій уряду, і видалила до 25 терабайт конфіденційних даних і резервних копій.

Група, яка діяла під псевдонімом «ph1ns», оголосила у вівторок, що націлилася на сервери департаменту, скомпрометувала два підключених до мережі пристрої зберігання даних, отримала доступ до віртуальних серверів і пристроїв співробітників, а також видалила всі дані та резервні копії, до яких вона могла отримати доступ.

Департамент інформаційних і комунікаційних технологій, урядове агентство з кібербезпеки, повідомило в четвер, що кібератака заблокувала постраждалих співробітників департаменту від їхніх комп'ютерів. Речник DICT, помічник секретаря Ренато Параісо, заявив місцевим інформаційним агентствам на прес-конференції в Zoom, що уряд знає про претензії групи хакерів і вживає заходів для відновлення доступу до системи DOST.

«Перше повідомлення суб'єктів загрози було дещо політичним. Отже, ми не скидаємо з рахунків, що це частина хактивізму або щось більш мерзенне чи

підступне», — сказав він, додавши, що атака скомпрометувала «в основному дані, які знаходяться під опікою та опікою ДОСТ».

«Сюди входять пропозиції щодо винаходів, і навіть їх резервне копіювання та резервування також були скомпрометовані», - сказав Параісо. DICT повідомив, що кібератака призвела до втрати до 25 терабайт даних, які зберігаються DOST.

Хактивістська група, яка здійснила напад під прапором #OpEDSA, називає себе групою за захист громадянських прав і черпає натхнення з EDSA People Power Revolution, великого антиурядового народного руху в 1986 році, який змусив тодішнього диктатора Фердинанда Маркоса старшого піти у відставку. вниз. Його син, Фердинанд Р. Маркос молодший, зараз є президентом країни.

Група регулярно здійснює кібератаки на урядову цифрову інфраструктуру, щоб знищити довіру до неї, створюючи ще один фронт для уряду, який також має справу зі значним зростанням атак на державу та шпигунських операцій, зокрема з Китаю.

Аналіз, проведений філіппінською компанією з кібербезпеки Deep Web Konek, показав, що хакерська група провела широку рекогносцировку серверів DOST, досліджувала веб-додатки департаменту на наявність вразливостей і перевіряла доступні домени, пов’язані з серверами, перш ніж розпочати атаку.

Спочатку хакери запустили шкідливий код, щоб отримати початковий доступ до інфраструктури сервера, а потім продовжили встановлення постійного доступу до пристроїв NAS і видалення даних, що зберігаються на пристроях. Вони також отримали кореневий доступ і адміністративний контроль над серверною інфраструктурою, перш ніж зробити пристрої NAS невідновними.

«Щоб забезпечити безперервний доступ до скомпрометованих систем, зловмисник встановив бекдори в інфраструктурі серверів DOST. Ці бекдори забезпечили їм постійний доступ, дозволяючи їм зберігати контроль навіть всупереч потенційним зусиллям виявлення та видалення», — повідомили в Deep Web Konek.

Коли компанія, що займається кібербезпекою, зв’язалася з членом групи хакерів, вона сказала, що вона спеціально націлилася на сервери DOST, щоб виявити вразливість технологічного відділу до атак.

«Я сканував різні агентства та виявив, що DOST досить вразливий. Я вирішив зосередитися на цьому, щоб показати іронію в тому, що агентство, що спеціалізується на технологіях, настільки погано захищене. Їхні мережі були налаштовані непогано, але вони припустилися серйозних помилок», - сказав хакер.

Deep Web Konek виявив, що дамп вкрадених і видалених даних включає електронні листи, якими обмінюються у відділі, HR-журнали, що стосуються співробітників DOST, вкладення, близько 70 000 HTML-документів Chrome і понад 10 000 вбудованих папок із зображеннями.

«Всеосяжний характер порушення та різноманітність скомпрометованих типів даних посилюють ризики для постраждалих осіб і організації. Серед потенційних наслідків — репутаційна шкода, фінансові втрати та правові наслідки», — заявили в компанії.

Департамент науки і технологій, який керує науково-технологічними проектами для стимулювання економіки країни, повідомив Manila Bulletin, що розслідує інцидент з кібербезпекою.

«Ми розуміємо, що цей інцидент може викликати занепокоєння серед наших зацікавлених сторін і громадськості, і ми хочемо запевнити вас, що ставимося до цього питання з максимальною серйозністю», — сказав секретар DOST Ренато У. Солідум-молодший.

«Наші технічні команди старанно працюють над усуненням будь-яких вразливостей і зміцненням нашого кіберзахисту. Ми продовжуватимемо вдосконалювати наші протоколи кібербезпеки, щоб запобігти подібним інцидентам у майбутньому», — сказав він.

Успішна атака на сервери DOST виявила постійну вразливість урядової цифрової інфраструктури до кібератак як з боку хакерів, так і зовнішніх ворогів. У лютому уряд звинуватив китайських зловмисників у зламі веб-сайтів кількох державних установ і проникненні в урядові системи електронної пошти.

У відповідь на зростання кількості кібератак на урядові установи Маркос у лютому схвалив довгоочікуваний п’ятирічний Національний план кібербезпеки DICT, надавши агентству більше повноважень для модернізації IT-інфраструктури, підвищення кіберобізнаності та координації реагування на інциденти.

У січні Маркос також підписав розпорядження про створення Національного координаційного агентства розвідки, яке тепер виконує роль провідного агентства для керування, координації та інтеграції зусиль уряду щодо захисту національної безпеки.

Виконавчим наказом також було створено Офіс заступника генерального директора з кібернетичних і нових загроз у рамках NICA для планування, контролю та координації реагування агентства на загрози кібербезпеці». ***(Jayant Chakravarti. Filipino Hacktivists Destroy Technology Agency Servers // Information Security Media Group, Corp. (https://www.databreachtoday.com/filipino-hacktivists-destroy-technology-agency-servers-a-24790?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 05.04.2024).***

***

«Міністерство охорони здоров’я та соціальних служб США (HHS) попереджає, що хакери зараз використовують тактику соціальної інженерії, щоб націлитися на служби підтримки IT у секторі охорони здоров’я та громадського здоров’я (HPH).

У секторальному попередженні, опублікованому цього тижня Координаційним центром кібербезпеки сектору охорони здоров’я (HC3), йдеться, що ця тактика дозволила зловмисникам отримати доступ до систем цільових організацій, зареєструвавши їхні власні пристрої багатофакторної автентифікації (MFA).

Під час цих атак зловмисники використовують місцевий код міста, щоб дзвонити в організації, видаючи себе за співробітників фінансового відділу, і

надавати вкрадені ідентифікаційні дані, зокрема ідентифікаційний код компанії та номер соціального страхування.

Використовуючи цю конфіденційну інформацію та стверджуючи, що їхній смартфон зламаний, вони переконують IT-службу підтримки зареєструвати новий пристрій у MFA під контролем зловмисника.

Це дає їм доступ до корпоративних ресурсів і дозволяє перенаправляти банківські транзакції під час компрометації бізнес-електронної пошти.

«Зловмисник спеціально націлився на інформацію для входу, пов'язану з веб-сайтами платників, де вони потім подали форму для внесення змін до ACH для облікових записів платників», — повідомляє HC3 [PDF].

«Після того, як було отримано доступ до облікових записів електронної пошти співробітників, вони надіслали інструкції платіжним процесорам щодо перенаправлення законних платежів на контрольовані зловмисниками банківські рахунки в США».

«Кошти потім були переведені на закордонні рахунки. Під час зловмисної кампанії зловмисник також зареєстрував домен з однолітерним варіантом цільової організації та створив обліковий запис, видаючи себе за фінансового директора цільової організації».

У таких інцидентах зловмисники також можуть використовувати інструменти клонування голосу штучного інтелекту, щоб обдурити цілі, ускладнюючи віддалену перевірку особистості. 25% людей стикалися з шахрайством з уособленням голосу ШІ або знають когось, хто це стикався Зараз це дуже популярна тактика: згідно з нещодавнім глобальним дослідженням.

Розсіяні павукові вібрації

Тактика, описана в попередженні Департаменту охорони здоров'я, дуже схожа на тактику, яку використовує група загроз Scattered Spider (також відома як UNC3944 і 0ktapus), яка також використовує фішинг, бомбардування MFA (так звану втому MFA) і заміну SIM-карти для отримання початкового доступу до мережі.

Ця банда кіберзлочинців часто видає себе за IT-працівників, щоб обманом змусити персонал служби підтримки надати їм облікові дані або запустити інструменти віддаленого доступу для зламу цільових мереж.

Хакери Scattered Spider нещодавно зашифрували системи MGM Resorts за допомогою програми-вимагача BlackCat/ALPHV. Вони також сумно відомі кампанією 0ktapus, у якій вони націлилися на понад 130 організацій, включаючи Microsoft, Binance, CoinBase, T-Mobile, Verizon Wireless, AT&T, Slack, Twitter, Epic Games, Riot Games і Best Buy.

У листопаді ФБР і CISA опублікували попередження, щоб висвітлити тактику, техніку та процедури (TTP) Scattered Spider у відповідь на їхню крадіжку даних і атаки програм-вимагачів проти довгої низки відомих компаній.

Однак HC3 каже, що подібні інциденти в галузі охорони здоров'я, про які повідомлялося досі, ще не віднесені до певної групи загроз.

Щоб блокувати атаки, спрямовані на їхні служби підтримки IT, організаціям у секторі охорони здоров'я рекомендується:

Вимагайте зворотних викликів для перевірки співробітників, які запитують скидання пароля, і нових пристроїв MFA.

Слідкуйте за підозрілими змінами ACH.

Перевірте всіх користувачів, які мають доступ до веб-сайтів платників.

Розглядайте особисті запити щодо делікатних питань.

Вимагайте від керівників перевірки запитів.

Навчіть персонал служби підтримки ідентифікувати та повідомляти про методи соціальної інженерії та перевіряти особи абонентів». ***(Sergiu Gatlan. US Health Dept warns hospitals of hackers targeting IT help desks // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/us-health-dept-warns-hospitals-of-hackers-targeting-it-help-desks/?utm_source=flipboard&utm_content=unsecurity%2Fmagazine%2FCybercrime%2C+Hacking+%26+CyberWar). 06.04.2024).***

***

«Минулого тижня розробники та експерти з безпеки в усьому світі були збентежені катастрофою, якої вдалося уникнути в програмній утиліті, яка використовується в популярних версіях операційної системи Linux з відкритим кодом.

Тиждень тому розробник Microsoft виправляв невідповідність у мережевому протоколі, коли, здається, натрапив на одну з найскладніших атак на ланцюг поставок, які коли-небудь виявляли.

Починаючи з лютого, тіньовий розробник, відомий як Цзя Тан, почав непомітно вставляти бекдор у програмне забезпечення, відоме як XZ Utils, яке є утилітою для стиснення, присутньою в більшості, якщо не у всіх версіях Linux, — частина програмного забезпечення, яка забезпечує одну з основні будівельні блоки Інтернету, як ми його знаємо.

Якби XZ Utils було вставлено в стабільні — на відміну від експериментальних — версії Linux, Цзя Тан і його (потенційні) співробітники, теоретично, змогли б зламати сервери Linux за допомогою утиліти та запускати довільний код.

Подробиці цього інциденту викликають ще більшу тривогу. Цзя Тан зміг отримати себе призначення супроводжувачем XZ Utils, скориставшись перевагами виснаженого самотнього розробника, який підтримував проект.

Ця катастрофа має всі ознаки дуже терплячої шпигунської операції, яку проводить досвідчена розвідка, але хто саме стоїть за нею, залишається загадкою.

XZ Utils підтримував в актуальному стані один супроводжуючий, який працював безкоштовно у вільний час. Він використовується в усьому світі, від невеликих проектів до компаній зі списку Fortune 500, що робить утиліту головною метою.

«Це не технологічна проблема; це проблема людей. І це робить ситуацію ще гіршою», — сказав Омкхар Арасаратнам, генеральний менеджер Open Source Security Foundation, що є частиною Linux Foundation. «Така ерозія довіри сталася не тому, що комп’ютер зламався. Це тому, що хтось обдурив людину».

Уразливість — CVE-2024-3094 — могла вплинути на значну частину світових серверів, але навіть якщо атака на ланцюжок постачання була остаточно невдалою, зухвалий характер і близькість цього інциденту послужили сигналом тривоги для спільноти безпеки. Не було жодного протоколу безпеки чи технології, які б виявили та зупинили цю атаку.

«Хороша новина полягає в тому, що ми знайшли це рано», — сказав Арасаратнам.

Агентство з кібербезпеки та безпеки інфраструктури надіслало попередження про пакет і вказало на попередження від Red Hat, компанії з відкритим вихідним кодом, про бекдор.

Схоже, що цей інцидент стався в жовтні 2021 року, коли особа, яка називалася «Цзя Тан», надіслала те, що мало стати першим із багатьох «виправлень» до списку розсилки для бібліотеки стиснення даних.

Кілька місяців потому, у березні, на сцену виходять ще дві особи під іменами «Джигар Кумар» і «Денніс Енс». Вони починають кампанію тиску, націлену на супроводжуючого проекту, Лассе Колліна, критикуючи його за відсутність оновлень з очевидною метою залучити Цзя Тана як нового супроводжуючого, згідно з графіком, складеним Рассом Коксом, програмістом Google.

У якийсь момент Джиґар запитує: «Цзя, я бачу, у вас є нещодавні зобов’язання. Чому ти не можеш це зробити сам?» «Коміт» — це термін для додавання коду до проекту, який доступний лише для тих, хто має певний доступ до цього репозиторію, і повідомлення Джигара, здається, спрямоване на те, щоб переконати Колліна надати Джіа більше повноважень над XZ Utils як супроводжувачу.

У той час Коллін страждав від проблем із особистим та психічним здоров’ям. Зрештою він погодився і призначив Цзя Тана супроводжувачем проекту майже через рік після того, як Тан надіслав перше виправлення.

Здобувши повноваження, яких він прагнув, Цзя Тан почав потроху додавати шкідливий код, доки бекдор не було додано до версії XZ.

Тоді Тан почав тиснути на різні дистрибутиви Linux, щоб вони додали шкідливу версію до своїх операційних систем.

Бекдор працює лише для кількох дистрибутивів Linux, таких як Debian і Fedora, але вони є одними з найбільших і найпоширеніших. також є ознаки того, що Тан прискорив атаку на ланцюг поставок в останні місяці, оскільки була налаштована інша програма для впровадження змін, які зробили б атаку марною. За словами дослідника Кевіна Бомонта,

Цзя Тан теж би зійшов з рук, якби не цікавий інженер-програміст на ім'я Андрес Фройнд. Фройнд, який працює в Microsoft, натрапив на бекдор, намагаючись усунути проблеми з продуктивністю SSH, мережевого протоколу, який є безпечним способом зв'язку між комп'ютерами та часто використовується для входу на віддалений робочий стіл або сервер. Саме відкриття було майже чистим щастям. Фройнд сказав, що для виявлення бекдору потрібно «багато випадковостей».

Потім Фройнд попередив спільноту відкритих кодів про те, що він знайшов, викликавши шалену серію офіційних попереджень, розслідувань, створення безкоштовних інструментів сканування та десятків публікацій у блогах про історичну аварію, яка могла бути катастрофічною.

Реакція найкраще ілюструє потужність проектів з відкритим вихідним кодом: протягом кількох днів аналітики нанесли графік GitHub на часові рамки, дослідники зловмисного програмного забезпечення розібрали код, чати IRC реєструвалися, а дослідники розібрали те, що сталося.

Для захисників відкритого коду цей інцидент є чимось на кшталт підтвердження передумови спільноти: що відкрито доступний код можна ретельно перевірити, щоб знайти вразливості.

Але це передбачає, що весь шкідливий код Jia Tan було виявлено.

Цзя Тан, здається, брав участь в інших проектах з відкритим вихідним кодом, таких як широко використовувана бібліотека стиснення libarchive, і зараз триває пошук того, чи його внесок у ці інструменти намагався підірвати їх.

За даними фірми з кібербезпеки NetRise, внески Tan у libarchive знайшли свій шлях до щонайменше 180 екземплярів мікропрограми операційної технології, пристроїв Інтернету речей і мережевих пристроїв. І хоча незрозуміло, чи є якийсь шкідливий код — особливо тому, що внески могли бути частиною створення особистості — ризик залишається.

Складний характер справи, роки, витрачені на роботу над утилітою, складний код і кілька осіб, очевидно, які працюють разом, змусили багатьох експертів з безпеки зробити висновок, що операція проти XZ Utils була здійснена національною державою.

На кого б не працювали Цзя Тан і його очевидні співвітчизники Денніс і Джигар, вони, здавалося, мали хорошу оперативну безпеку, оскільки, за словами журналіста Брайана Кребса, жоден з їхніх електронних листів не був помічен в інших місцях Інтернету, зокрема у витоках даних.

Хронологія зобов'язань Тана для GitHub показує, що це хтось із Китаю, як і його ім'я. Однак аналіз, проведений дослідниками Рі Карті та Саймоном Хеннігером, показує, що це може бути неправильним напрямком. Грунтуючись на невідповідності часового поясу в метаданих комітів і кілька разів, коли вони працювали під час китайських національних свят, вони припускають, що Тан насправді знаходиться десь у Східній Європі.

Занепокоєння щодо безпеки програмного забезпечення з відкритим кодом часто зосереджені навколо ненавмисних помилок у коді, які можуть створити вразливість у широко використовуваному програмному забезпеченні. І хоча занепокоєння зловмисним хакером, який зловживає пакетами з відкритим кодом, щоб відкрити шлях для майбутніх атак, не є новим, багато загальновідомих випадків мають фінансову мотивацію, наприклад майнери криптовалюти покладаються на те, що необізнаний користувач встановлює шкідливий пакет з відкритим кодом.

У грудні розповсюджувач пакетів Python PyPI тимчасово припинив нову реєстрацію через «велику кількість зловмисних користувачів і шкідливих проєктів».

У багатьох проектах з відкритим вихідним кодом є певна довіра до супроводжуючого, пояснив Арасаратнам. Сучасна економіка залежить і значною мірою існує завдяки кадрам волонтерів, які працюють, часто безкоштовно як побічний проект або хобі, над програмами, які лежать в основі майже всіх аспектів цифрового життя. Супроводжувачі часто є першою та останньою лінією захисту щодо якості коду, запитів на функції та, зрештою, ризиків.

Ймовірно, не буде «срібної кулі», яка зможе захистити від операцій національної держави, як у випадку XZ, сказав Арасаратнам.

«Проблема в цьому понятті довіри», — сказав Арасаратнам. «Довірений супроводжувач знайде інший спосіб маніпулювати цією довірою, якщо він поганий гравець у системі. Це та частина, де, я думаю, спільнота ще не має консенсусу щодо того, як це вирішити. І для нас це буде довга подорож». ***(Christian Vasquez. Supply chain attack sends shockwaves through open-source community // CyberScoop (https://cyberscoop.com/xz-utils-open-source/?utm_source=flipboard&utm_content=other). 05.04.2024).***

***

«Не дивно, що в 24-му щорічному глобальному опитуванні PwC керівники компаній поставили кібератаки на друге місце серед найсерйозніших з усіх можливих економічних, соціальних, політичних, бізнесових та екологічних загроз. На атаки з вимогою викупу припадає 12% порушень критичної інфраструктури в минулому році.

За оцінками експертів з кібербезпеки, цього року глобальні збитки від кіберзлочинності перевищать 7,5 трильйонів євро, згідно з даними CyberSecurity Ventures. Підприємства працюють на основі даних, і коли вони зламані або пошкоджені кіберзлочинцями, це може призвести до зупинки роботи за одну ніч, з багатомільйонними наслідками.

Іронія полягає в тому, що якщо наслідки кібератаки відбулися так швидко, відновитися від них буде менш проблематично. Необхідно негайно розпочати заходи з усунення несправності та мінімізувати будь-які збитки. Фактична

проблема набагато підступніша, оскільки, коли кібер-зловмисники атакують підприємство, вони зазвичай чекають майже шість місяців, перш ніж вжити заходів. Це збільшує їх силу викупу, і без належного контролю даних єдиним вибором для жертви може бути погодитися на будь-які висунуті фінансові вимоги. У цей проміжок часу їхні первинні дані, поточні дані, від яких залежать ваші бізнес-операції, могли бути піддані різним видам злочинної діяльності.

З цієї причини корпоративне сховище стало основною мішенню кіберзлочинців для найшкідливіших і важковиявлених атак програм-вимагачів і шкідливих програм. Однією з причин, чому підприємства все ще потрапляють у пастку, є те, що стратегія кібербезпеки, як правило, зосереджена на тому, щоб не допустити злочинців, а не на те, що атаки, швидше за все, відбудуться, і є поштовх для стратегії водонепроникності. Вовк обов'язково продовжить стукати і проникне у ваш будинок. Отже, які кроки ви можете зробити?

По-перше, акцент у сфері кібербезпеки має бути зосереджений на трьох сферах – виявленні, стійкості та відновленні – і заповнити прогалину вразливості, якою користуються кіберзлочинці. Комбінована стійкість, тобто здатність застосовувати захисні заходи безпеки для відбиття атак; виявлення, тобто здатність дізнатися, коли дані пошкоджені та чи відома справна копія даних вільна від програм-вимагачів або шкідливих програм; а відновлення, яке є здатністю відновлюватися та відновлення за допомогою завідомо справної копії даних після кібератак, є ключем до зміцнення інфраструктури зберігання.

Об'єднання кібервідмовостійкості, виявлення та відновлення на інтегрованій корпоративній платформі зберігання даних є прогресом у порівнянні з попередніми ізольованими підходами, які покладаються на різні інструменти та технології. Це робить кібер-можливості більш герметичними та забезпечує швидке відновлення даних за лічені хвилини, щоб перешкодити кібер-злочинцям, зводячи нанівець вимоги викупу та мінімізуючи простої чи збитки для бізнесу.

Існує кілька ключових особливостей корпоративного сховища, які повинні бути на місці, щоб забезпечити кіберстійкість від сучасних кіберзлочинців, усі з яких є висококваліфікованими експертами з технологій. Вони включають

забезпечення незмінного характеру даних, відновлених із копії, якій можна довіряти. Повітряний проміжок для відокремлення площини керування та даних для захисту даних. Безпечне криміналістичне середовище для ретельного аналізу даних і забезпечення найшвидшої швидкості відновлення має вирішальне значення.

Незмінні знімки дозволяють кінцевому користувачеві повернути годинник назад і відновити гарантовано непошкоджені копії своїх даних перед виконанням будь-якого шкідливого програмного забезпечення або програмного коду-вимагача, введеного зловмисником. Незмінні знімки забезпечують цілісність даних, оскільки вони запобігають зміні чи видаленню копій даних. Навіть внутрішні системні адміністратори заблоковані від маніпулювання незмінними знімками. Підприємство може бути впевнене, що будь-який збій або збиток, спричинений вторгненням, мінімальний.

Логічний повітряний проміжок додає ще один рівень безпеки, створюючи безпечну відстань між рівнем керування сховищем і незмінними знімками. Існує три типи повітряних зазорів. Локальний вентиляційний зазор зберігає дані в приміщеннях, віддалений зазор використовує віддалену систему, а гібридний зазор поєднує обидва.

Огороджене криміналістичне середовище допомагає пришвидшити процес відновлення, забезпечуючи безпечну зону для проведення криміналістичного аналізу незмінних знімків після атаки. Мета тут полягає в тому, щоб ретельно відібрати дані-кандидатів і знайти завідомо хорошу копію. Останнє, чого хоче підприємство після атаки, — це відновити дані, заражені шкідливим програмним забезпеченням або програмами-вимагачами.

Коли ці ключові елементи з’являться у вашій інфраструктурі зберігання, усе відновлення може просуватися як по маслу. Ось чому ми як організація зосереджені на навчанні IT-лідерів необхідності конвергентного тристороннього підходу. Такий, який поєднує кібервідмовостійкість, виявлення та відновлення на одній платформі зберігання. Покладатися лише на резервне копіювання та запобігання атакам уже недостатньо для захисту систем зберігання». ***(Isha Jain. Storage must form the core of an enterprise cyber security strategy // All Things Media***

Ltd (https://dcnnmagazine.com/security/storage-must-form-the-core-of-an-enterprise-cyber-security-strategy/). 02.04.2024).

***

«В епоху, коли цифрова трансформація прискорюється, привид кіберзагроз затьмарює кожен наш крок до прогресу. Тільки за останні 18 місяців ми стали свідками безпрецедентної хвилі кібератак, що знаменує нову еру цифрової вразливості. Звіт IBM про вартість витоку даних за 2023 рік висвітлює цей похмурий ландшафт, показуючи тривожну середню вартість у 4,35 мільйона доларів за витік, цифра, яка постійно зростала протягом останніх п'яти років. Однак це не тільки фінансова кровотеча, що вражає; це зухвалість і витонченість цих атак, підкреслених такими інцидентами, як закриття Colonial Pipeline, що відбилося в енергетичному секторі, спричинивши масовий дефіцит палива та громадську тривогу. Це не поодинокі випадки, а скоріше провісники системного виклику, який виявляє кричущу прірву між технологічним прогресом і готовністю до кібербезпеки.

Незважаючи на невпинний сплеск резонансних кібератак за останні 18 місяців, які завдали компаніям мільярдних збитків і серйозно порушили роботу, залишається вражаючий брак розуміння кібербезпеки та визначення пріоритетів на рівні правління та вищого керівництва. Згідно з нещодавнім опитуванням KPMG, 55% генеральних директорів визнають, що вони не повністю готові до потенційної кібератаки, тоді як звіт Deloitte показує, що лише 12% членів правління відчувають себе добре обізнаними щодо ризиків кібербезпеки. Цей розрив між ескалацією ландшафту загроз і недостатньою концентрацією керівництва наражає організації на потенційно руйнівні наслідки.

У цю епоху цифрових технологій кібербезпека виходить за рамки просто IT-занепокоєння, перетворюючись на критично важливий бізнес-імператив. Нещодавня кібератака на MGM Resorts у вересні 2023 року яскраво підкреслює цю реальність, служачи жахливим нагадуванням для лідерів C-suite про першочергову важливість захисту цифрових кордонів. Ця стаття має на меті проаналізувати

кібератаку MGM, надавши інформацію та корисні уроки для керівників, щоб зміцнити свою кіберстійкість.

Інцидент: ближчий погляд на кібератаку MGM

MGM Resorts, титан у секторі гостинності та розваг, став жертвою складної кібератаки, приписуваної фракціям, як вважають групу Scattered Spider і сумнозвісну банду програм-вимагачів AlphV/BlackCat. Ці зловмисники, застосовуючи хитру тактику соціальної інженерії, обманом змусили нічого не підозрюючих співробітників порушити безпеку системи. Порушення призвело до значних збоїв у роботі: казино були частково закриті, банкомати та ігрові автомати не працювали, а цифрова система бронювання, система онлайн-бронювання, була виведена з ладу.

Після цього сталося жахливе викриття — крадіжка конфіденційних даних клієнтів, включаючи імена, контактну інформацію, а в більш серйозних випадках — номери соціального страхування та паспорти. Фінансові втрати для MGM були приголомшливими, приблизні збитки коливалися близько 100 мільйонів доларів. Як стався такий напад?

На основі наявної інформації ось що нам вдалося зібрати:

Соціальна інженерія: група Scattered Spider розпочала хакерство, націлившись на співробітників MGM, ймовірно, через LinkedIn або інші соціальні платформи. Вони збирали інформацію для створення переконливої фішингової атаки або телефонного шахрайства, видаючи себе за законну особу (наприклад, IT-підтримку). Співробітник пішов на хитрість і розкрив облікові дані або дозволив віддалений доступ.

Початкове проникнення: хакери використали скомпрометовані облікові дані, щоб увійти в мережу MGM. Ймовірно, вони рухалися вбік і шукали слабкі місця в протоколах безпеки.

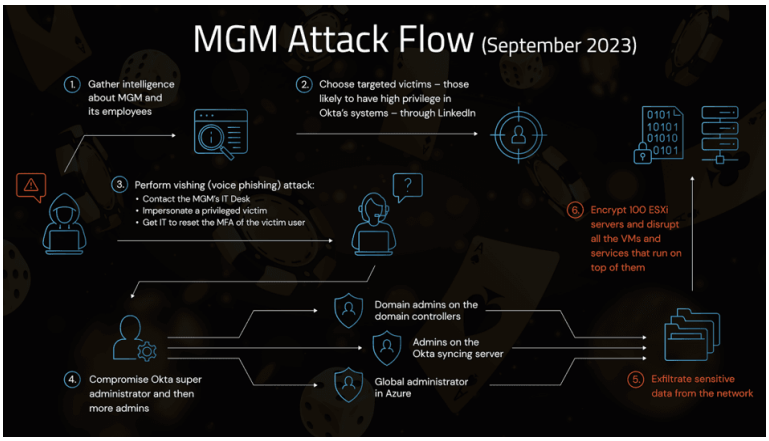
Підвищення привілеїв: хакери зосередилися на отриманні підвищеного доступу. Це могло статися через використання вразливостей програмного забезпечення або використання методів грубої сили для злому паролів. З доступом вищого рівня вони могли б вільніше переміщатися в системі.

Збір облікових даних: хакери отримали облікові дані від контролерів домену та інструментів, таких як сервер синхронізації Okta, що надає їм доступ до облікових записів і систем інших співробітників.

Викрадання даних: з часом група зібрала терабайти конфіденційних даних клієнтів, включаючи імена, контактну інформацію, ідентифікатори та потенційні фінансові записи. Дані були тихо виведені з мережі.

Розгортання програми-вимагача: програму-вимагач, яка, як вважають, створила група AlphV/BlackCat, була розгорнута в системах MGM, шифруючи файли та порушуючи роботу. Тоді атака стала повністю помітною.

Нижче наведено графічну схему можливої атаки на MGM:



На діаграмі показано потік атак CyberAttack на MGM у вересні 2023 року

Поки це відбувалося, ви можете дивуватися, чому команда MGM Cyber не втрутилася. Частково причиною може бути те, що вони могли пропустити наступне:

Навчання: співробітники не були достатньо навчені розпізнавати тактику соціальної інженерії. Один працівник скомпрометував всю мережу, і іноді може бути невідомо, що один скомпрометований співробітник може дозволити хакерам проникнути в мережу.

Виправлення вразливостей: ймовірно, хакери використали відомі вразливості програмного забезпечення, які MGM не виправила досить швидко.

Сегментація мережі: неадекватне розділення мережі дозволило хакерам переміщатися вбік усередині системи. Правильно сегментовані ділянки можуть мати обмежені пошкодження.

Багатофакторна автентифікація: якщо вона була присутня не скрізь або її можна було обійти, критичні системи залишалися вразливими.

Моніторинг і виявлення. Можливо, системи не створили достатньо сповіщень або журналів, щоб зафіксувати початкове вторгнення, що дозволяє хакерам діяти непомітно.

Цілком можливо, що команда з кібербезпеки MGM все зробила правильно, і хакери все-таки пройшли. Кіберзахист ніколи не є надійним. Хакери постійно адаптуються та стають все більш досконалими. Атака MGM підкреслює, що кіберзагрози постійно розвиваються і що навіть великі компанії зі значними ресурсами можуть бути вразливими. Для компаній надзвичайно важливо постійно інвестувати в безпеку (використовувати нові технології кібербезпеки, такі як SSHepherd тощо), навчати співробітників і підтримувати проактивну, багаторівневу стратегію захисту.

Розпакування уроків

Розповідь про вторгнення MGM — це лише одна нитка у цьому величезному, заплутаному гобелені кібербезпеки, що тягнеться через галузі та кордони, змушуючи нас зіткнутися з незручною правдою: у наших цифрових фортецях ворота широко відчинені. Кіберсага MGM рясніє уроками, кожен з яких є наріжним каменем для розробки надійної стратегії кібербезпеки. Ось ключові висновки та стратегії для керівників старших класів:

Загроза соціальної інженерії

Атака MGM підкреслює небезпеку соціальної інженерії. Ці схеми, використовуючи психологічну маніпуляцію, використовують вразливість людей для порушення безпеки.

Дійсне розуміння: організації повинні надавати пріоритет програмам навчання, які дають змогу співробітникам розпізнавати та запобігати таким атакам. Включення регулярних тренувань, інструктажів з питань безпеки та сесій для підвищення обізнаності може значно зменшити цей ризик. Витрати на навчання співробітників і керівників вищої ланки здатності швидко розпізнавати тривожні сигнали значно перевищуватимуть потенційні втрати від матеріальної загрози

Висока вартість витоку даних

Фінансові наслідки порушення MGM є яскравим нагадуванням про економічні ставки. Окрім негайних фінансових втрат, репутаційна шкода та ерозія довіри клієнтів можуть мати довготривалі наслідки.

Дійсне розуміння: інвестування в передові засоби кібербезпеки – це не витрати, а захист від потенційно руйнівних фінансових та репутаційних наслідків. Варто інвестувати в нову технологію кібербезпеки на основі стелсів, як-от SSHerpherd, та інші технології, які є набагато досконалішими

Імператив прозорості

Підхід MGM до негайного розкриття порушення заслуговує похвали. У часи кризи прозорість стає ключовим інструментом побудови довіри між зацікавленими сторонами.

Дійсне розуміння: розробіть комунікаційну стратегію, яка забезпечує швидке, прозоре та чесне розкриття інформації постраждалим сторонам, зміцнюючи довіру та відданість захисту клієнтів.

Стратегічні вдосконалення кібербезпеки

Керівники C-suite повинні розглядати кібербезпеку через призму стратегічної стійкості бізнесу. Ось основні стратегії зміцнення захисту:

Надійні рішення з кібербезпеки: розгортайте сучасне програмне забезпечення для кібербезпеки на основі стелсів, брандмауери, системи виявлення вторгнень і протоколи шифрування. Регулярно оновлюйте ці засоби захисту, щоб випереджати нові кіберзагрози.

Планування реагування на інциденти: розробіть комплексний план реагування на кіберінциденти, у якому детально описано швидкі й ефективні дії для мінімізації збитків. Цей план слід регулярно оновлювати та відпрацьовувати з ключовими зацікавленими сторонами.

Регулярні перевірки безпеки: проводите періодичні оцінки безпеки для виявлення вразливостей. Ці перевірки повинні інформувати про безперервну еволюцію заходів безпеки.

Розвиток культури безпеки: плекайте організаційний дух, у якому кожен співробітник є вартовим кібербезпеки. Регулярне навчання та ініціативи з підвищення обізнаності можуть посилити важливість пильності та відповідальності.

Висновок: заклик до дії

Розповідь про кібератаки MGM є яскравим закликом до керівників команди переглянути свої стратегії кібербезпеки. В епоху, коли цифрові загрози загрозливі, захист цифрових активів і даних клієнтів є першорядним. Взявши уроки з досвіду MGM, керівники можуть не лише захистити свої підприємства від подібних доль, але й сприяти розвитку культури стійкості та довіри, яка виступає оплотом проти кіберзагроз завтрашнього дня.

На шляху до досконалої кібербезпеки приклад MGM є не просто застереженням, а планом стратегічних дій. Сага про кібератаку MGM виходить за межі простої застереження; це проголошує нагальний імператив для залів засідань по всьому світу. В епоху цифрових загроз, настільки ж поширених, наскільки й згубних, управління кібербезпекою є не лише питанням технічної старанності, а й наріжним каменем стратегічного лідерства.

Це гучний заклик до членів правління перейти від пасивного нагляду до активної участі в управлінні кібербезпекою. Ставки виходять за рамки фінансових втрат, досягаючи сфер довіри, репутації та довгострокової життєздатності. Як лідери, нагальність зміцнення наших цифрових сфер проти привидів завтрашнього дня вимагає не простого визнання — це вимагає повного культурного зрушення в бік кіберстійкості.

Нехай уроки MGM стануть суворим нагадуванням і закликом до об’єднання: інвестувати в кібербезпеку означає інвестувати в саму основу нашого майбутнього процвітання. Настав час об’єднати нашу колективну рішучість, ресурси та винахідливість, щоб створити захист настільки ж надійний, наскільки загрози невблаганні, і застосувати нову технологію, яка дозволить захистити ваші критично важливі сервери.

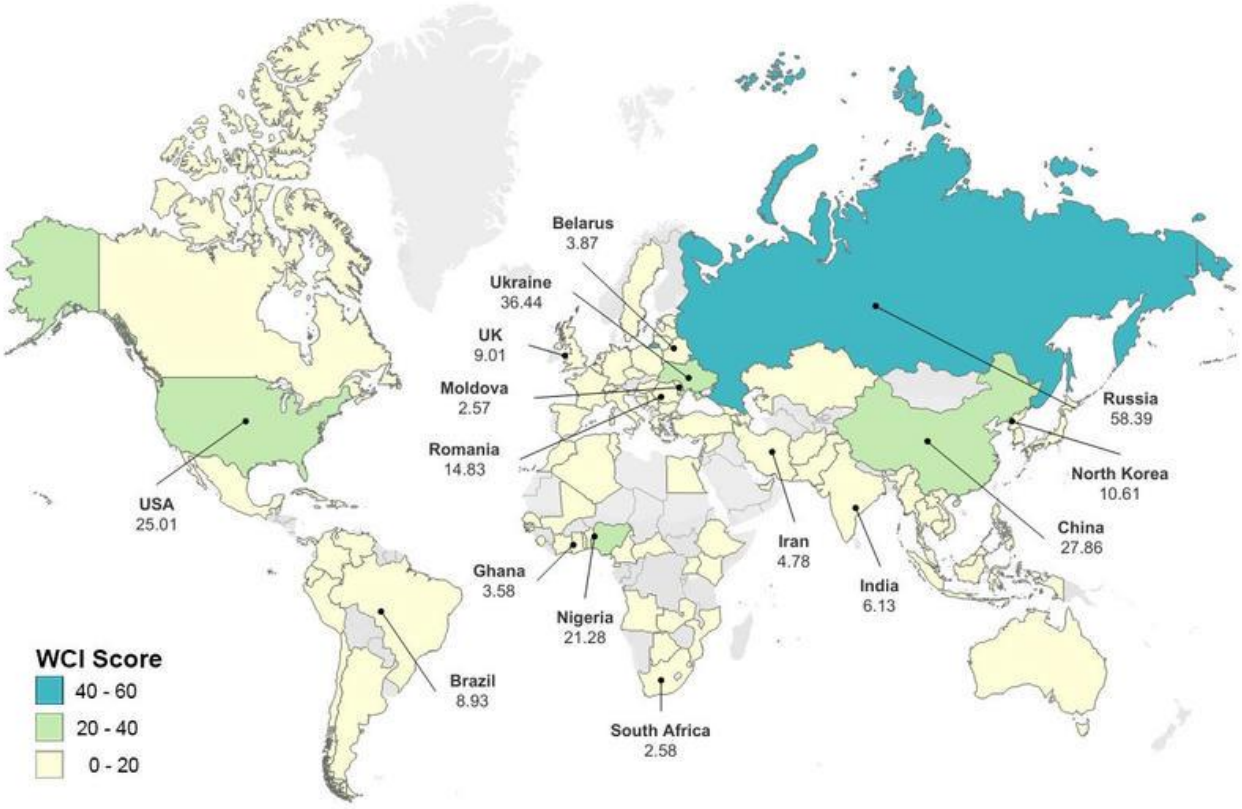
Шлях до досконалої кібербезпеки сповнений труднощів, але для тих, хто хоче лідирувати, він пропонує безцінний приз — захист нашої цифрової ери. Настав час діяти. Для керівників старших класів і керівників правлінь повідомлення чітке: настав час для надійного, проактивного кіберзахисту. Нехай цей інцидент стане каталізатором змін, спонукаючи нас прийняти більш пильний, поінформований і стратегічний підхід до кібербезпеки». ***(Roshan Thiran, Danny Kim. Cybersecurity For Boards & Senior Leadership: Exploring the MGM Hack // Leaderonomics Sdn. Bhd. (https://www.leaderonomics.com/articles/functional/cybersecurity-for-boards-senior-leadership-exploring-the-mgm-hack). 11.04.2024).***

***

«Перший в історії світовий рейтинг кіберзлочинності, створений у рамках дослідження Оксфордського університету та Університету Нового Південного Вельсу, очолила Росія.

Як передає Укрінформ, про це повідомляється на сайті Оксфордського університету.

Науковці зазначають, що загроза кіберзлочинності нерівномірно розподілена по всьому світу. Так, найпершою у рейтингу кіберзлочинності стала Росія (58,39 бала), за нею із великим відривом йдуть Україна (36,44 бала), Китай (27,86 бала), США (25,01 бала), Нігерія (21,28 бала) та Румунія (14,83 бала). Велика Британія посіла восьме місце у списку із 9,01 балами.



В Оксфордському університеті зауважили, що російські кіберзлочинці вважаються найпрофесійнішими та технічно найбільш кваліфікованими у світі, і що їхні злочини мають найбільший вплив.

Світовий рейтинг кіберзлочинності (World Cybercrime Index) був розроблений авторами із Оксфордського університету та Університету Нового Південного Вельсу і є результатом трьох років інтенсивних досліджень.

Дані, які лежать в основі рейтингу, були зібрані шляхом опитування провідних експертів із кіберзлочинності з усього світу. Учасників просили розглянути п’ять основних категорій кіберзлочинності та назвати країни, які вони вважають найбільш значними джерелами кожного із видів злочинності. Після цього учасники опитування оцінили кожну країну відповідно до впливу, професіоналізму та технічних навичок кіберзлочинців». ***(Росія - перша в світовому рейтингу кіберзлочинності // Укрінформ (https://www.ukrinform.ua/rubric-technology/3851230-rosia-na-persij-shodinci-v-svitovomu-rejtingu-kiberzlocinnosti.html). 11.04.2024).***

***

«Нідерландська компанія Nexperia, що спеціалізується на виробництві мікросхем, зазнала атаки хакерів.

Як повідомляє Укрінформ, з посиланням на RTL, зловмисники погрожують Nexperia опублікувати цінні дані, якщо не буде виплачено викуп.

«Нідерландський виробник мікросхем Nexperia, відомий своїми комп'ютерними чипами, які використовуються в телефонах, пилососах і автомобілях, зазнав хакерської атаки. Кіберзлочинці, які стоять за атакою, погрожують опублікувати цінні дані, якщо викуп не буде сплачено», - йдеться у повідомленні.

За даними RTL, в результаті кібератаки було викрадено сотні гігабайт конфіденційної інформації, у тому числі комерційні таємниці, конструкції мікросхем та дані таких клієнтів, як SpaceX, Apple та Huawei. Як доказ злочинці опублікували десятки документів у даркнеті, у тому числі адресу внутрішньої електронної пошти та паспортні дані колишнього старшого віцепрезидента компанії.

RTL запевняє, що переконався у справжності цих документів. У Nexperia підтвердили атаку хакерів, але відмовилися від подальших коментарів, оскільки триває розслідування.

Деякі з вкрадених даних можуть бути дуже цінними, вважає професор електроніки Брам Наута з Університету Твенте. «Nexperia має інформацію не тільки про самі мікросхеми, які відносно прості, а й про процеси їх виробництва. Дані про обладнання для виготовлення мікросхем вкрай засекречені, і ніхто не хоче, щоб ця інформація потрапляла у відкритий доступ», - зазначив він.

Одразу після атаки компанія Nexperia звернулася до поліції, яка разом з Управлінням із захисту даних Нідерландів та фахівцями в галузі кібербезпеки проводить розслідування.

Як стверджує RTL, за атакою може стояти нове хакерське угруповання Dunghill, жертвою якого вже стали десятки компаній. Зловмисники називають себе «міжнародною командою технічних фахівців, які проводять дослідження у сфері інформаційної безпеки».

Nexperia, придбана китайськими інвесторами у 2019 році, раніше була частиною NXP, ще одного відомого виробника мікросхем. NXP зосереджується в основному на чіпах для платіжних операцій, Nexperia виготовляє простіші чіпи для повсякденних товарів – від автомобіля до холодильника. Nexperia виробляє понад 100 млрд мікросхем на рік, які використовуються у всьому світі.

У 2023 році було виявлено, що мільйони цих чіпів потрапили в російську зброю, таку як безпілотники та ракети». ***(Нідерландський виробник мікросхем Nexperia зазнав атаки хакерів // Укрінформ (https://www.ukrinform.ua/rubric-world/3851691-niderlandskij-virobnik-mikroshem-nexperia-zaznav-ataki-hakeriv.html). 12.04.2024).***

***

«Жахлива та надзвичайно прогресивна кібератака вразила користувачів iPhone щонайменше з 92 країн, включаючи Індію, повідомляє Reuters.

Материнська компанія Apple попередила цільових користувачів в електронному листі, що хакери прагнуть «віддалено скомпрометувати iPhone», і оновила свої вказівки щодо цих випадків проникнення в складні пристрої в середу.

Вони, які називаються «атаками найманців», насправді не намагаються звичайних користувачів витягнути номер банківського рахунку чи іншу особисту інформацію. Звичайні люди, як правило, взагалі ніколи не стають мішенню.

Натомість вони зазвичай націлені на високопоставлених людей — «ймовірно, через те, ким вони є або чим займаються» — у невеликій кількості.

За словами Apple, до них зазвичай входять політики, дипломати, журналісти та активісти.

«Надзвичайна вартість, складність і всесвітній характер атак найманих шпигунських програм робить їх одними з найдосконаліших цифрових загроз, які існують сьогодні», — написала Apple у своїх нових інструкціях.

«Такі атаки набагато складніші, ніж звичайна діяльність кіберзлочинців і споживче зловмисне програмне забезпечення, оскільки зловмисники-шпигуни

застосовують виняткові ресурси, щоб націлитися на дуже невелику кількість конкретних осіб та їхні пристрої».

«Найманні шпигунські атаки фінансуються виключно добре, і вони з часом розвиваються».

Хоча останнє попередження видаляє термін «спонсорований державою» (Reuters повідомляв, що минулої осені Apple зазнала критики через інцидент з урядом Індії та лідерами його опозиції), технічний гігант все ще зазначає, що ці атаки «історично були пов'язані з державними акторами».

В інших випадках проксі можна використовувати від імені нації.

З 2021 року Apple попереджала користувачів принаймні в 150 країнах, що на їхні пристрої можуть вплинути «виключно добре фінансовані» атаки, які з часом удосконалюються та розвиваються.

Якщо це стосується, «Сповіщення про загрозу» з'явиться онлайн у верхній частині веб-сторінки Apple після того, як користувачі ввійдуть за допомогою свого Apple ID через appleid.apple.com.

Потім Apple надішле електронний лист і пінг iMessage на телефон користувача та пов'язану адресу електронної пошти». ***(Alex Mitchell. Apple hit with 'mercenary spyware attacks' — iPhone users warned worldwide of 'most advanced digital threats' // NYP Holdings, Inc. (https://nypost.com/2024/04/11/lifestyle/apple-hit-with-mercenary-spyware-attacks-iphone-users-warned-worldwide/?utm_campaign=nypost&utm_medium=social&utm_source=flipboard&utm_content=NYPost%2Fmagazine%2FEverything+New+York+Post). 11.04.2024).***

***

«Хакер, який нібито викрав критично важливу базу даних, яку підтримує Лондонська фондова біржа, що містить інформацію про терористів, потенційних злочинців і осіб високого ризику, тепер погрожує витоком конфіденційних даних в Інтернеті.

Зловмисник, відомий як GhostR, заявив у четвер, що незабаром почне оприлюднювати деякі з 5,3 мільйона вкрадених записів із World-Check,

перевірочної бази даних, яка використовується банками та іншими установами для боротьби з фінансовими злочинами та забезпечення виконання державних санкцій.

Хакер стверджував, що отримав доступ до бази даних через сінгапурську фірму з доступом World-Check. Фірма мала сервер безперервної інтеграції, який мав адміністративний доступ за замовчуванням, згідно з повідомленнями на популярному хакерському форумі, перевіреному Information Security Media Group. повідомив TechCrunch. Першим про витік

Група Лондонської фондової біржі підтвердила TechCrunch порушення набору даних третьої сторони та заявила, що хакери не отримали доступу до жодної з її систем LSEG.

«Ми підтримуємо зв'язок із постраждалою третьою стороною, щоб забезпечити захист наших даних і забезпечити сповіщення будь-яких відповідних органів», — сказав речник LSEG.

World-Check раніше стикався з компрометацією даних з моменту свого створення в 2014 році, в тому числі через два роки, коли копію бази даних було виявлено на незахищеному сторонньому сервері.

Хакерська група повідомила, що спочатку оприлюднить список «тисяч членів королівської родини з 46 країн, які активно включені до цього чорного списку». Вони стверджували, що викрали всі записи World-Check до 29 березня, коли база даних востаннє оновлювалася перед хакерством.

За даними TechCrunch, які перевірили частину вкрадених даних, записи включають підозрюваних у тероризмі, осіб, пов'язаних з організованою злочинністю, та інших осіб, які «піддаються більшому ризику причетності до корупції чи хабарництва». Повідомляється, що імена включають як нинішніх, так і колишніх урядовців з усього світу, а дані включають все: від номерів соціального страхування та паспортів до ідентифікаторів онлайн-рахунків у криптовалюті та банківської інформації». ***(Chris Riotta. Hacker Threatens to Expose Sensitive World-Check Database // Information Security Media Group, Corp. (https://www.databreachtoday.com/hacker-threatens-to-expose-sensitive-world-check-database-a-***

24909?utm_source=flipboard&utm_content=HamsterBoomer%2Fmagazine%2FHACKER+-+HACKED). 19.04.2024).

***

«Згідно з останнім звітом уряду Великобританії, кіберзлочинці здійснили 7,78 мільйона атак на британський бізнес і майже 1 мільйон – на благодійні організації. Але менше половини цих фірм повідомили про інциденти владі, що, на думку дослідників, є тривожною тенденцією.

У вівторок був опублікований звіт про порушення кібербезпеки за 2024 рік, проведений Департаментом науки, інновацій і технологій. Під час опитування 2000 компаній і 1004 благодійні організації запитали про звітність про інциденти, і в звіті говориться, що «у багатьох із цих випадків організації просто повідомляють про порушення своїм зовнішнім постачальникам кібербезпеки або IT-провайдерам і нікому більше».

Ніколас Райдер, професор права в Університеті Кардіффа, сказав, що багато організацій не бажають повідомляти про кіберінциденти, тому що вони бояться великих штрафів від регуляторних органів, а також репутаційної шкоди, яку завдає розкриття інформації.

Управління комісара з питань інформації Великобританії вимагає від компаній та інших організацій повідомляти про кіберінцидент протягом 72 годин, але зобов’язання щодо звітування залежать від серйозності атаки на цільові системи та кількості постраждалих клієнтів.

Оскільки напади на невеликі організації та благодійні організації, як правило, менш серйозні, звітність є добровільною, що дозволяє деяким організаціям-жертвам уникнути належного регуляторного контролю, сказав Райдер, який також є спеціальним радником Спеціального комітету внутрішніх справ парламенту Великобританії з розслідування шахрайства.

Відсутність реагування на інцидент — це «червоний прапорець», незалежно від масштабу атаки для будь-якої організації, сказав Раян Макконечі, технічний директор компанії Barrier Networks у Глазго. Організації, які покладаються на

стратегію пом’якшення атак, яка є «неформальною» та демонструє «слабке розуміння», як правило, у підсумку «втрачають час і зазнають більш серйозних атак», – сказав він.

МакКонечі сказав, що невеликі організації, які борються з кібербезпекою, повинні використовувати вказівки Національного центру кібербезпеки як відправну точку для покращення свого захисту.

Оскільки керівництво, як правило, є добровільним за своєю природою, фірми не змушені їх дотримуватися, сказав Райдер. За його словами, один із способів вирішення цієї проблеми — зробити обов’язковим звітування про кібератаки та кібершахрайство.

Малі та середні підприємства під загрозою

Згідно з опитуванням, більшість атак були спрямовані на малі та середні організації, і їм бракувало складності. В основному вони стосувалися фішингових схем і видавання себе за іншу особу в Інтернеті. Хоча NCSC раніше попереджав про потенційне збільшення атак програм-вимагачів, націлених на британські благодійні організації, у звіті йдеться, що лише 3% опитаних організацій були мішенню програм-вимагачів.

Багато опитаних організацій повідомили про брак ресурсів і досвіду з кібербезпеки. Під час опитування респондентів запитували про їхню обізнаність щодо вказівок NCSC, таких як 10 кроків до кібербезпеки, які розроблені, щоб допомогти організаціям боротися з кіберризиками. Багато хто не дотримувався повних рекомендацій і приділяв менший пріоритет таким сферам, як управління ризиками ланцюга поставок, регулярне навчання персоналу та виправлення вразливостей». ***(Akshaya Asokan. Half of UK Firms, Charities Failed to Report Cyber Incidents // Information Security Media Group, Corp. (https://www.databreachtoday.com/half-uk-firms-charities-failed-to-report-cyber-incidents-a-24827). 10.04.2024).***

***

«Злом і вторгнення в систему за допомогою різних інструментів стали серйозною проблемою для людей і організацій у всьому світі. Сьогодні зловмисники часто використовують складні підходи з вивчення даних, щоб зламати систему.

Чи можна використати науку про дані, щоб зупинити злом системи, якщо її можна використовувати для отримання контролю над системою? Застосування науки про дані в кібербезпеці спростило передбачення вразливостей системи, зменшивши ймовірність злому шляхом впровадження необхідних запобіжних заходів.

У «Звіті про глобальні ризики 2023» Всесвітнього економічного форуму зазначено, що напади на технологічні ресурси та послуги, такі як фінансові системи та комунікаційна інфраструктура, залишатимуться ризиком у 2024 році, а кібербезпека залишатиметься постійною проблемою.

Спектр цілей розширився, оскільки кібер-зловмисники проникають у різні галузі, включаючи охорону здоров'я, фінанси та роздрібну торгівлю. Кібербезпека та наука про дані є ефективними інструментами для пом'якшення цих втрат. У наступній статті буде детально розглянуто зв'язок між наукою про дані та кібербезпекою.

Що означає Data Science з точки зору кібербезпеки?

Використання науки про дані в кібербезпеці революціонізувало спосіб протидії шахрайським діям. Наука про дані передбачає можливість вторгнення або нападу за допомогою методів машинного навчання на історичних даних. Це передбачає створення алгоритмів для визначення тенденцій з попередніх атак і надання попереджень щодо надійності використовуваної системи.

Наприклад, виявлення незаконного проникнення на об'єкт. Лише попередньо зареєстрованим користувачам буде надано доступ за допомогою моделі AI, яка перевірятиме їхню активність, щоб переконатися, що не відбувається жодної активності, що перевищує дозволене. Усі ці заходи спрямовані на припинення витоку даних і зловживання інформацією.

Як виглядала кібербезпека до Data Science?

На початку розвитку кібербезпеки страх і невпевненість були пов'язані між собою. Плани безпеки корпорацій ґрунтувалися виключно на припущеннях, що викликало цю особливу тривогу. Певні характеристики були засновані на припущеннях, таких як режим роботи атаки та цільовий регіон.

Увесь кібербізнес змінився, коли на сцену вийшла наука про дані. Оскільки технологічні рішення складають більшість рішень щодо кібербезпеки, прогнози даних науки допомогли зменшити ймовірність того, що рішення приймаються неправильно, оскільки більшість суджень базується на фактах.

Завдяки розширенню діапазону ресурсів ці керовані даними технології значно покращили роботу аналітиків і спеціалістів з кібербезпеки, які тепер можуть створювати ефективніші стратегії розвитку безпеки.

Зв'язок між кібербезпекою та наукою про дані

Кібербезпека спрямована на виявлення та припинення таких ризиків, як зловмисне програмне забезпечення, вторгнення та атаки, а також шахрайство. Машинне навчання (ML) – це інструмент, який науковці використовують для виявлення та запобігання цим ризикам. Експерти з безпеки, наприклад, можуть переглянути дані з кількох зразків, щоб знайти проблеми з безпекою. З найменшою можливою кількістю помилкових спрацьовувань цей метод намагається визначити атаки та вторгнення.

Методи дослідження даних використовуються такими системами безпеки, як User and Entity Activity Analytics (UEBA), щоб виявити аномалії в активності користувачів. Як правило, існує зв'язок між порушеннями безпеки та незвичною діяльністю користувача. Кібербезпека значно виграла від науки про дані. Подібно до того, як вивчення даних є вирішальним для конкурентоспроможності в будь-якій галузі, ми обговоримо основні впливи даних на кібербезпеку в цьому розділі.

Як кібербезпека покращується за допомогою прикладної науки про дані та машинного навчання разом?

З кожним днем технології прогресують. У результаті кіберзлочини стають більш імовірними. Наука про дані для кібербезпеки є найкращою відповіддю на цей

запит. Оскільки збирання конфіденційних даних в організації щодня зростає, дослідження даних має бути включено до кожного плану аналізу ризиків. Науку про дані можна застосовувати багатьма різними способами, щоб зменшити небезпеку; наступні приклади висвітлюють деякі з них:

1. Покращений моніторинг безпеки

З розвитком технологій хакери тепер використовують різні методи зламу системи. Удосконалені методології ускладнили корпораціям визначення шляхів проникнення в систему. Моделі машинного навчання, створені з використанням історичних і поточних даних про атаки, пропонують повне розуміння моделювання різних типів атак. Потім ці моделі прогнозують вид нападу та ймовірність злому системи.

2. Захист даних

Кожна фірма сильно залежить від своїх даних, які потрібно захищати будь-якою ціною. Наука про дані використовує алгоритми машинного навчання, щоб допомогти розробити непроникні канали даних для передачі даних.

3. Ефективне прогнозування

Передбачення охоплює більше, ніж просто визначення справжніх позитивів. Крім того, модель кібербезпеки даних повинна давати відносно мало помилкових спрацьовувань, що допоможе в боротьбі зі спамом. За допомогою цих методів можна встановити теорії кіберризиків і загроз, які більше ґрунтуються на реальності, ніж на застарілих уявленнях.

4. Аналіз поведінки

Недостатньо просто зрозуміти характер атаки або ймовірність того, що вона вплине на систему; також потрібно розуміти моделі поведінки хакерів. Це може бути дуже вигідно, оскільки це дозволить нам передбачити його чи її наступний хід чи атаку. Для виконання цього поведінкового аналізу кілька наборів даних об’єднуються, мережеві журнали перевіряються та виявляються кореляції між системами. Це дозволяє виявити модель поведінки хакера та відповідно скорегувати заходи профілактики.

Як виглядає майбутнє?

Одне з найяскравіших майбутніх – наука про дані. Оскільки хакери завжди шукають нові способи проникнути в системи, наука про дані стане довгостроковою відповіддю, щоб зупинити їх. У міру вдосконалення тактики з'являються більш складні атаки. Оскільки протягом наступних кількох десятиліть спостерігатиметься експоненціальне збільшення даних, моделі науки про дані працюватимуть краще, оскільки вони матимуть дедалі більше інформації, щоб з'єднати точки.

Сфера науки про дані виходить за рамки створення моделей і алгоритмів. Одним із ключових обов'язків у цій галузі є аналіз і підтримка поточної моделі науки про дані. Аналіз полегшує диференціацію поведінки на нормальні та аномальні категорії. Масові збитки загрожують великому бізнесу в результаті витоку даних. Їм відчайдушно потрібно з'ясувати, як скоротити ці втрати.

Висновки

За короткий період наука про дані має значний вплив на кібербезпеку. Кожна компанія щодня отримує все більший обсяг даних. Здатність передбачити моделі науки про дані зростатиме разом із обсягом даних. Кожна стадія процесу вимагає співпраці між командами безпеки та аналізу даних. Дані є життєво важливими для всіх компаній, незалежно від розміру, тому захистити їх будь-якою ціною має вирішальне значення для кожного з них. Внесок Data Science в кібербезпеку підняв планку вимог до безпеки». ***(Exploring the Intersection of Data Science and Cyber Security: Insights and Applications // HackerNoon (https://hackernoon.com/exploring-the-intersection-of-data-science-and-cyber-security-insights-and-applications). 15.04.2024).***

***

«Для багатьох компаній у всьому світі «питання коли, а не якщо» звучить дедалі актуальніше, коли йдеться про загрози кібербезпеці. Від фішингових атак до атак програм-вимагачів – і навіть першої в Азіатсько-Тихоокеанському регіоні гучної глибокої фейкової фінансової афери вартістю 200 мільйонів гонконгських доларів – кіберзлочинність є невід'ємною

частиною цифрового ландшафту, здається неминучим і невід'ємним від сучасної цифрової ери.

Немає сумніву, що кіберзлочинність зростає, але ця неприємна тенденція має відчутний фінансовий вплив на організації в усьому світі, втрачаючи загалом 8 трильйонів доларів США у 2023 році, що еквівалентно третьому за величиною ВВП у цій роботі після лише США та Китаю. до 2027 року ця цифра потроїться до приблизно 24 трильйонів доларів США. Згідно з прогнозами ФБР і МВФ,

Кіберзлочини стали «щоденною неприємністю» для компаній і окремих осіб

У Малайзії ситуація лише погіршилася.

Останні звіти показують, що тільки в 3-му кварталі ця країна Південно-Східної Азії була восьмою країною в світі за кількістю зловмисних даних, з майже півмільйона облікових записів, витоку через витоки даних – на 144% більше, ніж кількість витоків у 2-му кварталі. Крім того, тільки в 2023 році підприємства по всій Малайзії стикалися з 74 000 атак на день, що становить 26,85 мільйонів за рік.

Для звичайних малазійців – 76% з яких у своєму житті стикалися з тією чи іншою формою онлайн-чи телефонного шахрайства – такі атаки, гучні чи ні, стали свого роду «щоденною неприємністю». Безумовно, не допомогло те, що багато компаній зараз не зобов'язані законом повідомляти споживачам про порушення даних, що підірвало довіру суспільства до існуючої інфраструктури кібербезпеки.

Підхід Малайзії

Оскільки підприємства продовжують боротися з кіберзлочинністю, уряд виконав свою обіцянку внести цього року законопроект про кібербезпеку, ухваливши його наприкінці березня через нижню палату парламенту. Прем'єр-міністр Анвар Ібрагім рекламував законопроект як шлях до зміцнення потенціалу кібербезпеки країни. Хоча до законопроекту можуть бути внесені зміни під час його обговорення в Сенаті, поточні положення спрямовані на зміцнення Національного агентства з кібербезпеки та створення Національного комітету з кібербезпеки, який контролюватиме повідомлення про порушення для державних і приватних організацій, які вважаються національною критично важливою

інформаційною інфраструктурою (NCII), які варіюються від державних комунальних компаній до фінансових установ.

Організації, що працюють у місті-державі, за законом зобов'язані повідомити Комісію із захисту персональних даних не пізніше ніж через 3 дні з моменту порушення — і повідомити про це постраждалих осіб, якщо вони заподіюють «значну шкоду».

Як і у випадку з правозастосуванням, успіх впровадження законопроекту про кібербезпеку – після того, як він стане законом – значною мірою залежатиме від чіткого інформування урядом про стандарти організацій NCII. У свою чергу, останньому доведеться оптимізувати внутрішні механізми розкриття інформації та передавати відповідні процеси працівникам, які беруть участь у процесі, щоб уникнути плутанини та недомовок.

На момент написання законопроекту Малайзії про кібербезпеку не визначено часові параметри для організацій, які мають звітувати до Національного комітету з кібербезпеки у разі кіберінциденту. Створення механізму, який заохочує терміновість звітності, допоможе зміцнити можливості компаній у сфері кібербезпеки, щоб захистити їх репутацію та підвищити довіру споживачів, чого можна досягти за допомогою індивідуального плану комунікації з кібербезпеки.

Крім того, змусити організації проводити оцінку ризиків щодо своїх можливостей кібербезпеки було б безпрограшним для створення більш безпечного бізнес-середовища та посилення зусиль щодо конфіденційності та захисту даних. Уряд Малайзії може орієнтуватися на знаковий Акт Європейського Союзу про кібернетостійкість, який, як очікується, набуде чинності наприкінці 2025 року.

Хоча нормативні рамки потрібно поєднувати з правильною технологією для боротьби з кіберзагрозами, прийняття відповідних законів, які готують організації до неминучого, слугує надійною відправною точкою для створення більш успішного та безпечного бізнес-ландшафту». ***(Eli Serota and Hezril Azmin. How Malaysia is regulating the rise in cybersecurity threats // FTI Consulting Asia Pacific (https://viewpoints.fticonsulting.com/post/102j5ze/how-malaysia-is-regulating-the-rise-in-cybersecurity-threats). 23.04.2024).***

***

«Mandiant виявив, що хоча час перебування зловмисників у 2023 році скоротився, програми-вимагачі та інші загрози продовжували зростати.

Компанія з кібербезпеки опублікувала у вівторок свій «Спеціальний звіт M-Trends 2024», який запропонував деякі яскраві моменти для організацій на тлі дедалі складнішої та експансивної картини загроз. Відповідно до звіту, який ґрунтується на дослідженнях Mandiant Consulting протягом 2023 року, глобальний середній час перебування зловмисників впав до найнижчої позначки з тих пір, як компанія почала відстежувати показник у 2011 році. Час перебування, тобто кількість днів, протягом яких зловмисник присутні в середовищі до того, як його виявили, зменшилася майже за тиждень — із 16 днів у 2022 році до 10 днів минулого року.

Лише шість років тому середній час перебування становив 78 днів, згідно з Mandiant. У звіті також зазначено, що в 2023 році внутрішнє виявлення вторгнень покращилося, а глобальне медіане знизилося до дев’яти днів з 13 днів роком раніше.

«Загалом, довгострокові тенденції зменшення середнього часу перебування та підвищення рівня внутрішнього виявлення компромісів свідчать про те, що організації досягли значущих, вимірних покращень у своїх захисних можливостях», — йдеться у звіті.

Ще одним позитивним моментом стало збільшення кількості компрометацій, виявлених внутрішньо цільовою організацією, на які припадає 46% усіх вторгнень минулого року порівняно з 37% у 2022 році. «Це, ймовірно, вказує на те, що можливості виявлення продовжують удосконалюватись у всіх організаціях», — сказав Mandiant, який дає змогу командам безпеки виловлювати загрозливих суб’єктів під час початкового зараження та етапів розвідки атаки.

Mandiant сказав, що загальне зменшення часу перебування свідчить про те, що зв’язок між цільовими організаціями та зовнішніми сторонами, такими як компанії з кібербезпеки, які виявляють зловмисну активність і повідомляють жертвам, покращився. Однак компанія також заявила, що збільшення кількості атак

програм-вимагачів також могло бути чинником, оскільки суб'єкти загроз зазвичай повідомляють своїх жертв про вторгнення через повідомлення про викуп.

Програми-вимагачі та нуль днів

Як і інші компанії з кібербезпеки, Mandiant спостерігала зростання активності програм-вимагачів у 2023 році. Минулого року кількість розслідувань, пов'язаних із програмами-вимагачами, зросла до 23% порівняно з 18% у 2022 році. «Це повертає відсоток вторгнень, пов'язаних із програмами-вимагачами, до рівня, який був у 2021 році», - йдеться в повідомленні.

Багато постачальників засобів кібербезпеки спостерігали зниження активності програм-вимагачів у 2022 році, і експерти загалом пояснюють тимчасове зниження такими факторами, як вторгнення Росії в Україну та діями правоохоронних органів, такими як санкції та операції з видалення.

Окрім незначного зростання кількості атак, Mandiant також повідомила, що виявлення вторгнень із використанням програм-вимагачів займало більше часу, ніж виявлення атак без програм-вимагачів. Компанія зазначила, що у 70% вторгнень програм-вимагачів цільові організації були сповіщені зовнішніми сторонами, переважно через вимоги викупу зловмисниками.

Однак Mandiant також повідомив про деякі позитивні тенденції. «Вторгнення з використанням програм-вимагачів було виявлено через шість днів, коли сповіщення надійшло з внутрішнього джерела, порівняно з 12 днями у 2022 році», — йдеться у звіті. «Захисники отримали сповіщення про вторгнення, пов'язані з програмами-вимагачами, від зовнішньої сторони за п'ять днів у 2023 році, на два дні швидше, ніж у 2022 році».

Нік Річард, старший менеджер Mandiant Intelligence у Google Cloud, сказав, що учасники програм-вимагачів не обов'язково вдосконалюють свої методи ухилення. Але вони намагаються пришвидшити час атаки, щоб випередити захисників.

«Зростання поширеності вторгнень, пов'язаних із програмами-вимагачами, на п'ять відсотків у 2023 році в поєднанні зі зміною глобального часу перебування програм-вимагачів з дев'яти днів до п'яти, може бути більшою мірою вказівкою на

спроби зловмисників прискорити час до страти викупу через підвищений ризик. зараження, оскільки Mandiant спостерігав покращення часу очікування для всіх типів розслідувань і джерел сповіщень», — сказав він редакційній редакції TechTarget.

Незважаючи на обнадійливі дані, Mandiant попередив, що зловмисники всіх типів зосередилися на методах ухилення, насамперед через використання вразливостей нульового дня. «У 2023 році, коли було виявлено початковий вектор вторгнення, експлойт спостерігався у 38% випадків. Mandiant продовжує спостерігати як за кібершпигунством, так і за фінансово мотивованими зловмисниками, які використовують уразливості нульового дня для здійснення своїх операцій».

Mandiant заявив, що найпоширенішим нульовим днем у 2023 році була CVE-2023-34362, критична вразливість у продукті для керованої передачі файлів MoveIt Transfer від Progress Software. За оцінками Emsisoft, атаки торкнулися понад 2000 клієнтів MoveIt Transfer.

Незважаючи на те, що групи китайського кібершпигунства використовували більшість нульових днів у 2023 році, Mandiant попередив, що такі загрози «більше не є нішевою можливістю», обмеженою для суб'єктів національної держави. «Посилення використання програм-вимагачів і крадіжок даних у режимі «нульового дня», триваюча експлуатація, що підтримується державою, і зростання готових або готових можливостей, які можна придбати у комерційних постачальників систем стеження, продовжуватимуть сприяти ідентифікації нульових вразливості та експлойти, націлені на них», – йдеться у звіті.

Поряд із нульовими днями в «Спеціальному звіті M-Trends 2024» зазначено, що зловмисники також використовують інші підходи, щоб уникнути виявлення, наприклад тактику «жити за рахунок землі». Вони включають загрозливих суб'єктів, які використовують законні продукти та наявні інструменти в цільовому середовищі для переміщення вбік і отримання доступу до конфіденційних даних.

Річард зазначив, що протягом останніх трьох років зловмисники відійшли від популярних бекдорів, таких як Cobalt Strike Beacon. «Це, ймовірно, пов'язано з тим,

що зловмисники переходять від явного використання зловмисного програмного забезпечення до використання резидентного зловмисного програмного забезпечення в пам’яті, зловживають сторонніми інструментами віддаленого адміністрування та використовують більше методів, що живуть за межами землі, які загалом зроблять зловмисників більш успішними в ухиленні від технологій захисту кінцевих точок», – сказав він.

Крім того, зловмисники все частіше націлюються на периферійні мережеві пристрої та інші технології, які можуть бути незахищені продуктами виявлення та реагування. Mandiant також попередив про збільшення кількості скомпрометованих хмарних ідентифікацій через обхідні атаки MFA. «Найбільш помітним є все більш широке впровадження веб-проксі або фішингових сторінок «супротивник посередині», які здатні зробити більшість реалізацій MFA неефективними шляхом крадіжки конфіденційних маркерів сеансу входу». ***(Rob Wright. Mandiant: Attacker dwell time down, ransomware up in 2023 // TechTarget (https://www.techtarget.com/searchsecurity/news/366581738/Mandiant-Attacker-dwell-time-down-ransomware-up-in-2023). 23.04.2024).***

***

«У своєму кабінеті на одному з верхніх поверхів штаб-квартири оргкомітету Олімпійських ігор у Парижі Франц Регул не сумнівається в тому, що нас чекає.

«Нас атакуватимуть», — сказав пан Регул, який очолює команду, відповідальну за захист від кіберзагроз на цьогорічних Літніх іграх у Парижі.

Компанії та уряди в усьому світі зараз мають команди, подібні до пана Регула, які працюють у спартанських кімнатах, обладнаних банками комп’ютерних серверів та екранами з індикаторами, які попереджають про вхідні хакерські атаки. У паризькому операційному центрі навіть є червоне світло, щоб попередити персонал про найсерйознішу небезпеку.

Наразі, за словами пана Регула, серйозних збоїв не було. Але оскільки місяці до Олімпійських ігор зводяться до тижнів, а потім днів і годин, він знає, що

кількість спроб злому та рівень ризику зростатиме експоненціально. Однак, на відміну від компаній і урядів, які планують можливість нападу, пан Регул сказав, що точно знає, коли очікувати найгіршого.

«Не багато організацій можуть сказати вам, що вони будуть атаковані в липні та серпні», - сказав він.

Занепокоєння щодо безпеки під час великих подій, таких як Олімпійські ігри, зазвичай зосереджувалися на фізичних загрозах, як-от терористичні атаки. Але оскільки технології відіграють все більшу роль у розгортанні Ігор, організатори Олімпіади все частіше розглядають кібератаки як більш постійну небезпеку.

Загрози різноманітні. Експерти кажуть, що хакерські групи та такі країни, як Росія, Китай, Північна Корея та Іран, тепер мають складні операції, здатні відключати не лише комп'ютери та мережі Wi-Fi, але й цифрові системи продажу квитків, сканери облікових даних і навіть системи синхронізації подій.

Побоювання щодо хакерських атак не просто гіпотетичні. На зимових Олімпійських іграх у Пхенчхані 2018 року в Південній Кореї успішна атака ледь не зірвала Ігри ще до того, як вони почалися.

Ця кібератака почалася холодної ночі, коли вболівальники прибули на церемонію відкриття. Ознаки того, що щось не так, з'явилися відразу. Мережа Wi-Fi, важливий інструмент для передачі фотографій і новин, раптово припинила роботу. Водночас офіційний додаток для смартфонів Олімпійських ігор — той, у якому зберігалися квитки для вболівальників і важлива транспортна інформація — перестав функціонувати, не даючи деяким уболівальникам потрапити на стадіон. Трансляційні безпілотники були приземлені, а підключені до Інтернету телевізори, призначені для показу зображень церемонії в різних місцях, зникли.

Але церемонія тривала, як і Ігри. Десятки співробітників відділу кібербезпеки працювали всю ніч, щоб відбити атаку та усунути збої, і на наступний ранок майже не було ознак того, що катастрофу вдалося запобігти, коли почалися перші події.

Відтоді загроза Олімпіаді лише зросла. Команда з кібербезпеки на останніх літніх Іграх у Токіо в 2021 році повідомила, що зіткнулася з 450 мільйонами спроб «подій безпеки». Паріс очікує зіткнутися у вісім-12 разів більше, сказав пан Регул.

Можливо, щоб продемонструвати масштаб загрози, чиновники з кібербезпеки Парижа 2024 вільно використовують військову термінологію. Вони описують «військові ігри», призначені для перевірки спеціалістів і систем, і посилаються на відгуки «ветеранів Кореї», які були інтегровані в їхній розвиток захисту.

Офіційні особи Paris 2024 заявили, що готуються до нападів, подібних до того, що зірвало церемонію відкриття зимової Олімпіади в Пхенчхані 2018 року. П'єр-Філіп Марку/Агентство Франс-Прес — Getty Images

Експерти кажуть, що за більшістю кібератак стоять різні актори, зокрема злочинці, які намагаються отримати дані в обмін на прибутковий викуп, і протестувальники, які хочуть висвітлити конкретну причину. Але більшість експертів сходяться на думці, що лише національні держави можуть здійснити найбільші напади.

У атаці 2018 року в Пхенчхані спочатку звинуватили Північну Корею, антагоністичний сусід Південної Кореї. Але експерти, включно з агенціями США та Британії, пізніше дійшли висновку, що справжній винуватець — зараз широко визнано Росію — навмисно використовував методи, спрямовані на те, щоб покласти провину на когось іншого.

Цього року Росія знову в центрі уваги.

Збірну Росії не допустили до Олімпіади після вторгнення країни в Україну в 2022 році, хоча невеликій групі окремих росіян буде дозволено змагатися як нейтральних спортсменів. Відносини Франції з Росією погіршилися настільки, що нещодавно президент Еммануель Макрон звинуватив Москву в спробі підірвати Олімпійські ігри через кампанію з дезінформації.

Міжнародний олімпійський комітет також вказав пальцем на спроби російських груп завдати шкоди Іграм. У листопаді МОК опублікував незвичайну заяву, в якій говориться, що став мішенню для наклепницьких «фейкових повідомлень новин» після того, як на YouTube з’явився документальний фільм із закадровим голосом, згенерованим штучним інтелектом, який нібито був актором Томом Крузом.

Пізніше окрема публікація в Telegram — платформі зашифрованих повідомлень і контенту — імітувала фейкову новину, яку транслювала французька мережа Canal Plus, і опублікувала неправдиву інформацію про те, що МОК планує заборонити ізраїльським і палестинським командам брати участь в Олімпійських іграх у Парижі.

На початку цього року російським пранкерам, видаючи себе за високопоставленого африканського чиновника, вдалося додзвонитися до президента МОК Томаса Баха. Дзвінок був записаний і опублікований на початку цього місяця. Росія використала зауваження пана Баха, щоб звинуватити олімпійських чиновників у «змові», щоб не допустити її команду до Ігор.

У 2019 році, за даними Microsoft, російські державні хакери атакували комп'ютерні мережі щонайменше 16 національних і міжнародних спортивних і антидопінгових організацій, включаючи Всесвітнє антидопінгове агентство, яке на той час було готове оголосити про покарання проти Росії, пов'язані з її державою. підтримувана допінгова програма.

Три роки тому Росія атакувала антидопінгових чиновників на літній Олімпіаді в Ріо-де-Жанейро. Відповідно до звинувачень кількох офіцерів російської військової розвідки, поданих Міністерством юстиції Сполучених Штатів, оперативники цього інциденту підробили мережі Wi-Fi у готелях, які використовували антидопінгові чиновники в Бразилії, щоб успішно проникнути в мережі електронної пошти та бази даних їхніх організацій.

Кіаран Мартін, який працював першим виконавчим директором Британського національного центру кібербезпеки, сказав, що минула поведінка Росії зробила її «найочевиднішою загрозою» на Паризьких іграх. Він сказав, що сфери, які можуть стати ціллю, включають планування заходів, публічні трансляції та системи продажу квитків.

«Уявіть собі, що всі спортсмени прибули вчасно, але система, яка сканує iPhone біля воріт, вийшла з ладу», — сказав пан Мартін, який зараз є професором Школи державного управління Блаватника при Оксфордському університеті.

«Проходите при напівпорожньому стадіоні чи зволікаємо?» він додав. «Навіть бути поставленим у таке становище, коли вам доведеться або відкладати це, або мати спортсменів світового класу, які виступають перед напівпорожнім стадіоном у найбільшій події свого життя, — це абсолютний провал».

Пан Регул, голова відділу кібербезпеки Парижа, відмовився говорити про будь-яку конкретну країну, яка може націлитися на Ігри цього літа. Але він сказав, що організатори готуються протидіяти методам, характерним для країн, які представляють «сильну кіберзагрозу».

Цього року паризькі організатори проводили те, що вони назвали «військовими іграми» разом з МОК і такими партнерами, як Atos, офіційний технологічний партнер Ігор, щоб підготуватися до атак. Під час цих навчань так званих етичних хакерів наймають для атаки на системи, встановлені для Ігор, а тим, хто виявляє вразливі місця, пропонуються «нагороди за помилки».

Раніше хакери атакували спортивні організації за допомогою шкідливих електронних листів, вигаданих персонажів, вкрадених паролів і шкідливого програмного забезпечення. Починаючи з минулого року, нові співробітники паризького оргкомітету пройшли навчання, щоб виявити фішингові афери.

«Не всі хороші», — сказав містер Регул.

Принаймні в одному випадку співробітник Ігор оплатив рахунок на рахунок після того, як отримав електронний лист, який видавав себе за іншу посадову особу комітету. Співробітники служби кібербезпеки також виявили обліковий запис електронної пошти, який намагався видати себе за обліковий запис, призначений керівнику Paris 2024 Тоні Естанге.

Попереду ще мільйони спроб. Кібератаки зазвичай були «зброєю масового роздратування, а не зброєю масового знищення», — сказав пан Мартін, колишній британський чиновник з кібербезпеки.

«У гіршому випадку, — сказав він, — вони були зброєю масового ураження». ***(Дмитро Сизов. Експерти з кібербезпеки очікують потужні атаки під час Олімпійських ігор в Парижі // internetua (https://internetua.com/eksperti-z-kiberbezpeki-ocsikuuat-potujni-ataki-pid-csas-olimpiiskih-igor-v-pariji). 17.04.2024).***

***

«Національне агентство кібербезпеки Італії зафіксувало збільшення кількості кібератак на 29% у 2023 році порівняно з 2022 роком, причому 248 з 319 атак, пов'язаних з війною в Україні, були здійснені проросійськими хакерськими угрупованнями.

Національне агентство з кібербезпеки Італії зафіксувало зростання хакерських втручань, пов'язаних з війною рф в Україні та на Близькому Сході; значну кількість акцій взяли на себе проросійські хакери, передає УНН із посиланням на Rai та ANSA.

Деталі

Національним агентством кібербезпеки Італії виявлено збільшення кількості кібератак в країні у 2023 році, - на 29% більше, ніж у 2022-му. Кількість постраждалих зросла втричі: з 1 150 до 3 302 осіб. У країні зростає кількість хакерських атак пов'язаних з війнами, - агресії рф проти України та війни на Близькому Сході.

Втім більшість атак, а саме 248 з 319, були здійснені проросійськими угрупованнями. Водночас пропалестинська група провела єдину кампанію, здійснивши 15 атак. Відповідні дані містяться у щорічному звіті Акнальського парламенту, представленому сьогодні уповноваженим з питань безпеки республіки Альфредо Мантовано та директором Агентства Бруно Фраттазі.

Щодо загальної кількості випадків, найбільшу кількість атак становили Ddos - 319 (це розподілена відмова в обслуговуванні, блокування сайту шляхом переповнення його запитами на доступ);

У 275 випадках йшлося про поширення шкідливого програмного забезпечення через електронну пошту;

240 - фішинг (надсилання фальшивих електронних листів з метою викрадення конфіденційної інформації);

165 - ransomware (атака з вимогою викупу).

Найбільш постраждалими секторами були телекомунікації (216); за ними йдуть центральні органи державної влади (201) та місцеві органи державної влади

(140)». ***(Італію кібератакують: майже 30% зростання кібервтручань у 2023 році, зокрема 248 диверсій з боку проросійських хакерів // Інформаційне агентство «Українські Національні Новини» (https://unn.ua/news/italiiu-kiberatakuiut-maizhe-30percent-zrostannia-kibervtruchan-u-2023-rotsi-zokrema-248-dyversii-z-boku-prorosiiskykh-khakeriv). 24.04.2024).***

***

«Volkswagen, автомобільний гігант, опинився в центрі масштабної кібероперації, підозри в якій спрямовані на хакерів, що працюють з Китаю. Кібератака Volkswagen, яка сталася понад десять років тому, але продовжує відгомін і сьогодні, проливає світло на китайських хакерів та їхню шпигунську діяльність.

Викрадені дані під час багаторічної кібератаки Volkswagen, описаної як «вибухонебезпечна», включають конфіденційну інформацію про внутрішню роботу Volkswagen, починаючи від планів розвитку бензинових двигунів і закінчуючи важливими деталями щодо ініціатив електронної мобільності. Розслідування під керівництвом ZDF frontal і Der Spiegel оприлюднили понад 40 внутрішніх документів, які причетні китайських хакерів до складної операції.

Багаторічна кібератака Volkswagen китайськими хакерами

Хронологія кібератак на Volkswagen, що охоплює з 2010 по 2015 роки, підкреслює ретельне планування та виконання зловмисниками. Згідно з повідомленнями, хакери ретельно проаналізували IT-інфраструктуру Volkswagen, перш ніж зламати її мережі, що призвело до викрадання приблизно 19 000 документів.

Серед викраденої інтелектуальної власності були бажані ідеї щодо нових технологій, таких як електричні та водневі автомобілі, які мають вирішальне значення для конкурентоспроможності Volkswagen на світовому ринку.

Хоча Китай прямо не звинувачується, докази вказують на його причетність, оскільки IP-адреси простежуються до Пекіна, а час атак узгоджується з робочим днем Китаю.

Крім того, використовувані хакерські інструменти, в тому числі горезвісний «China Chopper», ще більше припускають китайське походження, хоча переконливі докази залишаються невловимими.

Наслідки витоку даних Volkswagen

Наслідки цих порушень даних Volkswagen виходять за межі корпоративного шпигунства, викликаючи занепокоєння щодо чесної конкуренції в автомобільній промисловості. Професор Гелена Вісберт з Університету Остфалії підкреслює стратегічну перевагу, отриману тими, хто знайомий з планами конкурентів, підкреслюючи значення викрадених даних у формуванні динаміки ринку.

Визнання інциденту Volkswagen підкреслює серйозність ситуації, а також запевнення щодо посилених заходів безпеки IT. Однак Федеральне відомство з інформаційної безпеки (BSI) попереджає про постійні загрози, підкреслюючи привабливість німецького досвіду як мішені для шпигунства.

У той час як німецькі компанії готуються до виставки Auto China, кібератака на Volkswagen ставить під сумнів наміри китайських хакерів та їхні цілі в автомобільній промисловості. Cyber Express буде уважно стежити за ситуацією, і ми оновимо цю публікацію, щойно отримаємо більше інформації про ймовірні атаки або будь-які оновлення від Volkswagen.

Кібератаки на автомобільну промисловість

З розвитком автомобільних технологій транспортні засоби стають дедалі вразливішими до кібератак, особливо з розвитком електроніки, програмного забезпечення та підключення до Інтернету. Експерти попереджають, що навіть електромобілі (EV) піддаються підвищеному ризику через свої складні електронні системи. Атаки програм-вимагачів можуть бути націлені на такі критичні функції, як системи рульового керування та гальмування, що створює значні проблеми з безпекою.

Велика кількість програмного коду в сучасних автомобілях створює широкі можливості для кіберзагроз, які впливають не лише на самі автомобілі, але й на всю їх екосистему. У той час як захист кібербезпеки вдосконалюється, автомобільна

промисловість стикається з проблемами в управлінні життєвими циклами програмного забезпечення та забезпеченні наскрізного управління ризиками.

Співпраця між зацікавленими сторонами галузі, урядом і приватними гравцями є важливою для вирішення цих проблем. Оскільки глобальний ринок автомобільної кібербезпеки зростає, потреба в надійних заходах кібербезпеки стає все більш критичною, що спонукає постачальників програмного забезпечення пропонувати локалізовані та економічно ефективні рішення». ***(Ashish Khaitan. Multi-Year Cyberattack: Chinese Hackers Suspected in Breaching Volkswagen // The Cyber Express (https://thecyberexpress.com/chinese-hackers-behind-volkswagen-cyberattack/?utm_source=flipboard&utm_content=FlipboardCanada%2Fmagazine%2FTechnology). 26.04.2024).***

***

«…Школи та навчальні заклади можуть стати легкою мішенню для зловмисних хакерів з кількох причин. Загроза кібербезпеці для освітнього сектору Великобританії вважається значною та зростає. Сектор все більше залежить від цифрових технологій для викладання, навчання та адміністрування, що посилюється потребою у швидкому переході на нові технології в останні роки через пандемію. Кілька факторів сприяють підвищенню кіберризику в цьому секторі:

Цінні дані

Навчальні заклади зберігають велику кількість конфіденційних даних, включаючи особисту інформацію про студентів і співробітників, дані досліджень і фінансові записи, що робить їх привабливими мішенями для кіберзлочинців.

Ресурсні обмеження

Особливо в початковій та середній освіті часто існують обмежені бюджети та брак внутрішнього досвіду, присвяченого кібербезпеці, що робить ці заклади більш уразливими до атак.

Збільшена поверхня атаки

Широке впровадження платформ онлайн-навчання, цифрових інструментів і технологій віддаленого доступу, прискорене пандемією COVID-19, розширило поверхню атак і з'явило нові вразливості.

Загрози програм-вимагачів

Навчальні заклади стали відомими цілями для атак програм-вимагачів, причому зловмисники роблять ставку на терміновість і тиск, з яким стикаються ці заклади, щоб відновити доступ до навчальних матеріалів і оперативних даних. Сектор стикається з особливим тиском, оскільки існує непряма та явна згода та очікування, що наші діти будуть у безпеці – і ця безпека має поширюватися на онлайнове та цифрове середовище. Нашою метою має бути захист конфіденційної інформації та систем, а також забезпечення безперервності освітніх послуг перед обличчям зростаючих кіберзагроз.

Поліпшити захист

Сектор освіти може швидко посилити свій кіберзахист за допомогою багаторівневого підходу, зосереджуючись на негайних покращеннях і створюючи основу для довгострокової стійкості. Ви повинні провести термінову оцінку кібербезпеки, щоб виявити вразливі місця в мережі та системах школи. Вибираючи, хто може проводити оцінку кібербезпеки, враховуйте складність мережі, чутливість даних, що зберігаються, і потенційний вплив загроз кібербезпеці. Незалежно від того, хто проводить оцінювання, воно має бути ретельним, охоплювати всі аспекти кібербезпеки (включно з політикою, практикою та технічним захистом) і давати дієві рекомендації. Тут у вас є цілий ряд можливостей, від вашої внутрішньої IT-команди до зовнішніх консультантів з кібербезпеки, спеціалізованих аудиторів з кібербезпеки, постачальників технологій, державних чи освітніх організацій або однорангових мереж.

Системи оновлення та виправлення

Дуже часто ми чуємо, що хакери отримали доступ до мережі просто через невиправлену вразливість. Застаріле програмне забезпечення та IT-пристрої, які не отримують необхідних виправлень, оновлень і обслуговування, можуть бути

джерелом уразливостей. Переконайтеся, що все ваше мережеве програмне забезпечення та системи оновлені з останніми виправленнями безпеки.

Безпечна конфігурація

Застосуйте безпечні конфігурації до всіх пристроїв і мереж. Це включає відключення непотрібних служб, захист конфіденційних даних і забезпечення належного контролю доступу.

Багатофакторна автентифікація (MFA)

Застосуйте MFA, де це можливо, особливо для доступу до важливих систем та інформації. Це додає додатковий рівень безпеки, крім паролів, таких як фізичний маркер або ключ. Шукайте рішення з оптимальним користувацьким засобом, яке спрощує ввімкнення автентифікації.

Брандмауери та безпека кінцевих точок

Встановлення надійних брандмауерів захищає периметр вашої мережі. Додавання веб-блокувальників із фільтрацією URL-адрес блокує зловмисне програмне забезпечення в Інтернеті, допомагає забезпечити безпечне віддалене з'єднання та забезпечує жорсткий контроль над веб-серфінгом. Переконайтеся, що всі пристрої захищено найновішим антивірусним програмним забезпеченням і розгляньте можливість додавання можливостей EDR для постійного моніторингу, який запобігає виконанню невідомих процесів.

Впровадьте надійний і безпечний Wi-Fi

Wi-Fi у навчальних закладах часто має вирішальне значення для навчання та викладання. Щоб надати безпечний доступ до Інтернету, зосередьтеся на приватних мережах і точках доступу, які можуть обслуговувати щільність без ризиків. Розгляньте рішення Wi-Fi, керовані хмарою, для оптимізації продуктивності, кращої видимості та звітності.

Плани резервного копіювання та відновлення

Регулярно створюйте резервні копії даних і систем і переконайтеся, що ці резервні копії надійно зберігаються за межами сайту. Розробіть комплексний план аварійного відновлення, який включає процедури відновлення даних і систем у разі кібератаки.

Фреймворки кібербезпеки

Прийняти визнані рамки та стандарти кібербезпеки, такі як стандарти NCSC. Вони містять корисні найкращі практики та вказівки щодо покращення стану кібербезпеки.

Співпрацювати

Беріть участь у платформах для обміну інформацією та співпраці, таких як регіональні та секторальні групи з кібербезпеки. Вони можуть надати цінну інформацію про нові загрози та передові практики.

Професійна підтримка

Розгляньте можливість найняти фірму з кібербезпеки або консультанта для надання експертних порад і підтримки. Вони можуть допомогти в оцінці вразливостей, посиленні захисту та навчанні персоналу.

Навчання обізнаності

Відомо, що багато атак відбуваються через уразливості у «wetware» – нас, людей. Досвідчені зловмисники знають, як використовувати шкідливі методи електронної пошти, наприклад, щоб отримати паролі та конфіденційну інформацію від непомітних членів команди, яких часто змушують розголошувати інформацію, не усвідомлюючи, що відбувається. Впроваджуйте регулярні тренінги з кібербезпеки для всіх співробітників і студентів, зосереджуючись на важливості надійних паролів, розпізнавання спроб фішингу та безпечних методах роботи в Інтернеті. Розкажіть викладачам, співробітникам і адміністраторам про атаки соціальної інженерії, щоб обмежити ризик. Ключова освіта з питань безпеки має включати:

- Виявлення спроб фішингу
- Використання передових методів безпеки електронної пошти
- Уникайте слабких або відкритих паролів
- Повідомлення про інциденти в IT-відділ

Планування реагування на інциденти

Розробіть і протестуйте план реагування на інциденти, в якому описано ролі, обов’язки та процедури реагування на кіберінциденти. Це має включати стратегії

комунікації як усередині компанії, так і з зовнішніми зацікавленими сторонами. Якщо у вашій школі чи закладі було виявлено порушення, повідомте про це відповідним органам, таким як Action Fraud, Національний центр кібербезпеки (NCSC), Управління інформаційного комісара (ICO) або місцеві органи влади. Доведення проблем до відома державних службовців може створити додаткові можливості для надання більшого фінансування або ресурсів, допомагаючи навчальним закладам отримати підтримку, необхідну для оптимізації кібербезпеки.

Прийняття єдиного підходу до кібербезпеки

Управління IT-системами для будь-якого навчального закладу – непроста справа. Освітній сектор потребує рішень безпеки, які дають освітянам змогу забезпечувати інклюзивне навчання. Контроль доступу, захист активів, безпека ідентичності та захист кінцевих точок — це лише деякі з рішень, необхідних для створення надійного середовища навчання. Відключена безпека більше не є варіантом у складному ландшафті загроз 2024 року. Навчальні заклади повинні прийняти єдиний і спрощений підхід до безпеки». ***(OLI VENN. It's 2024 – time for schools to fight back against cyber security threats // Education Today Magazine (https://education-today.co.uk/its-2024-time-for-schools-to-fight-back-against-cyber-security-threats/). 26.04.2024).***

***

Вірусне та інше шкідливе програмне забезпечення

«Дослідники безпеки попереджають про відносно нове шкідливе програмне забезпечення під назвою Latrodectus, яке, як вважають, є еволюційним наступником завантажувача IcedID. Він був виявлений у зловмисних електронних кампаніях з листопада 2023 року, і останні вдосконалення ускладнили його виявлення та пом'якшення.

Команда Proofpoint Threat Research у партнерстві з Team Cymru S2 Threat Research помітила майже десяток кампаній, які доставляють Latrodectus, починаючи з лютого 2024 року. Зловмисне програмне забезпечення, яке

використовується брокерами початкового доступу, завантажує корисні дані та виконує довільні команди.

Хоча початковий аналіз припустив, що Latrodectus є новим варіантом IcedID, подальше дослідження виявило, що це нове зловмисне програмне забезпечення, швидше за все, назване Latrodectus через рядок, визначений у коді. Latrodectus використовує інфраструктуру, яка використовувалася в історичних операціях IcedID, що вказує на потенційні зв'язки з тими самими суб'єктами загрози. IcedID, вперше виявлений у 2017 році, був описаний як банківський троян і троян віддаленого доступу.

Дослідники виявили інформацію про діяльність загрозливих акторів TA577 і TA578 – основних розповсюджувачів Latrodectus, які ілюструють еволюцію тактики, яку використовували загрозливі особи з часом.

TA577, раніше відомий розповсюдженням Qbot, використовував Latrodectus у трьох кампаніях у листопаді 2023 року, перш ніж повернутися до Pikabot. Навпаки, TA578 переважно розповсюджує Latrodectus із середини січня 2024 року, використовуючи контактні форми та методи видавання себе за іншу особу, щоб доставити зловмисне програмне забезпечення до цілей.

Latrodectus функціонує як завантажувач, і його основна мета — завантажувати корисні дані та виконувати довільні команди. Його методи ухилення від пісочниці заслуговують на увагу, і він має схожість зі шкідливим програмним забезпеченням IcedID. Ця оцінка свідчить про те, що Latrodectus, ймовірно, був розроблений тією ж групою, що й IcedID.

Функції шкідливих програм

Latrodectus використовує складні методи, щоб уникнути виявлення, включаючи динамічну роздільну здатність функцій Windows API. Він перевіряє наявність налагоджувачів, збирає системну інформацію та обходить пісочниці. Його протокол зв'язку, подібний до IcedID, шифрує реєстраційну інформацію перед передачею її на сервери керування, забезпечуючи приховану роботу.

Його модульна структура дозволяє адаптуватися до різних середовищ і виконувати широкий спектр шкідливих дій.

Аналіз інфраструктури Latrodectus, проведений командою Cymru, виявив значне збігання з операціями IcedID, що свідчить про спільну участь учасників загрози. Шаблони тривалості життя та швидкості налаштування C2 дають змогу зрозуміти динаміку роботи Latrodectus, висвітлюючи постійний цикл активності та еволюції інфраструктури.

Він використовує спрощений алгоритм дешифрування рядків, замінюючи попередній генератор псевдовипадкових чисел (PRNG) на рухливий ключ XOR для ефективного дешифрування.

Зловмисне програмне забезпечення забезпечує стійкість в заражених системах, інсталюючись, встановлюючи ключі автозапуску та створюючи заплановані завдання. Зв'язок із сервером керування шифрується за допомогою алгоритму RC4 із узгодженим ключем 12345. Кожен заражений хост генерує унікальний ідентифікатор бота на основі свого серійного ідентифікатора, який шифрується та надсилається на сервер C2 для ідентифікації.

Розподілена інфраструктура C2 включає сервери рівня 1 і рівня 2 і демонструє шаблони, які вказують на діяльність оператора та підключення до історичних операцій IcedID. Ідентифікатори кампаній хешуються за допомогою алгоритму FNV-1a, який співвідноситься з конкретними кампаніями учасників загрози для атрибуції.

За словами дослідників, ця тактика, а також її механізми стійкості та зашифрований зв'язок ускладнюють ефективне виявлення та пом'якшення традиційними заходами безпеки». ***(Prajeet Nair. Sophisticated Latrodectus Malware Linked to 2017 Strain // Information Security Media Group, Corp. (https://www.databreachtoday.com/sophisticated-latrodectus-malware-linked-to-2017-strain-a-24794). 05.04.2024).***

***

«Згідно з новими дослідженнями, кампанія зловмисного програмного забезпечення, яка викрадає популярне антивірусне рішення для встановлення бекдорів у великих корпоративних мережах, триває принаймні з 2018 року.

Спеціаліст із безпеки Avast опублікував звіт, у якому детально описано ланцюг зараження кампанії зловмисного програмного забезпечення GuptiMiner, описуючи, як його розробники вдосконалювали свої методи обфускації та доставки протягом багатьох років.

У липні 2023 року Avast виявив кампанію GuptiMiner, націлену на індійське антивірусне програмне забезпечення eScan, підкресливши докази того, що кампанія була активна принаймні п’ять років, а ймовірно, довше.

Сама атака використовувала вразливість у механізмі оновлення програмного забезпечення eScan для розповсюдження бекдорів і майнерів у цільовій мережі.

У звіті описано, що ланцюжок зараження GuptiMiner дуже складний, у ньому використовується низка різних атакувальних методів, зокрема надсилання DNS-запитів на DNS-сервери зловмисника, стороннє завантаження DLL, вилучення корисних навантажень із, здавалося б, безпечних файлів зображень і підписання корисних навантажень за допомогою спеціального довіреного кореневого центру сертифікації. щоб уникнути виявлення.

Експлуатація вразливості eScan покладається на виконання атаки «людина посередині», як виявилося у звіті, коли зловмисник захоплює пакет оновлення та замінює його шкідливою версією.

Дослідники Avast не змогли підтвердити, як зловмисники змогли перехопити пакети, припускаючи, що зловмисник уже скомпрометував цільову мережу, щоб перенаправити трафік через її зловмисного посередника.

Коли пакет оновлення успішно вилучено, процес оновлення eScan розпаковує та виконує пакет, після чого DLL завантажується з чистими двійковими файлами eScan, щоб підвищити привілеї зловмисного програмного забезпечення для продовження ланцюга зараження.

Ранні версії ланцюга зараження GuptiMiner використовували техніку маніпулювання DNS для розподілу різних корисних даних, які використовувалися в атаці, але Avast зазначив, що учасники загрози, що стоять за кампанією, відмовилися від цього підходу на користь більш ефективної техніки маскування IP-адрес.

Атака часто використовує зображення PNG як транспортний засіб для доставки зловмисних шелл-кодів у цільову мережу, маскуючи корисне навантаження, яке складалося з кількох бекдорів і пакету криптомайнінгу XMRig.

Infostealer нагадує північнокорейський груповий кейлоггер Kimsuky

Avast каже, що вони знайшли два приклади різних варіантів бекдорів, які поширюються в мережах жертв. Перший із них — це розширена збірка інструменту підключення командного рядка PuTTY Link.

Цей вдосконалений PuTTY Link оптимізує збірку для сканування локальної мережі SMB і, зрештою, полегшує бічне переміщення в мережі з потенціалом для використання машин Windows 7 і Windows Server 2008 шляхом маршрутизації трафіку SMB через скомпрометований пристрій жертви.

Інший бекдор, виявлений Avast, — це модульний бекдор, який спеціально націлений на величезні корпоративні мережі. Це складається з двох окремих фаз: спочатку зловмисне програмне забезпечення сканує пристрої жертви на предмет будь-яких закритих ключів або цінних активів, що зберігаються локально, а потім зловмисне програмне забезпечення впроваджує бекдор у вигляді шелл-коду.

Розглянутий шелл-код був розроблений як багатомодульний, оскільки він має можливість додавати більше модулів до потоку виконання. Після розповсюдження бекдор розшифровує жорстко закодовану конфігурацію, яка гарантує, що вона функціонує належним чином і не виявляється.

Ця конфігурація містить відомості про те, з яким сервером спілкуватися, який мережевий порт він має використовувати та тривалість затримок, які він має використовувати між командами та запитами.

Дослідники припустили, що група, яка стоїть за кампанією GuptiMiner, може бути пов’язана з північнокорейським колективом загроз Kimsuky, після того як помітили викрадача інформації, який мав схожість із шляхом PDB, який використовується в кейлоггері Kimsuky.

У 2023 році Avast оприлюднив уразливість як для антивірусу eScan, так і для індійської команди реагування на надзвичайні ситуації в області комп’ютерів, India CERT, показавши, що eScan не виявляла проблему принаймні п’ять років.

Згідно зі звітом, 31 липня 2023 року eScan підтвердив, що проблему вирішено та успішно вирішено.

Avast заявив, що продовжує спостерігати за новими зараженнями GuptiMiner, однак, вказуючи на те, що клієнти продовжують використовувати застарілі та вразливі версії.

Охоронна фірма завантажила на свою сторінку GitHub повний список індикаторів компрометації (IoC), щоб допомогти розпізнати кампанію GuptiMiner». ***(Solomon Klappholz. Hackers have been abusing a popular antivirus solution to crack corporate networks for five years // Future US, Inc. (https://www.itpro.com/security/hackers-have-been-abusing-a-popular-antivirus-solution-to-crack-corporate-networks-for-five-years?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 25.04.2024).***

***

Програми-вимагачі

«У липні 2023 року найбільший порт Японії, Нагоя, став жертвою атаки програмного забезпечення-вимагача lockbit, що призвело до зупинки операцій, а Toyota призупинила свої пакувальні лінії для імпорту та експорту. Це був лише один із багатьох нещодавніх інцидентів у великій системі морського транспорту, який демонструє, наскільки цей сектор вразливий до таких профілів атак.

21 лютого адміністрація Байдена випустила розпорядження, розроблене для вирішення довгострокових проблем, необхідних для покращення кібербезпеки національних портів, кораблів, морського промислового ланцюга постачання та систем даних, які працюють у них. Хоча це позитивний крок для частини критичної інфраструктури США, яку часто ігнорують, цього недостатньо і він недостатньо швидкий. Подолання загроз кібербезпеці для морського сектору вимагає не тільки стандартів і довгострокових інвестицій у промислову базу. На додаток до

поточного наказу інші кроки, які адміністрація повинна вжити, включають надання береговій охороні США більше коштів для ефективного реагування на інциденти, створення єдиного ресурсу звітності про морські кібератаки та інвестиції в існуючі організації з обміну інформацією.

Кіберуразливості в портах і на кораблях

Ні для кого не секрет, що порти та морське судноплавство є одними з найпопулярніших нових цілей для кібератак. Система морського транспорту є дуже прибутковою для злочинних програм-вимагачів. Згідно зі звітом CyberOwl, кількість атак зросла на 350 відсотків порівняно з 2022 роком, а середня ціна викупу становить трохи більше 3,2 мільйона доларів. Ще гірше те, що тривають викриття щодо VoltTyphoon, китайської державної групи, яка проникла в критичну інфраструктуру США та союзників. Операційні системи даних суден, навігаційні системи та навіть технології, які керують самими портами, мають вразливі місця в системі кібербезпеки. У цих прогалинах зловмисники, включаючи злочинців і противників держави, продовжують діяти з дуже незначним опором.

Серед занепокоєння громадськості та Конгресу новий указ адміністрації Байдена передбачає дві фундаментальні зміни. По-перше, він усуває таємничу прогалину в правоохоронних органах берегової охорони. По-друге, він виділяє 20 мільярдів доларів на відновлення національного промислового виробництва контейнерних кранів — фізичних машин, які піднімають контейнери на кораблі та з них. Крани «судно-берег» не є, як може здатися, просто тупими шматками металу та кабелю — вони комп’ютеризовані. І, як і з усіма комп’ютерами та датчиками, можливість шпигувати та втручатися, не виходячи з офісу в Пекіні, є кошмаром Ради національної безпеки. Інвестиції в промислову базу є спробою гарантувати, що Сполучені Штати не будуть залежати виключно від китайських кранів, побудованих Shanghai Zhenhua Heavy Industries Company.

Органи берегової охорони

Указ Байдена є хорошим першим кроком — його просто недостатньо і недостатньо швидко, факт, який, як ми підозрюємо, вже відомий його авторам. Тим не менш, у розпорядженні вдалося усунути прогалину в повноваженнях берегової

охорони. Берегова охорона США є унікальною організацією з дуже «унікальними можливостями». Коли аналітики говорять про «унікальні» повноваження, вони насправді мають на увазі масштаби та посилення двох давніх наборів органів безпеки на морі.

Закон про шпигунство 1917 року надає Береговій охороні повноваження над кораблями у водах США для захисту від актів заколоту, оскільки вантажі, такі як боєприпаси, завантажувалися та розвантажувалися під пильним наглядом капітана порту. Згодом Закон Магнусона 1950 року розширив повноваження, включивши повноваження здійснювати посадку на борт і контролювати судна в територіальних водах США. Обидва ці акти були написані задовго до існування Інтернету або занепокоєння кібербезпекою. З розширенням і впровадженням Інтернету обов'язки берегової охорони, як і всіх інших правоохоронних органів, значно зросли в сфері кібербезпеки. У пристосуванні повноважень берегової охорони до включення кіберінцидентів виконавчий наказ є невеликою зміною з великим впливом.

Тепер берегова охорона має повноваження безпосередньо боротися з кіберінцидентами або потенційними кіберзагрозами, що ховаються в системі морського транспорту. Це агентство з найкращими можливостями для цього в галузі, в якій від комерційних компаній очікується захист лише власних систем. Інші федеральні агентства та центри досліджень і розробок, які фінансуються з федерального бюджету, які вивчали ризики кібербезпеки в морській транспортній системі, включно з іншими компонентами Департаменту внутрішньої безпеки, дійшли висновку, що Берегова охорона має найкращу визначену Конгресом пісочницю для підтримки кібербезпеки на морі. зацікавлені сторони транспортної системи. Цей виконавчий наказ підтверджує це, але, що важливіше, він дає Береговій охороні платформу для володіння ареною. Якщо вони забезпечені достатніми ресурсами, вони матимуть хороші позиції, щоб нести відповідальність за — а не лише відповідальність — за підвищення рівня кібербезпеки морських інтересів США.

Але ось проблема: влада без спроможності не є владою. Хоча виконавчий наказ надає Береговій охороні повноваження контролювати судна, які вважаються

кіберзагрозою, принципово незрозуміло, як це має статися з уже перевантаженою силою та гострою конкуренцією за компетентних працівників, які залишаться й розвиватимуться разом із ними. організація.

Особливо це стосується кіберсил берегової охорони. Просте надання повноважень чарівним чином не змусить компанії відкрити двері для примусового виконання. берегової охорони Групи кіберзахисту, на відміну від своїх колег з Міністерства оборони, спільно покладаються на індустрію, яка запрошує їх до співпраці в галузевій інфраструктурі. Берегова охорона не має ані спроможності, ані бажання намагатися втручатися. Крім того, встановлюючи обов'язкове звітування промисловістю, виконавчий наказ передбачає, що малі та середні зацікавлені сторони та оператори суден розуміють, як повідомляти про кіберінцидент, і мають засоби розпізнати, що вони стикаються з інцидентом. Це ризиковане припущення, оскільки галузеві вимоги дуже різняться. Це буде складною перешкодою для берегової охорони.

Берегова охорона досягла значного прогресу в оснащенні та зміцненні своїх обмежених сил кваліфікованих кібероператорів і досягла феноменальних успіхів під нинішнім керівництвом у визначенні можливостей, які можна перепрофілювати, створити або перекваліфікувати для адаптації до нових вимог кібербезпеки. Однак поки що достатнього фінансування, схоже, не надійшло. Берегова охорона не отримала додаткового фінансування для виконання цих або будь-яких інших додаткових обов'язків, незважаючи на свої запити. Натомість береговій охороні довелося розпочати реорганізацію, спрямовану на вирішення 10-відсоткової нестачі робочої сили, поставивши кілька своїх кораблів у стоянку. Недостатньо тіл означає менше кораблів для примусу.

Без чіткого шляху до збільшення фінансування та деяких інноваційних коригувань найму та утримання персоналу, вимога виконавчого наказу просто збільшує навантаження на Берегову охорону. Результатом є те, що жінки та чоловіки, відповідальні за продовження спроб скріпити безпеку морської транспортної системи, відчайдушно прагнуть перебалансувати пріоритети. Очікується, що товари вартістю 5,4 трильйона доларів, які пересуваються

морською транспортною системою та живлять економіку США, будуть забезпечені працівниками правоохоронних органів, фінансування яких становить менше ніж чверть 1 відсотка від цієї суми. Застосування, не кажучи вже про кібербезпеку, неможливо — або, принаймні, не добре і ненадовго.

Інвестиції в промислову базу: від спадщини до автономії

Корисно також те, що указ закликає до довгострокових інвестицій для забезпечення безпеки портової інфраструктури. Однак вузькі інвестиції в промислову базу для вирішення проблеми «кранів» не вирішать проблем кібербезпеки, характерних для системи морського транспорту. Подумайте про масштабність проблеми кібербезпеки. Зараз система морського транспорту залежить від застарілих систем, протоколів, обладнання та процесів, які протягом десятиліть накладалися один на одного. Щоб транспортний контейнер дістався від місця відправлення до складу в центральних Сполучених Штатах і до кінцевого пункту призначення, він буде залежати від кількох і часто несумісних комп'ютерних систем. Створення електронного маніфесту та плану розміщення в порту відправлення, митне очищення та перевірка перед прибуттям до Сполучених Штатів, а також бронювання та розміщення контейнера перед завантаженням – усе це передбачає окремі системи, які майже не сумісні. Навіть система управління вантажем і навігаційні системи на борту океанських суден управляються по-різному. Кожна діяльність покладається на окрему систему даних, якою керує незалежна компанія в рамках глобального ланцюжка поставок, щоб перейти до наступного кроку. Ці мережі та процеси часто є сумішшю традиційних бізнес-інформаційних технологічних систем із оперативними технологічними механізмами.

Окрім цих систем, глобальна система автоматичної ідентифікації кораблів — ключовий засіб навігації — виявилася вразливою до підробки та збою з боку дослідників безпеки та зловмисників. І, нарешті, майже кожна частина морської транспортної системи рухається до інтеграції з автономними та автоматизованими операціями, що залежать від складних систем керування, розроблених (і реалізованих) через різноманітну та глобальну екосистему виробників та об'єктів,

включаючи Європу, Сполучені Штати, Австралію та Китай. Складність цього глобального комплексу компаній і ланцюгів постачання відображена майже в кожному портовому комплексі Сполучених Штатів, переплетеному з внутрішньою американською системою морського транспорту. Навіть компанії, які, здавалося б, управляються США, є багатонаціональними. Кілька найбільших судноплавних компаній під прапором США насправді є американськими дочірніми компаніями більших іноземних судноплавних гігантів.

Це означає, що зосередженість на кранах китайського виробництва, таких як крани Shanghai Zhenhua Heavy Industries Company, є лише частиною глобалізованої — і вразливої — критичної інфраструктури США. Аналітики морської кібербезпеки також відзначають, що це лише питання часу, коли автоматизовані контейнерні та залізничні операції, а згодом і автономні судна без екіпажу або частково екіпажу стануть мішенню для хакерських дій як приватних, так і державних. на українські системи, а Атака NotPetya нещодавно злом Viasat наочно продемонстрували, що система морського транспорту взаємозалежна з багатьма іншими критично важливими інфраструктурами — залізничною, енергетичною, водною тощо. Оскільки ці інформаційні системи є взаємозалежними, кіберініційованими події можуть спричинити оперативний вплив в інших секторах критичної інфраструктури.

Право бум інвестицій

Якщо загроза існує зараз, тоді Вашингтон має інвестувати у її вирішення. Однією з перших областей уваги має бути підвищення здатності реагувати відразу після нападу — праворуч від стріли, а не ліворуч від неї. Додаткові короткострокові інвестиції, які можуть підвищити здатність реагування, можуть принаймні закрити критичні вразливості, поки ми чекаємо довгострокових рішень.

Зрештою, це ризик, чи зростання внутрішньої виробничої потужності для інфраструктури, як крани, фундаментально зменшить вразливість Америки до кібербезпеки. Мало того, що базові промислові рішення стають ефективними, потрібні роки, але просто розміщення ланцюжка поставок на суші не робить його захищеним від кібератак. Вважайте, що індустрія кібербезпеки операційних

технологій наголошує як на загрозах, так і на вразливості — частково це пов’язано з невід’ємною структурою пріоритетів системи. Вони розроблені з урахуванням перш за все надійності — і, як наслідок, вони, швидше за все, мають недоліки прямо з коробки з точки зору безпеки системи.

Крім того, такі критичні інфраструктури, як морська область, є середовищами «з низьким рівнем зрілості кібербезпеки». У середовищі з низьким рівнем зрілості найшвидші та найефективніші результати досягаються завдяки покращенню середнього часу до відновлення — після нападу. Таким чином, першим правильним кроком є звернення до найнижчих плодів і інвестування в реагування на інциденти та пов’язані з ними заходи з відновлення.

Ми приймаємо та вітаємо те, що додаткове «Повідомлення про запропоновану нормотворчість» берегової охорони зосереджено на каталогізації ризиків і впровадженні базових стандартів. Це, звичайно, частина рівняння. Але зрілість кібербезпеки системи морського транспорту вже є дуже неоднаковою, і, як наслідок, пройде багато часу, доки можливості запобігання стануть можливими однаково в усій системі.

Ми рекомендуємо уряду США негайно зробити акцент на низьких результатах для більшості зацікавлених сторін порту, додавши додаткове фінансування зусиллям, які зараз здійснюються. берегової охорони Групи кіберзахисту мають унікальну можливість, за наявності відповідних ресурсів, співпрацювати з галуззю, щоб перевірити плани реагування на інциденти під час спільно розроблених настільних навчань або навіть виконувати власні оперативні кіберзаходи для виявлення слабких місць.

По-друге, просте нарощування потенціалу, щоб допомогти зацікавленим сторонам системи морського транспорту повідомляти про атаки, також, швидше за все, принесе швидкі результати. Це може здатися дивно простим, але порти історично не мали дуже чіткої ідентифікації або «єдиного скла», через який можна було дізнаватися про інциденти кібербезпеки та передавати їх. Берегова охорона має механізми для забезпечення оперативної підтримки реагування на інциденти, але незрозуміло, як різні федеральні гравці в просторі будуть інтегруватися з ними.

Прийняття Закону про звітність про кібер-інциденти для критичної інфраструктури Департаменту внутрішньої безпеки з питань кібербезпеки та безпеки інфраструктури може усунути деякі з цих проблемних моментів, але двозначність залишається невирішеною. Саме тому, хто зацікавлені сторони галузі наберуть номер у свій найгірший день, може стати удачею. Хтось може зателефонувати на свою гарячу лінію InfraGard, хтось може зателефонувати до постачальника технологій, як-от Dragos, а хтось може зателефонувати до відповідної федеральної адміністрації безпеки (наприклад, Адміністрації з безпеки трубопроводів і небезпечних матеріалів). Звітування дуже мало сприяє створенню ефективної скоординованої відповіді, якщо його не можна ефективно сортувати. Цей виконавчий наказ має потенціал для активізації зусиль багатьох агенцій в єдину оперативну структуру. Але знову ж таки, берегова охорона потребує відповідних ресурсів, щоб це сталося.

Звичайно, з часом промисловість неминуче візьме лідерство, але шлях буде болісним. Проблема галузевого підходу до портових споруд і активів на плаву полягає в самих галузях. Немає єдиних заходів зі зменшення ризику, які б відповідали різноманіттю потреб кожного представленого. Експедитори, порти, круїзні лінії, вантажні перевезення — усім цим зацікавленим сторонам потрібна низка різних рішень.

Нарешті, це істина, що обмін інформацією є основною вимогою кібербезпеки. І все ж ріст і розвиток такої спільноти для морської транспортної системи залишається лише зародковим у порівнянні з іншими центрами та організаціями обміну інформацією та аналізу.

команда непохитних волонтерів (включно з авторами цієї статті), які називають себе «MarSec@ICSVillage зібралася Протягом останніх кількох років на DefCon (однієї з найбільших і найстаріших хакерських конференцій у світі)», щоб стукати по барабану та розвиватися. ця спільнота інтересів. Ми беззаперечно продовжуватимемо це робити, щоб розвивати таланти та пропонувати рішення тим, хто буде слухати. Ми робимо це без прибутку для себе — ми віддана спільнота, яка любить виклик.

Таким чином, якщо фінансування федеральних грантів або підтримка приватного сектору має бути кудись застосовано, це має бути для стимулювання тих видів обміну на низовому рівні та мереж, які створюють ці спільноти. Центр обміну та аналізу інформації про систему морського транспорту та незліченна кількість зацікавлених спільнот волонтерів значно перевищують свою вагу у пошуку рішень і впровадженні найкращих практик. Це пояснюється тим, що за своєю природою вони поєднують представництво як федеральних, так і галузевих зацікавлених сторін. Асоціації для обміну інформацією – це недорогий і водночас недостатньо фінансований спосіб обміну найкращими практиками, обговорення стратегій зменшення ризиків і, зрештою, розвитку м'язів співпраці, призначених для роботи в разі виникнення інцидентів.

Система морського транспорту, як і вся критична інфраструктура, є вразливою. Довгострокові виправлення важливі, але Вашингтон повинен зробити більше прямо зараз». ***(Nina Kollars, Blake Benson, Austin Reid. The Rising Ransomware Tide, Chinese Spy Cranes, and the Biden Executive Order on Maritime Cyber Security // METAMORPHIC MEDIA (https://warontherocks.com/2024/04/the-rising-ransomware-tide-chinese-spy-cranes-and-the-biden-executive-order-on-maritime-cyber-security/?singlepage=1). 17.04.2024).***

***

«Якщо ваша організація отримала запит на програму-вимагач, CL0P може бути знайомим ім'ям. У 2023 році CL0P була третьою найбільш плідною групою програм-вимагачів після Lockbit і ALPHV.

Пов'язана з Росією кіберзлочинна організація CL0P стала однією з найуспішніших організацій з програм-вимагачів у світі. Використовуючи модель Ransomware-as-a-Service (RaaS), філії CL0P можуть сплачувати депозит і використовувати програми-вимагачі CL0P для злому організацій і викрадення даних, які потім зберігаються як викуп за багатомільйонні платежі. Якщо жертви не сплачують затребувані викупи, то викрадені дані публікуються на сайті «CL0P^_-LEAKS».

З 2019 року CL0P використовує тактику «подвійного вимагання»: краде дані та погрожує їх витоком. Інші банди програм-вимагачів також займаються «потрійним вимаганням». Цей додатковий крок передбачає загрози участі в атаках розподіленої відмови в обслуговуванні (DDoS), які вимикають системи та роблять їх непрацездатними, тим самим посилюючи тиск на жертв, щоб вони виконували вимоги зловмисників.

Зараз CL0P почав використовувати методи «чотирьохкратного вимагання». На додаток до вищезазначеного, якщо жертви не дотримуються вимог, CL0P надсилатиме повідомлення для переслідування клієнтів, ділових партнерів, співробітників, ЗМІ та керівників високого рівня, щоб повідомити їх про те, що організацію було зламано. Ці методи призвели до зростання середніх платежів за програми-вимагачі.

Націлившись на деякі з найбільших організацій світу, банда програм-вимагачів CL0P зосередилася на фінансовій, виробничій галузях і галузях охорони здоров'я. У травні минулого року CL0P став відомим завдяки використанню вразливостей у керованому рішенні для передачі файлів MOVEit, отриманню конфіденційних даних з урядових установ США, шкіл, закладів охорони здоров'я та великих фірм. нульового дня Раніше у 2023 році група програм-вимагачів CL0P використала подібну вразливість в платформі керованої передачі файлів Fortra GoAnywhere і надіслала повідомлення про викуп керівникам компанії.

CISA та ФБР рекомендують наступні заходи кібербезпеки для пом'якшення кіберзагроз CL0P:

Інвентаризація активів і даних для ідентифікації авторизованих і неавторизованих пристроїв і програмного забезпечення.

Надавайте адміністративні привілеї та доступ лише за необхідності та запускайте лише законні програми.

Відстежуйте мережу та активуйте конфігурації безпеки на пристроях мережевої інфраструктури.

Регулярно виправляйте та оновлюйте програмне забезпечення та програми.

Проводьте регулярні оцінки вразливості». ***(CL0P ransomware gang is on the rise // Hogan Lovells (https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9VaqAAqGCsqQRxl7eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF3dzoxprWhI6w%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true). 19.04.2024).***

***

«Хвиля дешевого, грубого, аматорського програмного забезпечення-вимагача була помічена в дарк-мережі – і хоча воно може не потрапити в стільки заголовків, як LockBit, Rhysida та BlackSuit, воно все ще становить серйозну загрозу для організацій.

Що таке програма-вимагач «сміттєва зброя»?

Це назва, придумана дослідниками Sophos для простих програм-вимагачів, які часто продаються дешево як одноразова покупка. Програми-вимагачі типу Junk gun привабливі для злочинців, які хочуть діяти самостійно, але не мають технічних навичок.

Чи можете ви навести кілька прикладів?

звичайно Програмне забезпечення-вимагач Kryptina було виставлено на продаж у грудні 2023 року всього за 20 доларів США (800 доларів, якщо вас цікавив вихідний код, щоб, можливо, налаштувати його або створити нові варіанти). Kryptina пообіцяла повний готовий набір інструментів для здійснення атак.

Інші приклади програм-вимагачів «сміттєвої зброї» включають Diablo, Evil Extractor, Yasmha, HardShield, Jigsaw, LoliCrypt і CatLogs.

Дослідники Sophos відзначають, що розробник Kryptina намагався зробити будь-які продажі, а пізніше випустив програму-вимагач безкоштовно.

Ха! Вони навіть не могли продати його за 20 доларів!

Якось соромно, чи не так? Деякі інші приклади саморобних програм-вимагачів для продажу також пропонуються за низькою ціною – 50 або 60 доларів США.

Однак середня ціна, зафіксована в дослідженні Sophos , становила близько 375 доларів США — значно менше, ніж тисячі доларів, які готові заплатити деякі філії «звичайних» операцій із програмами-вимагачами як послуга (RaaS).

Звучить погано, якщо роздобути програми-вимагачі дешево

Правильно. Низький вхідний бар'єр означає потенційно більше зловмисників-вимагачів.

Крім того, правоохоронним органам потенційно важче відстежити кіберзлочинців, які уникають шляху, щоб стати афілійованими особами для більш широких операцій з програмами-вимагачами, через брак доступних розвідувальних даних.

Але чи ця програма-вимагач «сміттєва зброя» все ще є потужною, якщо вона низькотехнологічна?

Не обманюйте себе. Можливості цього типу програм-вимагачів можуть відрізнятися, і найбільшими перевагами є їх простота (потрібна незначна допоміжна інфраструктура або зовсім не потрібна) і той факт, що користувачі залишають собі весь прибуток.

Атаки програм-вимагачів із використанням «сміттєвої зброї» можуть не мати такого масштабу та популярності, як у великих груп програм-вимагачів, але все одно можуть бути дуже прибутковими для тих, хто націлений на окремих осіб і малий бізнес.

«Що більше занепокоєння, так це те, що ця нова загроза програм-вимагачів створює унікальний виклик для захисників», — сказав Крістофер Бадд з Sophos. «Оскільки зловмисники використовують ці варіанти проти малого та середнього бізнесу, а вимоги щодо викупу є невеликими, більшість атак, ймовірно, залишаться непоміченими та про них не повідомлятимуть. Це залишає прогалину в розвідувальних даних для захисників, яку доведеться заповнити спільноті безпеки». ***(Graham Cluley. "Junk gun" ransomware: the cheap new threat to small businesses //***

Fortra, LLC (https://www.tripwire.com/state-of-security/junk-gun-ransomware-cheap-new-threat-small-businesses?utm_source=flipboard&utm_content=HamsterBoomer%2Fmagazine%2FMALWARE+-+RANSOMWARE-PHISHING). 25.04.2024).

***

Фішингові атаки

«Visa попереджає своїх партнерів і клієнтів про триваючу фішингову атаку, метою якої є розповсюдження банківського трояна.

Підрозділ Visa Payment Fraud Disruption (PDF) надіслав попередження безпеки емітентам карток, процесорам і еквайрам, зазначивши, що спостерігав нову фішингову кампанію, яка почалася наприкінці березня цього року.

Кампанія націлена переважно на фінансові установи в Південній та Південно-Східній Азії, на Близькому Сході та в Африці, і спрямована на відмову від нової версії банківського трояна під назвою JsOutProx. «Хоча PFD не зміг підтвердити кінцеву мету нещодавно виявленої кампанії зловмисного програмного забезпечення, ця група eCrime могла раніше націлюватися на фінансові установи для здійснення шахрайської діяльності».

На жаль, ми не знаємо імені загрози, яка стоїть за цією кампанією, або кількості компаній, які стали жертвами. Дослідники припускають, виходячи зі складності атак, профілю жертв і їхнього географічного розташування, що нападники, швидше за все, знаходяться в Китаї або принаймні пов’язані з Китаєм.

Ми також знаємо, що JsOutProx — це троян віддаленого доступу, який вперше був помічений наприкінці 2019 року, і описується як «дуже заплутаний» бекдор JavaScript, який дозволяє користувачам запускати команди оболонки, завантажувати додаткове шкідливе програмне забезпечення, запускати файли, робити знімки екрана, контролювати різні периферійні пристрої та встановити стійкість на цільовій кінцевій точці. Мабуть, він розміщений у сховищі GitLab.

У фішингових електронних листах зловмисники видають себе за законні установи, показуючи жертвам підроблені сповіщення про платежі SWIFT і MoneyGram.

Фішинг залишається одним із найприбутковіших способів розгортання шкідливих програм. Це дешево і легко масштабується, а тепер за допомогою генеративного штучного інтелекту його відносно важко помітити. IT-командам рекомендовано навчити своїх співробітників виявляти фішингові атаки, а також встановити програмне забезпечення для захисту електронної пошти, брандмауери та антивірусні засоби». ***(Sead Fadilpašić. Visa warns dangerous new malware is attacking financial firms // Future US, Inc. (https://www.techradar.com/pro/security/visa-warns-dangerous-new-malware-is-attacking-financial-firms?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 05.04.2024).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Дослідник загроз розкрив нову довільну ін’єкцію команди та жорстко закодований бекдор у багатьох моделях пристроїв D-Link Network Attached Storage (NAS), що вийшли з експлуатації.

Дослідник, який виявив недолік, Netsecfish, пояснює, що проблема знаходиться в сценарії '/cgi-bin/nas_sharing.cgi', впливаючи на його компонент HTTP GET Request Handler.

Дві основні проблеми, які сприяють виникненню недоліку, відстежуваного як CVE-2024-3273, — це бекдор, створений через жорстко закодований обліковий

запис (ім’я користувача: «messagebus» і порожній пароль), і проблема введення команди через параметр «system».

При об’єднанні будь-який зловмисник може віддалено виконувати команди на пристрої.

Помилка ін’єкції команди виникає через додавання команди в кодуванні base64 до параметра «система» через запит HTTP GET, який потім виконується.

«Успішне використання цієї вразливості може дозволити зловмиснику виконувати довільні команди в системі, потенційно призводячи до несанкціонованого доступу до конфіденційної інформації, зміни конфігурацій системи або умов відмови в обслуговуванні», — попереджає дослідник.

CVE-2024-3273 впливає на такі моделі пристроїв:

DNS-320L Версія 1.11, Версія 1.03.0904.2013, Версія 1.01.0702.2013

DNS-325 Версія 1.01

DNS-327L Версія 1.09, Версія 1.00.0409.2013

DNS-340L Версія 1.08

Netsecfish каже, що сканування мережі показує, що понад 92 000 вразливих пристроїв D-Link NAS доступні в Інтернеті та піддаються атакам через ці недоліки.

Зв’язавшись з D-Link щодо недоліку та щодо того, чи буде випущено виправлення, постачальник повідомив нам, що термін служби цих пристроїв NAS закінчився (EOL) і вони більше не підтримуються.

«Усі мережеві сховища D-Link закінчилися протягом багатьох років [і] ресурси, пов’язані з цими продуктами, припинили свою розробку та більше не підтримуються», — заявив речник.

«D-Link рекомендує припинити використання цих продуктів і замінити їх продуктами, які отримують оновлення прошивки».

Представник також повідомив BleepingComputer, що постраждалі пристрої не мають можливостей автоматичного онлайн-оновлення або функцій охоплення клієнтів для доставки сповіщень, як поточні моделі.

Таким чином, постачальник обмежився бюлетенем безпеки, опублікованим учора, щоб підвищити обізнаність про недолік і необхідність негайного зняття з експлуатації або заміни цих пристроїв.

Компанія D-Link створила спеціальну сторінку підтримки для застарілих пристроїв, де власники можуть переглядати архіви, щоб знайти останні оновлення безпеки та мікропрограми.

Тим, хто наполягає на використанні застарілого апаратного забезпечення, слід принаймні застосувати останні доступні оновлення, навіть якщо вони не вирішуватимуть нещодавно виявлені проблеми, такі як CVE-2024-3273.

Крім того, пристрої NAS ніколи не повинні підключатися до Інтернету, оскільки вони зазвичай призначені для крадіжки даних або шифрування під час атак програм-вимагачів». ***(Bill Toulas. Over 92,000 exposed D-Link NAS devices have a backdoor account // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/over-92-000-exposed-d-link-nas-devices-have-a-backdoor-account/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FALAN+NISHIHARA). 06.04.2024).***

***

«Дві уразливості нульового дня в продуктах Ivanti, які були розкриті в січні (і виправлені тижнями пізніше), виявилися джерелом зламу MITRE, дослідницького центру кібербезпеки, який фінансується урядом США і підтримує широко використовувану базу даних ATT&CK. Цілком можливо, що за атакою стоять хакери національної держави Китаю, враховуючи схожість у використанні цих же вразливостей в інших інцидентах, але це поки що не підтверджено.

Одна мережа досліджень і розробок MITRE проникла, можливо, винні хакери національної держави

Ivanti – це фірма з кібербезпеки зі штату Юта, яка спеціалізується на корпоративних продуктах VPN. Зловмисники MITER використали дві вразливості

нульового дня в пристроях Connect Secure VPN компанії, які були оприлюднені на початку січня: CVE-2023-46805 і CVE-2024-21887. Ці уразливості використовувалися зловмисниками принаймні тиждень до публічного оприлюднення, що спричинило раннє повідомлення; Іванті знадобилося близько трьох тижнів, тобто до початку лютого, щоб випустити патчі.

MITER повідомляє, що зловмисники проникли в одну з дослідницько-розробних мереж мережевого середовища експериментів, досліджень і віртуалізації (NERVE) після проведення розвідки та виявлення вразливостей нульового дня. Потім зловмисники змогли перемістити в середовище VMware, захопити принаймні один обліковий запис адміністратора, встановити веб-оболонки та бекдори для постійного доступу та викрасти дані.

MITER також підтвердив, що вони вважають, що за атакою стоять хакери національної держави, але вони не назвали національність. Сторонні дослідницькі фірми безпеки, включаючи Mandiant, помітили, що за останні місяці велика кількість китайських хакерів, що працюють на національних державах, використовують ці вразливості Ivanti у своїх різноманітних експлойтах. Ці хакери також використовували дуже схожі дії після зламу в процесі бічного руху.

MITRE заявив, що хакери не мали доступу до їхньої корпоративної мережі та партнерських систем. Каллі Ґюнтер, старший менеджер відділу дослідження кіберзагроз у Critical Start, розповідає про ймовірні наслідки інциденту: «Осяг зламу обмежений NERVE без впливу на основну корпоративну мережу MITRE або системи партнерів, що свідчить про те, що збиток локалізовано. Однак витонченість і характер атаки підкреслюють постійні ризики, з якими стикаються організації, що займаються національною безпекою та передовими технологічними дослідженнями. Цей інцидент, ймовірно, призведе до переоцінки заходів безпеки, зокрема щодо того, наскільки захищені конфіденційні несекретні мережі. Відповідь MITRE, включаючи стримування, відновлення та судово-медичний аналіз, матиме вирішальне значення для зменшення безпосередніх ризиків і запобігання майбутнім інцидентам. Більш широке співтовариство безпеки буде зацікавлене в

тому, щоб пізнати досвід MITRE, щоб зрозуміти методологію суб'єктів загрози та покращити свої власні оборонні стратегії».

Уразливості нульового дня залишаються непотрібними ще довго після випуску виправлень

Виправлення невиконаних завдань продовжує залишатися серйозною проблемою для організацій, оскільки вразливості нульового дня, які можна виправити, які відомі громадськості, часто залишаються місяцями просто через інерцію або опускаються занадто низько в списку пріоритетів для напружених IT-відділів. Інцидент у MITRE може бути одним із таких випадків, оскільки, як повідомляється, зловмисники проникли в компанію в січні незабаром після того, як уразливості були вперше виявлені, але вторгнення було виявлено лише в березні. Він також відповідає розгулу китайських державних хакерів незабаром після першої появи вразливості Ivanti.

Атака MITER вважається відносно незначною, оскільки мережа досліджень і розробок, яку було зламано, не є секретною, але далеко не чутно, щоб оцінки збитку від порушення переглядалися через кілька тижнів або місяців. Шум, пов'язаний з хакерами китайської національної держави, дав деяку потенційно більш шкідливу інформацію, використовуючи ці конкретні вразливості нульового дня Ivanti, можливо, найбільш помітну атаку на Агентство кібербезпеки та безпеки інфраструктури (CISA), яка скомпрометувала «CISA Gateway». використовується для координації безпеки критичної інфраструктури та інструмент, який зберігає інформацію про плани безпеки хімічних заводів.

Сам MITER не був зламаний протягом 15 років, але Ivanti потрапив у новини у 2021 році через злом його служби Pulse Connect Secure. Це порушення також було пов'язане з хакерами китайської національної держави. Mandiant вважає, що конкретні хакери з національних держав, які стоять за нещодавньою серією зломів Ivanti, — це UNC5221, відносно нова група, яку іноді називають «Red Dev 61». Схоже, що група зосереджена на міжнародних цілях, які, як відомо, становлять інтерес для китайської розвідки, і здебільшого націлювалася на приватний сектор під час свого розгулу компрометації близько 2100 невиправлених пристроїв Ivanti

по всьому світу. Схоже, що група стежить за можливостями більше, ніж за конкретним вибором цілей, переслідуючи все, від малого бізнесу до компаній зі списку Fortune 500. Mandiant каже, що інші китайські хакери національних держав, ймовірно, також використовували вади Ivanti з початку року.

Рік розпочався дослідженням відділу безпеки Microsoft, яке виявило, що близько 80% зломів стосуються невиправлених уразливостей програмного забезпечення, для яких на той час був доступний патч. Відтоді стан виправлення та оновлень програмного забезпечення суттєво не покращився. Основні причини затримок у виправленні відомих уразливостей нульового дня залишаються тими самими: проста нестача робочої сили, щоб не відставати від ручних дій, страх зламати мережеві програми та необхідність чекати постачальників, які самі напружені та відстають серед провідних факторів. Нещодавнє дослідження Help Net Security показало, що більшість організацій, як правило, затримують необхідні виправлення приблизно на два місяці, а галузеві галузі з найгіршою ефективністю в середньому відстають на чотири місяці.

Кен Данем, директор відділу дослідження загроз Qualys Threat Research Unit, зазначає, що поява штучного інтелекту наразі не надає переваги захисникам з точки зору усунення вразливостей нульового дня: «Змагання за виправленням вразливостей і зниженням ризиків є реальними у світі. де вороги підстерігають, щоб атакувати за нагоди. У 2024 році компанії повинні застосовувати належну обачність на кожному етапі всього життєвого циклу життєвого циклу керування загрозами та вразливістю (TVM), маючи можливість швидко визначати пріоритетність виправлень, обхідних шляхів та інших форм виправлення, якщо це виправдано ескалацією загроз. Потреба в потужних програмах розвідки про кібернетичні загрози (CTI) для проактивного зниження ризиків, швидкого виявлення та якнайшвидшого усунення загроз у війні проти кібернетичних загроз ще ніколи не була такою. Досконалість у SecOps включає зниження впливу інциденту шляхом забезпечення внутрішнього контролю для швидкого виявлення та видалення загроз, а також зменшення радіусу вибуху під час атаки».

Даррен Гуччіоне, генеральний директор і співзасновник Keeper Security, пропонує платформу PAM як негайний крок для організацій, які борються з проблемами виправлення: «Платформа керування привілейованим доступом (PAM) допомагає організаціям керувати та захищати привілейовані облікові дані, а також забезпечити найменш привілейований доступ. PAM працює, ретельно відстежуючи доступ і активність у привілейованих облікових записах. Якщо кіберзлочинцю вдається отримати доступ до мереж організації, платформи PAM можуть мінімізувати радіус вибуху, запобігаючи бічному руху. Компанії також повинні мати моніторинг подій безпеки. Прийнявши структуру нульової довіри у своїй інфраструктурі, керівники підприємств матимуть сильніші позиції, щоб не лише виявляти та реагувати на атаки на свою організацію, але й зменшувати будь-який потенційний збиток». ***(Scott Ikeda. Nation-State Hackers Leverage Zero-Day Vulnerabilities to Penetrate MITRE Cybersecurity Research Network // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/nation-state-hackers-leverage-zero-day-vulnerabilities-to-penetrate-mitre-cybersecurity-research-network/). 25.04.2024).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«RETN, провідний незалежний глобальний постачальник мережевих послуг, оголошує про запуск своєї нової платформи пом'якшення DDoS-атак, розробленої для поєднання найсучаснішої кібербезпеки із захистом на рівні мережі та підвищення потужності очищення для клієнтів на 5000%.

Платформа RETN забезпечує прямий контроль трафіку, покращену видимість, а також великий масштаб і охоплення для захисту від атак розподіленої відмови в обслуговуванні (DDoS) у розгалуженій мережі протяжністю 135 000 кілометрів від Європи до Азії. Завдяки здатності впроваджувати ефективні та негайні заходи пом'якшення безпосередньо на рівні мережі, RETN має унікальну

позицію, щоб допомогти компаніям зупинити атаки ближче до їх джерела, забезпечуючи спокій і безперервність обслуговування навіть за умов атаки.

Тоні О'Салліван, генеральний директор RETN, сказав: «Перед обличчям дедалі складніших кіберзагроз, нова платформа RETN для пом’якшення DDoS є значним кроком вперед у забезпеченні безпеки магістралі Інтернету та забезпечення цифрової безпеки компаній у всьому світі. Пом’якшення DDoS-атак зараз є важливим, і його слід очікувати всім підприємствам і критично важливим мережам, яким потрібен захист у режимі реального часу. Ми раді представити рішення, яке чудово виявляє атаки, сповіщає користувачів і швидко реагує на них».

Платформа RETN DDoS забезпечує:

Автоматизоване та інтелектуальне пом’якшення: використання машинного навчання та штучного інтелекту для автоматичного виявлення та пом’якшення загроз, гарантуючи блокування зловмисних спроб до того, як вони досягнуть мережі або онлайн-додатків.

Значно збільшена потужність очищення в кількох центрах, стратегічно розгорнутих у Глобальній мережі RETN

Цілодобовий оперативний центр безпеки (SOC)

Портал безпеки клієнтів для внутрішньої видимості та контролю

Автоматизовані сповіщення та звіти в реальному часі

Настроювані профілі для кожного ресурсу мережі/хоста

Клієнти IP-транзиту та виділеного доступу до Інтернету (DIA) отримають переваги від:

Захист від об’ємних атак: платформа RETN відволікає величезний трафік від цільової мережі, відфільтровуючи шкідливі пакети та забезпечуючи плавне проходження законного трафіку. Цей підхід має вирішальне значення для підтримки онлайн-доступності та безперервності обслуговування під час масштабних подій DDoS.

Захист від атак на протокол: Виявлення та пом’якшення підозрілих шаблонів трафіку, що вказують на атаки на протокол, наприклад SYN-флуд або TCP-флуд,

таким чином захищаючи мережеві ресурси від перевантаження зловмисним трафіком.

Захист додатків: Платформа містить хмарний брандмауер корпоративного рівня (WAF), який захищає веб-додатки, API та онлайн-сервіси від безлічі загроз, включаючи, але не обмежуючись, автоматичних ботів, ін'єкційних атак і додатків-рівень відмови в обслуговуванні. Пропонуючи багаторівневий захист L3/4 і L7, RETN забезпечує комплексний захист від атак на загальнодоступні веб-сайти, програми та API, дотримуючись 10 найпоширеніших уразливостей OWASP.

Захист DNS: підтримується повністю резервованою та глобально розподіленою інфраструктурою DNS, яка здатна поглинати широкомасштабні DDoS-атаки на основі DNS, безперешкодно відповідаючи на законні запити користувачів. Він захищає відбиті атаки, атаки посилення та вдосконалені атаки на основі DNS, а також DNS-спуфінг, пошкодження кешу, тунелювання та викрадення, забезпечуючи цілісність і доступність онлайн-сервісів». ***(RETN Announces Increased Scrubbing Capacity for DDoS Mitigation by 5000% as part of New Cyber Security Platform Launch // Media (https://itsecuritywire.com/news/retn-announces-increased-scrubbing-capacity-for-ddos-mitigation-by-5000-as-part-of-new-cyber-security-platform-launch/). 03.04.2024).***

***