**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

## № 11 (листопад)

**Київ – 2023**

**Кібербезпека в інформаційному суспільстві:** Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №11 (листопад) . – 300 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

**«Американська транснаціональна корпорація - технологічний гігант Cisco за підтримки Пентагону поставив НЕК «Укренерго» спецобладнання для протистояння кібератакам.**

Про це представник Cisco повідомив виданню The Register, передає Мілітарний.

Обладнання має впоратися з російськими радіоперешкодами, які впливають на системи GPS. Вони спрямовані на порушення роботи систем наведення ракет та заважають видимості для операторів електромереж України.

Видання пояснює, що оператори покладаються на системи GPS, щоб управляти потоком електроенергії в країні. Порушення в роботі можуть призвести до того, що спеціалісти не зможуть відстежити місце обриву лінії.

«Наша команда поставила собі за мету розробити рішення з використанням нашої власної технології», – сказали в Cisco.

Cisco надіслала Укренерго модифіковані версії своїх мережевих комутаторів після стрес-тестів у лабораторії в США.

За даними CNN, вартість створення та постачання обладнання оцінюється приблизно в 1 млн дол, але Cisco відправила його безплатно.

Пентагон організував рейси для доставлення вантажу в Україну, Міністерство енергетики займалося логістикою, а Міністерство торгівлі організувало зустрічі між американськими технічними експертами та Укренерго». ***(Анастасія Жарикова. Cisco поставила "Укренерго" обладнання для перешкоджання кібератакам на мільйон доларів // Економічна правда (https://www.epravda.com.ua/news/2023/11/24/706962/). 24.11.2023).***

***

***Кібервійна проти України***

**«Хакери, пов'язані з російською військовою розвідкою, наприкінці минулого року проникли та зламали частину електроенергетичної мережі**

**України за допомогою нових складних інструментів злому, йдеться в новому звіті.**

Висновки американської фірми з кібербезпеки Mandiant додають додаткові докази про інструменти, які використовує агенція, відома як ГРУ, для націлювання не лише на Україну, а й на інші місця по всьому світу.

«Ця атака являє собою останню еволюцію можливостей Росії щодо кіберфізичних атак, яка стає все більш помітною після вторгнення Росії в Україну», — йдеться у звіті Mandiant.

Підрозділ ГРУ, відомий як підрозділ 74455, звинувачують у деяких з найруйнівніших кібератак у світі за останнє десятиліття. Широко відомий під прізвиськом «Пісочний черв'як», підрозділ отримав сумну популярність, коли в 2015 році проник в енергомережу України, відключивши від електроенергії понад 200 000 людей.

У 2020 році прокуратура США оголосила про пред'явлення обвинувачення шістьом офіцерам підрозділу 74455 у серії хакерських атак, спрямованих на президентські вибори у Франції, Олімпійські ігри в Пхенчхані 2018 року та міжнародну організацію, яка розслідує використання Росією смертоносної нервово-паралітичної речовини.

Офіцери ГРУ також були звинувачені Сполученими Штатами у зламі американських політичних партій напередодні президентських виборів 2016 року.

У жовтні 2022 року Росія завдала хвилі ракетних і безпілотних ударів по енергомережі України, спричинивши знеструмлення в багатьох частинах країни. Київ намагався локалізувати збитки і був змушений тимчасово залишити без світла чотири області.

У той же час, за словами Mandiant, хакери Sandworm змогли відключити електроенергію в одному невстановленому регіоні України, спрацювавши автоматичні вимикачі на електропідстанції. Потім група використовувала програмне забезпечення, щоб стерти деякі з пов'язаних комп'ютерних серверів, щоб замести сліди.

«За межами України, група продовжує підтримувати шпигунські операції, які є глобальними за масштабом і є ілюстрацією далекосяжних амбіцій та інтересів російської армії в інших регіонах», — сказав Mandiant.

Російські служби розвідки та безпеки здійснюють кібероперації, що збігаються, іноді конкурують. Окрім ГРУ, Службу зовнішньої розвідки звинувачують у хакерських атаках на політичні кампанії США у 2016 році.

Головне відомство внутрішньої безпеки Росії, Федеральна служба безпеки, має два відомі кіберпідрозділи. Перший, «Центр 18» або «Центр інформаційної безпеки», у 2019 році охопив масштабний скандал із державною зрадою.

Інший – Центр 16, офіційно відомий як Центр радіоелектронної розвідки засобами зв'язку, або військова частина 71330, який контролює можливості ФСБ із сигнальної розвідки, включаючи перехоплення комунікацій, дешифрування та обробку даних.

Центр 16 стояв за унікальним фрагментом шкідливого коду, який десятиліттями ховався на комп'ютерних серверах на Заході, здійснюючи таємне стеження за користувачами. У травні органи влади п'яти країн оголосили, що успішно відключили шкідливе програмне забезпечення, відоме як Snake, Uroburos або Venomous Bear.

Російські неурядові організації також причетні до хакерських спроб. У 2018 році Міністерство юстиції США висунуло звинувачення Агентству інтернет-досліджень — так званій «фабрикі тролів», контрольованій покійним Євгеном Пригожиним, на той час близьким довіреним особою президента Володимира Путіна, — яка спеціалізувалась на створенні фейкових акаунтів у соціальних мережах і поширенні дезінформації. і пропаганда.

Департамент також висунув звинувачення самому Пригожину та ще 15 російським особам у ймовірному шахрайстві «з метою втручання в політичні та виборчі процеси США, включаючи президентські вибори 2016 року». ***(Mike Eckel. Hackers Linked To Russian Intelligence Blamed For 2022 Ukraine Grid Disruption // RFE/RL, Inc. (https://www.rferl.org/a/russia-hackers-ukraine-power-grid-gru-attack-2022/32677652.html?utm_source=flipboard&utm_content=other). 09.11.2023).***

***

**«Російська фінансова організація Сбербанк повідомляє в прес-релізі, що два тижні тому вона зіткнулася з найпотужнішою розподіленою атакою на відмову в обслуговуванні (DDoS) в новітній історії.**

Сбербанк є найбільшою державною банківською та фінансовою компанією та найбільшим інститутом у Росії, якому належить близько третини всіх активів у країні.

Після вторгнення Росії в Україну банк зіткнувся з міжнародною блокадою та санкціями та неодноразово ставав мішенню західних хактивістів.

Російське видання Interfax повідомляє, що атака досягла одного мільйона запитів на секунду (RPS), що, за словами організації, приблизно в чотири рази перевищує розмір найпотужнішого DDoS-атак, який Сбербанк зазнав до того часу.

«Ми помітили, що це нові хакери. Їхні відбитки пальців нам невідомі. Тобто на ринку з’явилися нові, дуже кваліфіковані злочинці, які почали планомірно атакувати найбільші російські ресурси», – заявив глава «Сбербанку».

Хоча один мільйон RPS є безперечно значним, це не можна порівняти з рекордними DDoS-атаками, які використовують нову техніку «HTTP/2 Rapid Reset», щоб створити вплив у сто разів більший, ніж той, який зазнав Сберсбанк.

Наприкінці серпня Amazon виявив DDoS-атаку, яка досягла піку в 155 мільйонів RPS. Cloudflare пом'якшив 201 мільйон RPS, тоді як Google впорався з DDoS-атакою, яка досягла піку в 398 мільйонів запитів на секунду.

*Попередні напади*

У травні 2022 року Сбербанк оголосив, що став жертвою безпрецедентних хакерських атак, у тому числі масових хвиль DDoS, спрямованих на його онлайн-сервіси для клієнтів.

Банк заявив, що йому вдалося відбити DDoS-атаку зі швидкістю 450 ГБ/с, яка була згенерована ботнетом із 27 000 скомпрометованих пристроїв.

Недавній удар, який завдала російська фінансова система, стосується Національної системи платіжних карток (NSPK), оператора карток «Мир», чий веб-

сайт став недоступним 30 жовтня 2023 року, а пізніше був зіпсований, щоб опублікувати повідомлення про витік даних клієнта.

NSPK повідомила пресі, що зловмисники не могли викрасти конфіденційні дані клієнтів, оскільки веб-сайт не зберігає таку інформацію, і запевнила, що кібератака не вплинула на платіжну систему.

Пізніше TheRecord повідомив, що відповідальність за атаку взяли на себе хактивісти з групи DumpForums і Українського кіберальянсу, які також заявили про викрадення 31 ГБ даних». ***(Bill Toulas. Russian state-owned Sberbank hit by 1 million RPS DDoS attack // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/russian-state-owned-sberbank-hit-by-1-million-rps-ddos-attack/?utm_source=flipboard&utm_content=other). 08.11.2023).***

***

**«У вересні Естонія, Люксембург та Україна утворили IT-коаліцію, мета якої – зміцнення кібербезпеки і підтримка ЗСУ. Міністр оборони Естонії, Ханно Певкур, розповів про перші кроки організації та її плани, передає DOU.**

За словами Ханно Певкура, Люксембург обіцяв надати 10 мільйонів доларів на підтримку цього проєкту. Разом з цим організатори планують залучати ще більше держав до коаліції.

Однією з перших сфер уваги є покращення зв’язку на рівні батальйонів у співпраці зі Збройними Силами України та Міністерством оборони. Крім того, особлива увага приділяється захисту даних та їх збереженню поза межами країни, відомому як data embassies.

Надалі планується створення спеціального комітету, який виступатиме посередником між ЗСУ та НАТО щодо підтримки та постачання. Цей орган буде відповідальний за здійснення закупівель необхідного обладнання та технологій для досягнення цілей IT-коаліції.

Певкур зауважив, що питання безпеки та гарантії для України є в центрі уваги. Членство в НАТО є найкращою гарантією безпеки для України, і країна

повинна бути готовою відповідати всім вимогам для членства в альянсі». ***(Нові партнери та захист даних. Міністр оборони Естонії розповів про плани IT-коаліції // Інформаційне агентство ЛІГА Бізнес Інформ (https://tech.liga.net/ua/technology/novosti/novi-pratnery-ta-zakhyst-danykh-ministr-oborony-estonii-rozpoviv-pro-plany-it-koalitsii). 02.11.2023).***

***

**«Колишні співробітники Служби безпеки України в Криму, які після анексії Криму в 2014 році перейшли на бік ФСБ РФ, входять до одного з найактивніших угруповань хакерів, що працюють проти України.** Про це повідомляє Державна служба спеціального зв'язку та захисту інформації України.

Як зазначається в аналітичному звіті українського Держспецзв'язку Russia's Cyber Tactics H1'2023, найбільше кібератак на Україну (тільки у 2022 році – понад 100), здійснила група Armageddon/Gamaredon.

У Gamaredon входять хакери ялтинського підрозділу ФСБ – колишні співробітники СБУ в АРК, що перейшли на бік РФ. Основною метою Gamaredon є шпигунство.

Відмінною рисою фішингових розсилок угруповання є високий рівень їхньої підготовки: знання українського контексту та розуміння специфіки роботи тих чи інших організацій.

Це угруповання атакує державний сектор України, українські державні підприємства, сектор безпеки та оборони і правоохоронні органи. Наприклад, Хакери Gamaredon намагаються отримати доступ до всіх можливих баз даних й одержати максимум інформації про автомобілі, їх пересування, камери спостереження, ситуацію на дорогах, арешти тощо.

При цьому Gamaredon вдалося значно збільшити загальну кількість операцій. Якщо за весь 2022 рік CERT-UA зареєструвала 128 випадків, то лише за перше півріччя 2023 року – вже 103. Проте не всі були настільки успішними, як раніше, зазначається в аналітичному звіті.

У вересні Міністерство оборони Великої Британії з посиланням на дані своєї розвідки повідомляло, що Росія використала шкідливе програмне забезпечення Infamous Chisel для викрадення української конфіденційної військової інформації.

На початку серпня СБУ повідомила про блокування спроби російської військової розвідки отримати доступ до бойової системи обміну даних ЗСУ. За даними української спецслужби, російські хакери намагалися проникнути в українські військові мережі та організувати збір розвідданих.

Як заявив тоді керівник департаменту кібербезпеки СБУ Ілля Вітюк, відповідальність за російські кібератаки лежить на хакерському угрупуванні Sandworm, підконтрольному російській військовій розвідці. За даними СБУ, загалом фахівці відомства виявили майже 10 російських шпигунських програм, призначених для отримання інформації із системи обміну даних ЗСУ». ***(Колишні співробітники СБУ з Криму входять до одного з активних угруповань хакерів, що працюють проти України – Держспецзв'язку // Крим.Реалії (https://ua.krymr.com/a/news-krym-kolyshni-spivrobitnyky-sbu-khakerske-uhrupovannia-derzhspetszviazku/32667712.html). 03.11.2023).***

***

**«Служба безпеки України знає про те, що в рф створюють національну систему кібернападу. російські спецслужби навчають хакерству навіть студентів.** Про це розповів начальник Департаменту кібербезпеки СБУ Ілля Вітюк, повідомляє прес-служба відомства.

«Це вже тепер не тільки про кадрових спецслужбістів. У нас є інформація, що в низці освітніх закладів вже викладають предмети “кібератаки на цивільну інфраструктуру». Вони хочуть наростити масштаби атак і кількість людей, які можуть це професійно робити. До речі, навчають атакувати не лише українські системи, а і країн-партнерів», – заявив Вітюк.

Це відбувається на тлі того, що тисячі російських хакерів, зокрема й кіберзлочинці, яких найняла рф, уже працюють проти України. Вони фінансуються російськими спецслужбами, чиї дослідницькі лабораторії та інститути допомагають

розробляти засоби кібервпливу. «Їхня мотивація – не хакінг заради грошей, а знищення нашої держави. А при такому підході від російської кіберагресії серйозно страждатимуть й інші країни», – додав Вітюк.

Зокрема, за 10 місяців 2023 року українська спецслужба нейтралізувала вже майже чотири тисячі кібератак.

Водночас, за словами Вітюка, впродовж 2022-2023 років СБУ заблокувала діяльність 76 ботоферм, які діяли на території України та відпрацьовували проросійські наративи.

«Ворог регулярно намагається розхитати ситуацію в інформаційному просторі України. Один із інструментів такого впливу – це ботоферми, які розганяють проросійські наративи в інтернеті. Від початку повномасштабного вторгнення рф СБУ заблокувала уже 76 таких ботоферм загальною потужністю понад 3 млн акаунтів», – повідомив Ілля Вітюк». ***(СБУ заблокувала більш як 3 млн ботів, що брали участь в кібератаках рф // Internetua (https://internetua.com/sbu-zablokuvala-bilsh-yak-3-mln-botiv-sxo-brali-ucsast-v-kiberatakah-rf). 07.11.2023).***

***

**«На Донеччині цьогоріч українські кіберфахівці нейтралізували 11 російських кібератак на держустанови та військові об’єкти.**

Як повідомила на брифінгу керівниця прес-служби ГУ СБУ в Донецькій та Луганській областях Галина Прищепа, РФ долучає до кібератак навіть студентів, передає кореспондент Укрінформу.

«Протягом 2023 року наші кіберфахівці нейтралізували 11 кібератак, а також ліквідували їх наслідки на державні установи, об’єкти критичної інфраструктури і так само військові об’єкти», - сказала Прищепа, говорячи про Донеччину.

Вона також нагадала, що на території Донецької області протягом повномасштабного вторгнення Росії в Україну СБУ заблокувала діяльність однієї ботоферми, яка працювала в Покровську і в Києві.

Прищепа пояснила, що департамент кібербезпеки СБУ володіє інформацією, що Росія створює національну систему кібернападу, впроваджуючи відповідні

предмети в освітні програми навчальних закладів, щоб залучати до хакерської діяльності навіть студентів.

«І це звичайно проводиться під контролем російських спецслужб. Тобто тепер мова йде не тільки про кадрових спецслужбівців, а й про те, що в освітніх закладах вже викладають предмет «кібератака на цивільну інфраструктуру». Росіяни хочуть наростити масштаби атак і кількість людей, які можуть це професійно робити. І, до речі, навчають, як атакувати не лише українські системи, а і системи країн-партнерів», - зазначила працівниця СБУ.

За її словами, вже тисячі російських хакерів і кіберзлочинців, наняті Росією, працюють проти України та фінансуються спецслужбами РФ…» ***(На Донеччині цьогоріч нейтралізували 11 російських кібератак – СБУ // Укрінформ (https://www.ukrinform.ua/rubric-technology/3784603-na-doneccini-cogoric-nejtralizuvali-11-rosijskih-kiberatak-sbu.html). 09.11.2023).***

***

**«Наразі Україна є країною, на яку приходиться найбільша кількість кібератак у світі, що у 2022 році зросла втричі. Нападають на все: критична інфраструктура, бізнес, фінансовий сектор, особисті дані.** Через це у певного відсотка людей з’явилося бажання захистити себе у цифровому просторі. Але є і трохи сумніші новини: велика кількість людей все одно не розуміє, навіщо дотримуватися правил.

Moonlock, наш підрозділ кібербезпеки у MacPaw, нещодавно провів дослідження серед наших користувачів. Результати наступні: 22% використовують однаковий пароль усюди. 31% не оновлюють операційну систему на пристроях. А кожен третій вважає, що його дані нецікаві для кібершахраїв.

Опитування Fortinet серед майже 2 тисяч бізнесів виявило, що 84% компаній зазнавали хоча б однієї кібератаки на рік. 48% це коштувало понад 1 мільйон доларів. А чому? Бо 68% опитаних зізналися, що їхні працівники мають слабкі навички кібербезпеки.

Зрозуміло, що не всі забувають про власну безпеку у мережі. Але дослідження демонструють: певна кількість людей проявляють до питань кібербезпеки легковажність, яка згодом може призвести до непередбачуваних наслідків.

*Як продуктовий бізнес може змінити цю статистику*

Українські компанії за останні півтора року отримали великий досвід у кібербезпеці. Бо країна стала своєрідним плацдармом для різноманітних цифрових атак. Це не тільки додало нам ґрунтовної експертизи. А й змусило світ також діяти. Кібербезпека стала однією з головних тем на професійних конференціях, а кількість стартапів у цій сфері зросла.

Це питання вже неможливо ігнорувати. З ним треба працювати, транслювати його нагальність. І можна це робити навіть через свої продукти. Демонструвати, що кібербезпека може бути людяним явищем, а що найголовніше — простим у використанні. Так ми оптимізували наш ClearVPN. Щоб він отримував результат у кілька кліків, не треба було обирати країну сервера чи розбиратися у швидкості підключення. Все має працювати, ніби запит у пошуковику. «Хочу захистити приватність у мережі» чи «Хочу дивитися BBC». І це викликає довіру у користувача. На основі цієї довіри можна доносити свої знання про кібербезпеку. Розповсюджувати їх якомога ширше й в усіх можливих формах.

*Як навчити людей правил кібербезпеки? Є кілька варіантів.*

Створіть джерело інформації. Приміром, корпоративний блог. У ньому розповідайте про правила кібербезпеки, які застосунки та пристрої варто використовувати. Також викладайте кейси, із яким довелося зіткнутися. Люди люблять читати про людей, які мали чи мають однакові проблеми. Такі тексти резонують всередині читача, до них більше прислухаються.

Зробіть кілька навчальних продуктів. Можна почати з простих форм. До прикладу, серія лекцій із питаннями-відповідями. Або ж онлайн-курс з кількох уроків, що матиме практичні завдання й невеликий екзамен наприкінці. Великі талмуди не обов’язкові, але пара мануалів з чіткими порадами як створити

безпечний простір у мережі чи навчити співробітників необхідним навичкам також стануть у пригоді.

Гейміфікуйте досвід. Кібербезпека для більшості вважається чимось нудним, але досвід вивчення нового можна зробити цікавішим. Наприклад, через квізи у сторіз в Instagram чи на спеціальних платформах. Або через інтерактивний квест із кількома завданнями, що перевірять рівень навичок кібербезпеки, і підкажуть які з них необхідно підтягнути.

Призначте амбасадорів кібербезпеки у компанії. Розповідайте про кібербезпеку через тіммейтів, які стануть амбасадорами з цього питання, і усіляко чіпатимуть цю тему під час виступів, інтерв'ю тощо. Необхідно прищеплювати користувачам думку, що кібербезпека важлива так само як і правильно харчуватися й спати 8 годин на добу.

Беріть участь у різних міжнародних ініціативах з кібербезпеки. Такі події - чудовий майданчик для поширення інформації на велику аудиторію.

Наприклад, Cybersecurity Awareness Month. До неї долучаються великі бізнеси. Мета заходу — підвищувати й зміцнювати знання про кібербезпеку. Спільно доносити чіткі меседжі про важливість кібербезпеки, а також об’єднати зусилля тисяч бізнесів з усього світу для цього. До речі, ініціативі цього року 20 років.

Крім прояву соціальної відповідальності, такі івенти — можливість нетворкінгу, обміну досвідом і, як потенційний результат, виникнення несподіваної колаборації. Це значущий для розвитку сфери момент. Можна скільки завгодно придумувати неймовірні ідеї та реалізовувати їх сам на сам. Але ніщо не додасть ефективності як спільна робота із колегами. Бо тільки так можна розвинути максимальні можливості напряму і створити дієві й зрозумілі рішення у кібербезпеці для усіх людей. Бо багатьох насправді тривожить саме слово «кібербезпека». Воно здається складним, а у голові одразу з’являються асоціації із програмістами, які розмовляють незрозумілими термінами. По факту кібербезпека — це дуже просто і вона не вимагає технічної освіти. А ось трошки уважності й мотивації для засвоєння інформації ніколи не завадить». ***(Олександр Косован.***

***Навіть у IT компаніях. Що робити зі слабкими навичками кібербезпеки співробітників // ТОВ «ВИДАВНИЧИЙ ДІМ «МЕДІА-ДК» (https://biz.nv.ua/ukr/experts/bezpeka-roboti-v-it-kompaniji-kosovan-pro-prosti-pravila-dlya-programistiv-50370949.html). 25.11.2023).***

***

**«Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено факт масового розповсюдження електронних листів, начебто, від імені СБ України із вкладенням у вигляді RAR-файлу «Електронна вимога СБУ України.rar».**

Згаданий архів містить ще один одноіменний архів в якому знаходиться черговий, захищений паролем RAR-файл «Вимога СБУ 543 від 13.11.2023.pdf.rar».

Останній містить виконуваний файл "Вимога СБУ 543 від 13.11.2023.pdf.exe" (дата компіляції: 2023-11-12 16:15:36), запуск якого призведе до встановлення на ЕОМ програми для віддаленого управління Remcos RAT (дата компіляції: 2023-09-07 10:23:27).

Персистентність Remcos RAT забезпечується шляхом створення запису в гілці Run реєстру операційної системи.

Конфігураційний файл містить 8 IP-адрес серверів управління, що функціонують на технічних потужностях компанії Shinjiru (Малайзія). Доменні імена зареєстровано 11.11.2023 через толерантну до кіберзлочинності російську компанію REG.RU.

CERT-UA вжито невідкладних заходів з протидії кіберзагрозі.

Активність відстежується за ідентифікатором UAC-0050». ***(Ihor Romanets. Кібератака замаскована під «запит СБУ» // Навчально-науковий центр інформаційних технологій (https://nncit.wunu.edu.ua/kiberataka-zamaskovana-pid-zapyt-sbu/). 23.11.2023).***

***

**«Росіяни чи інші зловмисники намагаються зламати телефони українців через месенджер Signal.**

Про це повідомляє РБК-Україна з посиланням на Повітряні сили ЗСУ.

Так, зловмисники розсилають фішингові повідомлення під виглядом нібито техпідтримки з метою отримати доступ до месенджера.

«Чимало військовослужбовців користуються сьогодні найбільш захищеним від русні месенджером SIGNAL. Але і тут ворог чи інші зловмисники намагаються отримати доступ до вашого ґаджета, персональних даних і, здавалося б, конфіденційних переписок!» - написали Повітряні сили.

В ПС наголосили, що громадянам необхідно бути пильними та не надсилати відповіді на схожі запити.

*Російські кібератаки*

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

Після початку повномасштабної війни російські хакери неодноразово здійснювали кібератаки на українські держоргани і не тільки.

Зокрема, під удар потрапляли і країни-союзники України. У січні хакери РФ намагалися атакувати Німеччину після того, як вона вирішила передати нашій країні танки». ***(Антон Малиновський. Росіяни намагаються зламати акаунти українців в Signal // ТОВ «УБТ» (https://www.rbc.ua/rus/news/rosiyani-namagayutsya-zlamati-akaunti-ukrayintsiv-1700082780.html). 15.11.2023).***

***

**«З початку війни російські хакери атакують українську інфраструктуру. У Міністерстві фінансів США назвали кількість виявлених випадків.**

Про це повідомляє РБК-Україна з посиланням на Міністерство фінансів США.

У перші тижні війни в Україні росіяни здійснили низку кібератак на українську інфраструктуру, у тому числі фінансові організації. Однак до квітня 2023 року кількість таких інцидентів різко скоротилася, і їхня активність знизилася.

«Протягом кількох тижнів після вторгнення Росії в Україну спонсоровані російською державою кіберзлочинці провели хвилю кібератак на українську інфраструктуру, включаючи кілька атак, спрямованих проти організацій сектору фінансових послуг. До квітня 2023 року кількість подібних інцидентів значно скоротилася, і затишшя у діяльності, яка спонсорується державою продовжувалося», - заявили в міністерстві.

Крім цього, Росія продовжує здійснювати кібератаки в Україні, спрямовані на руйнування та дестабілізацію. Вона також проводить мережеве проникнення та шпигунство у країнах, які підтримують Україну. Крім того, Росія проводить операції з кібервпливу на людей по всьому світу.

«Група реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) зафіксувала майже 4000 випадків кібератак у період з початку війни в Україні до вересня 2023 року. Це втричі більше, ніж кількість кібератак за аналогічний період до війни», - сказали у міністерстві.

Кібервійна між Росією та Україною не обмежується лише атаками державних структур. Хакери з обох сторін конфлікту також націлилися на широке коло організацій, включаючи фінансові установи. Для цього вони використовували відносно прості методи, такі як розподілені атаки типу "відмова в обслуговуванні" (DDoS).

«В червні 2023 року проросійська хакерська група NoName057 (16) пригрозила атакувати фінансовий сектор України. У наступні чотири дні численні українські банки зазнали DDoS-атак. Метою були чотири найбільші комерційні банки країни, в тому числі Перший український міжнародний банк (ПУМБ), Державний ощадний банк України (Ощадбанк), Креді Агріколь Банк та Юніверсал Банк», - повідомили у Мінфіні США.

*Кібератаки росіян на Україну*

Раніше ми писали, що російські хакери намагаються зламати телефони українців через месенджер Signal. Повітряні сили порадили, як убезпечити себе від втрати даних.

Нещодавно стало відомо, що російські хакери минулого року провели кібератаку на енергосистему України. Вона збіглася з масованим обстрілом енергетики російськими військами.

Раніше Служба безпеки України повідомила, що українські кіберфахівці завадили російським спецслужбам отримати доступ до електронної системи планування операцій ЗСУ». ***(Владислав Прийменко. Названа кількість кібератак російських хакерів проти України // ТОВ «УБТ» (https://www.rbc.ua/rus/news/nazvana-kilkist-kiberatak-rosiyskih-hakeriv-1700267159.html). 18.11.2023).***

***

**«Росія відмовилася від проведення кібератак на українську енергетичну систему. Такі атаки жодного разу не призвели до відключень в Україні, а тому агресор усвідомив їхню марність.**

Про це заявив член правління, IT-директор «Укренерго» Сергій Галаган. За його словами, компанія почала вибудовувати свій кіберзахист ще до повномасштабного вторгнення РФ.

Основним поштовхом стала кібератака у 2016 році. «Ми почали інвестувати в нашу інформаційну безпеку та винаймати високопрофільних фахівців», – пояснив Галаган.

За його словами, IT-фахівці «Укренерго» помітили різке збільшення кількості кібератак на систему в січні 2022. А одразу після 24 лютого того ж року кількість інцидентів зросла втричі порівняно з попереднім роком.

Для дестабілізації енергопостачання в Україні російські хакери використовували різні підходи: від сканування IT-периметра до, наприклад, DDoS-атак – навмисного перевантаження сервісу запитами. Зокрема, під час однієї з

таких з DDoS-атак на «Укренерго» кількість запитів могла перевищувати 5 млн за кілька годин, розповів Галаган.

Однак ці кібератаки не спричинили відключення автоматичних систем на підстанціях «Укренерго», яке призвело б до обмеження енергоживлення. Цього не сталося жодного разу від початку повномасштабного вторгнення.

Як уточнив у коментарі Forbes, заступник міністра енергетики України Фарід Сафаров, у 2022 році росіяни переконалися, що одних лише кібератак на енергосистему недостатньо, і почали комбінувати їх з атаками ракетами та дронами. «Спочатку б'ють ракетами, і одразу після цього кібератака, щоб суттєво ускладнити відновлення», – пояснив він.

Зрештою, РФ майже відмовилася від кібератак як неефективного інструменту, підкреслив Галаган. «Жодна з кібератак на інфраструктуру компанії не досягла успіху», – заявили в «Укренерго» і запевнили: рівень кібербезпеки компанії зараз відповідає міжнародному стандарту, що щороку підтверджують тести». ***(Чому рф припинила кібератаки на енергосистему України // BusinessUA.Com (http://businessua.com/benzin/91848chomu-rf-pripinila-kiberataki-na-energosistemu-ukraini.html). 16.11.2023).***

***

**«Протягом кількох тижнів після вторгнення Росії в Україну російські державні кіберактори здійснили хвилю кібератак на українську інфраструктуру, включно з кількома атаками на фінансові компанії, прозвітувала на Конференції з катастрофічних кіберзагроз в Нью-Йорку в п’ятницю заступниця міністра фінансів США Грем Стіл.**

Вона додала, що Росія координувала руйнівні та підривні кібератаки, спрямовані проти України, проникнення в мережу та шпигунство в країнах, які сприймаються як союзники України, а також операції кібервпливу на людей у всьому світі. Стіл зазначила, що Команда реагування на надзвичайні ситуації пов'язані з комп’ютерами в Україні (CERT-UA) зафіксувала майже 4000

кіберінцидентів у період з січня 2022 року по вересень 2023 року. Це втричі більше, ніж у довоєнний період.

Кіберактивність у контексті російсько-українського конфлікту не обмежується урядовими акторами, зауважила посадовця.

«Ми помітили, що недержавні кіберактори обох сторін конфлікту атакували широкий спектр організацій, у тому числі в секторі фінансових послуг, за допомогою відносно нескладних інцидентів, відомих як розподілені атаки на відмову в обслуговуванні (DDOS)», - зазначила Стіл…» ***(Від початку 2022 року Україна зазнала втричі більше кібератак з боку Росії, ніж до війни // Голос Америки (https://www.holosameryky.com/a/kybernapady-rosija/7359675.html). 17.11.2023).***

***

**«Росію масово атакують хакери. Дані, отримані зі зламів установ та підприємств в РФ, хакери передають українським спецслужбам, а ті використовують інформацію у своїх операціях.**

Хакерські атаки почалися з моменту повномасштабного вторгнення Росії 24 лютого 2022 року, і відтоді не припинялися: проукраїнські хакери атакували російські державні компанії, збираючи таємну інформацію, пише Worldcrunch.

Цього року Роскомнадзор, російський цифровий наглядовий орган, виявив 150 великих витоків, а російська компанія з кібербезпеки "Лабораторія Касперського" повідомила про 168 витоків, загальною кількістю близько 2 мільярдів рядків даних, у тому числі 48 мільйонів — із секретними паролями.

Після російського вторгнення значна кількість хакерів у всьому світі висловили солідарність з Україною. «Ми з колегами діємо за принципом: "Якщо це можна зламати, значить, це потрібно зламати», — сказав представник групи Cyber.Anarchy.Squad.

«BlackBird», один із засновників спільноти DC8044, пояснив, що основною метою зламу російських структур є отримання даних, корисних для українських силовиків. «Особисті дані, отримані нашими групами, як правило, передаються

службам безпеки. Вони збирають і аналізують цю інформацію для ефективної підтримки своїх операцій», — сказав він.

Хакери тісно співпрацюють з українськими спецслужбами: займаються розвідувальними, диверсійними та інформаційними операціями.

Андрій Баранович, співзасновник групи Ukrainian CyberAlliance, зазначив, що «якщо ми витрачаємо 24 години на злам чогось, наші жертви повинні відновлюватися щонайменше тиждень, а в оптимальному випадку — жертва не повинна одужувати взагалі».

*Росія не може захистити себе від хакерських атак: у чому причина*

Хакери кажуть, що відомі витоки — це лише «верхівка айсберга», переважно, отримавши доступ до даних, вони намагаються не розголошувати інформацію публічно, щоб організація, яку зламали, не змогла відреагувати. «Деякі бази даних, до яких хакери вже мають доступ, постійно насичуються великою кількістю нових даних, і публічне викладання цих даних означає втрату доступу», — каже BlackBird.

Витоки даних стають публічними, коли хакери хочуть завдати шкоди ворогові або створити собі репутацію. Звісно, дані також продаються за гроші – спамерам, шахраям, агрегаторам даних. «Ми постійно продаємо та зливаємо дані», — визнав Майкл Майєрс, член хакерської групи UHG.

Нині Росія є одним із світових лідерів за використанням Інтернету, і пандемія COVID-19 лише посилила цю залежність. Економічні санкції Заходу ускладнили питання захисту даних: багато західних IT-компаній, чиї антихакерські рішення були раніше придбані російськими бізнесами — Cisco, IBM, Imperva, Fortinet, Norton, Avast — обмежили або припинили свою діяльність у Росії.

«Якщо раніше російські компанії могли дозволити собі використовувати найбільше, найвідоміше, найперевіреніше антихакерське програмне забезпечення, то тепер їм доводиться імпровізувати», — зазначив один з експертів на умовах анонімності.

Теоретично Роскомнадзор має повноваження захищати персональні дані. Однак, зараз цей орган більше зосереджений на блокуванні опозиційних сайтів та

впровадженні цензури в Росії. «Уся боротьба з витоками сьогодні полягає в розсилці листів і симуляції бурхливої діяльності. Якісь мізерні штрафи застосовуються лише після скандалу в ЗМІ», — пояснив експерт з інформаційної безпеки.

У разі витоку компанія зобов'язана повідомити про це Роскомнадзор, який, як правило, починає розслідування, а потім, можливо, притягує компанію до адміністративної відповідальності. Максимальний штраф — 100 тисяч рублів (1100 доларів)». ***(Олена Ковальська. Проукраїнські хакери зламали в Росії 48 млн рядків із секретними паролями // Експрес (https://expres.online/podrobitsi/proukrainski-khakeri-zlamali-v-rosii-48-mln-ryadkiv-iz-sekretnimi-parolyami). 21.11.2023).***

***

**«У межах проєкту USAID «Кібербезпека критично важливої інфраструктури України» 25 закладів вищої освіти, де проводять навчання за спеціальністю «Кібербезпека та захист інформації», отримають обладнання та програмне забезпечення.** Про це повідомив міністр освіти і науки України Оксен Лісовий.

«Сьогодні галузь кібербезпеки є критично важливою, особливо в контексті повномасштабної війни. Вдячний партнерам за підтримку українських ЗВО у вигляді обладнання, яке допомагатиме навчати кіберфахівців. Це однозначно інвестиція у глобальну безпеку», — написав він.

Загалом, у рамках цієї ініціативи проєкт USAID передасть близько 5 тисяч одиниць техніки та 4 тисячі ліцензій загальною вартістю 2,5 млн доларів.

22 листопада техніку та програмні ліцензії передали Київському національному університету будівництва та архітектури та Маріупольському державному університету, що наразі розташований на території КНУБА.

«Більш, ніж коли-небудь, українці потребують залучення все нових і нових кваліфікованих спеціалістів з кібербезпеки, які допомагатимуть у війні проти російських кібератак. Саме тому USAID підтримав українські ЗВО, в яких

викладається цей фах, допомагаючи їм належно готувати наступне покоління українських кіберекспертів», — сказала представниця місії USAID в Україні Енн Хоппер». ***(Юлія Поліковська. 25 українських університетів отримають техніку від проєкту USAID для підготовки кіберфахівців // «MEDIASAPIENS» (https://ms.detector.media/internet/post/33541/2023-11-22-25-ukrainskykh-universytetiv-otrymayut-tekhniku-vid-proiektu-usaid-dlya-pidgotovky-kiberfakhivtsiv/). 22.11.2023).***

***

## Міжнародне співробітництво у галузі кібербезпеки

**«Керівник управління забезпечення діяльності НКЦК Апарату Ради національної безпеки та оборони України Сергій Прокопенко 3 листопада 2023 року зустрівся із представниками Посольства Королівства Данія в Україні.** Обговорили шляхи поглиблення практичного співробітництва у сфері протидії кібератакам, обміну інформацією, а також подальше партнерство в освітніх проєктах.

«Жодна країна не може протистояти сучасним викликам кібербезпеки самостійно. Наша держава має унікальний досвід у протидії агресії рф у кіберпросторі, яким ми готові ділитись з країнами-партнерами. Адже завдяки спільній роботі та обміну інформацією ми зможемо забезпечити безпеку та стійкість в кіберпросторі не лише України, а і Європи», – зазначив Сергій Прокопенко.

За особистий внесок у справу гарантування національної безпеки та оборони України, ефективну співпрацю з Апаратом РНБО України та Національним координаційним центром кібербезпеки нагороджено відзнакою РНБО України заступника Аташе з питань оборони Якоба Хансена. Також С. Прокопенко подякував Королівству Данія за всебічну підтримку України та внесок у зміцнення Національної системи кібербезпеки України». ***(Говорили про безпеку та стійкість в кіберпросторі: фахівці НКЦК провели робочу зустріч з***

***представниками Посольства Королівства Данія в Україні // Рада національної безпеки і оборони України (https://www.rnbo.gov.ua/ua/Diialnist/6696.html). 03.11.2023).***

***

**«ЄС зміцнив зв'язки з Україною щодо співпраці у сфері кібербезпеки за допомогою нової офіційної угоди, спрямованої на покращення обміну інформацією та нарощування потенціалу.**

Оголошена сьогодні угода формалізує обговорення, розпочаті у Варшаві під час Діалогу з кібербезпеки між Україною та ЄС минулого року. Його підписали безпекове агентство ЄС ENISA, Національний координаційний центр з кібербезпеки України (НКЦК) та Адміністрація Державної служби спеціального зв'язку та захисту інформації України (ДССКІ).

За словами ENISA, широка домовленість охоплює «короткострокові структуровані заходи співпраці», але також зосереджується на довгостроковій політиці. Він охоплює три сфери:

Кіберобізнаність і розвиток потенціалу для підвищення стійкості. Це може включати участь України в загальноєвропейських навчаннях і тренінгах з кібербезпеки, можливі домовленості про відрядження, а також обмін і просування інструментів і програм кіберобізнаності.

Узгодження законодавства та впровадження, включаючи NIS2, і зосередження на секторах критичної інфраструктури, таких як телекомунікації та енергетика

Більш систематичний обмін знаннями та інформацією для підвищення обізнаності про ситуацію

Цей крок стався після того, як минулого тижня Європейська комісія рекомендувала запросити Україну розпочати переговори про членство в ЄС, як тільки вона зможе виконати ряд останніх умов.

Цей процес, ймовірно, триватиме роки, але є важливим кроком для країни, враховуючи її боротьбу відвоювати позиції від Росії в рамках широко розрекламованого контрнаступу.

Віце-президент Європейської комісії із закордонних справ Жозеп Боррель стверджував, що підтримка України також допоможе ЄС підвищити стійкість до російської агресії в кіберпросторі.

«Зловмисне маніпулювання інформацією та кібератаки є ключовим елементом агресії Росії проти України. Добре відома гібридна тактика використовується Росією в нових масових масштабах, націлених не лише на Україну, а й на Європейський Союз», – сказав він.

«Це робить сьогоднішню домовленість про посилену співпрацю для кібербезпеки ще важливішою. Ця домовленість є додатковим важливим компонентом нашої загальної підтримки, щоб допомогти Україні захиститися від Росії, а також нашої довгострокової відданості безпеці України». ***(Phil Muncaster. EU Formalizes Cybersecurity Support For Ukraine // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/eu-formalizes-cybersecurity/). 13.11.2023).***

***

**«НАТО допомагає Україні з кіберзахистом, але своєю чергою також багато чого може повчитися в нашої країни.**

Про це заявила міністерка закордонних справ ФРН Анналена Бербок на першій конференції НАТО з кібербезпеки, що відбулася в Берліні, передає кореспондент Укрінформу.

Альянс, за її словами, може досягти стійкості проти кібератак, допомагаючи в захисті партнерам.

«Підтримуючи Україну в кіберзахисті, ми також захищаємо себе. Тому Німеччина надала Україні 10 тисяч наземних станцій для супутникової інтернет-системи... І ми робимо внесок у кіберпотенціал України, навчаючи персонал кібербезпеки... Безперечно, нам також є чого повчитися в України. На цей момент

наші українські друзі, ймовірно, мають більше досвіду кіберзахисту, ніж усі ми разом узяті», - заявила глава німецького МЗС.

Вона визнала: якщо близькі партнери НАТО уразливі, сам Альянс також є уразливим. Це стало зрозуміло, коли Росія в день початку повномасштабного вторгнення в Україну атакувала мережу зв'язку ViaSat. Атака не лише призвела до інформаційного затьмарення в частині України, ефект поширився на мережі по всій Європі, а в Німеччині постачальники відновлюваної енергії тимчасово втратили зв'язок із понад 3000 вітровими електростанціями.

«Кібератаки - це не гра. Вони впливають на реальний світ. Вони загрожують життю та економіці. Вони становлять небезпеку для нашої демократії та верховенства права… Кіберпростір став нервовою системою нашого суспільства», - підкреслила Бербок.

Крім того, додала вона, кібератаки стали добре налагодженою справою для організованої злочинності, спрямованої на викрадення даних і вимагання грошей. Цей нелегальний бізнес іноді тісно переплетений з державними акторами.

Міжнародне право повністю застосовується в кіберпросторі, але воно порушується щодня, сказала очільниця німецького МЗС. Вона закликала не сидіти склавши руки і спостерігати за цією «безперервною ерозією», а побудувати визнану в усьому світі державну практику відповідальної поведінки в кіберпросторі…» ***(НАТО може повчитися в України кіберзахисту – Бербок // Укрінформ (https://www.ukrinform.ua/rubric-technology/3784988-nato-moze-povcitisa-v-ukraini-kiberzahistu-berbok.html). 10.11.2023).***

***

## Світові тенденції в галузі кібербезпеки

**«Незважаючи на додавання майже півмільйона працівників за рік, глобальна нестача кадрів у сфері кібербезпеки зросла на 26% порівняно з минулим роком.** Тим часом захист систем, мереж і даних від кібератак, що постійно розвиваються, став більш складним і складним, ніж будь-коли. Оскільки

попит значно перевищує пропозицію, спеціалісти з кібербезпеки користуються великим попитом на сучасному ринку праці, пропонуючи високу зарплату та багатообіцяючі перспективи роботи для нової групи нових кіберталановитих кадрів.

Проте проникнення в кібербезпеку та досягнення досвіду є складним подвигом. Це вимагає років безперервного навчання та цілеспрямованих зусиль, і люди без попередніх знань у галузі можуть зіткнутися з проблемами, орієнтуючись на невизначених шляхах навчання. Кіберпрофесіонали повинні надавати пріоритет поточній освіті та сертифікаціям, щоб забезпечити довгостроковий успіх, одночасно прокладаючи чітку траєкторію в цій галузі.

Як можна підтримати нове покоління талантів у сфері кібербезпеки у створенні портфоліо облікових даних безпеки для просування їхньої кар'єри?

*Виховання досвідчених професіоналів безпеки*

Сертифікати з кібербезпеки охоплюють широкий спектр дисциплін, навичок і нових тенденцій безпеки. Від аналізу загроз і тестування на проникнення до управління, ризиків і відповідності, ці сертифікати надають професіоналам всеохоплюючу основу для вдосконалення своїх знань і кваліфікації. Вони також стали нормою в багатьох посадових інструкціях служби безпеки, оскільки організації шукають вимірні показники досвіду майбутніх працівників.

Сертифікація — це щось більше, ніж просто аркуш паперу чи резюме. Це означає, що особа інвестувала в свою постійну освіту та продемонструвала свою досконалість у цій галузі. Сертифікація також говорить про їхній характер як професіонала, демонструючи їхню прихильність до кодексу етики та часто передбачаючи схвалення існуючих власників облікових даних.

Незважаючи на це, людина з численними сертифікатами, але обмеженим реальним досвідом не обов'язково перевершить когось із практичним досвідом, але не має повноважень у сфері кібербезпеки. Вкрай важливо знайти правильний баланс між сертифікатами та практичним досвідом. Організації повинні надавати новим кіберталантам доступ до різних спеціалізацій і вертикалей, що дозволяє їм застосовувати свої сертифіковані знання в практичних сценаріях. Наприклад,

програма ротаційного циклу дозволить професіоналам досліджувати різноманітні напрямки в галузі.

Замість того, щоб відчувати страх перед своїми старшими колегами та набором сертифікатів і спеціалізацій, які вони мають, організації повинні заохочувати новачків у сфері кібербезпеки активно співпрацювати з ними. Це дозволить їм розширити свої перспективи, отримати цінну інформацію та бути в курсі найцінніших кібердовідок у цій галузі.

*Забезпечення шляху*

Це захоплюючий час для кібербезпеки, і нові розробки продовжують рухати галузь вперед. Незалежно від того, чи йдеться про аналіз вразливостей за допомогою тренувань з об'єднання команд чи про забезпечення безпеки нових технологій, таких як IoT та хмарні обчислення, ця сфера має багато можливостей для кіберпрофесіоналів.

Відповідно Рада кібербезпеки Великобританії розробила структуру кібершляхів, яка охоплює 16 чітких спеціалізацій. Це включає новий інструмент картографування сертифікації, який детально описує кваліфікацію та досвід, необхідні для різноманітних дисциплін кібербезпеки.

Запровадження цієї основи забезпечує прозорість і підтримку новачків у галузі, проливаючи світло на низку можливостей кар'єрного зростання. Це, у свою чергу, дозволяє організаціям залучати та утримувати кіберталанти, забезпечуючи чіткі кар'єрні шляхи разом із необхідною підтримкою навчання та розвитку.

Хоча в США ще немає подібного інструменту картографування, спостерігається помітний поштовх до галузевої стандартизації. Сертифікати, які демонструють прямі кореляції або мають ширшу спрямованість за межі конкретних муніципалітетів, набувають популярності. Наприклад, існують суттєві збіги між Загальним регламентом захисту даних ЄС (GDPR) і законами штатів США, наприклад у Каліфорнії, які, по суті, прийняли принципи GDPR.

У результаті сертифікації безпеки набувають більшої можливості передачі між різними регіонами, що призводить до кращого узгодження шляхів розвитку та ширших можливостей для нового покоління талантів у сфері кібербезпеки.

Примітно, що Google також нещодавно запустив сертифікат кібербезпеки початкового рівня, який пропонує практичний досвід роботи з галузевими стандартами та інструментами, тоді як універсальні фреймворки, такі як фреймворк MITRE ATT&CK, продовжуватимуть формувати спосіб використання сертифікатів у реальному світі.

*Розблокування висхідної мобільності*

На додаток до отримання сертифікатів, висхідна мобільність у сфері кібербезпеки вимагає від професіоналів розширення свого бачення за межі безпеки «чорної скриньки» та розуміння ширшого бізнес-контексту своїх ролей. Розуміння того, як кібербезпека узгоджується із загальними цілями організації, має вирішальне значення для ефективного прийняття рішень і управління ризиками.

Компанії можуть почати ліквідовувати прогалину в навичках кібербезпеки, сприяючи зсередини, постійно підвищуючи кваліфікацію та перекваліфіковуючи свою робочу силу, щоб підвищити свій колективний інтелект безпеки. Це може включати заохочення людей із ширшого бізнесу створити портфоліо сертифікатів безпеки або навіть перейти до команди з кібербезпеки. Наприклад, хтось, який переходить із відділу маркетингу, принесе цінне розуміння перетину між безпекою та іншими організаційними сферами, сприяючи тіснішій співпраці та узгодженню з зовнішніми зацікавленими сторонами.

Незалежно від фону чи попереднього досвіду існують сертифікати кібербезпеки, призначені для зустрічі з людьми там, де вони є. Однак, щоб справді віддати пріоритет розвитку талантів у сфері кібербезпеки та надати варті можливості для навчання, організації повинні подолати такі бар’єри, як часові обмеження та витрати на сертифікацію. Один із способів вирішити цю проблему – це виділення часу для навчання та підтримки, що дозволяє працівникам скористатися цінними можливостями навчання та просуватися вперед у власному темпі.

Будучи відносно молодою галуззю, кібербезпека готова до подальшої еволюції та трансформації. Зараз організації мають чудову можливість скористатися моментом, поєднавши постійне навчання, сертифікати та практичний

досвід. Роблячи це, вони не тільки зміцнять свою довгострокову безпеку, але й позиціонуватимуть себе як привабливе місце для кращих кіберталантів». ***(Paul Ponzeka. Mapping The Next Generation Of Cyber Talent With Certifications // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/11/02/mapping-the-next-generation-of-cyber-talent-with-certifications/?utm_source=flipboard&utm_content=LeBui2014%2Fmagazine%2FSecuCybe&sh=369008fa30a5). 02.11.2023).***

***

**«Сучасні організації піддаються постійним змінним ландшафтам загроз. У цій «новій нормі» застосування звичайних стратегій до викликів, таких як програми-вимагачі, вже недостатньо.** Важливо, щоб IT-групи, групи безпеки та члени правління знали, на чому зосередити зусилля з безпеки та стійкості підприємства, щоб вони могли передбачити, протистояти та відновлюватися після сучасних кібератак.

Наближаючись до останнього кварталу 2023 року, ми дивимося вперед на три головні тенденції загроз кібербезпеці, які фахівці з безпеки повинні готуватися відбивати.

1. Методи «Життя поза межами землі» (LOL).

Тихі атаки, які залишаються прихованими протягом тривалого часу, становлять унікальний ризик для бізнесу. Сучасні хакери використовують набагато менше шкідливих програм. Замість цього вони живуть поза межами землі (LOL), використовуючи операційну систему проти неї самої, використовуючи власні легітимні інструменти, такі як підписані двійкові файли (LOLBins), сценарії (LOLScripts) і бібліотеки, щоб маскувати зловмисну активність, інтегрувати та обходити навіть найдосконаліші захист безпеки.

На відміну від традиційних атак, які використовують зловмисне програмне забезпечення, LOL-атаки використовують власні утиліти ОС, необхідні для запуску ОС і допомоги IT-операціям. За своєю суттю вони не шкідливі. Отже, хоча звичайні інструменти реєструють дії LOL на кожній кінцевій точці, вони не попереджають

про них. Наприклад; Cmd.exe, інтерпретатор командного рядка за замовчуванням для Windows, можна використовувати для ухилення від захисних контрзаходів або для приховування як механізм збереження.

Це створює складну дилему для безпеки. Як вони можуть попередити, коли законні інструменти використовуються, як і розроблено, але з мерзенних причин? Чи можна взагалі сповістити про намір? LOLBins стають технікою вибору, оскільки вони гармонійно вписуються. Це метод, використаний групою Volt Typhoon для спостереження за водопостачанням та електропостачанням, які обслуговують військові об’єкти в Сполучених Штатах і за кордоном.

Традиційні інструменти безпеки збирають докази зловмисності в мережі та на кінцевій точці. Вони є критично важливим рівнем захисту, який виявляє шкідливі файли та дії, але вони не створені для виявлення методів скритності, таких як LOLBins, які використовує група Volt Typhoon. Щоб захистити дані від такого роду атак, організаціям потрібно буде ввімкнути поступову зміну захисту, запровадивши реалістичні приманки, які змусять зловмисників залучити ці фальшиві ресурси та викрити їхні методи; крок, який, у свою чергу, попереджає команди безпеки організації про потенційну приховану загрозу.

2. Штучний інтелект (AI)

Сучасні хакери використовують передові інструменти, такі як ШІ та машинне навчання, щоб автоматизувати та координувати атаки та підвищувати їхню ефективність. Вони також використовують штучний інтелект, щоб зрозуміти, які засоби захисту запровадили організації, щоб запобігти проникненню зловмисників у їхнє середовище. Більше не обмежуючись необхідністю вручну створювати свої кампанії загроз, зловмисники використовують легкодоступні генеративні інструменти штучного інтелекту, як-от ChatGPT, і точно налаштовують їх відповідно до своїх потреб – чи то створюється високоперсоналізований фішинговий вміст у великих масштабах, чи генерується зловмисне програмне забезпечення для натискання клавіш і базовий код шкідливого програмного забезпечення. який спеціально адаптований для «злому» облікових даних і алгоритмів цільової системи.

Згідно з нещодавнім звітом, експерти з кібербезпеки на великих підприємствах кажуть, що генеративний ШІ вже спричинив значне зростання атак. Щоб боротися зі зростанням обсягу, організаціям потрібно буде використовувати захисний штучний інтелект і машинне навчання, що дає змогу: автоматизувати виявлення та виправлення невідповідних систем; застосовувати автоматизовані виправлення, конфігурацію та оновлення для активів програмного забезпечення; і виконувати традиційно трудомісткі дії, такі як керування ідентифікацією та доступом (IAM) і звітування. Іншими словами, використання штучного інтелекту для забезпечення відповідності вимогам архітектури нульової довіри та прямого протидії загрозам за допомогою видимості в реальному часі та ранніх попереджень, що підтримує позицію проактивного захисту.

3. Програмне забезпечення-вимагач як послуга

Програми-вимагачі становлять одну з найбільших загроз для компаній будь-якого розміру в усіх галузях промисловості. Добре організовані групи розробили складні моделі підписки та розповсюдження Ransomware-as-a-Service (RaaS), які спрощують загрозливих суб'єктів, які мають невеликий досвід або зовсім без них, створити найсучаснішу атаку, що складається з більшості сучасні методи протягом життєвого циклу атаки.

Спеціалізуючись на конкретних елементах процесу атаки, сучасні оператори RaaS пропонують набори, які включають усе: від платіжних порталів і «служб підтримки» для жертв до вибору варіантів програм-вимагачів (таких як LockBit, Revil і Dharma). Інші діють як посередники доступу, які спеціалізуються на відкритті. Філіали, які купують або орендують ці комплекти RaaS, можуть вільно об'єднувати всі ці елементи для здійснення атаки програм-вимагачів, сплачуючи комісію або ділячись частиною свого прибутку.

Поява бізнес-моделі RaaS означає, що частота та складність атак програм-вимагачів зростає. Зважаючи на це, організаціям потрібно буде подвоїти свою діяльність у сфері кібербезпеки. Незалежно від того, чи йдеться про посилення стратегій керування вразливістю та впровадження інструментів раннього попередження про кібервиявлення чи розгортання автоматизованого виправлення

та даних резервного копіювання та відновлення у виробничих середовищах, щоб забезпечити їх швидке відновлення після атаки.

*Прийняття стійкого мислення*

Поширення нових і нових кіберзагроз означає, що організаціям потрібно буде розірвати розрив між безпекою та IT-операціями та змінити своє мислення на спільну стратегію стійкості та IT-інфраструктуру, яка бореться з кібератаками. Це спільна відповідальність, включаючи сегментацію, резервування, обман, контекстну обізнаність, обмеження привілеїв тощо.

Розуміючи, що ймовірність кібератаки є випадком «коли ні, якщо», їм потрібно буде запустити засоби раннього виявлення та забезпечити активний пошук загроз, щоб вони могли швидко реагувати на атаки та інциденти безпеки. Повернення до звичайних операцій після події, пов'язаної з безпекою, тепер має стати головною метою безпеки, тому надійні процедури відновлення даних є обов'язковими». ***(Steve Preston. The top three cybersecurity threats you didn't know to look out for // Future US, Inc. (https://www.techradar.com/pro/the-top-three-cybersecurity-threats-you-didnt-know-to-look-out-for?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 03.11.2023).***

***

**«Індустрія кібербезпеки переживає хвилю звільнень і скорочень бюджету згідно з новим опитуванням майже 15 000 професіоналів галузі.**

Принаймні 47% респондентів сказали, що вони були свідками скорочення своїх робочих місць протягом останнього року, згідно з даними промислової торгової групи ISC2, яка провела опитування у співпраці з Forrester Research. Близько 22% цих респондентів повідомили про звільнення своєї команди, а 53% сказали, що їхні компанії відклали закупівлю та впровадження нових технологій для протидії загрозам кібербезпеки.

Опитування виявило загальне відчуття серед представників галузі, що роботодавці звужують свої бюджети та не витрачають стільки на модернізацію

інфраструктури кібербезпеки, щоб протистояти новим загрозам, включно з тими, які створює штучний інтелект.

Опитування показало, що індустрія розваг і медіа скоротила більшість робочих місць у сфері кібербезпеки. Будівельна галузь, технологічні компанії, автомобільні та хмарні послуги хостингу також значно скоротили, і скорочення, схоже, починають впливати на те, наскільки добре співробітники служби кібербезпеки можуть адаптуватися до нових загроз.

«Ми повинні бути стурбовані скороченнями», - сказав Клар Россо, виконавчий директор ISC2, в інтерв'ю Wall Street Journal. «Нам належить виконати масу роботи над керівництвом, щоб змусити їх зрозуміти ризики, на які вони наражають свою організацію». ***(Abubakar Idris. Huge Cybersecurity Industry Survey Reveals Concerns Over Cuts Amid New Threats // JAF Communications Inc. (https://themessenger.com/tech/cybersecurity-industry-survey-cuts-ai-threats?utm_source=flipboard&utm_content=TheMessenger%2Fmagazine%2FThe+Messenger+Latest). 01.11.2023).***

***

**«Згідно з новими дослідженнями, вигорання серед старших спеціалістів із кібербезпеки посилюється різким зростанням рівня кібератак.**

Опитування, проведене CyberArk, показує, що підвищені загрози безпеці впливають на здатність практиків ефективно виконувати свої функції, причому майже дві третини з усіх сил намагаються боротися зі зростаючим навантаженням.

Понад дві третини керівників старших класів також вважають, що на виснаження впливає підвищений рівень загрози, що впливає на їх здатність приймати важливі рішення високого рівня.

Навантаження на вищий персонал безпеки відбувається паралельно зі сплеском атак в останні місяці. Дослідження CyberArk показало, що понад 80% організацій зазнали спроби атаки програм-вимагачів протягом 2023 року, що свідчить про зростання порівняно з попереднім роком.

Девід Хіггінс, старший директор відділу польових технологій у CyberArk, сказав, що зростаючий рівень вигорання серед практиків безпеки викликає серйозні занепокоєння щодо їх здатності протистояти зростаючим загрозам.

«Здатність відстежувати втручання в технічну інфраструктуру організації та зміни в ландшафті загроз є невід'ємною частиною ролі кожного спеціаліста з безпеки, враховуючи швидкий і потужний характер кібератак», — сказав він.

«Вигорання викликає занепокоєння в цьому контексті, оскільки воно погіршує здатність захищати свою організацію. Одне неправильне рішення або пропущений сигнал може відкрити двері для репутаційної та грошової шкоди для організації».

*Стрес спеціаліста з безпеки*

Звіт містить останнє попередження про стрімке зростання рівня стресу в індустрії кібербезпеки: нещодавнє дослідження Чартерного інституту інформаційної безпеки (CIISec) виявило, що майже чверть спеціалістів із безпеки працюють більше 48 годин на тиждень.

Дослідження Gartner на початку 2023 року показало, що майже половина керівників служби безпеки можуть змінити кар'єру до 2025 року через те, що консультант назвав «нестійким рівнем стресу».

Прогнозований відтік, пов'язаний зі стресом, відбувається в критичний період для утримання талантів у ширшій галузі безпеки.

Цього тижня звіт ISC2 показує, що глобальна нестача фахівців з кібербезпеки склала 3,4 мільйона минулого року, у порівнянні із загальною кількістю кіберпрацівників у 4,7 мільйона.

Респонденти сказали ISC2, що їх найбільше хвилюють прогалини в навичках, скорочення їхніх команд і збільшення робочого навантаження.

Дослідження CyberArk узгоджуються з поточними прогнозами щодо утримання талантів. Фірма виявила, що понад шість із десяти професіоналів із кібербезпеки вважають, що «регулярне» відтік працівників протягом наступних 12 місяців також спричинить проблеми з безпекою.

Подібним чином, майже одна третина заявила, що прогалини в навичках кібербезпеки перешкоджають захисту безпеки.

«Проблему виснаження співробітників, яка впливає на команди з кібербезпеки, необхідно вирішити – і швидко – якщо організації хочуть зберегти надійність свого кіберзахисту», – говорить Хіггінс.

«Перш за все, безпосередня реакція на поточні загрози – з внутрішніх чи зовнішніх джерел – потребує робочої сили, розумово, фізично та технічно підготовленої для запобігання атакам. І це має бути абсолютним пріоритетом». ***(Emma Woollacott. Surging cyber threats exacerbating security staff burnout // Future US, Inc. (https://www.itpro.com/security/surging-cyber-threats-exacerbating-security-staff-burnout). 02.11.2023).***

***

**«Професіонали з кібербезпеки не можуть позбутися роботи, навіть коли вони перебувають у вільний час або у відпустку, стверджує нове дослідження.**

Звіт Centripetal, який опитував 200 професіоналів безпеки, показав, що майже всі (90%) кіберпрофесіоналів регулярно перевіряють свою електронну пошту, Slack та інші пов’язані з роботою платформи обміну миттєвими повідомленнями під час щорічної відпустки.

Майже третина (32%) проводить кожну ніч, виконуючи хоча б якусь роботу, тоді як 70% перериваються принаймні раз на тиждень. Більше того, приблизно п’ята частина (18%) працює понад один повний день на тиждень (8+ годин) додатково, без оплати.

Більшість респондентів (46%) вирішили працювати додатковий час, відповідати на електронні листи допізна та працювати під час щорічної відпустки, оскільки вони були лояльними до своїх роботодавців. Ще чверть (23%) зробили це через посилення кіберзагроз. Нарешті, 16% сказали, що це тому, що їх команда була недостатньо укомплектована. Кожен десятий сказав, що він єдиний, хто здатний виконати цю роботу.

Але перевантажені спеціалісти з кібербезпеки, які працюють в умовах нестачі персоналу та обладнання, є проблемою та ризиком для всієї організації. Дослідники роками попереджали, що багато професіоналів безпеки страждають від виснаження, через що вони пропускають загрози, забувають важливі оновлення для своїх кінцевих точок тощо.

У звіті експертів з кібербезпеки Vectra AI, опублікованому минулого літа, виявилося, що майже всі (97%) хвилюються, що пропустять важливі заходи безпеки, тоді як 71% зізналися, що, можливо, були скомпрометовані, але не знають.

У середньому IT-команди отримують майже 4500 сповіщень, але можуть вирішити лише приблизно дві третини з них (67%). Двоє з п’яти вважають, що це лише питання часу, коли вони пропустять щось важливе, і погоджуються, що інструменти безпеки, з якими вони працюють, лише збільшують навантаження. Вони також вважають, що їх засипають «безглуздими сповіщеннями». ***(Sead Fadilpašić. Cybersecurity pros are putting everyone at risk by working too much // Future US, Inc. (https://www.techradar.com/pro/security/cybersecurity-pros-are-putting-everyone-at-risk-by-working-too-much?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 08.11.2023).***

***

**«План реагування на інциденти (IRP) — це індивідуальний структурований набір процедур і вказівок організації, яких вона дотримується, коли стикається з інцидентом безпеки або руйнівною подією.**

Це може загрожувати конфіденційності, цілісності або доступності їхніх систем інформаційних технологій та/або скомпрометувати їхні дані.

Основною метою плану реагування на інциденти є пом’якшення впливу таких інцидентів, мінімізація потенційної шкоди та якнайшвидше відновлення нормальної роботи.

Хороший IRP складається з кількох елементів, таких як ідентифікація активів, класифікація інцидентів, стримування та ліквідація, а також відновлення з урахуванням отриманих уроків.

Щоб переконатися, що організація належним чином підготовлена до неминучої атаки, найкраще, щоб вона дотримувалася процесу реагування на інциденти, побудованого в рамках, наприклад Національного інституту стандартів і технологій (NIST) Cybersecurity Framework.

Процес реагування на інциденти згідно з NIST дозволить організації оптимізувати процес, про який більшість спеціалістів із безпеки дізнаються на ранніх етапах своєї кар'єри.

Це добре відомий процес у спільноті кібербезпеки, який може дозволити міжорганізаційну співпрацю. Використання цієї структури також допоможе більшості організацій дотримуватися місцевих нормативних вимог.

Процес реагування на інцидент NIST складається з чотирьох основних компонентів, які можна включити в план: підготовка, виявлення/аналіз, стримування/ліквідація та відновлення. Це забезпечує постійне навчання та цикл організаційного вдосконалення.

До цього можна додати більше елементів, але для більшості планів це має бути базова лінія та/або мінімум, включений у план.

Для розробки добре структурованого плану, який можна узгодити з бізнес-цілями організації та толерантністю до ризику, життєво важливо використовувати структуру, подібну до тієї, яку пропонує NIST.

Це перший крок до отримання та забезпечення підтримки з боку керівництва організації та підвищення готовності організації реагувати на будь-які інциденти безпеки». ***(Theodore Wiggins. The plan for the inevitable cyber attack: Get the gist of NIST // TechTarget (https://www.computerweekly.com/opinion/The-plan-for-the-inevitable-cyber-attack-get-the-gist-of-NIST?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology) . 08.11.2023).***

***

***«Аоп (NYSE: AON Глобальне дослідження управління ризиками) за 2023 рік, оприлюднене генеральним директором Грегом Кейсом, визначило кібератаки та витік даних як головний бізнес-ризик у всьому світі.*** Опитування зібрало думки 3000 ризик-менеджерів і керівників у 61 країні. Переривання діяльності займає друге місце серед найбільших ризиків, що відображає зростаючу частоту таких подій, які одночасно впливають на кілька галузей і компаній.

Опитування висвітлило проблеми людського капіталу як значний бізнес-ризик, спричинений різким зростанням витрат на охорону здоров'я, гострою конкуренцією за таланти, нестачею робочої сили та поганою готовністю до пенсії. Примітно, що «залучення та утримання найкращих талантів» у 2021 році підскочило на четверте місце в усьому світі, опинившись за межами першої десятки. Незважаючи на таке зростання обізнаності, лише 11% респондентів кількісно оцінили ці ризики, що свідчить про значний розрив між сприйняттям ризику та діями.

Ламброс Ламбру, генеральний директор Human Capital в Aon, попередив, що дефіцит талантів або спеціалізованих навичок може обмежити інновації та конкурентоспроможність, водночас збільшуючи вразливість до кібератак, нормативних порушень, збоїв у ланцюзі постачання, перерв у бізнесі та репутаційної шкоди.

Збої в ланцюзі поставок були оцінені як значний ризик через геополітичні та економічні зміни. Проте менше 40% організацій провели оцінку стійкості постачальників, і менше 20% диверсифікували своїх постачальників, щоб зменшити цей ризик. Цей ризик, пов'язаний із збоями в ланцюзі постачання та дистрибуції, досяг 14-річного максимуму в опитуванні.

Енді Марселл, генеральний директор Risk Capital в Aon, висловив занепокоєння з приводу того, що ризики, пов'язані зі зміною клімату та штучним інтелектом, не включені до першої десятки рейтингу. Він підкреслив безпосередні ризики зміни клімату, включаючи пошкодження майна, суворий вплив погоди, стихійні лиха та наслідки пов'язаних із кліматом нормативних змін. Він також

підкреслив трансформаційну роль штучного інтелекту в зміні ландшафту корпоративних ризиків у різних галузях. Широкомасштабні ініціативи штучного інтелекту можуть підвищити ризик кібербезпеки та посилити ризики для людського капіталу, як-от дефіцит необхідних навичок.

Опитування також виявило високу готовність до ризику для кібератак, низьку втрату прибутку та високий відсоток дій із зменшення ризику для всіх десяти основних ризиків. Проте лише два з п'яти найпоширеніших поточних ризиків підлягають страхуванню, а половина із загальної десятки не підлягає страхуванню». ***(Pollock Mondal. Cyber attacks top global risks, talent retention surges in Aon 2023 survey // Fusion Media Limited (https://www.investing.com/news/economic-indicators/cyber-attacks-top-global-risks-talent-retention-surges-in-aon-2023-survey-93CH-3225146?utm_source=flipboard&utm_content=Investingdotcom%2Fmagazine%2FEconomic+Indicators). 07.11.2023).***

***

***«Наступ цифрової ери надав компаніям інструменти для експоненціального зростання та зв'язку з клієнтами такими способами, які раніше не були можливими.*** Однак швидка цифровізація послуг і операцій також наражає компанії на широкий спектр загроз кібербезпеці. Оскільки кіберзлочинці стають все більш витонченими у своїй тактиці, компанії повинні залишатися пильними та адаптувати свої стратегії, щоб захистити себе від цих нових загроз. У цій статті буде досліджено поточний ландшафт кібербезпеки та запропоновано стратегії захисту бізнесу в епоху цифрових технологій, спрямовані на подолання як зовнішніх, так і внутрішніх загроз.

*Ландшафт кібербезпеки: масштаб і складність кіберзагроз*

Цифровий ландшафт став живильним середовищем для кіберзагроз, і хакери постійно розробляють нові способи зламати системи та отримати доступ до конфіденційної інформації. Складність цих атак зросла, оскільки зловмисники використовують передові інструменти, такі як штучний інтелект і машинне

навчання, щоб обійти заходи безпеки. Величезний масштаб цих загроз ускладнив підприємствам не відставати.

Помітні інциденти з кібербезпекою за останні кілька років підкреслили вразливість навіть найвідоміших організацій. Такі резонансні зломи, як атака програм-вимагачів WannaCry, атака на ланцюжок поставок SolarWinds і витік даних Equifax, служать яскравим нагадуванням про потенційні наслідки недостатніх заходів кібербезпеки.

*Стратегії захисту бізнесу в епоху цифрових технологій*

Щоб захистити бізнес від зростаючих загроз у кіберпросторі, важливо застосувати багаторівневий підхід, який включає як превентивні заходи, так і заходи реагування. Ось вісім ключових стратегій, які компанії можуть застосувати для забезпечення надійної кібербезпеки:

1. Навчання та обізнаність співробітників: кібербезпека – це не лише питання IT; це залучає всю організацію. Регулярне навчання співробітників безпечним онлайн-практикам і потенційним загрозам може допомогти запобігти кібератакам. Заохочуйте культуру кібербезпеки, надаючи ресурси та вказівки для співробітників, як-от уникання підозрілих електронних листів і використання надійних унікальних паролів.

2. Регулярні оцінки безпеки. Проведення регулярних оцінок безпеки може допомогти виявити потенційні вразливості в цифровій інфраструктурі вашої організації. Це включає тестування на проникнення, сканування вразливостей і перевірки безпеки, щоб оцінити ефективність ваших заходів безпеки та внести необхідні коригування. Проактивність у виявленні слабких місць може допомогти запобігти майбутнім атакам.

3. Шифрування даних і безпечне зберігання: Шифрування даних є вирішальним заходом для захисту конфіденційної інформації. За допомогою шифрування даних у стані спокою та під час передачі компанії можуть гарантувати, що їхні цінні дані залишаються в безпеці, навіть якщо зловмиснику вдасться проникнути в систему. Використання безпечних рішень для зберігання,

таких як хмарні служби з надійним шифруванням і контролем доступу, може ще більше посилити захист ваших даних.

4. Багатофакторна автентифікація (MFA): впровадження MFA для всіх облікових записів користувачів додає додатковий рівень безпеки для запобігання неавторизованому доступу. Вимагаючи від користувачів надання кількох форм ідентифікації, наприклад пароля та унікального коду підтвердження, MFA ускладнює зловмисникам доступ до ваших систем і даних.

5. Реагування на інциденти та планування відновлення: навіть за наявності найкращих профілактичних заходів можливість кібератаки неможливо повністю усунути. Наявність чітко визначеного плану реагування на інцидент може допомогти підприємствам мінімізувати наслідки атаки та швидко відновитися. Це включає визначення ролей і обов'язків в організації, встановлення каналів зв'язку та розробку дорожньої карти для відновлення роботи.

6. Співпрацюйте та будьте в курсі: кібербезпека є сферою, що швидко розвивається, і бути в курсі останніх загроз і найкращих практик дуже важливо. Співпраця з галузевими партнерами, урядовими установами та експертами з кібербезпеки може допомогти компаніям випереджати нові загрози та впроваджувати найефективніші стратегії захисту своїх цифрових активів.

7. Кіберстрахування. У міру того, як підприємства все більше покладаються на цифрові технології, кіберстрахування стало важливим компонентом управління ризиками. Комплексний поліс кіберстрахування може забезпечити фінансовий захист у разі кібератаки або витоку даних, покриваючи витрати, пов'язані з реагуванням на інциденти, судові збори та потенційні регуляторні штрафи. Кіберстрахування також може допомогти підприємствам отримати доступ до експертних ресурсів для допомоги у реагуванні на інциденти та відновленні.

8. Симуляції атак. Проведення регулярних симуляцій атак, таких як тренування червоної команди та настільні сценарії, може допомогти компаніям виявити слабкі місця в їхній системі кібербезпеки та розробити стратегії їх усунення. Імітуючи атаки в реальному світі, організації можуть краще зрозуміти

свої вразливі місця, оцінити свої можливості реагування на інциденти та підвищити загальну готовність до безпеки.

*Розширення поверхні атак: вплив SaaS, PaaS і хмарних рішень*

Оскільки компанії все більше використовують програмне забезпечення як послугу (SaaS), платформу як послугу (PaaS) і хмарні рішення для оптимізації своїх операцій, поверхня атак розширюється, створюючи нові точки входу для кіберзлочинців. Хоча ці технології пропонують численні переваги, вони також створюють унікальні проблеми безпеки. Щоб зменшити ризики, пов’язані з розширеною поверхнею атаки, компанії повинні інвестувати в надійні заходи безпеки, такі як шифрування даних, контроль доступу та постійний моніторинг хмарних середовищ. Співпраця з постачальниками хмарних послуг також має вирішальне значення для забезпечення узгодженості обох сторін у впровадженні комплексних заходів безпеки.

*Орієнтація на відомі компанії та стартапи*

Кіберзлочинці часто націлюються на компанії, які нещодавно потрапили в заголовки газет, наприклад, стартапи, які отримали значне фінансування. Ці підприємства сприймаються як більш прибуткові цілі через їхній потенціал швидкого зростання та збільшення фінансових ресурсів. Щоб захистити себе, відомі компанії та стартапи повинні з самого початку надавати пріоритет кібербезпеці, включаючи надійні заходи безпеки та політику як невід’ємну частину своєї бізнес-стратегії.

*Зв'язок між кібербезпекою та інноваціями*

Кібербезпека та інновації тісно пов’язані, оскільки сильна позиція кібербезпеки може допомогти захистити та сприяти інноваціям в організації. Захищаючи інтелектуальну власність і конфіденційну інформацію, підприємства можуть підтримувати конкурентоспроможність і продовжувати розробляти передові продукти та послуги. Крім того, інвестиції в кібербезпеку можуть викликати довіру серед клієнтів і партнерів, зміцнюючи репутацію компанії та сприяючи зростанню…

*Боротьба з інсайдерськими загрозами за допомогою заходів кібербезпеки*

Окрім захисту від зовнішніх кібератак, ефективна стратегія кібербезпеки має також боротися з ризиком внутрішніх загроз. Інсайдерські загрози – це інциденти безпеки, які виникають всередині організації, як правило, за участю співробітників, підрядників або сторонніх постачальників. Ці особи можуть мати законний доступ до конфіденційної інформації, систем або засобів, що полегшує для них навмисне чи ненавмисне порушення заходів безпеки.

Щоб зменшити ризик внутрішніх загроз, компанії повинні впровадити комбінацію технічних, процедурних і поведінкових заходів:

1. Контроль і моніторинг доступу: встановіть суворий контроль доступу, який обмежує доступ співробітників до конфіденційної інформації на основі їхніх посадових ролей і принципу найменших привілеїв. Гарантуючи, що працівники мають доступ лише до інформації, необхідної для їхньої роботи, організації можуть мінімізувати ймовірність несанкціонованого доступу або зловживання. Крім того, постійний моніторинг активності користувачів може допомогти виявити підозрілу поведінку та потенційні порушення безпеки в режимі реального часу.

2. Аналітика поведінки користувачів (UBA): інструменти UBA можна використовувати для виявлення ненормальних або підозрілих моделей у поведінці користувачів, таких як несанкціонований доступ до даних або незвичайний час входу. Використовуючи розширену аналітику, машинне навчання та штучний інтелект, UBA може виявляти потенційні внутрішні загрози та сповіщати команди безпеки про вжиття відповідних заходів.

3. Перевірка репутації та перевірка. Проведення ретельних перевірок репутації та процесів перевірки нових співробітників, підрядників і сторонніх постачальників може допомогти виявити потенційні ризики до того, як вони отримають доступ до конфіденційної інформації чи систем. Це включає перевірку стажу роботи, перевірку довідок і, за необхідності, проведення перевірок кримінального минулого.

4. Поінформованість про безпеку та навчання: регулярне навчання співробітників потенційним ризикам, пов’язаним із внутрішніми загрозами, може

сприяти формуванню культури безпеки в організації. Навчання має наголошувати на важливості дотримання політики компанії, повідомлення про підозрілу поведінку та збереження конфіденційності.

5. Підтримка та управління працівниками: невдоволення або стрес співробітників можуть сприяти ймовірності внутрішніх загроз. Надання систем підтримки, таких як програми допомоги працівникам, і підтримання відкритих каналів зв'язку можуть допомогти вирішити будь-які проблеми чи занепокоєння, які можуть виникнути, зменшуючи ризик того, що працівники вдадуться до зловмисних дій.

Підсумовуючи, підприємства, що працюють у цифрову епоху, повинні адаптуватися до складних викликів кібербезпеки, з якими вони стикаються, запровадивши комплексний, багаторівневий підхід до безпеки. Це включає навчання співробітників, регулярні оцінки безпеки, шифрування даних, багатофакторну автентифікацію, планування реагування на інциденти, співпрацю, кіберстрахування та моделювання атак.

Визнаючи розширення площі атаки, пов'язаної з новими технологіями, і потенційну мішень для відомих компаній, компанії можуть краще захистити свої інновації та забезпечити довгостроковий успіх у цифровому середовищі. Крім того, боротьба з внутрішніми загрозами за допомогою поєднання технічних, процедурних і поведінкових заходів може значно підвищити загальну кібербезпеку організації, захищаючи її конфіденційну інформацію та системи як від зовнішніх, так і від внутрішніх джерел». ***(Amit Jaju. Adapting to Complex Cybersecurity Challenges: Strategies for Safeguarding Businesses in the Digital Age // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102irna/adapting-to-complex-cybersecurity-challenges-strategies-for-safeguarding-busines?utm_source=mondaq&utm_medium=syndication&utm_term=Technology&utm_content=articleoriginal&utm_campaign=article). 07.11.2023).***

***

**«Коли ви проводите нове дослідження стану кібербезпеки підприємства, певною мірою ви підтверджуєте припущення та очікування.** Це не менш важлива робота: виявлення правдивості в тенденціях і їх значимості допомагає нам точно їх зважувати й таким чином приймати кращі рішення. Тим не менш, можна з самого початку передбачити, про що повідомлятимуть респонденти: зростання кількості атак; значні збитки, завдані порушеннями фінансово, операційно та репутаційно; і посилення тиску з боку бізнес-лідерів щодо пошуку нових стратегій.

Уявіть наше здивування, коли у звіті Kyndryl про стан IT-ризиків за 2023 рік було виявлено, що 88% керівників IT-рішень впевнені в готовності їхньої організації до збоїв. Насправді 65% оцінили себе як випереджаючих інші організації, і лише 8% сказали, що вони навіть дещо відстають від своїх однолітків у підготовленості.

Такий оптимізм контрастує зі страхом і сумнівами, якими зазвичай керують такі дослідження. Також, зрозуміло, математично неможливо, щоб це було точним відображенням відносного рівня підготовки цих організацій. Наші висновки стають ще більш дивовижними, коли ми зазначаємо, що серед тих самих респондентів 92% повідомили, що зазнали побічної події протягом останніх 24 місяців.

Було б поспішним стверджувати, що це саме по собі є кризою: існує багато нюансів, як технологічних, так і психологічних, у тому, як респондент може оцінити свою довіру до організації, і довіра за своєю суттю не шкодить продуктивності. Однак, враховуючи цілком реальну ймовірність надмірної самовпевненості, що призводить до недостатньої підготовки, варто подумати про деякі з можливих причин цієї невідповідності, які кожен IT-лідер може і повинен визначити та виправити.

*Невідомі невідомі*

Основним кроком для будь-якої стратегії кібербезпеки – і часто одним із найважчих кроків – є залучення та узгодження з бізнесом у цілому. Коротше кажучи, команди безпеки повинні знати та розуміти, що саме вони захищають: найскладніші інструменти та процедури не мають значення, якщо користувачі виконують роботу та обмінюються даними на неконтрольованих платформах.

Нездатність провести вичерпний аудит цифрової нерухомості, залучаючи голоси не-IT-спеціалістів до столу, щоб поділитися основною правдою про операції, може зробити команди надзвичайно впевненими щодо ризиків, які вони знають, і абсолютно сліпі до ризиків, які мають значення. Розмова, яка залучає всі ланки бізнесу на рівних умовах, також допомагає забезпечити цілісне поширення найкращих практик і безпечної поведінки, а не лише серед тих, хто все одно найбільше схильний звертати увагу.

*Неправильна надмірна корекція*

Існує іронічна ймовірність того, що висновок про 92% підприємств, які зазнали несприятливих подій, зовсім не суперечить нашим висновкам щодо впевненості: що, якщо після усунення недоліку, який призвів до порушення, команди в кінцевому підсумку почуватимуться впевненіше, ніж вони були перш ніж щось пішло не так?

Впровадження нового інструменту чи процесу, який гарантує, що нещодавня стресова ситуація не повториться, природно, супроводжується почуттям гордості та полегшення. Однак було б серйозною помилкою навіть несвідомо припускати, що наступна подія буде схожа на попередню. Стати жертвою зловмисного програмного забезпечення цілком може надихнути на нову стратегію захисту від зловмисного програмного забезпечення, але пам’ятайте, що наступною проблемою так само легко може стати атака на відмову в обслуговуванні або внутрішня загроза.

*Реальна внутрішня загроза*

Говорячи про внутрішні загрози, слід зазначити, що IT-команди не застраховані від помилки приділяти більше уваги більш драматичним або захоплюючим загрозам, які існують. Існує причина, чому вигадані історії про кіберзагрози частіше показують інсайдерські атаки чи діяльність національної держави, ніж неправильні конфігурації сервера чи збої в комутаційному обладнанні мережі.

Проте проста правда полягає в тому, що більшість несприятливих подій не виникають через навмисні напади. Такі речі, як збої в центрі обробки даних і

невдалі оновлення програмного забезпечення, можуть відчуватися по-іншому на емоційному рівні, але з точки зору стійкості бізнесу їхній вплив на продуктивність, репутацію та дохід абсолютно схожий на події в кібербезпеці. У нашому опитуванні шостою найпоширенішою причиною подій була просто «людська помилка»: якщо такі речі чітко не враховані, ваша впевненість може бути марною.

*Прийняття критичного погляду*

Нарешті, ми повинні визнати, що наші респонденти працюють день у день у контексті, який заохочує почуття впевненості. У середовищі, де все більше керується показниками, легко отримати інформаційні панелі, наповнені статистичними даними, які з гордістю повідомляють про стан працездатності платформ безпеки: 99% систем виправлено протягом тижня, 99% кінцевих точок охоплено рішеннями для захисту від зловмисного програмного забезпечення тощо.

Для багатьох сфер IT оцінка 99% за показником буде розглядатися як відмінна продуктивність. Однак для відмовостійкості справді важливий 1%: кожна сотня систем не виправлена, кожна сотня кінцевих точок відкрита. Навчитися сприймати критичний погляд, навіть коли всі системи, здається, звітують зелено, є життєво важливою – і занадто часто нею – навичкою.

*Коли впевненість стає надмірною?*

Як я вже згадував раніше, впевненість — це не обов'язково погано. Організації повинні прагнути до такого стану, коли вони знають, що неминучі майбутні збої є те, що можна відновити, і добре розроблена стратегія кібербезпеки може досягти цієї мети.

Однак людині властиво помилятися, як і схильність віддавати перевагу втішній інформації над правдивою. Якщо ви належите до тих 65%, які вважають себе лідерами у сфері готовності до кібербезпеки, можливо, настав час переглянути ваші попередні знання або навіть залучити незалежну точку зору, щоб зробити це за вас». ***(Duncan Bradley. Should cybersecurity overconfidence be on your threat radar? // yahoo! finance (https://finance.yahoo.com/news/cybersecurity-overconfidence-threat-radar-152215225.html?fr=sycsrp_catchall). 10.11.2023).***

***

**«Багато компаній вважають працівників своїм найбільшим слабким місцем, коли йдеться про кібербезпеку.** Це пов’язано з тим, що зазвичай для успіху зловмисників все ще покладаються на соціальну інженерію, яка змушує користувачів виконувати дії, яких вони не повинні виконувати, зокрема такі ризиковані дії, як відкриття підозрілих вкладень електронної пошти та натискання посилань.

Але хоча компанії швидко звинувачують користувачів, коли щось йде не так, у сучасному бізнесі необхідна культура спільної безпеки. Такий, у якому IT-відділи та відділи безпеки працюють разом з користувачами, щоб забезпечити безпечне середовище для співробітників, щоб вони могли виконувати свою роботу. Зважаючи на те, що складні загрози постійно розвиваються, навчання з питань безпеки не є надійним.

*Ви не можете виправити поведінку користувача*

Майже будь-яка робота сьогодні вимагає від користувачів комп’ютера, який зазвичай надається роботодавцем. І хоча компанії просять їх не натискати нічого «ризикованого», це часто необхідно для виконання їх повсякденної ролі. У таких галузях, як фінанси, рахунки-фактури потрібно надсилати у вигляді PDF-електронною поштою додатків для обробки. Отже, чому слід звинувачувати працівників у відкритті «не того» PDF? Якщо кінцевим користувачам потрібно клацати та відкривати файли, щоб виконувати свою роботу, нереалістично очікувати, що вони будуть кіберекспертами, які можуть виявити кожну частину шкідливого вмісту, перш ніж клацнути, особливо з урахуванням деяких переконливих фішингових атак, націлених на них сьогодні.

Це означає, що всебічна освіта з питань безпеки та навчальні програми мають вирішальне значення. Користувачів потрібно навчити, як розпізнавати підозрілі електронні листи, включно з тим, як дивитися не лише на ім’я того, хто надіслав електронний лист, а натомість на структуру доменного імені для електронної адреси.

Однак у зв’язку з останнім зростанням кількості викрадення потоків користувачам також слід остерігатися вмісту з надійних джерел. Коли вони отримують електронний лист від когось внутрішнього або від зовнішньої компанії, з якою вони працювали, їм потрібно подумати; чи релевантний електронний лист у контексті ланцюжка електронних листів? Або вкладення електронної пошти не відображаються належним чином? Якщо так, це може бути червоним прапором.

Наприклад, під час нещодавньої атаки, проаналізованої HP Wolf Security, зловмисники скомпрометували користувача, який увійшов у Outlook для Інтернету. Потім зловмисники використовували цю скомпрометовану адресу, щоб поширювати шкідливі файли Word під виглядом фінансових документів по всій організації. Оскільки файли надійшли з організації, більша ймовірність того, що працівники довірятимуть цьому.

Компанії можуть виправляти IT-системи, але неможливо виправити поведінку користувачів. І кіберзлочинці продовжують використовувати це, незважаючи на те, що компанії регулярно проводять тести на фішинг. Кожен робить помилки, і щоб ініціювати порушення, потрібно лише один клік користувача.

Як і здоров’я та безпека на робочому місці, кібербезпека є колективною відповідальністю. Кожен має зіграти свою роль. Хоча освіта важлива для зменшення ризику клацання користувачами, компаніям настав час припинити покладатися лише на навчання безпеки та звинувачувати користувачів у тому, що вони не можуть помітити загрози. Натомість організації повинні використовувати належні технології та стратегії для захисту користувачів, які перебувають на передовій у кібервійні. Це можна зробити, реалізувавши три ключові стратегії:

1. Застосування NGAV як перший крок

По-перше, бізнесу потрібен хороший захист. На щастя, у цьому просторі є багато чудових продавців. Але хоча антивірус (AV) або антивірус наступного покоління (NGAV) є хорошим місцем для початку, однієї цієї технології недостатньо для захисту від сучасних кіберзагроз.

Насправді більшість організацій, які постраждали від атаки програм-вимагачів чи іншого злому, використовували AV на вражених пристроях. Якби одних лише AV або NGAV було достатньо, порушень більше не було б. Належним чином реалізований якісний інструмент NGAV – це лише перший крок.

2. Знання – це сила

Організаціям потрібна видимість програм, які працюють на пристроях співробітників, і того, як вони поводяться. Для цього потрібен хороший інструмент видимості, який часто має форму виявлення кінцевої точки та відповіді (EDR) або розширеного виявлення та відповіді (XDR).

Наприклад, користувач може завантажити новий файл.exe, який починає зчитувати файли з папки OneDrive користувача та завантажувати їх на сервер в іншій країні, що свідчить про викрадення даних користувача. У цьому випадку антивірусний інструмент пропустив зловмисне програмне забезпечення та запустив поганий виконуваний файл. Але компанії з хорошими інструментами видимості можуть помітити цю незвичну поведінку та зменшити будь-які потенційні ризики.

Хоча традиційно інструменти EDR та XDR були дорогими та трудомісткими для впровадження, завдяки потужності хмари зі штучним інтелектом та машинним навчанням ці інструменти стають ефективнішими. Однак подібно до того, як AV-інструменти не можуть належним чином виявити всі шкідливі програми, інструменти видимості також не вловлять усе вчасно, перш ніж станеться серйозна шкода.

3. Ізоляція проблеми

Щоб значно зменшити загрозу, з якою стикаються кінцеві користувачі, організації повинні запровадити технологію ізоляції разом із засобами захисту та видимості. Існує два ключових підходи до реалізації та запуску ізоляційних контейнерів: у хмарі та на пристрої. Завдяки підходу на пристрої контейнер працює локально на пристрої користувача та використовує можливості апаратної віртуалізації для ізоляції контейнера від вашої ОС Windows і внутрішньої мережі.

Використовуючи апаратні контейнери ізоляції, підприємства можуть використовувати технологію ізоляції, щоб створити віртуальну мережу безпеки для

кінцевих користувачів, щоб захистити їх, коли вони натискають на вміст високого ризику. Це може бути вкладення електронної пошти, файл, завантажений з Інтернету, файл, відкритий на USB-накопичувачі, або посилання на веб-сайт, на яке натиснув користувач. Якщо вміст виявляється зловмисним, зловмисне програмне забезпечення ізольовано всередині контейнера та не може завдати шкоди ПК користувача чи вашій внутрішній мережі.

*Захистіть своїх кінцевих користувачів*

Організації повинні почати будувати культуру безпеки, що ґрунтується на більшій співпраці, коли вони влаштуються в майбутнє гібридної роботи. Але незважаючи на це, вони повинні бути готові до того, що більшість користувачів зрештою клацатимуть те, що їм не слід.

Щоб захистити користувачів, дуже важливо, щоб IT- та кіберпрофесіонали також використовували багаторівневий підхід, починаючи з кінцевої точки з вбудованою безпекою, а також були якомога менш помітними, щоб уникнути спроб кінцевих користувачів обійти її. Це дасть співробітникам інструменти та системи, необхідні для безпечного виконання їх роботи – замість того, щоб звинувачувати їх у порушеннях, які вони не можуть контролювати!» ***(Dan Allen. Three strategies to protect users from cyberattacks // Future US, Inc. (https://www.techradar.com/pro/three-strategies-to-protect-users-from-cyberattacks). 13.11.2023).***

***

**«… Жодна організація не застрахована від небезпеки кібератак.**

Тому організаціям необхідно відійти від вузької уваги до захисту своїх цифрових просторів і перейти до більш комплексної та стійкої стратегії.

Поки ми очікуємо завершення розробки законопроекту Намібії про кіберзлочинність, ми повинні разом старанно працювати над досягненням цілей, зазначених у Національній стратегії кібербезпеки та Плані підвищення обізнаності на 2022-2023 роки, відповідно під назвою «Крок до кіберстійкості та цифрової безпеки».

Головною метою цієї стратегії є створення безпечного онлайн-середовища, яке стимулює творчість і сприяє соціальному та економічному розвитку Намібії.

Щоб реалізувати це бачення, організації повинні взяти на себе зобов'язання посилити свою політику кібербезпеки та впровадити надійні технічні засоби захисту своїх систем, мереж, пристроїв, програм і веб-сайтів.

Крім того, для зміцнення кібербезпеки цих організацій необхідно запровадити сувору та послідовну програму навчання та кампаній з підвищення обізнаності.

Важливо, що обізнаність у кібербезпеці тепер є базовою грамотністю, якою повинні володіти всі цифрові громадяни – це більше не є виключною сферою технічних експертів.

Крім того, кожна організація відіграє вирішальну роль у підвищенні загальної стійкості кібербезпеки країни.

Це означає, що політики кібербезпеки повинні суворо дотримуватися на всіх організаційних рівнях, а їх ефективність повинна систематично оцінюватися.

Настав час переглянути наш підхід до інвестицій у кібербезпеку, як влучно зазначено в темі сьомого Саміту з інформаційних та комунікаційних технологій (ІКТ) у 2023 році.

Щоб захистити цифрову економіку та скористатися її можливостями, нам потрібно переоцінити наші стратегії.

Крім того, через постійні зміни характеру цифрової безпеки Намібії зараз терміново потрібно створити національний центр кібербезпеки на додаток до національної групи реагування на інциденти комп'ютерної безпеки.

Місія центру кібербезпеки буде багатогранною, охоплюючи як технічні, так і управлінські аспекти кібербезпеки, з основним акцентом на захист критично важливої національної інфраструктури ІКТ Намібії та зміцнення цілісності мереж країни.

Метою цієї ініціативи є зміцнення стійкості цифрової екосистеми нашої країни та активна боротьба з появою кіберзагроз.

Підсумовуючи, очікується, що організації вдосконалюватимуться, змінюватимуться та адаптуватимуться до середовища кібербезпеки, що швидко розвивається, як розпорядники критичних цифрових активів і конфіденційних даних…» ***(Iyaloo Wainganjo. Embracing Collective Responsibility: A Paradigm Shift in Cybersecurity // The Namibian (https://www.namibian.com.na/embracing-collective-responsibility-a-paradigm-shift-in-cybersecurity/). 11.11.2023).***

***

**«Мало що так важливо для малого бізнесу, як кібербезпека. У 2020 році через витоки даних було виявлено 155,8 мільйонів конфіденційних записів, і оскільки компанії все більше покладаються на цифрові технології, ці порушення стають більш імовірними.** З огляду на ці загрози, управління ризиками кібербезпеки є обов'язковим.

*Що таке управління ризиками кібербезпеки?*

Управління ризиками кібербезпеки – це практика виявлення ризиків і планування захисту. Хоча практично кожен бізнес стикається з загрозами кібербезпеці, що саме вони представляють і наскільки кожен тип відповідний, може відрізнятися. Цей процес має на меті допомогти вашій компанії адаптувати свої стратегії кібербезпеки відповідно до вашої унікальної ситуації.

*Які переваги управління ризиками кібербезпеки?*

Управління ризиками кібербезпеки має кілька переваг. Оскільки останні дані показують, що 43% кібератак спрямовані на малий бізнес, важко не помітити переваги.

Наявність більш надійної стратегії кібербезпеки також може покращити репутацію вашого бізнесу. Потенційні партнери та клієнти оцінять акцент на безпеці, що сприяє підвищенню лояльності та, отже, прибутку.

*Як розрахувати ризик кібербезпеки*

Ефективне управління ризиками кібербезпеки починається з оцінки того, які загрози є найбільш актуальними для вашого бізнесу. Щоб виявити їх, компанії зазвичай дотримуються цього рівняння:

Ризик = Вплив атаки х Ймовірність атаки

Це рівняння є досить відкритим, оскільки кожна його сторона може містити багато змінних, деякі з яких легко визначити кількісно, а інші – ні. Отже, визначення ризику не завжди є точною наукою, але воно дає корисну відправну точку. ІТ-відділи та фахівці з безпеки повинні мати можливість принаймні оцінити, наскільки ймовірними та шкідливими можуть бути різні типи атак.

*Структури управління ризиками кібербезпеки*

У той час як визначення кіберризику залишає простір для тлумачення, кілька загальноприйнятих структур забезпечують більш простий шлях. Це стандарти, які різні організації встановили, щоб керувати ними цим процесом. Стандарти часто включають конкретні методи для вимірювання загроз, визначення пріоритетів кіберзахисту, впровадження цих засобів контролю та оцінювання зрілості кібербезпеки.

Деякі компанії розробляють власні рамки, але дотримання попередньо встановленої може бути корисним для вашого бізнесу. Оскільки ці стандарти походять від галузевих органів влади, дотримання їх може допомогти вам встановити довіру з потенційними партнерами чи клієнтами. Це чотири найпоширеніші системи управління ризиками.

1. NIST CSF

Мабуть, найпопулярнішою структурою управління ризиками є кібербезпека (CSF) Національного інституту стандартів і технологій (NIST). NIST CSF складається з трьох основних компонентів:

| | |
|---|---|
| Ядро | Ядро окреслює бажані результати кібербезпеки. |
| Рівні впровадження | Рівні реалізації організовують практики в кілька рівнів, що представляють багато рівнів безпеки. |
| Профілі | Профілі пропонують конкретні шляхи отримання основних результатів у списку відповідно до бажаного рівня організації та інших унікальних міркувань. |

2. ISO

Міжнародна організація стандартизації (ISO) надає більше ніж одну структуру для управління ризиками кібербезпеки. Першим і найбільш актуальним є ISO/ISE 27000, який охоплює понад дюжину стандартів для пошуку та управління загрозами кібербезпеці.

ISO також керує стандартом ISO 31000. ISO 31000 — це не конкретний стандарт кібербезпеки, а загальна структура управління бізнес-ризиками, яка включає управління кіберризиками. Розгляньте цю структуру, якщо ваша компанія стикається з різними загрозами, окрім кіберзлочинності.

3. Міністерство оборони США

Структура управління ризиками (RMF) Міністерства оборони (DoD) – це набір стандартів, більш специфічних для галузі. Як випливає з назви, цю структуру використовує Міністерство оборони для оцінки та усунення своїх загроз кібербезпеці та захисту. Він включає суворі стандарти, розбиті на ці шість кроків:

Класифікуйте

Виберіть

Реалізувати

Оцінити

Авторизувати

Монітор

Міністерство оборони вимагає управління ризиками на більшості рівнів сертифікації моделі зрілості кібербезпеки. департаменту CMMC поширюється на всіх понад 300 000 підрядників.

Незважаючи на те, що ця структура розроблена для підрядників Міністерства оборони, вам не обов’язково працювати в оборонній промисловості, щоб скористатися нею. Його високі стандарти та конкретні вказівки роблять його ідеальним для будь-якої компанії.

4. СПРАВЕДЛИВИЙ

Структура факторного аналізу інформаційних ризиків (FAIR) спрямована на поширення обізнаності та дії щодо інформаційних ризиків. Багато лідерів галузі в

усьому світі дотримуються цих стандартів. Окрім надання вказівок для підприємств, FAIR співпрацює з університетами, щоб привернути увагу до освіти з кібербезпеки.

FAIR стверджує, що пропонує більш чіткі та кількісно визначені вказівки щодо управління ризиками кібербезпеки, ніж інші структури. Він прагне вдосконалити управління ризиками в чотирьох категоріях: люди, процеси, технології та політика.

*Найкращі практики для нагляду за управлінням ризиками кібербезпеки*

Незалежно від того, яку структуру ви використовуєте для своєї організації, є кілька речей, які слід враховувати під час управління ризиками кібербезпеки. Незважаючи на те, що процес виглядатиме по-різному для кожного бізнесу, деякі кроки, практики та міркування залишаються незмінними в усіх середовищах. Ці константи можуть служити дорожньою картою для вирішення змінних, які виникають у процесі.

Загалом, управління ризиками починається зі збору й упорядкування інформації про мережі, ваших користувачів, минулі інциденти та подібні порушення компаній. Звідти ви можете ідентифікувати та ранжувати відповідні загрози, а також визначити відповідні відповіді.

Коли ваша компанія починає цей процес, пам’ятайте про ці 10 найкращих практик:

1. Цільові внутрішні загрози.

Легко зосередитися на зовнішніх загрозах, таких як хакери та зловмисне програмне забезпечення, але це не єдині ризики, з якими зіткнеться ваш бізнес. Насправді внутрішні загрози часто важливіші, ніж загрози ззовні вашої організації. Дослідження показують, що ці внутрішні загрози зросли на 31% за останні два роки, втративши 11,45 мільйонів доларів.

Ці загрози часто походять не від зловмисників, а скоріше від незнання чи самовдоволення. Будь-яка ефективна стратегія управління ризиками повинна вирішувати це. Ретельніше навчання працівників кібербезпеці, жорсткіший

контроль доступу та подібні кроки можуть допомогти пом’якшити ці внутрішні загрози.

2. Пріоритезуйте ризики.

В ідеалі ваш бізнес міг би захиститися від усіх можливих загроз, але це нереалістичне очікування. Обмежені бюджети, час і персонал унеможливлюють вирішення кожного ризику однаковою мірою. У результаті, визначивши, з якими загрозами стикається ваша компанія, ви повинні визначити їх пріоритетність за терміновістю.

Найкраще приділяти найбільше часу та ресурсів тим ризикам, які найбільше стосуються вашої фірми. Ось чому наведене вище рівняння настільки важливе: ви повинні розуміти потенційно шкідливі загрози, щоб знати, що заслуговує їхньої негайної уваги. Після створення засобів захисту від цих ризиків можна переходити до менш пріоритетних елементів.

3. Встановіть ефективні канали зв'язку.

Однією з найважливіших – але легко пропущених – частин управління ризиками кібербезпеки є обмін інформацією. Оскільки загрози можуть надходити звідки завгодно, усі відділи, команди та співробітники повинні їх розуміти. Вашій IT-службі має бути легко попередити різних працівників про ризики, з якими вони можуть зіткнутися, щоб вони могли їх уникнути.

Це спілкування працює в обох напрямках. Ви повинні встановити канали, які дозволять співробітникам повідомляти про будь-які потенційні ризики, які вони помічають. Це дозволить вашим співробітникам зупинити більше порушень і пом’якшити вплив тих, які все-таки проникнуть.

4. Увімкніть постійний моніторинг.

Іншим важливим аспектом управління ризиками є постійний моніторинг. Ваша IT-команда не зможе точно визначити ризики та їх причини, якщо у них немає детальних і точних журналів того, що відбувається в мережі. Так само, якщо цей облік не ведеться безперервно, ваша команда може не виявити кібератак, доки не стане надто пізно.

Більшість організацій не мають персоналу для моніторингу своїх мереж вручну, але програмні рішення можуть автоматизувати цей процес. Деякі програми шукають злами, деякі шукають незвичайну активність користувачів, інші шукають неактивне шкідливе програмне забезпечення. Незалежно від того, що передбачає ваша ситуація, ви, ймовірно, знайдете програмне забезпечення для моніторингу, яке відповідає вашим потребам.

5. Дотримуйтеся встановленої системи кібербезпеки.

Навіть після аналізу ризиків, з якими стикається ваш бізнес, не завжди стає зрозумілим, як з ними боротися. Звернення до встановлених структур кібербезпеки може дати певні вказівки в цій сфері.

Так само, як існують рекомендації щодо управління ризиками, кілька організацій публікують загальні рамки кібербезпеки. NIST, ISO та Center for Internet Security (CIS) – усі чудові місця для початку. Ви не обов'язково дотримуєтеся всіх правил цих інструкцій, але вони можуть стати корисною відправною точкою.

6. Розробіть план реагування на інцидент.

Кожна стратегія управління ризиками кібербезпеки повинна містити план реагування на інциденти. Цей план має бути якомога детальнішим, включно з кількома кроками, до яких можна повернутися, якщо одна відповідь не дасть результату.

Стримування кібератак – питання, чутливе до часу. Ваш бізнес не може дозволити собі чекати, поки з'явиться загроза, щоб визначити, як з нею впоратися. Кожен ризик потребує відповідного плану реагування. Кодування та реєстрація цих планів гарантує, що майбутні команди зможуть дотримуватися їх після того, як працівники, які їх написали, залишать вашу компанію.

7. Забезпечення безперервності бізнесу.

У цьому ж ключі стратегії управління ризиками також повинні включати план безперервності. Нереалістично думати, що витік даних ніколи не відбудеться, тому вам знадобиться резервний план, щоб залишатися функціональним у

надзвичайних ситуаціях. План безперервності забезпечить доступ до критично важливих систем, поки експерти з безпеки справляються з втратою даних.

Ваш план безперервності бізнесу може виглядати по-різному. Однак загалом вони включають стратегії стримування, резервне копіювання критично важливих даних і послуг, а також надійні канали зв'язку.

8. Розгляньте можливість страхування відповідальності за кібербезпеку.

Страхування відповідальності може бути хорошим варіантом, оскільки жодна стратегія кібербезпеки не є надійною. Це може допомогти зменшити різні витрати, пов'язані з витоком даних, зокрема кредитний моніторинг, сповіщення постраждалих сторін, регуляторні штрафи та судові позови. Індустрія кіберстрахування зросла, оскільки кіберзлочинність стає все більш поширеною.

Багато провідних постачальників страхування відповідальності бізнесу пропонують так зване кіберстрахування. У середньому ці плани коштують 124 долари на місяць. Провідні страхові компанії, такі як Chubb і AIG, пропонують кіберстрахування.

Немає однозначної відповіді на питання, яке найкраще страхування кібервідповідальності. Враховуйте свої потреби та бюджет, щоб знайти постачальника та план, який найкраще відповідає вашим потребам.

9. Культивуйте культуру кібербезпеки.

Пам'ятати про кібербезпеку – це відповідальність кожного на вашому сучасному робочому місці. Загрози можуть надходити звідки завгодно, тому кожен працівник повинен робити все можливе, щоб запобігти їм. Управління ризиками кібербезпеки має бути центральною частиною культури вашої компанії.

Культивування культури кібербезпеки починається з освіти. Усі працівники повинні знати, звідки можуть виникнути ризики та які методи можуть їм запобігти. Керівники повинні показувати приклад і визнавати гідну подиву поведінку, щоб заохотити більше уваги до безпеки.

10. Регулярно переоцінюйте кіберризики.

Кібербезпека – це постійний процес. Кіберзлочинці постійно знаходять нові способи обійти популярні засоби захисту, тому стратегії безпеки також повинні

адаптуватися до цих нових загроз. Управління ризиками повинно бути регулярним явищем, коли команди проводять оцінку кожні кілька років, якщо не щорічно.

Тестування на проникнення, коли спеціалісти з безпеки намагаються зламати мережу, щоб виявити її вразливі місця, може допомогти забезпечити постійну безпеку. Ця інформація може виявити загрози та рішення, які були упущені під час початкової оцінки управління ризиками. Хоча жодна система не є досконалою, впровадження культури постійного вдосконалення може гарантувати, що захист залишатиметься максимально оновленим.

*Управління ризиками кібербезпеки має вирішальне значення для будь-якого бізнесу*

Кібербезпека стала важливою, оскільки цифрові технології та дані стають все більш важливими для роботи вашого бізнесу. Дотримання кроків з управління ризиками дасть вашій компанії ефективні стратегії безпеки. Без цього процесу ви можете зіткнутися з тривалим збитком від витоку даних». ***(Shannon Flynn. Cybersecurity and Risk Management // Business.com (https://www.business.com/insurance/cybersecurity-risk-management/). 07.11.2023).***

***

**«В офіційному звіті Cybersecurity Ventures про вакансії в сфері кібербезпеки за квітень 2023 року, спонсорованому компанією eSentire, повідомлялося, що кількість незаповнених вакансій у сфері кібербезпеки вирівнялася у 2022 році та залишилася на рівні 3,5 мільйона у 2023 році, причому понад 750 000 із цих вакансій у США.**

Важливо зазначити, що з мого особистого досвіду є багато відкритих вакансій для досвідчених фахівців з кібербезпеки. Тим не менш, деяка золота лихоманка для вивчення кібербезпеки породила багато людей початкового рівня або недосвідчених, яких компанії не обов’язково шукають.

Перш ніж приступити до кібербезпеки, майте на увазі, що спроба ввійти в кібербезпеку буде однією з найскладніших частин початку вашої кар’єри, і це має бути основним напрямком у всьому, що ви робите, коли вивчаєте тонкощі

кібербезпеки. Це означає, що вам потрібно спілкуватися з усіма, кого ви зустрічаєте, і шукати наставників, які можуть навчити вас і допомогти відкрити двері, коли ви будете готові.

Зважаючи на це, все ще є способи виділитися з натовпу, і потреба в досвідчених, обізнаних і надійних зірках кібербезпеки буде тільки зростати в міру розвитку штучного інтелекту та інших нових технологій, з'являючи нові загрози та вразливості.

Є два основні шляхи, якими ви можете скористатися на шляху до отримання знань і досвіду з кібербезпеки. Традиційний підхід полягає в тому, щоб отримати ступінь бакалавра або навіть аспірантуру з кібербезпеки, а інший – зосередитися на престижних сертифікатах.

Багато успішних кандидатів, які хочуть розпочати роботу в сфері кібербезпеки, іноді поєднують обидва. Які плюси та мінуси кожного варіанту? Чи варто робити те й інше одночасно і як це зробити ефективно? Давайте поглянемо.

*Чи варто мені йти до школи на кібербезпеку?*

Зараз в університетах по всій країні існують сотні програм з кібербезпеки. USNews має список найкращих студентських програм з кібербезпеки, що є хорошою відправною точкою, але для більшості людей ці школи будуть недоступні. Деякі з найкращих історій успіху, про які я чув, походять від місцевих університетів, які зосереджені на технологіях, подібно до Університету передових технологій в Арізоні.

Найкращий спосіб дізнатися про чудові шкільні програми у вашому регіоні – зв'язатися з фахівцями з кібербезпеки у ваших особистих колах або на LinkedIn і запитати, які школи вони б порекомендували.

Ще одна дискусійна тема: онлайн чи особисті програми кращі. Я вважаю, що для досягнення успіху в кібербезпеці це має стати стилем життя, хобі та одержимістю, тому що потрібен такий рівень відданості, щоб досягти успіху в цій галузі та мати можливість боротися з виснаженням, коли ви нарешті опинитеся в ній. двері.

З огляду на це, на мій погляд, якщо у ваших силах піти на особисту програму, де ви зможете пройти заняття з групою людей, познайомитися та налагодити контакти зі своїми викладачами, а також навчитися не просто навчальна програма, представлена в матеріалах курсу, це буде величезною перевагою. Таке навчання є складним для онлайн-курсів, оскільки більшість людей, у тому числі професори, вписують ці курси в інші свої обов'язки.

*Чи корисні онлайн-класи для вивчення кібербезпеки?*

Онлайн-курси можуть працювати, якщо відвідати очну програму неможливо. Я вважаю, що найкращі онлайн-курси зосереджені на отриманні сертифікатів, як-от у Western Governors University. Кожен курс, який ви відвідуєте, навчатиме вас проходженню корисної та цінної сертифікації, яка може перетворитися на реальні пропозиції роботи. Кілька інших університетів пропонують подібні типи занять, але якщо ви збираєтеся навчатися в галузі кібербезпеки, отримання ступеня, який допоможе вам отримати сертифікати під час навчання, є величезним бонусом.

Ви також можете триматися подалі від навчальних таборів з кібербезпеки. Хоча вони можуть бути чудовим місцем для початку та початку вашої подорожі, для більшості роботодавців вони насправді не дорівнюють корисному досвіду чи навчанню.

Останнє слово про те, як ходити до школи, щоб вчитися. Це класичний шлях, і, безсумнівно, є компанії, які не візьмуть на роботу претендента, якщо він не має ступеня бакалавра. Однак вартість ступеню бакалавра в Сполучених Штатах різко зросла, і з огляду на такі високі процентні ставки, будьте дуже обережні, беручи позики на ступінь, яким ви не впевнені, чи збираєтеся в кінцевому підсумку скористатися. Зазвичай розумніше розпочати навчання для отримання сертифіката початкового рівня, переглядаючи відео на YouTube із таких каналів, як John Hammond, David Bombal або Professor Messer, щоб побачити, чи справді ця сфера вам подобається.

*Які найкращі сертифікати, щоб почати роботу з кібербезпеки?*

Майже загальновизнаним найкращим місцем для початку вашої сертифікаційної подорожі є CompTIA. Вони пропонують визнані галуззю

сертифікації, які є поглибленими, оновленими та досить складними, щоб, якщо ви можете отримати сертифікат, це продемонструвало роботодавцям, що ви добре розумієте цю концепцію.

Якщо ви новачок у комп'ютерній безпеці, важливо мати міцну основу для роботи в мережі. З цієї причини було б чудовою ідеєю спочатку отримати сертифікацію CompTIA Network+. Якщо ви є сертифікованим мережевим гуру і можете назвати кожен порт і його функцію, а також пояснити кожен рівень моделі OSI та як вони використовуються, тоді ви можете почати навчання для сертифікації CompTIA Security +. Ця сертифікація є базовою для більшості компаній. Мені сказали, що більшість державних підрядників із допуском безпеки вимагатимуть цього сертифікату для найму кандидата.

Отримавши цю базову лінію, ви повинні вирішити, куди ви хочете рухатися в кібербезпеці. Червона команда, або тестувальники проникнення, є найвідомішою групою, яка втілює в життя фантазії хакерів, але на кожного члена червоної команди припадає десятки синіх команд або захисників. У синій команді є аналітики центру безпеки (SOC), мисливці за загрозами, служби реагування на інциденти та аналітики управління вразливістю. Ці люди фактично займаються повсякденним захистом організації. Тим не менш, ціла група інженерів повинна налаштувати брандмауери, написати код для належного сповіщення та налаштувати безпеку на кожному рівні інфраструктури компанії.

Справжнє питання, яке вам потрібно задати, чи хочете ви бути тестувальником проникнення? Якщо ні, чи хочете ви бути аналітиком, що займається реальними загрозами, чи інженером, що розробляє серверну безпеку та інфраструктуру? Ознайомившись із цими питаннями, ви зможете більше зосередитися на тому, які сертифікати вам знадобляться. Indeed.com склав список деяких найпопулярніших сертифікатів і те, як вони можуть допомогти вам у вашій кар'єрі.

*Скільки заробляють фахівці з кібербезпеки?*

Salary.com стверджує, що середня зарплата спеціаліста з кібербезпеки початкового рівня становить 99 164 долари США. Це може значно коливатися

залежно від того, у якому стані ви перебуваєте, а також підвищуватиметься для інженерів і більш досвідчених аналітиків. Кібербезпека — це чудова галузь. Тим не менш, оскільки все більше шкіл і організацій звертаються до монетизації викладання кібербезпеки та реклами позитивних сторін галузі, існує потік людей, які біжать, щоб навчитися навичкам професії…» ***(Colton Stradling. How to get started in cybersecurity: The best tips from a seasoned professional // Future US, Inc. (https://www.windowscentral.com/software-apps/how-to-get-started-in-cybersecurity). 10.11.2023).***

***

**«У новому звіті Fastly стверджується, що компанії платять величезну ціну за те, що вони не захищають належним чином свої цифрові активи.**

Після опитування майже 1500 ключових IT-керівників у всьому світі компанія Fastly виявила, що протягом минулого року компанії зазнавали в середньому 46 атак, що призвело до втрати 9% річного доходу.

Але є й інші способи, якими кібератаки завдають шкоди цим підприємствам: збої в мережі (34%), втрата даних (29%), веб-додатки залишаються в автономному режимі (24%), компрометація облікових записів клієнтів (22%) також є результатами витоку даних, і ці може ще більше зашкодити бізнесу.

*Хронічна нестача талантів*

Щоб вирішити цю проблему, багато компаній повертаються до креслярської дошки. Три чверті (76%) навіть планують витрачати більше на кібербезпеку. Однак це не обов’язково означає більш безпечне середовище. Фактично, третина (35%) вважає, що їх фірма витратила занадто багато на інструменти кібербезпеки за останній рік (на відміну від 18%, які хотіли б бачити більші бюджети). Ті, хто виступає проти збільшення витрат, стверджують, що лише 55% закуплених інструментів безпеки повністю розгортаються.

Фірмам також важко знайти відповідних кадрів. Майже третина (30%) респондентів вважає, що проблеми, з якими вони зіткнулися протягом останніх 12 місяців, пов’язані з хронічною нестачею талантів. Більше того, 33% очікують, що

це продовжиться в найближчі місяці. Половина (46%) вважає, що їхнім працівникам бракує досвіду протидії загрозам, третина (36%) вважає, що вони не мають навичок або нездатні працювати в масштабах. Майже половина (47%) намагається залучити більше талантів, здебільшого за рахунок збільшення бюджету.

Багато респондентів (51%) бачать рішення в інструментах Generative AI і планують інвестувати в них і далі протягом наступних двох років. Третина (37%) також зосереджена на безпеці штучного інтелекту». ***(Sead Fadilpašić. Businesses are losing huge chunks of their revenue to cyberattacks // Future US, Inc. (https://www.techradar.com/pro/security/businesses-are-losing-huge-chunks-of-their-revenue-to-cyberattacks?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 16.11.2023).***

***

**«За останні роки середовище кібербезпеки суттєво трансформувалося завдяки прийняттю більш суворих правил.** Оскільки хакери з кожним днем стають все більш досвідченими та зухвалими, уряди та регулятори в усьому світі вживають профілактичних заходів для захисту як громадян, так і компаній.

Після революційного Загального регламенту захисту даних (GDPR) ЄС у 2018 році ми стали свідками того, як США і навіть НАТО просуваються вперед у війні проти кіберзлочинців. Для генеральних директорів розуміння та адаптація до цього ландшафту, що розвивається, є не просто питанням відповідності, а стратегічним імперативом.

*Динаміка сучасного регулювання кібербезпеки*

Правила стали складнішими та суворішими у відповідь на зростання загроз. Яскравим прикладом є минулорічні правила кібербезпеки SEC, які зобов’язують публічні компанії оприлюднювати вичерпну інформацію про свої ризики кібербезпеки та стратегії їх пом’якшення. Крім того, ці правила також виступають за активну участь генеральних директорів у нагляді за політикою кібербезпеки. Це

означає зміну парадигми в бік більш проактивного та пильного підходу до захисту активів компанії.

Виконавчі директори також повинні визнати, що правила кібербезпеки відрізняються від однієї країни до іншої. Залежно від фізичного положення своїх клієнтів підприємствам, можливо, доведеться дотримуватися кількох правил. Взяти, наприклад, GDPR ЄС. Це одне з найсуворіших правил кібербезпеки в усьому світі, яке застосовується до будь-якої організації, яка обробляє персональні дані громадян ЄС. Уявіть собі, що бізнес обслуговує США, Європу та Індію, а також правила кібербезпеки SEC і GDPR, національна стратегія кібербезпеки США, індійський законопроект про конфіденційність даних і багато іншого вимагають від генеральних директорів володіти глибокими знаннями конкретних правил, що застосовуються до даних. вони обробляють.

Штрафи – лише верхівка айсберга з точки зору фінансових наслідків невиконання. Судові витрати, судово-медичні розслідування та потенційні судові позови можуть мати великі втрати. Візьмемо як приклад GDPR. Порушення суворих правил захисту даних може призвести до штрафів у розмірі 4% від загального доходу компанії або 20 мільйонів євро, залежно від того, що більше. Це яскраве нагадування про те, що недотримання вимог може мати серйозні фінансові наслідки та потенційно завдати шкоди навіть найбільшим корпораціям. Крім того, існує менш відчутна, але однаково значна вартість втрачених можливостей і частки ринку, оскільки клієнти переходять до конкурентів, яких вони вважають більш безпечними.

Крім фінансових наслідків, репутація є ще однією валютою, яку жоден генеральний директор не може дозволити собі розтратити. Порушення кібербезпеки може завдати величезної шкоди репутації компанії, підриваючи довіру серед зацікавлених сторін, клієнтів і партнерів. Виконавчі директори повинні усвідомлювати, що комплаєнс — це не просто прапорець, а основоположний елемент корпоративної відповідальності та зміцнення довіри.

*Навігація в нормативному ландшафті та забезпечення відповідності*

Як генеральний директор, ви можете зробити стратегічні кроки, щоб підготувати свою організацію до лабіринту правил кібербезпеки. Ця подорож починається з вирушення у всебічну подорож для оцінки ризиків, щоб зрозуміти тонкощі ландшафту кібербезпеки вашої організації. Це передбачає визначення обсягу зібраних і збережених даних, ідентифікацію систем і програм, що використовуються, і передбачення потенційних загроз. Озброївшись цим розумінням, ви можете визначити пріоритетність ризиків і розробити індивідуальний план пом'якшення.

Надійна програма кібербезпеки є стрижнею стійкості вашої організації. Він повинен охоплювати спектр засобів контролю безпеки, включаючи рішення ідентифікації та керування доступом для контролю доступу, рішення Unified Endpoint Management для керування пристроями та шифрування даних, а також рішення для виявлення кінцевих точок і відповіді для проактивного реагування. Крім того, установіть режим періодичного тестування та оцінки відповідності вимогам кібербезпеки, щоб забезпечити його ефективність.

Нарешті, ІТ-відділ і кожен співробітник відповідають за безпеку організації. Весь персонал повинен нести відповідальність за дотримання вимог кібербезпеки. Для цього необхідна відданість керівництва від верху до низу. Генеральні директори несуть відповідальність за активне виховання культури безпеки, надання співробітникам навичок і ресурсів, необхідних для розпізнавання й усунення потенційних ризиків, а також встановлення стандартів для всієї компанії. Це передбачає регулярну взаємодію зі стратегією кібербезпеки компанії, розуміння ризиків і прийняття обґрунтованих рішень. Добре навчена робоча сила є безцінним активом у боротьбі з кіберсупротивниками. Це зміцнює загальну безпеку компанії та демонструє відданість благополуччю працівників. Водночас організації також повинні інвестувати в кваліфіковану команду з кібербезпеки, щоб ефективно керувати своєю стратегією відповідності.

*Нижня лінія*

Відповідність не слід розглядати як нав’язування, а радше як спільну мету, яка узгоджується з ширшими цілями організації. Стимулювання дотримання нормативних вимог сприяє розвитку почуття колективної відповідальності та підсилює важливість кібербезпеки в усіх відділах. Хоча вони можуть ненавмисно ускладнити бізнес-операції, правила кібербезпеки більше не є вибором, а необхідністю в цифровому світі.

У міру того як регуляторний ландшафт посилює контроль над кібербезпекою, керівники стикаються з проблемами та можливостями. Дотримання нормативних вимог захищає організацію від регуляторних санкцій і зміцнює її репутацію та стійкість перед лицем нових загроз. Культивуючи культуру безпеки, зберігаючи пильність перед лицем зміни правил і визнаючи цілісний вплив відповідності, керівники можуть не тільки задовольнити вимоги сьогодення, але й процвітати в епоху кіберстійкості». ***(Apu Pavithran. The World is Doubling Down on Cybersecurity — Here's What Business Leaders Should Know // Entrepreneur Media, LLC (https://www.entrepreneur.com/leadership/the-world-is-doubling-down-on-cybersecurity-heres-what/465068?utm_source=flipboard&utm_content=user%2Fentrepreneur). 17.11.2023).***

***

**«…У вівторок Національний центр кібербезпеки Великобританії опублікував свій щорічний огляд, підкреслюючи потребу в ефективній та адаптивній кібербезпеці, яка може не відставати від зростаючих темпів онлайн-атак.** У звіті відзначається ризик, який штучний інтелект і агресивні державні групи становлять для критичної інфраструктури, а також для громадських процесів, таких як вибори.

Це попередження повинно викликати тривогу, але ми вже бачимо подібні загрози, що діють по всьому світу. Компанія DP World Australia, яка є частиною глобального оператора портів Дубая DP World, була змушена вжити термінових

заходів для відновлення наземних вантажних операцій у своїх портах після інциденту з кібербезпекою в п’ятницю. Атака на цю важливу частину торговельної інфраструктури та пов’язані з нею порушення були настільки серйозними, що до неї причетна міністр внутрішніх справ Австралії Клер О’Ніл, яка підтвердила, що Центр кібербезпеки країни надавав технічні консультації та допомогу DP World.

Небезпеки, пов’язані з провалом у кібербезпеці, особливо заслуговують на увагу на Близькому Сході, який є регіоном, що найшвидше розвивається у світі, коли йдеться про впровадження Інтернету – уже 98 відсотків населення країн GCC є онлайн. З таким підключенням і багатьма перевагами, які воно приносить, також постають проблеми; Раніше цього місяця голова Ради з кібербезпеки ОАЕ доктор Мохаммед Аль Кувейті заявив, що понад 71 мільйон спроб кібератак в Еміратах було заблоковано за перші три квартали цього року.

Кібербезпека, як на персональних комп’ютерах, наших смартфонах, так і в ширшому середовищі, наприклад у військових чи великих компаніях, залишається першою лінією захисту від онлайн-злочинців і терористів. Щоб бути на крок попереду такої загрози, потрібні постійні інвестиції, інновації та співпраця. ОАЕ завжди усвідомлювали ризики, пов’язані з високим рівнем розвитку цифрових технологій. Минулого місяця країна підписала угоду про співпрацю з Міністерством фінансів США щодо кібербезпеки та цифрової стійкості. За словами США, це співробітництво включатиме обмін інформацією, що стосується фінансового сектору, навчання персоналу та навчальні візити, а також транскордонні навчання з кібербезпеки.

Співпраця між бізнесом і владою також є життєво важливою. PureHealth, найбільша платформа охорони здоров’я на Близькому Сході, оголосила минулого тижня, що вона інтегрує свою онлайн-безпеку з Операційним центром національної безпеки ОАЕ для захисту конфіденційних клінічних даних і даних пацієнтів.

Фішинг, брендджекінг, блокчейн, клікджекінг – кіберзлочин може здаватися важким жаргоном, абстрактним і технічним, доки людина не стане його жертвою. Однак серйозні політичні, фінансові та економічні наслідки неспроможності впоратися з кіберзагрозами – які далекі від наукової фантастики чи шпигунських

трилерів – є нагадуванням про те, що в нашому все більш взаємопов'язаному світі онлайн-захист є невід'ємною частиною національної оборони». ***(Why cyber security is integral to national defence // The National (https://www.thenationalnews.com/opinion/editorial/2023/11/15/cyber-crime-security/). 15.11.2023).***

***

**«Нове дослідження стану автоматизації кібербезпеки за 2023 рік показує, що хоча впровадження зростає, тривалі перешкоди підривають його ефективність.**

Автоматизація кібербезпеки невпинно набирає обертів, оскільки організації прагнуть підвищити ефективність, усунути прогалини в кадрах і не відставати від ескалації загроз. Однак останнє дослідження показує, що, незважаючи на те, що все більше компаній використовують автоматизацію, вони продовжують боротися з перешкодами, які заважають їм повністю скористатися її перевагами.

У недавньому дослідженні, в якому взяли участь понад 700 фахівців з кібербезпеки, ThreatQuotient виявив кілька постійних проблемних моментів у впровадженні автоматизації. Дослідження показало, що відсутність довіри до автоматизованих результатів, недостатній досвід серед користувачів і погана комунікація між командами перешкоджають успіху автоматизації. У результаті організації намагаються зміцнити довіру до автоматизації та максимізувати її ефективність.

Дослідження виявило повсюдні труднощі з впровадженням автоматизації кібербезпеки: 100% респондентів повідомили про проблеми. Основними проблемами, які підривають впевненість у результатах, були відсутність довіри (31%), повільне сприйняття користувачами (30%) і неправильні рішення (29%).

Однак, якщо ми детально розберемося, CISO відрізняються від інших лідерів щодо конкретних завдань. 40% назвали «погані рішення» головною проблемою проти 29% загалом. Завдяки повній підзвітності щодо кіберризиків керівники

відділів інформаційних технологій відчувають на собі вплив поганих результатів автоматизації.

Автоматичні дії, як-от неправильне блокування законної електронної пошти/доменів, здаються підозрілими, але негативно впливають на бізнес. Ці помилки підривають довіру користувачів до того, що автоматизація покращує безпеку, і організації не можуть покладатися на неї.

Наприклад, автоматизована система може помилково заблокувати доступ до законного бізнес-домену, який деякі постачальники використовують для спілкування електронною поштою. Співробітники раптово виявляються нездатними спілкуватися з ключовими партнерами, а бізнес-операції зупиняються. Це не тільки негативно впливає на дохід, але й руйнує довіру кінцевих користувачів до цінності та точності автоматизованих систем безпеки. Тоді організації починають дуже вагатися, чи варто покладатися на автоматизацію через страх перед цими руйнівними результатами для бізнесу.

Без впевненості в надійних автоматизованих результатах підприємства не довірятимуть критичні процеси безпеки їм. Цей 31% звітів про відсутність довіри є основною перешкодою, яка перешкоджає повній реалізації переваг автоматизації. Щоб подолати це, потрібні рішення, які забезпечують прозорість автоматизованих рішень.

Недостатній досвід серед членів команди безпеки робить ефективне впровадження автоматизації складним завданням. Обмежені навички призводять до неправильних налаштувань, проблем інтеграції та інших проблем. Ці збої підсилюють 31% відсутність довіри до результатів. Коли автоматизація непередбачувано дає збій через неоптимальне впровадження, організації не можуть скористатися її перевагами.

Оскільки розрив у навичках кібербезпеки все ще зростає, а 25% CISO повідомляють про брак навичок як про їхню найбільшу проблему, підприємствам часто не вистачає персоналу для вмілого розгортання інструментів автоматизації та керування ними. Крім того, 23% респондентів шукали доступність навчання під час вибору рішень, що є ключем до успішного впровадження, і очевидно, що розвиток

навичок має бути ключовою сферою уваги для організацій, щоб отримати вигоду від потенціалу автоматизації.

CISO вказують на організаційні проблеми, які загострюють труднощі, а 25% вказали на те, що головною проблемою є висока плинність команд, що порушує безперервність експертних знань і навичок для безперебійного впровадження автоматизації.

Дослідження виявило розбіжності між ролями щодо перспектив автоматизації, де 42% CISO назвали ефективність головним рушієм впровадження автоматизації, тоді як для керівників SOC і MSSP відповідність нормативним вимогам була головною.

Ці змішані точки зору вказують на відсутність узгодженості щодо цілей і напрямків автоматизації. CISO повинні усунути прогалини за допомогою покращення передачі планів автоматизації та переваг. Встановлення чітких цілей, навчання всіх членів команди та демонстрація відчутних здобутків є критично важливими для тривалої участі.

Коли одна спеціалізована команда впроваджує автоматизацію у вакуумі, ширше впровадження відстає. Але всеосяжне повідомлення про те, як автоматизація допомагає кожній ролі працювати ефективніше, сприяє спільній участі.

Постійна взаємодія із зацікавленими сторонами також є життєво важливою. Керівники повинні демонструвати автоматизацію, що підвищує ефективність, дотримання вимог, продуктивність або інші цілі, важливі для кожного керівника.

З роз’єднаними поглядами на свою цінність і роль, автоматизація бореться за точку опори. Послідовне, переконливе повідомлення про переваги забезпечує надійну підтримку ініціатив у всій організації.

Дослідження 2023 року показує, що впровадження автоматизації кібербезпеки все ще стикається з перешкодами: 100% респондентів повідомили про проблеми. Однак розумніші інструменти та робочі процеси можуть допомогти організаціям подолати ці проблеми та реалізувати потенціал автоматизації.

Однією з ключових потреб є інструменти автоматизації, які забезпечують прозорість і огорожі, зміцнюючи довіру користувачів. Інтуїтивно зрозумілі інтерфейси також спрощують освоєння користувачами з усіма рівнями кваліфікації, пом'якшуючи дефіцит навичок, який 23% назвали головною проблемою.

Стандартизація процесів навколо автоматизації забезпечує послідовність, необхідну для максимізації переваг. Робочі процеси, такі як автоматичне сортування, уникають спеціальних підходів, які спричиняють фрагментовані прибутки.

Інтеграція між інструментами створює безперебійні потоки даних і уніфіковані робочі процеси, а не роз'єднані набори інструментів. У звіті говориться, що 24% бажають інтеграції з кількома джерелами даних при виборі рішень автоматизації.

Впровадження автоматизації без урахування довіри, зручності використання, навчання, інтеграції та стандартизованих процесів викликає розчарування. Дослідження показує, що ці розумніші інструменти та робочі процеси пропонують шлях до подолання перешкод і успіху автоматизації.

Це дослідження поточного ландшафту автоматизації кібербезпеки виявляє постійні проблеми, які заважають організаціям повністю реалізувати її переваги. Основні проблемні області включають недостатню довіру до результатів, дефіцит навичок серед персоналу та внутрішні розриви щодо ролі та цінності автоматизації.

Дотримуючись узгоджених дій, щоб підвищити довіру через прозорість, підвищити досвід команди через навчання та узгодити розуміння переваг автоматизації за допомогою послідовного обміну повідомленнями керівництва, CISO можуть подолати ці перешкоди.

Завдяки продуманим стратегіям адаптації, безпечним принципам проектування та інклюзивному управлінню змінами організації можуть скористатися величезною потужністю автоматизації для підвищення безпеки перед обличчям зростаючих загроз. Завдяки поєднанню розумніших інструментів, освічених користувачів і чіткого спілкування команди з кібербезпеки можуть досягти нових висот ефективності та результативності завдяки автоматизації.

Однак досягнення повного потенціалу автоматизації — це не одноразова спроба. Це вимагає постійної відданості ітераціям і оптимізації в міру розвитку технологій, загроз і потреб бізнесу. Регулярна оцінка процесів і налаштування систем допомагає підтримувати максимальну продуктивність з часом.

Керівники також повинні постійно оцінювати людську сторону рівняння. Спілкування з персоналом на всіх рівнях дає цінну інформацію для формування програм навчання, тактики управління змінами та внутрішнього обміну повідомленнями таким чином, щоб підтримувати сильну зацікавленість у всій організації. Завдяки персоналу, який наділений повноваженнями та об'єднався навколо спільних цілей автоматизації, організації можуть спритно адаптувати свої підходи для максимізації цінності». ***(Isha Jain. Navigating the promise and pitfalls of cyber security automation // All Things Media Ltd (https://dcnnmagazine.com/security/navigating-the-promise-and-pitfalls-of-cyber-security-automation/). 21.11.2023).***

***

**«Huntsman Security сьогодні оголосила про свої прогнози щодо кібербезпеки на 2024 рік, включаючи перехід організацій до кібербезпеки, керованої даними, і виклики, які створює ШІ.** Компанія розглядає, чому операційна стійкість буде головною проблемою в багатьох інших залах засідань і як компаніям потрібно буде реагувати на ці зміни керівних принципів управління.

*Кібербезпека стане «керованою даними»*

Стійкість кібербезпеки іноді може бути не помічена під час процесів цифрової трансформації. Це зміниться у 2024 році, оскільки більше усвідомлення необхідності операційної стійкості вимагатиме від директорів більш повної звітності про адекватність своїх операційних процесів управління регуляторам. Як наслідок, зростатиме популярність інформаційних систем безпеки, керованих даними, які краще підходять для нестабільних середовищ із загрозами. У наступні 12 місяців директори визнають здатність цифрових методів кіберуправління

надавати більш надійну інформацію та швидше, щоб керувати своїми рішеннями щодо безпеки.

*ШІ створює стільки ризиків, скільки й переваг*

Майже безпрецедентне впровадження ШІ ознаменувало одну з найбільших технологічних тенденцій у 2023 році. Але зі зростанням популярності технології зростатиме й потенціал її використання для інших цілей. У 2024 році ми можемо очікувати, що зловмисники тренуватимуть шкідливі механізми штучного інтелекту та створюватимуть код, який доповнить їхні підлі наміри. Організаціям потрібно буде адаптуватися для захисту від додаткової загрози з боку ворогів із підтримкою ШІ. Перегляд політик і засобів контролю в кіберуправлінні, а також оцінка їх адекватності будуть критично важливі, щоб не стати жертвою цих атак із застосуванням ШІ.

*Операційна стійкість стане мантрою зали засідань у 2024 році*

Вимоги до операційної стійкості у фінансовому секторі стають все більш схожими між урядами, і ми очікуємо, що ці вимоги швидко поширяться на інші сектори критичної інфраструктури. Регулятори вже посилюють кібербезпеку як питання бізнесу; і кібер, як і інші типи операційних ризиків, які можуть перебувати поза межами безпосереднього контролю організації, стануть специфічним елементом розширених вимог до операційного управління.

У свою чергу, це означатиме, що, незважаючи на те, що керівництво організації може делегувати ці спеціалізовані завдання, воно більше не може відволікати від себе відповідальність за їхню ефективну роботу та нагляд. Директорам потрібно буде постійно контролювати управління операційними ризиками, особливо кібербезпеку. Директори повинні визначити важливі бізнес-послуги, які вони надають. Вони повинні забезпечувати належний захист систем, процесів, ресурсів і 3 rd сторони, які об’єднуються для надання цих послуг клієнтам. Ми очікуємо більшої уваги до кібербезпеки зверху вниз.

*Нові технології змінять вимоги до навичок і допоможуть зменшити дефіцит навичок кібербезпеки*

Дефіцит навичок у сфері кібербезпеки протягом кількох років перешкоджав зусиллям багатьох організацій із забезпечення безпеки. Однак зростаючий перехід до цифрових інновацій та автоматизації самих процесів безпеки має дати певне полегшення. Запровадження керованих даними рішень і автоматизованих, заснованих на фактах звітів повинно дозволити менш кваліфікованим спеціалістам вийти на ринок – ефективно інтерпретувати, реагувати та керувати великими частинами процесу кібербезпеки. Це, у свою чергу, дозволить існуючим фахівцям у сфері безпеки вирішувати більш нагальні потреби, звертаючи увагу на викиди, такі як виняткові дані та аналітичні проблеми високого рівня, з якими ми завжди стикатимемося…» ***(Huntsman Security shares 2024 predictions: Data-driven cyber security to transform industry // Business Wire (https://www.businesswire.com/news/home/20231120644215/en/Huntsman-Security-shares-2024-predictions-Data-driven-cyber-security-to-transform-industry). 20.11.2023).***

***

**«Організації постійно стикаються з новою тактикою кіберзлочинців, які прагнуть скомпрометувати їхні найцінніші активи.** Проте, незважаючи на розвиток технологій, багато лідерів безпеки все ще покладаються на суб'єктивні терміни, такі як низький, середній і високий, щоб спілкуватися та керувати кіберризиками. Ці розпливчасті терміни не передають необхідних деталей чи розуміння для отримання дієвих результатів, які точно визначають, вимірюють, керують і повідомляють про кіберризики. У результаті керівники та члени правління залишаються необізнаними та погано підготовленими для ефективного управління організаційними ризиками.

У той же час керівники відчувають зростаючий тиск щодо вдосконалення програм кібербезпеки через зростання нещодавно прийнятих нормативних актів Комісії з цінних паперів і бірж США (SEC), які вимагають від публічних компаній

швидко розкривати кібератаки та суттєву інформацію про їх управління ризиками кібербезпеки, стратегію та управління.

Кіберризики (CRQ) стали найефективнішим способом максимізації програм управління кіберризиками шляхом переведення кіберризиків у конкретні фінансові наслідки. За даними Forrester Research, «CRQ кардинально революціонізує спосіб взаємодії лідерів із безпеки з радами директорів і керівниками для обговорення кібербезпеки».

*Повідомлення про кіберризики керівникам і радам директорів*

Заголовки новин про кібератаки та використання вразливостей нульового дня стали типовими темами для розмов у залах засідань. Насправді кіберризик став одним із п’яти найбільших ризиків, з якими стикаються організації. У сучасному світі для керівників відділів безпеки важливо чітко, лаконічно та зрозуміло повідомляти про кіберризики своїм радам директорів. Часто звіти про кібербезпеку наповнені занадто великою кількістю технічних деталей, що заважає керівникам приймати обґрунтовані рішення та точно оцінювати ландшафт ризиків кібербезпеки. Це може призвести до плутанини та суб’єктивного прийняття рішень.

Впроваджуючи CRQ, керівники служби безпеки можуть надавати звіти на керівному рівні, які повідомляють про фінансові наслідки кібератак, націлених на життєво важливі бізнес-активи, що призводять до збоїв у роботі, збоїв у системі та зниження виробництва та витрат, пов’язаних з відновленням.

Простіше кажучи, кіберризик — це бізнес-ризик, і про нього слід повідомляти в ділових термінах. Використовуючи результати програми CRQ, лідери можуть досягти узгодженості зі своїми радами та виконавчими командами та покращити свої загальні стратегії зниження ризиків та інвестиції.

*Оптимізація витрат на безпеку*

Керівники служби безпеки відчувають тиск, щоб посилити заходи захисту та зменшити ризик у найбільш економічно ефективний спосіб, беручи до уваги економічні обмеження та обмежені бюджети. Однак традиційні методи прийняття рішень часто покладаються на суб’єктивну інформацію, що ускладнює об’єктивне обґрунтування попередніх або майбутніх інвестицій у безпеку. Операціоналізація

CRQ додає об’єктивності процесу прийняття рішень. Це дозволяє організаціям оптимізувати програми кібербезпеки та інвестиції в інструменти, визначаючи пріоритетність витрат на основі зменшення фінансових ризиків і максимізації повернення інвестицій (ROI).

Без попередньої кількісної оцінки ризиків у контексті поточної системи контролю безпеки як базової лінії, організації не можуть точно оцінити ефективність своїх ініціатив безпеки або визначити свої наступні інвестиції. Розуміння фінансових ризиків організації дозволяє керівникам служби безпеки зосередитися на сферах з найбільш значними можливостями зниження ризиків і визначити пріоритетність ініціатив безпеки, які узгоджуються з бізнесом, щоб краще зменшити найбільш значні ризики, з якими стикається бізнес.

*Розробка програми ризиків підприємства*

Щоб надати особам, які приймають рішення, загальний профіль організаційних ризиків, кіберризики повинні бути повністю інтегровані в загальну програму управління ризиками підприємства (ERM). Однак це можливо лише за умови розуміння фінансових наслідків кіберзагроз, щоб організації могли узгодити свої зусилля зі зменшення ризиків із бізнес-цілями та підвищити загальну стійкість організації.

Історично склалося так, що багато організацій розробили незалежні процедури управління ризиками, включаючи ERM, ризики кібербезпеки, операційні ризики та відповідність та IT-ризики. CRQ стає найкращою практикою серед провідних організацій для розробки та впровадження ефективних програм управління ризиками, оновлення оцінки ризиків та інтеграції процедур ERM. Провідні організації, які використовували CRQ для вдосконалення своїх процесів управління, розробили єдину інтегровану операційну модель управління ризиками. Це дозволяє покращити аналітику для виявлення та відстеження тенденцій у бізнес-напрямках або функціональних сферах, а також системних ризиків для організації.

Незважаючи на те, що це вимагає нового підходу до мислення про управління ризиками, включаючи кілька функцій управління ризиками, результатом є стандартизований, послідовний і добре зрозумілий процес

ідентифікації ризиків, аналізу та звітування. CRQ надає організації єдине визначення ризику та усуває будь-яку невизначеність щодо того, як повідомляти про ризики керівництву та раді. Звітуючи про ризики з точки зору впливу на бізнес і фінансового ризику, CRQ усуває суб'єктивні інтерпретації, які покладаються на номінальні шкали або кольорові коди.

Як нещодавно поділився один із керівників відділу ризиків: «Ми зауважили, що багато ризиків, пов'язаних із різними напрямками діяльності, подібні за своєю природою та мають спільні першопричини. Використання єдиного процесу оцінки управління ризиками дозволяє нам швидко визначати очікуваний вплив і, що більш важливо, використовувати перевірені підходи до пом'якшення цих ризиків».

Оскільки компанії продовжують розвивати свої можливості щодо кіберризиків шляхом впровадження CRQ, їм слід розглянути можливість включення CRQ в інші функції ризиків і працювати над впровадженням інтегрованої операційної моделі управління ризиками.

*Початок роботи з кількісним визначенням кіберризиків*

Незалежно від того, чи намагаєтеся ви випереджати нормативні акти, реагуєте на кіберподію чи дієте на випередження, впровадження CRQ може допомогти вашій організації покращити звітність про кібербезпеку, оптимізувати бюджети, створити дорожні карти безпеки на основі ризиків, визначити пріоритети вразливостей і покращити ERM. Таким чином керівники служби безпеки дають своїм керівникам і членам правління можливість приймати добре поінформовані, засновані на ризиках і фінансово відповідальні рішення, коли йдеться про ризик.

Організації можуть зробити прості кроки, щоб досягти прогресу на цьому шляху. Ми рекомендуємо починати з малого, вибираючи один або два варіанти використання, які найкраще відповідають цілям безпеки вашої організації, і інтегрувати CRQ у бізнес-процеси, що забезпечує дієві результати». ***(Randy Spusta. Operationalize cyber risk quantification for smart security // Security Intelligence (https://securityintelligence.com/posts/operationalize-cyber-risk-quantification/). 20.11.2023).***

***

**«У швидкоплинному світі технологій 2023 рік обіцяє стати переломним періодом у постійно змінюваному ландшафті кібербезпеки. Поки ми проходимо еру безпрецедентного зв'язку, виклики та загрози цифровій безпеці продовжують зростати.** Крім того, у цій статті ми заглибимося в ключові тенденції, що формують ландшафт кібербезпеки в 2023 році, досліджуючи стратегії та технології, які мають вирішальне значення для випередження нових загроз.

*Посилення уваги до архітектури нульової довіри*

У 2023 році концепція архітектури нульової довіри (ZTA) набуває популярності як фундаментальний підхід до кібербезпеки. Традиційно моделі безпеки працювали на основі припущення, що загрози можна було б утримати на відстані, охороняючи периметр. Однак із зростанням складних кібератак модель Zero Trust працює за принципом «ніколи не довіряй, завжди перевіряй». Цей підхід передбачає, що загрози можуть надходити як зсередини, так і ззовні мережі, вимагаючи постійної перевірки ідентифікації користувача та безпеки пристрою.

*Розвиток ШІ та машинного навчання у виявленні загроз*

Штучний інтелект (AI) і машинне навчання (ML) стають невід'ємними компонентами стратегій кібербезпеки. Крім того, у 2023 році ці технології все частіше використовуються для розширеного виявлення загроз і реагування на них. Алгоритми штучного інтелекту та машинного навчання аналізують величезні набори даних, щоб виявити шаблони, аномалії та потенційні порушення безпеки в режимі реального часу, що дозволяє організаціям швидко реагувати на нові загрози.

*Квантово-безпечна криптографія*

Оскільки квантові обчислення наближаються до практичності, потреба в квантово-безпечній криптографії стає дедалі гострішою. Крім того, потужність квантових комп'ютерів може потенційно зламати існуючі методи шифрування, створюючи серйозну загрозу безпеці даних. У 2023 році організації інвестують у квантово-стійкі алгоритми, щоб захистити свої системи від нових можливостей квантового обчислення.

*Акцент на хмарній безпеці*

Перенесення даних і послуг у хмару змінило цифровий ландшафт, зробивши хмарну безпеку головним пріоритетом у 2023 році. Крім того, у міру впровадження хмарних сервісів компанії зосереджуються на надійних заходах безпеки для захисту конфіденційної інформації, що зберігається в хмарі. Це передбачає впровадження шифрування, багатофакторну автентифікацію та регулярні аудити безпеки для забезпечення цілісності хмарних систем.

*Боротьба з програмами-вимагачами триває*

Атаки програм-вимагачів зростають, націлюючись на окремих осіб, підприємства та навіть критичну інфраструктуру. Крім того, у 2023 році боротьба з програмами-вимагачами посилюється, а організації вживають профілактичних заходів для запобігання атакам і розробляють комплексні плани реагування на інциденти. Використання рішень для резервного копіювання, навчання співробітників і обмін інформацією про загрози є ключовими компонентами цілісного підходу до боротьби з програмами-вимагачами.

*Інтеграція практик DevSecOps*

DevSecOps, інтеграція методів безпеки в конвеєр DevOps, набирає популярності як проактивний підхід до кібербезпеки. У 2023 році організації запровадять DevSecOps для впровадження заходів безпеки на кожному етапі життєвого циклу розробки. Цей підхід зі зсувом вліво гарантує, що безпека не є запізнілою думкою, а є невід'ємною частиною процесу розробки, підвищуючи загальну стійкість цифрових систем.

*Постійна увага до безпеки кінцевих точок*

Кінцеві точки, включаючи такі пристрої, як ноутбуки, смартфони та пристрої Інтернету речей, залишаються вразливими цілями для кіберзагроз. Крім того, у 2023 році організації постійно приділяють увагу безпеці кінцевих точок для захисту від нових векторів атак. Це передбачає впровадження надійних рішень для захисту кінцевих точок. Крім того, регулярне оновлення програмного забезпечення та навчання користувачів найкращим практикам є важливими кроками для зменшення ризиків, пов'язаних із вразливістю кінцевих точок.

*Співпраця для обміну інформацією про загрози*

У взаємопов'язаному світі кібербезпеки співпраця стає все більш важливою. Крім того, у 2023 році організації активно беруть участь в ініціативах з обміну інформацією про загрози. Цей спільний підхід не тільки дозволяє спільноті кібербезпеки залишатися в курсі нових загроз, вразливостей і методів атак, але також дозволяє колективно та проактивно реагувати на кіберзагрози.

*Розширені заходи конфіденційності*

У зв'язку зі зростаючим занепокоєнням щодо конфіденційності даних організації віддають перевагу посиленим заходам із захисту конфіденційності у 2023 році. Суворіші нормативні акти, такі як Загальний регламент захисту даних (GDPR), і зміна очікувань користувачів щодо конфіденційності спонукають компанії впроваджувати надійні засоби контролю конфіденційності. Це включає анонімізацію даних, прозорі методи обробки даних і механізми отримання згоди користувачів, що забезпечує дотримання правил конфіденційності.

*Безперервне навчання з кібербезпеки*

Людська помилка залишається суттєвим фактором порушень кібербезпеки. Крім того, у 2023 році організації інвестують у безперервне навчання співробітників з кібербезпеки, щоб підвищити їхню обізнаність про потенційні загрози та найкращі практики безпеки. Цей комплексний підхід включає імітацію фішингових вправ, семінари з безпечного кодування та регулярні оновлення останніх тенденцій кібербезпеки. Ці зусилля спільно розширюють можливості співробітників як першої лінії захисту від кіберзагроз.

висновок:

*Навігація в майбутньому кібербезпеки*

Оскільки ми орієнтуємось у складний ландшафт кібербезпеки у 2023 році, ключові тенденції, згадані вище, підкреслюють необхідність проактивного та адаптивного підходу до цифрової безпеки. Крім того, організації повинні бути в курсі цих тенденцій, що розвиваються, впроваджуючи надійні стратегії та технології для захисту своїх цифрових активів. Крім того, співпраця між зацікавленими сторонами галузі, інтеграція передових технологій і прихильність

безперервному навчанню відіграватимуть важливу роль у створенні стійкої позиції кібербезпеки в майбутньому». ***(Hillary. The Evolving Landscape of Cybersecurity: Trends to Watch in 2023" // TechBullion (https://techbullion.com/the-evolving-landscape-of-cybersecurity-trends-to-watch-in-2023/). 24.11.2023).***

***

**«У величезному просторі Інтернету Dark Web є таємничим і часто неправильно зрозумілим царством. Як для професіоналів із кібербезпеки, так і для ентузіастів надзвичайно важливо розуміти загрози, які ховаються в цьому прихованому куточку цифрового світу.** У цій статті ми вирушаємо в мандрівку в тіні, досліджуючи ландшафт Dark Web і проливаючи світло на проблеми кібербезпеки, які вона створює.

Розкриття темної мережі:

*Уважніший погляд*

Темна павутина, яку часто називають «підчеревиною» Інтернету, існує поза межами досяжності звичайних пошукових систем. Доступний лише через спеціалізоване програмне забезпечення, таке як Tor, він працює як децентралізована мережа, що забезпечує анонімність і конфіденційність. Незважаючи на те, що Dark Web за своєю суттю не є зловмисним, він є живильним середовищем для незаконної діяльності, що робить його центром для проблем кібербезпеки.

*Криптовалютні ринки та незаконна торгівля*

Одним із визначних аспектів Dark Web є його роль як ринку для незаконної торгівлі, де транзакції переважно проводяться з використанням криптовалют для підвищення анонімності. Це включає в себе продаж викрадених даних, хакерських інструментів і навіть більш мерзенних пропозицій, таких як наркотики, зброя та підроблені документи. Навігація в цих каламутних водах вимагає заходів кібербезпеки, які виходять за рамки звичайного виявлення загроз.

*Загрози кібербезпеці: багатогранна загроза*

Заглиблюючись у Dark Web, користувачі стикаються з безліччю загроз кібербезпеці. Від фішингових схем і ринків програм-вимагачів до форумів, де обговорюються найновіші технології зловмисного програмного забезпечення, Dark Web є живильним середовищем для інновацій кіберзлочинців. Здійснення транзакцій у такому середовищі потребує підвищеної обізнаності про потенційні загрози та надійної стратегії кібербезпеки, щоб подолати постійну небезпеку.

*Підпільна економіка вкрадених даних*

Викрадені дані є товаром у Dark Web, де кіберзлочинці торгують особистою інформацією, обліковими даними для входу та фінансовими деталями. Крім того, ця підпільна економіка сприяє крадіжці особистих даних, фінансовому шахрайству та іншим кіберзлочинам. Для фізичних осіб і компаній захист конфіденційних даних має першочергове значення. Крім того, методи кібербезпеки повинні поширюватися на шифрування даних, безпечну автентифікацію та постійний моніторинг для виявлення можливих порушень.

*Платформи хакерства як послуги (HaaS).*

Dark Web розміщує платформи Hacking as a Service (HaaS), де кіберзлочинці пропонують свій досвід за плату. Більше того, це комерціалізація хакерства становить серйозну загрозу як для компаній, так і для окремих осіб. У відповідь фахівці з кібербезпеки повинні адаптуватися, випереджаючи нові методи злому, розуміючи ринкову динаміку та зміцнюючи свій захист, щоб перешкоджати потенційним атакам.

*Кібершпигунство та загрози національній державі*

Окрім злочинного світу, Темна павутина служить притулком для кібершпигунства та діяльності національних держав. Крім того, у цьому таємному просторі діють спонсоровані державою хакерські групи, які ведуть кібервійну, шпигунство та крадіжку конфіденційної інформації. У результаті стратегії кібербезпеки повинні розвиватися для боротьби з цими складними загрозами. Ця еволюція має наголошувати на зборі розвідданих, ретельному аналізі загроз і проактивних заходах захисту.

Захист вашої цифрової фортеці:

*Найкращі практики кібербезпеки*

Перед обличчям загроз Dark Web окремі особи та організації повинні застосовувати надійні найкращі методи кібербезпеки. По-перше, регулярно оновлюйте програмне забезпечення та системи. По-друге, використовуйте надійні та унікальні паролі. По-третє, запровадьте багатофакторну автентифікацію, щоб зміцнити свою цифрову фортецю. Крім того, важливо проводити регулярні перевірки безпеки. Крім того, надзвичайно важливим є навчання користувачів фішингу та тактиці соціальної інженерії. Нарешті, інвестування в розширені інструменти виявлення загроз є необхідним, щоб випереджати загрози, що розвиваються.

*Спільний захист кібербезпеки*

Dark Web створює виклики, які вимагають спільних зусиль у спільноті кібербезпеки. Крім того, обмін інформацією про загрози, співпраця в дослідженнях і участь у спільних ініціативах є важливими компонентами єдиного фронту проти загроз Dark Web. Крім того, професіонали з кібербезпеки повинні позбутися відокремленості, розвиваючи культуру співпраці для спільної боротьби з динамічними викликами, які постійно розвиваються через Темну мережу.

висновок:

*Безпечне пересування в тіні*

Навігація в Dark Web не для слабконервних, але розуміння загроз кібербезпеці, які вона таїть, має вирішальне значення для створення надійного цифрового захисту. Поринаючи в тінь, ми повинні озброїтися знаннями, обізнаністю та проактивними заходами кібербезпеки. Застосувавши цілісний підхід, який охоплює технологічний прогрес, обмін інформацією про загрози та стратегії спільного захисту, ми можемо безпечно переміщатися в Dark Web, зменшуючи ризики, пов’язані з цим загадковим і складним цифровим ландшафтом. Будьте в курсі, будьте пильними та залишайтеся в безпеці». ***(Hillary. Navigating the Dark Web: A Look into Cybersecurity Threats” // TechBullion***

***(https://techbullion.com/navigating-the-dark-web-a-look-into-cybersecurity-threats/). 25.11.2023).***

***

## ***Сполучені Штати Америки***

**«Агентство з охорони навколишнього середовища США (EPA) офіційно відкликало правила кібербезпеки, оприлюднені в березні, які вимагали від штатів повідомляти про загрози кібербезпеці для своїх систем громадського водопостачання (PWS).** Відмова сталася після судових позовів, поданих у Восьмому окрузі в липні Міссурі, Арканзасом і Айовою (штати), а також сторонами, які втручалися, Американською асоціацією водопостачання та Національною асоціацією сільського водопостачання (водні асоціації). У результаті відкликання штати та водні асоціації подали заяву про відхилення своїх позовів.

Штати стверджували, що Правила кібербезпеки EPA незаконно встановлюють нові правові вимоги до штатів і PWS, і що це правило перевищує статутні повноваження EPA, ігноруючи дії Конгресу, які обмежують вимоги кібербезпеки до великих PWS, і змінюють критерії санітарних обстежень через меморандум. Штати також стверджували, що це правило було довільним і примхливим, оскільки EPA (i) не визнало або не пояснило, що воно змінило політику щодо внесення змін до мінімальних критеріїв або обсягу санітарних досліджень, і (ii) не врахувало важливих аспектів правила, включно з тим, що державні органи, відповідальні за проведення опитувань, не мають достатнього рівня знань з кібербезпеки, необхідного для завершення оцінок, очікуваних EPA, а частота, з якою проводяться санітарні огляди (кожні три-п’ять років), не гарантує, що PWS усунуть нові загрози в своєчасна мода.

В окремому короткому звіті водні асоціації стверджували, що це правило перевищує повноваження EPA відповідно до Закону про безпечну питну воду, який надає EPA обмежені повноваження для усунення вразливостей кібербезпеки, і що Конгрес не має наміру використовувати EPA для нав’язування закону. санітарні обстеження, регулювати менші водопровідні системи або змушувати штати

збирати конфіденційну інформацію та оцінювати кібербезпеку в PWS. Водні асоціації стверджували, що це правило «суперечить продуманим політичним перевагам Конгресу щодо того, що кібербезпека в менших PWS вирішується за допомогою, а не регулювання, з боку EPA». Вони, зокрема, стверджували, що Конгрес знав, що цим меншим системам бракуватиме операційної та фінансової спроможності для виконання вимог, подібних до тих, що включені до Правил кібербезпеки, і що такі вимоги будуть навантажувати обмежені бюджети та персонал цих систем, не забезпечуючи пропорційних переваг. Публічне оприлюднення інформації про кібербезпеку PWS через державні закони про публічні записи також викликає занепокоєння.

Дії EPA були спрямовані на усунення зростаючих загроз кібербезпеці для громадської інфраструктури в США. У відповідь на відкликання адміністрація Байдена заявила, що вони будуть виконувати «план Б», який передбачатиме лобіювання Конгресу для прийняття подібного законодавства.

Відповідно, у червні двопартійна коаліція представників представила Закон про кібербезпеку для сільських систем водопостачання 2023 року, щоб забезпечити фінансування кібербезпеки та технічну допомогу сільським системам водопостачання та водовідведення. Водні асоціації підтримують ці зусилля.

Спроба EPA врегулювати кібербезпеку також відповідає іншим нещодавнім діям федерального агентства, спрямованим на кібербезпеку. 27 жовтня Федеральна торгова комісія (FTC) оголосила про нове правило, яке вимагає від фінансових установ, які підпорядковуються FTC, повідомляти агентство якомога швидше, але не пізніше ніж через 30 днів після виявлення несанкціонованого отримання незашифрованої інформації про клієнтів, що впливає 500 і більше клієнтів. У червні SEC прийняла правила, які вимагають від публічних компаній щорічно розкривати суттєві інциденти кібербезпеки та розкривати суттєву інформацію щодо їхнього управління ризиками кібербезпеки, стратегії та управління.

Компанії можуть очікувати подальшого поширення федеральних норм кібербезпеки в найближчому майбутньому, оскільки адміністрація Байдена зобов’язує всі федеральні агентства прийняти мінімальні стандарти кібербезпеки

для організацій, які підпорядковуються їхнім відповідним парасолькам». ***(Stephen C. Piepgrass and Samuel E. "Gene" Fishel. EPA Withdraws Cybersecurity Rule for Public Water Systems // Troutman Pepper Hamilton Sanders LLP (https://www.regulatoryoversight.com/2023/11/epa-withdraws-cybersecurity-rule-for-public-water-systems/). 03.11.2023).***

***

**«Минулого тижня набули чинності поправки до правил кібербезпеки Департаменту фінансових послуг Нью-Йорка («DFS»).** Ці правила кібербезпеки, кодифіковані 23 NYCRR 500 («Частина 500»), широко застосовуються до компаній, які пропонують фінансові послуги або страхові продукти в штаті Нью-Йорк. Частина 500 є суворо директивною, і організації, які мають ліцензію DFS, у тому числі банки, повинні активно вживати заходів для перегляду та встановлення відповідності новим вимогам, особливо з огляду на те, що DFS агресивно дотримується своїх правил кібербезпеки.

Основні поправки до Частини 500 правил кібербезпеки включають наступне:

Розширені вимоги до управління: відповідно до нещодавніх зусиль Комісії з цінних паперів і бірж, частина 500 посилила вимоги до кіберуправління для охоплених організацій. Серед іншого, керівники інформаційної безпеки («CISO») тепер зобов'язані повідомляти раду директорів про будь-яку значну подію кібербезпеки або зміну програми кібербезпеки. Крім того, ради керованих організацій зобов'язані мати достатній досвід у сфері кібербезпеки, який може включати використання радників, і повинні здійснювати нагляд за розробкою, впровадженням і підтримкою програми кібербезпеки організації, включаючи затвердження всіх письмових політик принаймні раз на рік.

Вимоги до багатофакторної автентифікації (MFA): Хоча Частина 500 ще більше посилює приписні вимоги безпеки в області низки областей, охоплені суб'єкти повинні звернути особливу увагу на оновлені вимоги MFA, враховуючи історичну спрямованість DFS на отримання багатомільйонних розрахунків за невиконання відповідати цій вимозі. Раніше реалізація MFA була потрібна лише

для віддаленого доступу до мережі охопленої організації. Тепер очікується, що суб'єкти, на які поширюється дія, запровадять MFA, щоб дозволити будь-якому користувачеві отримати доступ до своїх інформаційних систем, за обмеженим винятком для відповідних невеликих компаній, які зобов'язані запровадити MFA лише для віддаленого доступу до систем компанії, програм сторонніх розробників, які містять інформацію компанії. непублічну інформацію та привілейовані облікові записи. Компанії можуть уникнути вимоги MFA, якщо CISO щорічно засвідчує впровадження розумно еквівалентних або більш безпечних компенсаційних засобів контролю.

Зосереджено програмне забезпечення-вимагач і цифрове вимагання. Враховуючи різке збільшення кількості атак програм-вимагачів за останні кілька років і занепокоєність регуляторів щодо платежів злочинній екосистемі, Частина 500 накладає низку нових вимог щодо програм-вимагачів і випадків цифрового вимагання, зокрема:

Вимоги до резервного копіювання: щоб підвищити стійкість інформаційних систем до атак програм-вимагачів, охоплені суб'єкти тепер зобов'язані підтримувати резервні копії систем, необхідні для відновлення матеріальних операцій, і зобов'язані проводити щорічні тести щодо своєї здатності відновлювати свої системи з резервних копій.

Вимоги до звітності про програмне забезпечення-вимагач/кібервимагання: Частина 500 історично вимагала сповіщення DFS про інциденти з даними, які або (1) мають суттєвий вплив на діяльність суб'єкта, на який поширюється дія, або (2) у випадках, коли суб'єкт, на який поширюється дія, зобов'язаний повідомляти про інцидент. до іншого регулятора. Поправки до DFS додали новий тригер сповіщення, коли інцидент із даними призводить до розгортання програм-вимагачів у суттєвій частині інформаційних систем суб'єкта, на який поширюється дія. Крім того, суб'єкти, на яких поширюється дія, зобов'язані повідомити DFS протягом 24 годин про здійснення будь-якого платежу суб'єкту загрози, а також протягом 30 днів повинні надіслати звіт із детальним описом причин необхідності платежу, описом розглянутих альтернатив платежу, виконанням усіх заходів

ретельності. знайти альтернативи оплаті та дотримання інших нормативних актів, зокрема Управління з контролю за іноземними активами (OFAC). Хоча ці вимоги не забороняють виплати суб'єктам загрози, вони значно підвищують ставки для компанії, яка прагне заплатити суб'єкту загрози, вимагаючи від компанії брати участь у надійній, добре задокументованій перевірці, зокрема стосовно питань санкцій. Крім того, компаніям, які планують виплати суб'єктам загроз, слід розглянути, чи звіт до DFS означатиме порушення нових вимог частини 500 щодо створення доступних надійних систем резервного копіювання для відновлення операцій.

Посилені вимоги до сертифікації: Частина 500 історично вимагала від охоплених організацій щорічно сертифікувати відповідність, але не передбачала альтернативного варіанту для компаній, які не мали змоги повністю сертифікувати відповідність. Поправки тепер чітко пояснюють, що всі охоплені суб'єкти зобов'язані або підтвердити відповідність, або, як альтернативу, надати письмове підтвердження того, що суб'єкт суттєвої відповідності не відповідає всім вимогам. Будь-яке таке підтвердження вимагатиметься для виявлення прогалин і надання графіка виправлення. Крім того, сертифікати повинні бути підписані як CISO, так і керівником найвищого рангу відповідної організації. Компанії повинні приділяти особливу увагу перевірці дотримання Частини 500, оскільки сприйняті неправдиві або оманливі твердження в цих документах можуть бути використані DFS як підстава для примусових дій. Крім того, ці сертифікати збільшують ризики для керівників, які підписують підписи, оскільки правоохоронні органи все більше зосереджуються на примусових діях проти осіб, пов'язаних з проблемами кібербезпеки, як-от нещодавня Позов SEC проти керівників SolarWinds.

Розширені зобов'язання для нових компаній «Класу А». DFS також створив новий клас великих суб'єктів господарювання, які охоплюються компаніями «Класу А», які визначаються як компанії, що мають: (a) принаймні 20 мільйонів доларів США валового річного доходу в кожній за останні два фінансові роки в штаті Нью-Йорк; та (b) понад 2000 співробітників або 1 мільярд доларів США валового річного доходу для організації та її філій у будь-якій точці світу.

Компанії, які відповідають вимогам, повинні розробляти та проводити незалежні аудити своєї програми кібербезпеки, впроваджувати рішення для керування привілейованим доступом, автоматизований метод блокування часто використовуваних паролів для всіх облікових записів, рішення для виявлення кінцевих точок і реагування для моніторингу аномальної активності, а також централізованого журналювання та попередження про події безпеки.

Висновок. Розширені вимоги Частини 500 сигналізують про намір DFS продовжувати свою історію агресивного дотримання вимог кібербезпеки в широкому діапазоні компаній, які вона контролює. Підприємствам, на яких поширюється дія, слід звернути особливу увагу на нові вимоги до управління та технічного контролю, а також приділяти значну увагу сертифікаціям відповідності, щоб мінімізувати ризик відповідальності як для охоплених організацій, так і для їхніх офіцерів із сертифікації». ***(Timothy Howard, Brock Dahl, Beth George, David Sewell and Charlie Carroll. DFS Expands Scope of Cybersecurity Regulations // Freshfields Bruckhaus Deringer LLP (https://technologyquotient.freshfields.com/post/102is8r/dfs-expands-scope-of-cybersecurity-regulations#page=1). 09.11.2023).***

***

**«1 листопада 2023 року Міністерство внутрішньої безпеки США (DHS) оголосило, що готовність до кібербезпеки використовуватиметься як фактор оцінки для контрактів, які передбачають використання контрольованої несекретної інформації (CUI).** Це слідує за суттєвими правилами DHS, ухваленими на початку цього року, які вимагають від певних підрядників DHS, які мають CUI або керують інформаційними системами DHS, дотримуватись розширених засобів контролю кібербезпеки та вимог до звітності. DHS не повідомляє, коли політика набуде чинності, але запрошує коментарі до 17 листопада 2023 року на електронну адресу, зазначену в повідомленні на sam.gov.

DHS планує включити політику, відому як коефіцієнт готовності кібербезпеки, до закупівель, які оцінюються на основі найкращої вартості, і розділити підрядників на три групи:

Висока ймовірність готовності до кібербезпеки (для підрядників, які перевищують середнє значення популяції підрядників DHS, які обробляють дані CUI (вище 53-го процентиля))

Ймовірність готовності до кібербезпеки (для підрядників між 15-м і 53-м процентилем порівняно з іншими підрядниками DHS, які обробляють дані CUI)

Низька ймовірність готовності до кібербезпеки (для підрядників нижче 15 процентиля підрядників DHS, які обробляють дані CUI)

Готовність оцінюватиметься відповідно до стандартів кібербезпеки, розроблених Національним інститутом стандартів і технологій (NIST), зокрема спеціальної публікації NIST (SP) 800-171, версія 2 і NIST SP 800-172. Зауважте, що NIST зараз розробляє третю версію для NIST 800-171. Підрядники, які подають пропозиції, повинні будуть надати відповіді до DHS через анкету безпечного інструменту оцінки за моделлю, розробленою DHS, і присвоєний рейтинг базуватиметься на кількості та типі вимог кібербезпеки, які підрядник повністю або частково виконав. Незважаючи на відсутність перевірки третьою стороною, підрядникам слід остерігатися надання невірної інформації, оскільки DHS може стверджувати, що дотримання цих заходів контролю є суттєвим для ініціювання наслідків Закону про неправдиві претензії. Крім того, останній проект майбутнього стандарту NIST SP 800-171 включає вимогу сторонньої перевірки (на даний момент).

Примітно, що навіть підрядники, які мають низьку ймовірність готовності до кібербезпеки, не обов’язково будуть виключені з конкурсу, але, ймовірно, їм буде важче досягти успіху після оцінки найкращої вартості. Спосіб формування коефіцієнта оцінки буде особливим для кожного контракту, і йому можуть надаватися різні ваги залежно від характеру контракту та залученої інформації. Крім того, від підрядників, які не відповідають вимогам DHS щодо відповідності

вимогам щодо кібербезпеки, може знадобитися виконати плани дій і основні етапи в якості результату після укладання контракту.

Коли це стане можливим, підрядники повинні уважно вивчити запити з фактором оцінки готовності до кібербезпеки, щоб переконатися, що коефіцієнт оцінки та призначені ваги є чіткими. Якщо ні, підрядники повинні розглянути можливість взаємодії з DHS, якщо це дозволено, або подання протесту на тендерну пропозицію до присудження. Це також є додатковим стимулом для підрядників забезпечувати дотримання різноманітних (а в деяких випадках і різних) стандартів кібербезпеки. Зі свого боку, DHS також вимагає, щоб підрядники з CUI дотримувалися додаткових заходів безпеки, наведених на його веб-сайті. Нарешті, підрядники, які оцінюються за цим фактором, повинні, якщо це можливо, провести підсумковий аналіз, щоб переконатися, що оцінка кібербезпеки відповідає розумінню підрядником власної готовності». ***(Eric S. Crusius. Department of Homeland Security Using Cybersecurity Readiness as an Evaluation Factor // Holland & Knight LLP (https://www.hklaw.com/en/insights/publications/2023/11/department-of-homeland-security-using-cybersecurity-readiness). 10.11.2023).***

***

**«Через два роки після того, як Міністерство юстиції (DOJ) започаткувало Ініціативу проти шахрайства у цивільному кібернетичному середовищі, нещодавно відбулося пожвавлення правозастосування та регулятивної діяльності, пов'язаної з кібербезпекою.** Вересень розпочався розкриттям кримінального позову відповідно до Закону про неправдиві заяви (FCA) проти Університету штату Пенсільванія, стверджуючи, що школа не дотримується вимог кібербезпеки Міністерства оборони (DoD). Лише через кілька днів Міністерство юстиції оголосило про врегулювання у розмірі 4 мільйонів доларів США з Verizon Business Network Services LLC (Verizon) для вирішення претензій щодо того, що телекомунікаційний гігант не відповідав вимогам кібербезпеки під час надання безпечних публічних інтернет-з'єднань федеральним агентствам. А на початку жовтня Федеральна рада з регулювання закупівель

опублікувала два запропонованих правила, що підвищують вимоги до кібербезпеки для державних підрядників, що може створити для багатьох компаній нову або посилену відповідальність FCA.

На тлі цієї зростаючої активності FCA, пов’язаної з кібернетичною інформацією, технологічні компанії, які працюють з урядом, та інші організації, які отримують державні кошти, повинні розуміти, як регулятори та приватні інформатори використовують FCA для забезпечення дотримання необхідних стандартів кібербезпеки.

*Фон*

FCA є основним інструментом для боротьби зі звинуваченнями в шахрайстві в сфері державних контрактів. У жовтні 2021 року Міністерство юстиції запровадило Ініціативу протидії цивільному кібершахрайству, залучивши FCA до запобігання шахрайству, пов’язаному з кібербезпекою, з боку державних підрядників і одержувачів федеральних грантів, які свідомо надають неякісні продукти кібербезпеки, спотворюють свою практику чи статус у сфері кібербезпеки або порушують вимоги звітування про порушення. Відтоді федеральні відомства продовжують публікувати нові вимоги щодо кібербезпеки та зобов’язання щодо звітності в державних контрактах і угодах про фінансування, що може призвести до ще більших зусиль Міністерства юстиції та пов’язаних з ним відомств для переслідування ймовірного шахрайства, марнотратства та зловживань державними витратами згідно з FCA. FCA також містить положення qui tam, яке дозволяє інформаторам («родичам») подавати позови від імені уряду проти ймовірних шахраїв і брати участь у будь-якому відшкодуванні.

8 березня 2022 року Міністерство юстиції оголосило про перше врегулювання в рамках Ініціативи цивільного кібершахрайства за участю постачальника медичних послуг із Флориди Comprehensive Health Services LLC, який погодився виплатити 930 000 доларів США за усунення порушень FCA, пов’язаних із імовірним наданням неправдивих відомостей ВПС США та Державний департамент, що він дотримувався вимог договору безпеки щодо медичних послуг.

Лише через кілька місяців, 8 липня 2022 року, Міністерство юстиції оголосило про іншу врегулювання FCA, пов'язане з кібербезпекою, за участю підрядника Aerojet Rocketdyne, Inc., що займається оборонним і космічним сектором, який погодився на врегулювання у розмірі 9 мільйонів доларів США для вирішення звинувачень, висунутих у позові про те, що він спотворила свою відповідність нормам Міністерства оборони щодо захисту закритої оборонної інформації, яка включає контрольовану несекретну інформацію, а також правил Національного управління з аеронавтики та дослідження космічного простору (NASA) щодо захисту конфіденційної інформації. 14 березня 2023 року Міністерство юстиції оголосило про ще одну угоду FCA, пов'язану з кібербезпекою, з Jelly Bean Communications Designs LLC (разом із співвласником і менеджером компанії Джеремі Спінксом), яка погодилася виплатити майже 300 000 доларів США за вирішення звинувачень у порушенні компанією та Спінксом FCA через те, що вони не виправляли, оновлювали та підтримували веб-сайт дитячого медичного страхування, який фінансується федеральним бюджетом, який вони створили та розмістили, залишаючи особисту інформацію вразливою для атак.

Справи Університету штату Пенсільванія та Verizon відображають постійну тенденцію зосередження уваги на відповідності вимогам кібербезпеки як потенційному гачку для відповідальності FCA. Ця серія справ і врегулювання вказує на те, що на горизонті, ймовірно, з'являться додаткові дії FCA, пов'язані з кібернетичною інформацією, оскільки регулятори та інформатори намагаються виявити потенційні шахрайські претензії щодо федеральних коштів і заохотити державних підрядників приділяти більше уваги вимогам кібербезпеки, таким чином захищаючи федеральну інфраструктуру від небезпечних вторгнень у систему кібербезпеки.

*Справа інформатора штату Пенсільванія*

1 вересня 2023 року окружний суд США Східного округу Пенсільванії розпечатав позов FCA qui tam про те, що Університет штату Пенсільванія не забезпечив адекватну безпеку секретної інформації захисту. Відповідно до Доповнення щодо федеральних закупівель для оборони (DFARS) 252.204-7012,

підрядники повинні впроваджувати певні засоби контролю кібербезпеки, включаючи, як мінімум, адекватний захист закритої оборонної інформації, що вимагає впровадження 110 засобів контролю кібербезпеки з NIST SP 800-171. Після цього підрядники Міністерства оборони повинні провести самооцінку своєї відповідності цим 110 елементам контролю та надати свою оцінку Міністерству оборони.

Інформатор Метью Декер, колишній директор з інформації лабораторії прикладних досліджень Університету штату Пенсільванія, подав позов від імені уряду. У позові стверджується, що Університет штату Пенсільванія фальшиво засвідчив свою відповідність самооцінці NIST SP 800-171 і ніколи не досяг відповідності DFARS. У скарзі також стверджується, що керівництво університету неодноразово ігнорувало проблеми сертифікації та що конфіденційна інформація була під загрозою під час міграції даних у комерційне хмарне сховище. Хоча Міністерство юстиції відмовилося втручатися у справу, розслідування претензій триває, і воно може вирішити втрутитися пізніше.

Цей випадок підкреслює ризики судових процесів і правозастосування, з якими тепер стикаються державні підрядники через обширний контрольний список засобів контролю кібербезпеки, яким вони повинні відповідати, щоб отримати та зберегти свої контракти. Державні підрядники повинні ретельно вивчати свої самоатестації та реагувати на внутрішні скарги, щоб переконатися, що вони повністю відповідають цим обов'язковим вимогам.

*Врегулювання ініціативи Verizon щодо цивільного кібершахрайства*

Verizon погодилася заплатити приблизно 4 мільйони доларів, щоб розв'язати звинувачення FCA в тому, що компанія не задовольнила певні вимоги кібербезпеки, пов'язані з послугами інформаційних технологій, які надаються федеральним агентствам. Згідно з мировою угодою з Міністерством юстиції від 5 вересня 2023 року, звинувачення стосувалися служби керованого довіреного Інтернет-протоколу (MTIPS) Verizon, яка призначена для надання федеральним агентствам безпечного підключення до публічного Інтернету та інших зовнішніх мереж. Угодою було вирішено звинувачення в тому, що рішення MTIPS не

задовольняє контроль кібербезпеки, необхідний для контрактів на надійне підключення до Інтернету для адміністрування загальних послуг (GSA) на 2017-2021 роки.

Крім того, мирова угода відбулася після того, як компанія Verizon самостійно оприлюднила проблему та вжила заходів щодо її виправлення. Наприклад, Verizon ініціював власне незалежне розслідування та перевірку відповідності, надав докладні додаткові письмові розкриття інформації та співпрацював з урядовим розслідуванням, у тому числі шляхом виявлення осіб, відповідальних за проблеми, збереження відповідних документів і надання постійного розкриття відповідної інформації. Verizon також працював над оновленням плану безпеки системи MTIPS і вживав інших заходів для виправлення ситуації, щоб виконати свої договірні вимоги. У мировій угоді зазначено, що 2,7 мільйона доларів з мирової угоди було виділено як реституція, а приблизно 1,3 мільйона доларів залишилося від застосування урядом мультиплікатора. Згідно з FCA, уряд може вимагати відшкодування збитків у потрійному розмірі плюс встановлені законом штрафи, тобто Verizon, ймовірно, уникнув значно більшого загального штрафу, саморозголошуючи інформацію.

*Запропоновані кіберправила Федеральної ради з регулювання придбань (FAR).*

На тлі цього підвищеного інтересу FCA Рада FAR нещодавно запропонувала два широкі правила для підвищення вимог до кібербезпеки для федеральних підрядників. Перше запропоноване правило стандартизує договірні кібервимоги для «несекретних федеральних інформаційних систем». 12 Друге запропоноване правило вимагатиме від підрядників обмінюватися інформацією про кіберзагрози та повідомляти про кіберінциденти уряду протягом восьми годин після виявлення. 13 Ці загальні пропозиції стосуватимуться більшості федеральних підрядників, у тому числі організацій, які в іншому випадку звільнені від багатьох державних правил укладення контрактів і вимагатимуть точного та своєчасного реагування на інциденти для дотримання.

Обидва ці запропоновані правила додатково чітко стверджують, що зобов’язання щодо кібербезпеки та звітування про кіберінциденти є суттєвими для

відповідності державним контрактам і оплати, 14 тим самим створюючи умови для потенційної майбутньої відповідальності FCA за недотримання вимог. Розширення мережі, створеної цими запропонованими правилами, поряд із нещодавнім посиленням діяльності FCA, пов'язаної з кібербезпекою, може мати потенційно серйозні наслідки для зусиль підрядників із дотримання вимог.

Підрядники та інші зацікавлені сторони мають можливість прокоментувати ці запропоновані правила до 4 грудня 2023 року.

*Уроки для федеральних підрядників*

Важливість практики та політики кібербезпеки для організацій, які виконують державні контракти, лише зростатиме. Федеральні підрядники, університети та інші одержувачі федеральних грантів повинні почати повторно оцінювати свою відповідність вимогам кібербезпеки, звертаючи особливу увагу на точність їхньої самооцінки. Ландшафт відповідності кібербезпеці швидко розвивається і вимагає постійного внутрішнього моніторингу, а також системи розгляду внутрішніх скарг. Зовнішній консультант може допомогти забезпечити належну оцінку скарг у світлі зобов'язань компанії щодо кібербезпеки. Додаткове навчання та командне оцінювання також можуть допомогти підрядникам впоратися зі зростаючою та дедалі складнішою мережею вимог до кібербезпеки, з якими стикаються підрядники. Підрядники можуть очікувати, що найближчим часом побачать багато інших примусових дій як з боку уряду, так і з боку інформаторів, тому вони повинні скористатися цією можливістю вже зараз, щоб активізувати свої зусилля з дотримання вимог…» ***(Michelle A. Reed, Michael J. Vernick, Elizabeth Marie Dulong Scott, Angela B. Styles, Natasha G. Kohne, Rachel Claire Kurzweil, Joseph Hold. Government Contractors Beware: New Cybersecurity Rules and False Claims Act Enforcement Actions on the Rise // Akin Gump Strauss Hauer & Feld LLP (https://www.akingump.com/en/insights/alerts/government-contractors-beware-new-cybersecurity-rules-and-false-claims-act-enforcement-actions-on-the-rise). 02.11.2023).***

***

**«Індустрія кібербезпеки не може захистити економіку та спосіб життя нашої країни.**

Хоча це може здатися тривожним, статистика показує сувору реальність. Боротьба з кіберзлочинністю — це місія, яка виходить за межі індивідуальних посад і корпоративних інтересів. Ми боремося з асиметричним ворогом, якому мало що можна втратити і багато чого отримати.

Паралелі між кіберзлочинністю та глобальною війною з тероризмом незаперечні. Кібербезпека – це набагато більше, ніж бізнес-ініціатива. Це необхідна умова довгострокового виживання нашої нації. У нас немає іншого вибору, як змінити наш підхід, мислення та структуру, щоб захистити нашу націю.

*Розуміння ландшафту кібербезпеки*

Ні для кого не секрет, що кіберзлочинні організації набувають все більшого поширення. IBM Згідно зі звітом про вартість витоку даних за 2023 рік, середня глобальна вартість витоку даних у 2023 році становила 4,45 мільйона доларів США, що на 15% більше за три роки.

Очікується, що глобальні витрати на кіберзлочинність зростатимуть на 15% на рік з 2020 по 2025 рік і досягнуть 10,5 трильйонів доларів США на рік проти 3 трильйонів доларів у 2015 році.

«Трирічне порівняння кількості скарг щодо програм-вимагачів, поданих до Федерального бюро розслідувань (ФБР) між 2018 і 2020 роками, демонструє збільшення кількості жертв на 65,7 відсотка та приголомшливе збільшення скоригованих збитків на 705 відсотків», — йдеться у повідомленні. Комітет Сенату США з внутрішньої безпеки та урядових справ.

Це не просто статистика; вони представляють реальну загрозу для компаній, урядів та окремих осіб.

*Відданість серед професіоналів кібербезпеки*

Хоча ми повинні досягати кращих результатів як галузь, це не через помилки чи недоліки фахівців з кібербезпеки. Насправді галузь кібербезпеки наповнена неймовірно блискучими та захопленими людьми.

Професіонали безпеки віддані своїй справі чудово, з чим небагато галузей можуть зрівнятися. Кібербезпека – це мислення, пристрасть і місія багатьох практиків. На жаль, дуже небагато працюють у середовищі, де вони можуть справді рости та процвітати.

*Паралелі з глобальною війною з тероризмом*

Як і терористичні групи, кіберзлочинні групи діють децентралізовано без ієрархії чи етичних обмежень. Кіберзлочинці полюють на все: від компаній зі списку Fortune 500 до найменших компаній-власників-операторів — від лікарень до шкіл.

Кіберзлочинність не міститься в цифровій сфері. Платежі за програми-вимагачі є значним джерелом фінансування терористичних груп, які забирають невинні життя по всьому світу.

*Поточна ситуація*

Індустрія кібербезпеки не має належної структури для ведення асиметричної війни. Він зосереджений на неправильних цілях і не в змозі відповідати децентралізованій, гіперфокусованій природі ворога.

Багато хто поспішає назвати нестачу талантів у сфері кібербезпеки основною проблемою. Цитуючи слова міністра оборони США Дональда Рамсфельда, «ви йдете на війну з тією армією, яка у вас є, а не з тією армією, яку ви, можливо, бажаєте чи бажаєте мати пізніше».

Ми не можемо дозволити собі чекати десятиліттями, набираючи та розвиваючи достатньо нових талантів, щоб перемогти ворога величезною армією професіоналів із безпеки. Також потрібна дуже рідкісна особистість і мислення, щоб досягти успіху в багатьох галузевих ролях. Справжня пристрасть до ремесла є обов’язковою умовою для ефективності. Цю пристрасть неможливо змусити.

У розмові з багатьма спеціалістами з інформаційної безпеки та іншими фахівцями з кібербезпеки по всій країні стало зрозуміло, що значна частина наших нинішніх талантів у сфері кібербезпеки використовується недостатньо. Переважна більшість каже мені, що вони витрачають стільки часу на зустрічі та боротьбу з корпоративною бюрократією, що їм важко реалізувати ініціативи, які справді

зміцнять захист їхніх організацій. Це викликає розчарування, яке призводить до значних витрат і плинності кадрів, а фахівці з кібербезпеки залишають своїх роботодавців у пошуках кращого середовища.

Ми також відчуваємо надмірну увагу до інструментів і технологій безпеки. Значна частина наших спеціалістів із безпеки зосереджена на розробці продукту, а не на забезпеченні людської підтримки, якої потребує більшість організацій.

Ми завжди повинні вдосконалювати технології, але інструменти безпеки настільки хороші, наскільки хороші люди, які за ними стоять. Необхідно враховувати людей, процеси та технології, а людський досвід керує стратегією та тактикою справді стійкої безпеки. Галузі потрібно буде менше зосереджуватися на розробці продуктів, а більше на професійних послугах, щоб надати більше практичної підтримки компаніям середнього ринка та компаніям, що розвиваються, які її потребують найбільше.

*Переосмислення нашого підходу*

Щоб міцніше закріпитися в боротьбі з кіберзлочинністю, ми повинні краще використовувати талановитих професіоналів, які у нас уже є. Настав час по-іншому подумати про створення бізнес-структур і середовища для зростання та процвітання наших фахівців з кібербезпеки.

Щоб бути ефективними в цьому типі асиметричної війни, ми можемо віддзеркалити те, як уряд США переніс свою увагу від масивних звичайних підрозділів із натовпами солдатів і обладнанням до використання високопідготовлених підрозділів спеціальних операцій. Нам потрібні спритні та швидкі команди безпеки, які нададуть компаніям прямий доступ до необхідного досвіду та підтримки без додаткових витрат на посередників і зайвих накладних витрат.

Неможливо, щоб хтось був експертом у всіх сферах кібербезпеки. Нам потрібно заохочувати нішевий досвід, а не розвивати більше спеціалістів загального профілю. Організації можуть поділитися людьми з високим рівнем знань у дуже конкретних сферах. Це виявиться настільки ж ефективним у боротьбі з кіберзлочинністю, як і серед підрозділів військових спеціальних операцій.

Індустрія кібербезпеки має величезну кількість відданих і захоплених професіоналів, які вже знають, як захистити наші цифрові активи. Давайте зведемо до мінімуму ієрархію, усунемося від них і дозволимо їм працювати так, як це відповідає характеру спільного ворога.

Нам пощастило, що для багатьох у цій сфері кібербезпека — це не просто робота чи корпоративна ініціатива. Це покликання та місія, яку ми повинні прийняти, щоб захистити основу економіки та способу життя нашої країни». ***(Zach Fuller. Cybersecurity: It's Not A Job—It's A Mission // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/11/17/cybersecurity-its-not-a-job-its-a-mission/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff&sh=37f55ce84d1f). 17.11.2023).***

***

**«За словами старшого радника Білого дому з кібербезпеки, менш ніж через дев'ять місяців залишилося до публікації довгоочікуваної національної стратегії кібербезпеки.** Адміністрація Байдена працює над оновленням плану впровадження стратегічного документа.

Виступаючи в четвер на заході Scoop News Group CyberTalks, Кріс ДеРуша намалював картину документа, що розвивається, оскільки адміністрація Байдена працює над досягненням своїх цілей у сфері кібербезпеки.

«Ми збираємося оновити цей план впровадження — це не статична річ», — сказав ДеРуша, який також є головним федеральним офіцером з інформаційної безпеки. «Ми вже працюємо над версією 2.0. Коли ми перевіряємо успіхи, виконуючи наступну серію публічних зобов'язань, [ми хочемо] переконатися, що ми дійсно просуваємось вперед».

ДеРуша визнав, що хоча стратегія «представляє позитивне, досяжне бачення досягнення місця», де країна зможе керувати пов'язаними з кіберризиками, ці загрози «не зникнуть», особливо коли йдеться про критичну інфраструктуру.

Стратегія кібербезпеки базується на розпорядженні президента Джо Байдена від травня 2021 року та пропонує низку реформ, спрямованих на широкі покращення комп'ютерної безпеки. Адміністрація працює над модернізацією технології та покращенням кібербезпеки, але ДеРуша заявив у четвер, що сама по собі модернізація не забезпечить покращення безпеки, якого прагне Білий дім.

«Ми знаємо, що не можемо все модернізувати», — сказав ДеРуша. «Ви можете запровадити компенсаційні засоби контролю, але ми повинні мати видимість цього та гарантії, що ми справді керуємо ризиком» для критичної інфраструктури.

З цією метою ДеРуша сказав, що адміністрація вивчає «поточний робочий стан усіх кіберцентрів» і визначає ефективність. Результати цих запитів будуть проаналізовані та використані для «прибирання частини шуму».

Адміністрація Байдена також працює над оновленням національного плану реагування на кіберінциденти, і ДеРаша зазначив, що державно-приватна координація буде мати вирішальне значення для спільного реагування на загрози критичної інфраструктури.

Було досягнуто прогресу у знищенні та знищенні загрозливих суб'єктів, як того вимагає національна стратегія, де Руша зазначив, що нещодавно Білий дім прийняв 50 країн для саміту з боротьби з програмами-вимагачами, результатом якого були зобов'язання щодо обміну інформацією та відмови від викупу.

*Оголошення*

ДеРаша також сказав, що адміністрація Байдена «веде змістовні розмови» щодо федерального механізму захисту від кіберстрахування та залишається повністю відданою налагодженню нових міжнародних партнерств у всьому, що стосується кібернетики.

«Ми не можемо досягти істотного прогресу в управлінні кіберризиками як єдина нація», — сказав ДеРуша. Білий дім «інвестує в ці коаліції… і значуща співпраця буде однією з найважливіших речей, які ми робимо. І ця адміністрація безперечно прагне працювати з нашими однодумцями над спільними цілями». ***(Matt Bracken. White House is 'working on version 2.0' of cyber implementation plan***

*// CyberScoop (https://cyberscoop.com/national-cybersecurity-strategy-chris-derusha/?utm_source=flipboard&utm_content=other). 16.11.2023).*

***

**«Федеральний уряд оголосив про дві ініціативи, спрямовані на посилення підтримки малого та середнього бізнесу (МСП) для зміцнення їхніх навичок кібербезпеки.**

Уряд пообіцяв 7,2 мільйона доларів США на створення добровільної програми кіберперевірки, що дозволить отримати доступ до безкоштовної самооцінки зрілості кібербезпеки.

Він також виділив ще 11 мільйонів доларів США на службу підтримки кібернебезпечної стійкості малого бізнесу, яка пропонує індивідуальну допомогу у вирішенні кіберзавдань і покриває відновлення після кібератак.

Очікується, що підприємства зможуть використовувати ці нові перевірки кібернетичного стану, щоб розрахувати ефективність власних заходів і отримати доступ до навчальних інструментів або матеріалів, необхідних для підвищення кваліфікації.

Міністр малого бізнесу Джулі Коллінз сказала, що малий бізнес є «основою цифрової економіки Австралії, що становить 97 відсотків усіх австралійських підприємств».

«Саме тому уряд продовжуватиме ставити їх у центр наших зусиль із боротьби із загрозами кібербезпеці та сприятиме покращенню їхніх кіберможливостей для створення сильнішої Австралії».

Міністр внутрішніх справ і кібербезпеки Клер О'Ніл також сказала, що майбутня урядова «стратегія кібербезпеки забезпечить доступність підтримки, щоб допомогти підприємствам зрозуміти та покращити свою власну кібербезпеку».

«Стратегія підкріплена шістьма кіберщитами, в основі яких — сильні компанії та громадяни», — сказала вона.

«Підвищення кібербезпеки наших малих підприємств є невід'ємною частиною кіберзахищеної та стійкої нації, і ця спеціальна підтримка значно змінить їх готовність і стійкість».

В окремій публікації на LinkedIn у понеділок О'Ніл сказав, що ця робота доповнює 23,4 мільйона доларів, які вже були виділені протягом трьох років на програму кіберзахисників малого бізнесу, спрямовану на створення внутрішнього потенціалу для захисту від кіберзагроз.

У дописі О'Ніл сказав, що програма кібер-наглядачів «підтримає понад 15 000 малих підприємств для створення кіберрозумної робочої сили». ***(Kate Weber. Gov commits $18.2m for SME cyber security boost // nextmedia Pty Ltd. (https://www.itnews.com.au/news/gov-commits-182m-for-sme-cyber-security-boost-602584). 21.11.2023).***

***

## ***Країни ЄС та Великобританія***

**«У четвер (2 листопада) Управління інформаційної безпеки Німеччини (BSI) представило свій звіт про стан IT та кібербезпеки в країні, який охоплює період з червня 2022 року по червень 2023 року.**

У звіті зазначено, що рівень загрози «вищий, ніж будь-коли раніше», зафіксувавши найвищий середній приріст типів зловмисного програмного забезпечення з 332 000 нових варіантів на день протягом періоду спостереження.

Кількість жертв програм-вимагачів у Німеччині, чиї імена та отримані дані були опубліковані на сайтах витоку, також досягла історичного максимуму у другому кварталі – 65.

«Звіт BSI про стан IT-безпеки в Німеччині в 2023 році доводить, що ситуація із загрозами в кіберпросторі залишається напруженою», — заявила міністр внутрішніх справ Німеччини Ненсі Фазер.

*Програмне забезпечення-вимагач і технічний прогрес*

У звіті також виявлено, що програми-вимагачі залишаються головною загрозою.

Крадіжки особистих даних зростають, і державні установи відзначають збільшення прогресивних постійних загроз (APT) – кібершпигунських або диверсійних атак, які здійснюються з часом для отримання інформації або маніпулювання.

Оскільки зловмисники обирають шлях найменшого опору, малі та середні підприємства (МСП) і органи місцевого самоврядування особливо вразливі до кібератак. Оскільки МСП становлять близько 80% німецької економіки, потенціал загрози особливо високий.

Атаки на ланцюги поставок є ще однією тенденцією, висвітленою у звіті. Тут компанії не націлені безпосередньо, але зловмисне програмне забезпечення, наприклад віруси, поширюється через сторонніх постачальників. Це означає, що велика кількість жертв може бути атакована одночасно.

Згідно зі звітом, також складним є розвиток технологій.

На додаток до технологічного прогресу генеративного штучного інтелекту, який призвів до якісного покращення дипфейків, фішингових і шахрайських атак, розвиток потужної квантової технології та ймовірні загрози кібербезпеці, які вона сприятиме, також розглядаються як виклик.

У звіті також зафіксовано збільшення на 24% кількості вразливостей, виявлених у програмних продуктах. Вони часто є «першим портом заходу для кіберзлочинців». Кожна друга з 70 нових уразливостей, виявлених у середньому на день, була класифікована як критична.

«Кіберзлочинність як послуга» є ще одним ризиком для безпеки.

З професіоналізацію кіберзлочинності та зростання тіньової економіки кіберзлочинців, зловмисники все більше стають послугою, для якої зловмисники можуть придбати інструменти онлайн, зазначається у звіті.

Протягом звітного періоду BSI також зафіксував збільшення DDoS-атак з боку проросійських хактивістів.

«З минулого року ми маємо страшну загарбницьку війну Путіна в Україні. Цього року у нас в Ізраїлі жахлива війна. У нас є цей варварський напад ХАМАС. Це створює неймовірний виклик для органів безпеки», – сказав Фейзер.

*Заходи протидії*

Уряд Німеччини хоче надати BSI більше повноважень приймати рішення, щоб протистояти цій тенденції, розширивши його до центральної ролі у відносинах федерації та землі.

«Німеччина повинна сприймати себе як кібернацію і діяти відповідно. Для BSI створення загальнонаціонального центрального офісу з кібербезпеки має важливе значення в цьому контексті – хоча б для того, щоб створити єдину національну картину ситуації», – каже президент BSI Клаудія Платтнер.

BSI, як центральний офіс, має забезпечити більш скоординовану відповідь на кібератаки на критичну інфраструктуру.

«Якщо, наприклад, світло вимкнеться в Мюнхені та Бремені одночасно через кібератаку, яка може бути політично вмотивованою, я не хочу обговорювати, хто має повноваження приймати рішення, а хто відповідальний», — каже Фейзер.

З огляду на законодавство ЄС щодо підвищення кіберстійкості BSI робить ставку на його ефективність.

Наприклад, країни ЄС мають до жовтня 2024 року запровадити переглянуту Директиву про мережеву та інформаційну безпеку (NIS2) – нове правило, яке накладає на служби хмарних обчислень такі ж суворіші зобов'язання, що й на операторів критичної інфраструктури.

Крім того, інституції ЄС наразі обговорюють запропонований Закон ЄС про кібер-стійкість, метою якого є запровадження загальноєвропейських вимог до кібербезпеки та покладання більшої відповідальності на виробників.

«Я очікую багато руху тут у наступні кілька років. Ми вже готуємося до цього в BSI, щоб побачити, як ми можемо допомогти сформувати ринок відповідним чином», – сказав Платтнер про Закон про кібернетостійкість». ***(Alina Clasen. German government reports risk of cyber threats higher than ever // EURACTIV MEDIA NETWORK BV. (https://www.euractiv.com/section/cybersecurity/news/risk-of-cyber-threats-in-germany-higher-than-ever-government-***

***report/?utm_source=flipboard&utm_content=EURACTIV%2Fmagazine%2FEURACTIV). 03.11.2023).***

***

**«Нове опитування Dell Technologies спільно з Executive Institute показало, що дві третини компаній в Ірландії планують інвестувати у свою кібербезпеку, оскільки кіберзагрози продовжують зростати. Крім того, 93% організацій вже вжили заходів для покращення своїх заходів захисту даних за останні 12 місяців.**

Останнє опитування Digital Pulse Survey, в якому взяли участь понад 150 бізнес-лідерів, показало, що ірландський бізнес бореться під тягарем зростаючих кібератак. Більшість респондентів (64%) сказали, що постійно зростаюча кількість атак є основною перешкодою для підвищення кіберстійкості їхньої організації, причому 13% вказали на відсутність внутрішніх кібернавичок і досвіду, а 9% вказали на застарілу технологію та початкові інвестиції в рішення з кібербезпеки.

Підкреслюючи кібернебезпеки, пов'язані з гібридною роботою, 68% підприємств уже вжили заходів для пом'якшення кіберризиків гнучких і дистанційних моделей роботи.

Опитування Digital Pulse Survey показало, що ірландські компанії все частіше звертаються до технологій, щоб допомогти їм досягти своїх цілей сталого розвитку. Близько 84% бізнес-лідерів сказали, що технології позитивно вплинули на їхні цілі сталого розвитку. Більше третини (37%) використовували технологію для підвищення енергоефективності, 24% використовували її для полегшення гібридної або віддаленої роботи, а 20% використовували технологію для зменшення викидів вуглецю.

Крім того, майже половина (49%) ірландських бізнес-лідерів заявили, що розглядають можливість заміни застарілих технологій протягом наступних 12 місяців, щоб зменшити вищі витрати на електроенергію.

Кетрін Дойл, керуючий директор Dell Technologies Ireland, сказала: «Очевидно, що кіберризики продовжують серйозно обтяжувати бізнес-лідерів,

коли вони просувають свої плани цифрової трансформації. Переважна більшість з них вжили заходів для покращення захисту своїх даних, а дві третини планують збільшити ці інвестиції в наступному році. Проактивні та своєчасні дії будуть життєво важливими для посилення кіберзахисту.

«Оскільки компанії працюють над підвищенням своєї кіберстійкості, також позитивно бачити роль технологій у стимулюванні стійких інновацій. Від використання технологій для підвищення енергоефективності та полегшення віддаленої роботи до досягнення операційної ефективності, цифрова трансформація може допомогти лідерам сформувати більш стійке майбутнє».

Конор Морріс, керуючий директор Executive Institute, сказав: «Результати опитування свідчать про те, що загроза, яку представляють кібератаки, продовжує зростати та загрожує майбутньому успіху наших членських організацій. Ці напади стають все більш частими та все більш витонченими. Планування та прийняття стратегії безпеки, яка залишається актуальною та такою ж актуальною, як і самі нові кіберзагрози, стане ключовим фактором у майбутньому». ***(Two thirds of Irish businesses to increase investment in cyber security // Tech Network (https://www.techcentral.ie/two-thirds-of-irish-businesses-to-increase-investment-in-cyber-security/). 08.11.2023).***

***

**«Потенційний технічний розвиток може мати потенційно значні наслідки для постачальників хмарних послуг, заснованих за межами ЄС.** Запропонована схема сертифікації кібербезпеки ЄС для хмарних сервісів (EUCS), яка була розроблена агентством ЄС з кібербезпеки ENISA протягом останніх двох років і, як очікується, буде прийнята Європейською комісією як імплементаційний акт у першому кварталі 2024 року, якщо буде прийнята у своїй поточній формі встановити певні вимоги, які могли б:

виключити хмарних провайдерів із-за меж ЄС надання певних послуг («високого» рівня) європейським компаніям, а також заборонити клієнтам хмарних технологій ЄС отримати доступ до послуг цих постачальників поза ЄС.

*Локалізація даних і штаб-квартира ЄС*

EUCS випливає з Закону ЄС про кібербезпеку, який передбачає створення загальноєвропейської схеми сертифікації безпеки для хмарних провайдерів, розробленої ENISA та ухваленої Комісією через вторинне законодавство (як зазначено в попередньому блозі). Після публічних консультацій у 2021 році ENISA створила спеціальну робочу групу, якій доручено підготувати проект.

Франція, Італія та Іспанія подали пропозицію робочій групі, виступаючи за додавання нових критеріїв до схеми, щоб компанії могли кваліфікуватися як право пропонувати послуги, що забезпечують найвищий рівень безпеки. Запропоновані критерії включали локалізацію хмарних служб і даних у межах ЄС – по суті, це означає, що постачальники повинні мати штаб-квартиру в ЄС і надавати свої хмарні послуги з ЄС. Ірландія, Швеція та Нідерланди стверджували, що такі вимоги не належать до схеми сертифікації кібербезпеки, оскільки вимога, щоб хмарні провайдери базувалися в Європі, відображає політичні, а не кібербезпекові інтереси, і тому запропонували, щоб це питання було обговорене Радою ЄС.

Останній проект EUCS містить добровільну схему, яка визначає три рівні гарантії (базовий, суттєвий або високий) на основі рівня ризику, пов'язаного з передбачуваним використанням хмарних служб. Кандидатська схема, яка призначена для застосування в усіх державах-членах для всіх хмарних сервісів, включає такі вимоги, як локалізація даних і присутність у ЄС глобальної штаб-квартири для послуг із найвищим рівнем надійності.

Ці нові вимоги можуть означати, що європейські користувачі, які мають рекомендацію або вимогу щодо використання хмарних сервісів високого рівня гарантії, можуть більше не мати доступу до хмарних сервісів деяких іноземних постачальників. Натомість клієнтам хмарних технологій із ЄС може знадобитися використовувати постачальників, які зберігають і обробляють дані в межах ЄС відповідними компаніями з ЄС. Як і інші стандарти Закону про кібербезпеку, EUCS наразі є добровільним, але його можна зробити обов'язковим для певних категорій клієнтів хмарних технологій ЄС відповідно до Директиви NIS2 (як зазначено в нашому попередньому блозі) або Закону про кібернетостійкість. Хоча основною

метою EUCS є підвищення довіри до хмарних сервісів шляхом визначення еталонного набору вимог до кібербезпеки, вимоги до локалізації даних можуть позбавити багатьох компаній з-за меж ЄС можливості отримати найвищий рівень надійності.

*Хто вирішує?*

Одне фундаментальне питання, яке піднімає EUCS, полягає в тому, хто має визначати нові вимоги: ENISA та Комісія чи ширший набір зацікавлених сторін у Парламенті та Раді. Наприклад, якщо Комісія прийме EUCS через імплементаційний акт, Парламент і Рада не матимуть можливості голосувати або вносити зміни до тексту. Співзаконодавці зможуть заперечити, лише якщо вони вважатимуть, що Комісія перевищує свій мандат. Ця обмежена роль була підкреслена кількома членами Європарламенту, які нещодавно подали поправки до запропонованого Регламенту про керовані служби безпеки, що вносить зміни до CSA: зокрема, вони запропонували змінити процедуру прийняття схем ENISA через делеговані акти (де Парламент і Рада мали б a say) замість імплементаційних актів.

*Цифровий контроль, можливості та солідарність*

Дилеми, поставлені EUCS, відображають ширшу дискусію всередині ЄС щодо того, чи слід йому прагнути до «цифрового суверенітету» як до політичних цілей і як найкраще уявити цю мету. Цифровий суверенітет часто розглядається в ЄС як контроль: наприклад, вимагають, щоб штаб-квартира компанії або сервери були розташовані в ЄС. Але суверенітет також можна розуміти як потребу в спроможності ЄС, як стверджував серед інших президент Франції Еммануель Макрон. З цієї точки зору деякі стверджують, що правила, які обмежують доступ до провідних світових технологій, можна розглядати як такі, що суперечать прагненням ЄС щодо суверенітету, оскільки вони перешкоджають можливостям. Окрім цифрового суверенітету, деякі запропонували концепцію «цифрової солідарності», яка наголошує на сприянні партнерствам у сфері кібербезпеки з надійними приватними організаціями всередині та за межами ЄС на основі їх відповідності існуючим нормам і належної поведінки в цифровій сфері. Залежно

від основної інтелектуальної структури, EUCS можна розглядати по-різному». ***(Lisa Peets, Marty Hansen, Mark Young, Aleksander Aleksiev and Bart M.J. Szewczyk. Implications of the EU Cybersecurity Scheme for Cloud Services // Covington & Burling LLP (https://www.globalpolicywatch.com/2023/11/implications-of-the-eu-cybersecurity-scheme-for-cloud-services/#page=1). 01.11.2023).***

***

**«…Директива NIS 1 (Директива (ЄС) 2016/1148), абревіатура мережевої та інформаційної безпеки, була прийнята в 2016 році.** Це був перший законодавчий захід на європейському рівні з метою посилення співпраці між державами-членами та створення першого рівня гармонізації у сфері кібербезпеки.

*Коли?*

Прийнятий 6 липня 2016 р. з транспозицією до 9 травня 2018 р. (в Італії Законодавчим декретом 65/2018, Декрет NIS). Директива NIS 1 була скасована з набранням чинності Директивою NIS 2 (див. нижче).

*Кому воно адресоване?*

Директива NIS 1 визначає дві категорії суб'єктів, до яких поширюються спеціальні положення:

Оператори основних послуг (ESP): державні або приватні організації, які відіграють важливу роль для суспільства та економіки та надають основні послуги (зазвичай ідентифіковані як критична інфраструктура). Держави-члени безпосередньо визначають ESP у критичних секторах (енергетика, транспорт, банківська справа, фінансові ринки, охорона здоров'я, постачання та розподіл питної води та цифрова інфраструктура) на основі того, наскільки важливою є послуга та ризиків, пов'язаних з інцидентом, що впливає на послугу.

Постачальники цифрових послуг (DSP): компанії, які надають послуги електронної комерції, хмарних обчислень або пошукових систем (якщо вони не є МСП).

Директива NIS 1 дозволяє державам-членам розширювати сектори/категорії організацій, до яких мають застосовуватися кіберзобов'язання.

*Що це передбачає?*

Директива NIS 1 вимагає від держав-членів:

прийняти національну стратегію кібербезпеки, яка визначає стратегічні цілі та пріоритети, відповідну політику та регуляторні заходи на національному рівні;

забезпечувати міжнародне співробітництво та співпрацю з ENISA (Агентство Європейського союзу мережевої та інформаційної безпеки) через визначені механізми; і призначити національні органи влади, контактні пункти та CSIRT (групу реагування на інциденти комп'ютерної безпеки), відповідальні за моніторинг інцидентів безпеки на національному рівні.

Щодо ESP та DSP Директива NIS 1 по суті накладає два набори зобов'язань:

Заходи безпеки – застосуйте відповідні та пропорційні заходи безпеки для управління ризиками та запобігання та мінімізації впливу інцидентів безпеки (з деякими більш конкретними заходами для DSP).

Звітування про інциденти – повідомляйте без зайвої затримки органи влади чи CSIRT про інциденти, які мають значний вплив на безперервність надання основних послуг (на основі кількості постраждалих користувачів, тривалості та географічного поширення).

NIS Directive 1 також заохочує організації, які не визначені як ESP та DSP, повідомляти про інциденти зі значним впливом на добровільній основі.

*NIS Директива 2*

Директива NIS 2 (Директива (ЄС) 2022/2555) відповідає потребі оновити та зміцнити нормативну базу, передбачену Директивою NIS 1. Великі розбіжності у виконанні зобов'язань згідно з Директивою NIS 1 призвели до нерівномірних рівнів безпеки та вразливості між державами-членами з можливим впливом на ЄС в цілому.

Метою Директиви NIS 2, яка скасовує Директиву NIS 1, є усунення розбіжностей між правовими системами, посилення зобов'язань щодо кібербезпеки, розширення кількості залучених секторів і учасників і посилення співпраці між державами-членами для досягнення більшої однаковості застосування.

*Коли?*

Прийнятий 14 жовтня 2022 року, наразі чинний, але має бути транспонований у національне законодавство до 17 жовтня 2024 року.

*Кому воно адресоване?*

Директива NIS 2 усуває різницю між ESP та DSP. Натомість він запроваджує деякі уніфіковані критерії для визначення двох нових категорій суб'єктів господарювання, на які поширюватимуться зобов'язання Директиви, а саме:

«необхідні» предмети

«важливі» предмети

Ці суб'єкти мають бути визначені в «важливих» секторах, які включають як сектори, уже визначені відповідно до Директиви NIS 1, так і додатковий список «дуже критичних» секторів (наприклад, медичні послуги, поштові послуги, харчові продукти та сектор машин/обладнання, інші цифрові послуги). Також застосовується критерій розміру, який виключає малі та середні підприємства зі сфери застосування, за деякими винятками залежно від критичності наданої послуги (наприклад, електронні комунікації чи довірчі послуги).

Держави-члени мають визначити до 17 квітня 2025 року перелік важливих і важливих гравців, які повинні будуть надати необхідну інформацію.

*Що це передбачає?*

Директива NIS 2 суттєво посилює зобов'язання, які вже присутні в Директиві NIS 1, зокрема:

Директива NIS 2 містить мінімальний перелік заходів безпеки, які необхідно впровадити.

Заходи безпеки – підхід «багато ризиків» у прийнятті відповідних і пропорційних технічних, операційних та організаційних заходів безпеки має бути прийнятий для:

керувати ризиками безпеки мережевих та інформаційних систем, які суб'єкти використовують для своїх операцій або для надання своїх послуг; і

запобігання або мінімізація впливу інцидентів на одержувачів послуг та інших послуг.

Повідомлення про інциденти – посилення зобов'язань повідомляти та повідомляти про «значні інциденти» владі та CSIRT відповідно до багатоетапної схеми із заздалегідь визначеними часовими рамками (скорочено до 24 годин з моменту отримання інформації для надсилання раннього попередження з наступним повідомленням про детальний аналіз інциденту протягом 72 годин з моменту отримання інформації). Там, де це доцільно, також вимагається повідомлення без невиправданої затримки про значні інциденти.

На додаток до цих положень Директива NIS 2 вимагає від держав-членів ухвалити наглядові та примусові заходи (наприклад, аудити та перевірки), а також нові зобов'язання щодо обміну інформацією про кібербезпеку». ***(Maria Chiara Meneghetti. CyberItalia: The NIS 1 Directive and the new NIS 2 Directive in a nutshell // DLA Piper (https://www.dlapiper.com/en/insights/publications/law-in-tech/cyberitalia-the-nis-1-directive-and-the-new-nis-2-directive-in-a-nutshell). 07.11.2023).***

***

**«Підприємства зазнають дедалі більших обсягів кібератак з року в рік. Генеративний штучний інтелект підвищує складність тактики кіберзлочинців, у той час як галасливий ландшафт загроз створює постійні виклики для бізнесу, які необхідно подолати.** Ситуація посилюється через обмежені бюджети на кібербезпеку, які продовжують залишатися проблемою для компаній, які розробляють свої стратегії безпеки. Насправді в останньому звіті iomart про безпеку виявлено, що 27% організацій вважають, що їхні бюджети недостатні для повного захисту.

Оскільки кількість інцидентів зростає, уряд Великої Британії випустив кілька попереджень для компаній щодо посилення безпеки через підвищену загрозу нападів на національні держави. Під час нашого дослідження ми виявили, що, хоча організації вже виділяють приблизно 40 190 фунтів стерлінгів на оцінку вразливості, тестування пера та укладання червоних команд, цього не завжди достатньо, щоб впоратися з досвідченими зловмисниками. І зараз, як ніколи,

життєво важливо, щоб особи, які приймають рішення, зрозуміли ширшу картину середовища загроз і те, як вони можуть найкращим чином підійти до побудови надійної стратегії, яка є одночасно реактивною та проактивною. Однак на сьогоднішньому складному економічному фоні, геополітичній напруженості та згаданому вище запровадженні моделей AI та ML узгодження бюджетів відповідно до зростаючих потреб у безпеці є головним болем для керівників кібербезпеки.

Хоча не всі кіберстратегії вимагатимуть величезних бюджетів, лідери повинні збільшувати свої витрати на захист своєї організації та її активів, де це можливо, особливо тому, що менше половини (49%) фахівців із безпеки впевнені у здатності свого бізнесу протистояти різноманітним загрозам. як-от фішинг і зловмисне програмне забезпечення, тоді як ще менше (25%) вважають, що вони можуть боротися з програмами-вимагачами. Вже одне це підкреслює необхідність збільшення бюджетів для досягнення цілей кібербезпеки, зокрема зі зростанням страхових премій і значними витратами на відновлення.

*Закладання основи*

Якщо бізнес зробив необхідну основу, створення потужної стратегії кібербезпеки не повинно розбити банк. Насправді більшість організацій вже матимуть правильну технологію або достатній бюджет, щоб убезпечити себе; можливо, вони просто не використовують його ефективно.

Хмара та автоматизація, наприклад, є основою будь-якої кіберстратегії. Наше дослідження показує, що 74% організацій вже покладаються на приватну хмару, тоді як 65% покладаються на автоматизацію. Приватна хмара дозволяє організаціям не тільки зберігати всю свою інформацію в одному місці, але й обмежувати доступ до документів, маючи при цьому кращу видимість і повноваження щодо аудиту конфіденційних даних. Використання хмари забезпечує автоматичні входи в систему доступу користувачів і редагування будь-яких документів, що допомагає командам безпеки реагувати на інциденти безпеки, оскільки вони можуть бачити, як обробляється інформація.

Крім того, автоматизовані рішення, такі як моніторинг SIEM, допомагають організаціям бути в курсі будь-яких потенційних загроз або підозрілої поведінки.

Використовуючи автоматичний моніторинг і вирішення інцидентів безпеки, організації можуть легше фільтрувати шум сповіщень і отримати видимість того, що відбувається в їхніх мережах. Це лише дві існуючі технології, які більшість організацій уже використовує. Вони створюють гарну основу для стратегії безпеки, оскільки, як правило, економічно ефективні та безпечні. Зважаючи на це, життєво важливо, щоб організації знали, як найкраще розподіляти свої бюджети та в які технології та страхування інвестувати. Ось тут і виникає розуміння ризику.

*Максимальне збільшення бюджетів безпеки*

Щоб отримати максимальну віддачу від своїх бюджетів, вкрай важливо, щоб керівники бізнесу та безпеки розуміли ландшафт загроз і ризик, якому вони піддаються. Це можна зробити, провівши оцінку ризику, щоб оцінити ймовірність і наслідки атаки, одночасно обмірковуючи типи загроз, які можуть націлитися на ваш бізнес і чому. Це дозволить організації повністю оцінити людей, процеси та технології, необхідні для пом’якшення та обмеження загрози для їхнього бізнесу, а також дотримуватись нових вимог, що висуваються постачальниками полісів кіберстрахування.

Подібним чином у зв’язку зі зростанням страхових премій керівники підприємств повинні переконатися, що вони не платять за надлишкове покриття, яке їм може бути непотрібним, дотримуючись кваліфікаційних критеріїв, необхідних для покриття. Зазвичай поліси кіберстрахування тепер вимагають наявності наступного:

Сильний контроль доступу

Регулярні оцінки вразливості

Плани реагування на інциденти Навчання роботодавців/користувачів

Багатофакторна автентифікація (MFA)

Управління привілейованим доступом до шифрування (PAM)

Постійний моніторинг

Розуміючи свій ризик, організації можуть ефективно проаналізувати, від якого типу покриття вони отримають вигоду, а потім повинні розподілити правильний бюджет, щоб відповідати визначеним критеріям.

*Найбільша вразливість*

Невідомо, що люди є однією з найбільших причин кіберінцидентів. Насправді 95% порушень кібербезпеки можна пояснити людською помилкою. І це може бути так само просто, як недотримання найкращих практик щодо пароля або випадкове натискання фішингового посилання. На щастя, наш звіт показав, що більше половини (53%) керівників компаній погоджуються з тим, що регулярне навчання працівників має вирішальне значення для запобігання порушенням, пов'язаним з людьми. Адекватне навчання підвищить обізнаність про типи існуючих загроз, а також про те, як співробітники можуть допомогти їх ідентифікувати та запобігти.

Наші дані також показали, що 63% організацій вже інвестували в навчання співробітників протягом останніх двох років, а 55% планують розширити свою кібервільність до керівників, однак, якщо всі організації не запровадять ретельне навчання, уразливість залишиться. Що організації повинні пам'ятати, це те, що існує ймовірність поширення атаки через ланцюжок поставок; навіть найменша помилка може виявитися серйозною для організацій у цьому ланцюжку.

Використання існуючих технологій, навчання співробітників і вибір правильних премій є основою сильної стратегії безпеки. В ідеальному світі організації виділяли б більші бюджети на центр безпеки (SOC), а також на проактивний моніторинг і реагування на інциденти. Реактивність не дозволяє організаціям залишатися в курсі подій у їхніх мережах і може залишити їх в безвиході, коли стане надто пізно. Зрештою, кібербезпека не повинна бути недоглядом, і за допомогою правильної стратегії та розуміння того, де полягають їхні ризики, організації зможуть краще створювати та підтримувати безпечну стратегію кібербезпеки, щоб захистити себе від найновіших загроз, навіть якщо вони працюють із бюджетними обмеженнями». ***(Matt Dowson. Building a cybersecurity strategy on a constrained budget // Future US, Inc. (https://www.techradar.com/pro/building-a-cybersecurity-strategy-on-a-constrained-budget). 10.11.2023).***

***

**«Європейський Союз (ЄС) та його держави-члени справедливо відомі своєю відданістю правам людини, а також все частіше вважаються лідером у сфері кібербезпеки.** Однак Союз заслуговує на чорну мітку в одній сфері, яка вимагає ретельного балансу конфіденційності та безпеки в Інтернеті: кібернайманці. Ці приватні організації працюють на сірому ринку, часто розробляючи та продаючи агресивні кіберпрограми державним клієнтам. Шкідливі інструменти та послуги, які продають ці фірми, створюють одні з найскладніших ризиків, які загрожують цифровій екосистемі. Вони також підривають індивідуальні права людини.

На жаль, нещодавній звіт Комітету PEGA в Європейському парламенті показав, що принаймні 14 держав ЄС використовували один такий інструмент: шпигунське програмне забезпечення Pegasus від NSO Group. Деякі продовжують до цього часу використовувати цей та інші інструменти та служби з подібним впливом без чіткого контролю. Звіт Європейського парламенту є бажаним кроком, але він не має повноважень виконувати свої рекомендації. Настав час для ЄС та його держав-членів припинити ховатися за виправданнями національної безпеки та прийняти чіткі правила щодо використання кібернайманців.

Минулого тижня Паризький форум миру виніс це питання на перший план. Робоча група, членом якої є Microsoft, була створена в рамках Паризького заклику до довіри та безпеки в кіберпросторі та випустила вказівки для багатьох зацікавлених сторін, які пропонують конкретні дії для промисловості, урядів і громадянського суспільства. Сподіваюся, ЄС та його держави-члени, як підтримці Паризького заклику, прислухаються до нього та звітуватимуть про свій прогрес у виконанні вказівок на Паризькому форумі миру наступного року. Інша позиція полягає в тому, що уряди Франції та Британії за підтримки Фонду Карнегі за міжнародний мир прагнули просувати свою ініціативу щодо боротьби із загрозою комерційного кіберрозповсюдження, яка включає боротьбу з загрозою кібернайманців. Ми сподіваємося, що ця ініціатива набере обертів і призведе до глобального регулювання цього шкідливого ринку.

Відповідно до прийнятих вказівок ми сподіваємося, що країни розглянуть можливість прийняття таких заходів, як:

Розробіть чіткі вказівки щодо прийнятного використання: використання урядами кібернайманців і комерційного шпигунського програмного забезпечення повинно бути обмежено основним використанням відповідно до чітких вказівок щодо прийнятного використання. Це використання здійснюватиметься відповідно до внутрішнього законодавства держав, міжнародних зобов'язань і зобов'язань, відповідно до демократичних цінностей, поваги до універсальних прав людини, громадянських прав і громадянських свобод і верховенства права, і може включати такі принципи, як законність, необхідність, пропорційність або розумність.

Запобігання експорту: Уряди повинні запобігати експорту програмного забезпечення, технологій і обладнання кінцевим користувачам, які, ймовірно, використовуватимуть їх для зловмисної кіберактивності, включаючи несанкціоноване вторгнення в інформаційні системи, відповідно до відповідних правових, нормативних і політичних підходів і відповідного існуючого експорту режими контролю.

Вимагати нагляду: Уряди повинні запровадити відповідні внутрішні механізми нагляду, які допоможуть забезпечити дотримання національних законів, процедур і політики разом із застосовними міжнародними зобов'язаннями щодо прав людини.

Прийняти прозору практику закупівель: Уряди повинні бути прозорими у своїй практиці закупівель, вимагаючи від постачальників узгодженості з Керівними принципами ООН щодо бізнесу та прав людини; визначити запобіжні заходи для запобігання зловживанню або дискримінаційному використанню; і регулярно розкривати всі договірні відносини з кібернайманцями, у тому числі щодо закупівлі комерційного шпигунського програмного забезпечення.

Зобов'язати перевірку постачальників: Уряди повинні встановити та оприлюднити процедури моніторингу та перевірки, щоб переконатися, що кібернайманці – особливо ті, хто є їхніми громадянами, резидентами або підрядниками – дотримуються всіх чинних внутрішніх і міжнародних законів.

Чорний список порушників: Уряди повинні розглянути питання про заборону доступу до ринку для кібернайманців, які порушують міжнародні норми та права людини, і занесення до чорного списку, блокуючи доступ до певних ринків. Це також допоможе у боротьбі з розповсюдженням шкідливого програмного забезпечення, наприклад комерційного шпигунського програмного забезпечення.

Створіть огородження для колишніх державних службовців: Уряди повинні розробити необхідні огородження для колишніх державних службовців, включно з тими, хто служив у війську, розвідувальному співтоваристві, правоохоронних органах чи інших органах національної безпеки чи кібербезпеки, які бажають працювати в фірмах кібернайманців, у тому числі тих, продажу комерційного шпигунського програмного забезпечення після закінчення терміну державної служби. Уряди визначать відповідні механізми для зменшення ризиків і підвищення безпеки, включаючи вимоги до звітності для такого працевлаштування після служби, можливі обмеження та відповідні тренінги.

Галузь також посилила наші зусилля для боротьби з цією загрозою. Технологічна угода з кібербезпеки оголосила, що на майбутньому Саміті за демократію почне відстежувати, які уряди приймуть політику та правила, спрямовані на обмеження несумлінного використання цих інструментів і послуг, починаючи з держав, які підтримали Паризький виклик. Крім того, LinkedIn і Microsoft змогли розкрити інформацію про те, як кібернайманець, відомий як Blue Tsunami, протягом кількох років працював у LinkedIn і використовував профілі приманок, фальшиві вакансії та фальшиві компанії для участі в операціях або HUMINT (людський інтелект).) операції проти жертв, які мають доступ до організацій, що становлять інтерес для їхніх клієнтів.

Без належних огорож постійне зростання ринку кібернайманців і безвідповідальне використання цих можливостей з часом призведе до значної шкоди та системної нестабільності в кіберпросторі. Використовуючи мирні технології, ці фірми також наражають незліченну кількість інших на загрози безпеці, дестабілізуючи та підриваючи довіру в ширшому онлайн-середовищі. Ми вважаємо, що ці заходи є необхідними та можливими для захисту безпеки та прав

людини ЄС та його громадян, а також глобальної цифрової спільноти. Ми закликаємо ЄС та його держави-члени діяти швидко та рішуче, щоб протистояти загрозі з боку кібернайманців». ***(Nikolas Ott. Countering Cyber Mercenaries // Directions Blog (https://directionsblog.eu/cyber-mercenaries-a-human-rights-and-security-crisis-that-europe-must-address/). 15.11.2023).***

***

**«Постійні геополітичні виклики та ШІ також становлять загрозу для виборів у Великобританії, попередив Національний центр кібербезпеки (NCSC) у своєму щорічному огляді.**

За останній рік з'явився новий тип кіберсупротивника: державні суб'єкти, мотивовані ідеологічно, а не фінансово, йдеться у звіті NCSC.

NCSC, що входить до складу GCHQ, висвітлив Китай і Росію як тривалі та значні загрози кібербезпеці Великобританії, зазначивши, що багато нових державних груп, які, як він бачив, симпатизують вторгненню Москви в Україну.

Стосовно AI NCSC попередив, що наступні загальні вибори у Великій Британії, які очікуються наступного року, будуть першими, які відбудуться на тлі значного прогресу в технології, який, за його словами, дозволить і посилить існуючі проблеми.

Агентство з кібербезпеки заявило, що великі мовні моделі – технологічні програми, на яких побудовані такі як ChatGPT – майже напевно будуть використовуватися для створення підробленого контенту в рамках кампаній з дезінформації, щоб зруйнувати демократичний процес.

На першому саміті з питань безпеки штучного інтелекту, який відбувся у Великій Британії на початку цього місяця, представники галузі та світові лідери попередили про те, що ця технологія може допомогти кіберзлочинцям здійснювати більш витончені атаки.

«Минулого року відбулася значна еволюція кіберзагрози для Великобританії – не в останню чергу через триваюче вторгнення Росії в Україну, але також через

доступність і можливості нових технологій», – сказала виконавчий директор NCSC Лінді Кемерон.

«Як показує наш щорічний огляд, NCSC і наші партнери підтримали уряд, державний і приватний сектори, громадян і організації будь-якого розміру по всій Великобританії, щоб підвищити обізнаність про кіберзагрози та покращити нашу колективну стійкість.

«Крім нинішніх викликів, ми добре усвідомлюємо загрози на горизонті, включаючи швидкий розвиток технологій і зростаючий ринок кіберпрограм.

«Ми прагнемо протистояти їм прямо та утримувати Сполучене Королівство в авангарді кібербезпеки».

У щорічному огляді говориться, що необхідно працювати, щоб Велика Британія не відставала від мінливих загроз, зокрема щодо підвищення кіберстійкості національної інфраструктури». ***(Soraya Ebrahimi. AI deemed one of the biggest threats to UK cyber security // The National (https://www.thenationalnews.com/world/uk-news/2023/11/14/ai-deemed-one-of-the-biggest-threats-to-uk-cyber-security/). 14.11.2023).***

***

**«Майбутні правила кіберстійкості ЄС стануть актуальними для імпортерів, виробників і дистриб'юторів продуктів із цифровими елементами або так званих підключених продуктів.** Це сталося після того, як ЄС досяг узгодженої позиції щодо Закону ЄС про кібернетостійкість, який має застосовуватися з середини 2025 року для продуктів, розміщених на ринку ЄС.

Мета полягає в тому, щоб продукти з цифровими елементами, які розміщуються, продаються чи використовуються в ЄС, мали менше вразливостей у безпеці та щоб питання кібербезпеки враховувалися при проектуванні життєвого циклу продукту.

Щоб досягти цього, буде вплив на всі рівні ланцюга поставок. Він також прагне підтримувати продукти, які наразі не мають галузевих правил (наприклад, автомобілі та медичне обладнання вже є). Це буде актуально для таких предметів,

як домашні камери, смарт-телевізори, розумні холодильники та камери-няні, або нових продуктів із невбудованими або інтегрованими елементами даних, такими як програмне або апаратне забезпечення.

*Необхідність знати*

У щорічному огляді Національного центру кібербезпеки (NCSC) операційний директор попередив, що «у найближчі роки NCSC очікує, що поширення та комерційна доступність кіберможливостей збільшить загрозу кібербезпеці для Великобританії». За оцінками уряду Великобританії, за останні 12 місяців у всіх компаніях Великобританії було зареєстровано приблизно 2,39 млн випадків кіберзлочинності та приблизно 49 000 випадків шахрайства внаслідок кіберзлочинності.

На яку частину ланцюга постачання це впливає? Виробники зіткнуться з найбільшою кількістю вимог, але існують також заходи контролю, покладені на імпортерів і дистриб'юторів, такі як належна обачність. Це потенційно може вплинути на британські підприємства в тій мірі, в якій продукти, які вони виробляють або експортують, будуть продавати або постачати в ЄС.

*Основна кібербезпека*

Для виробників це означатиме забезпечення відповідності продуктів основним вимогам кібербезпеки. Додаткові відомості викладені в Додатку 1 до законодавства. Приклади включають проектування, розробку та виробництво, які:

Забезпечує належний рівень кібербезпеки на основі ризиків

Створює продукти без будь-яких відомих уразливостей

Включає проведення оцінки ризиків

Поставляється з безпечною конфігурацією за замовчуванням, включаючи можливість скинути продукт до початкового стану

Враховує захист від несанкціонованого доступу за допомогою відповідних механізмів контролю, таких як автентифікація, ідентифікація або система керування доступом

Захищає конфіденційність збережених, переданих, наприклад, шляхом шифрування відповідних даних у стані спокою або під час передачі за допомогою найсучасніших механізмів

Враховує цілісність збережених, переданих або оброблених даних (особистих чи інших) і забезпечує захист від будь-яких маніпуляцій або модифікацій, не дозволених користувачем, а також повідомляє про пошкодження

Обробляє лише дані, які є адекватними, актуальними та обмеженими тим, що необхідно для запланованого використання продукту (мінімізація даних), і

Захищає доступність основних функцій, зокрема стійкість до атак типу «відмова в обслуговуванні» та пом’якшення таких атак.

*Вимоги до обробки вразливостей*

Для виробників це означатиме, що вразливості можна усунути за допомогою оновлень безпеки, включаючи автоматичні оновлення та сповіщення користувачів про доступні оновлення. Інші вимоги включають:

Документація вразливостей і компонентів, що містяться в продукті

Негайне усунення вразливостей, зокрема шляхом надання оновлень безпеки

Застосування ефективних і регулярних тестів і оглядів безпеки продукту з цифровими елементами

Щойно оновлення системи безпеки стане доступним, публічно розкрийте інформацію про виправлені вразливості

Впровадження узгодженої політики розкриття вразливостей і механізмів для безпечного розповсюдження оновлень, щоб забезпечити своєчасне усунення або пом’якшення вразливостей, які можна використати

Переконайтеся, що доступні виправлення або оновлення безпеки для вирішення виявлених проблем безпеки розповсюджуються негайно та безкоштовно разом із консультативними повідомленнями, які надають користувачам відповідну інформацію, зокрема щодо можливих дій, які необхідно вжити

*Режим належної обачності*

Для дистриб’юторів та імпортерів буде діяти режим належної перевірки, що означає, що перед розміщенням на ринку вони повинні будуть провести оцінку

відповідності, маркування CE та спеціальну допоміжну документацію та інструкції з використання.

*Штрафи та недогляд*

Контроль за відповідністю здійснюватиметься як на рівні держав-членів, так і на рівні ЄС. Покарання за невідповідність включають штрафи та коригувальні чи обмежувальні заходи, такі як відкликання або вилучення продукції з відповідного ринку. Для виробників потенційні штрафи найвищі; порушення основних вимог, оцінки відповідності та зобов'язань щодо звітності може призвести до адміністративних штрафів у розмірі до 15 000 000 євро або 2,5% річного світового обороту, залежно від того, яка сума більша. Для імпортерів і дистриб'юторів можуть бути накладені адміністративні штрафи в розмірі до 10 000 000 євро або 2% річного світового обороту, залежно від того, яка сума більша.

*Горизонт кібербезпеки Великобританії*

Ландшафт змінюється з урахуванням майбутнього ландшафту кібербезпеки. Наприклад, Велика Британія також опублікувала Правила 2023 року щодо безпеки продуктів та телекомунікаційної інфраструктури (вимоги безпеки для відповідних продуктів, що підключаються), які застосовуються до «продуктів, які підключаються». Компанії, які працюють як у ЄС, так і у Великій Британії, повинні розуміти та дотримуватися обох наборів вхідних правил. ***(Beverley Flynn and Jessica Gregson. The implications of the EU's Cyber Resilience Act // Stevens & Bolton LLP (https://www.stevens-bolton.com/site/insights/articles/the-implications-of-the-eus-cyber-resilience-act). 15.11.2023).***

***

**«Відповідно до останнього проекту правил, Європейський Союз розглядає можливість розширення сфери застосування запропонованих правил маркування кібербезпеки, які стосуватимуться не лише Amazon, Alphabet Google і Microsoft, але й банків та авіакомпаній.**

Рух ЄС щодо створення такої системи стався в той момент, коли Big Tech сподівається на державний ринок хмарних технологій, щоб стимулювати зростання

в найближчі роки, а потенційний бум штучного інтелекту після вірусного успіху OpenAI's ChatGPT також може підвищити попит на хмарні послуги.

Остання пропозиція від агентства ЄС з кібербезпеки ENISA стосується схеми сертифікації ЄС (EUCS), яка гарантує кібербезпеку хмарних сервісів і визначає, як уряди та компанії в блоці обирають постачальників для свого бізнесу.

Документ зберігає ключові положення, що містяться в попередніх проектах, такі як вимога, щоб американські технічні гіганти створили спільне підприємство з компанією, що базується в ЄС, щоб мати право на маркування кібербезпеки ЄС.

В іншому положенні йдеться про те, що хмарні послуги повинні керуватися та підтримуватися з ЄС, а всі дані клієнтів хмарних послуг повинні зберігатися та оброблятися в ЄС, при цьому закони ЄС мають пріоритет над законами поза ЄС щодо постачальника хмарних послуг.

Ці зобов'язання стосуються найвищого рівня безпеки, яких чотири. Останній проект передбачає можливість розширення цих жорстких вимог до третього найвищого рівня безпеки.

Зараз країни ЄС розглядають останній проект, після чого Європейська комісія ухвалить остаточну схему.

Група технічного лобіювання CCIA заявила, що розширення сфери вплине на більшу кількість галузей.

«Мабуть, найбільш вражаючою частиною цього нового проекту є те, що ENISA тепер пропонує вимоги, які дискримінують іноземних хмарних провайдерів, також можна розширити до нижчих рівнів гарантії», — сказав Александр Рур, директор з громадської політики CCIA Europe.

«Це включатиме банки, а також авіакомпанії, комунальні компанії та жорстко регульовані сектори», - сказав він.

Європейська банківська федерація (EBF), спільно з Європейською групою ощадних банків (ESBG), Асоціацією фінансових ринків Європи (AFME), Європейською федерацією платіжних установ (EPIF) і Insurance Europe у вівторок розкритикували вимоги щодо суверенітету». ***(Foo Yun Chee. EU Mulls Wider Scope for Cybersecurity Certification Scheme – Paper // U.S. News & World Report L.P.***

***(https://www.usnews.com/news/technology/articles/2023-11-23/eu-mulls-wider-scope-for-cybersecurity-certification-scheme-paper). 23.11.2023).***

***

**«З 1 січня 2024 року компанії, які працюють в Угорщині, зіткнуться з новими значними зобов'язаннями щодо кібербезпеки відповідно до законодавства Угорщини, яке імплементує Директиву ЄС NIS2…**

Для імплементації положень Директиви NIS2 до законодавства Угорщини парламент ухвалив Закон XXIII від 2023 року про сертифікацію кібербезпеки та нагляд за кібербезпекою («Закон про сертифікацію кібербезпеки»).

*Відповідні компанії*

Постачальники послуг та організації, що працюють у секторах «високого ризику» та «ризикованих» секторах, підпадають під дію нового закону. Сектори високого ризику включають, наприклад, енергетику, транспорт, охорону здоров'я, цифрову інфраструктуру та електронний зв'язок. До ризикових секторів відносяться, зокрема, поштові послуги, харчова та хімічна промисловість, виробництво електронних продуктів і цифрові послуги.

Як правило, Угорський закон про сертифікацію кібербезпеки не поширюється на МСП, лише на компанії, у яких працює щонайменше 50 співробітників або річний чистий оборот чи загальний баланс якого перевищує 10 мільйонів євро.

Проте на компанії, які надають послуги електронного зв'язку, постачальники довірчих послуг, постачальники послуг DNS, реєстратори доменних імен верхнього рівня та постачальників послуг реєстрації доменних імен, поширюється дія закону незалежно від їх розміру.

*Основні зобов'язання*

Закон про сертифікацію кібербезпеки вимагає базових заходів кібербезпеки для електронних інформаційних систем суб'єктів, на яких поширюється дія цього закону.

У рамках основних заходів кібербезпеки компанії, яких стосується закон, повинні класифікувати свої електронні інформаційні системи. Виходячи з ризику

порушення конфіденційності, цілісності або доступності, має застосовуватися «базовий», «значний» або «високий» клас безпеки.

Спеціальні заходи безпеки, що застосовуються до кожного класу безпеки, будуть викладені в міністерській постанові та застосовуватимуться з 18 жовтня 2024 року.

Компанії, на які поширюється дія закону, мають до 30 червня 2024 року. в зареєструватися Органі нагляду за регульованою діяльністю

Крім того, до 31 грудня 2024 року компанії мають призначити незалежного аудитора, який проведе першу перевірку кібербезпеки відповідно до вимог NIS2 до 31 грудня 2025 року.

*Штрафи*

Згідно з Директивою NIS2, відповідні компанії, які не виконують зобов'язань щодо кібербезпеки, можуть зіткнутися з адміністративними штрафами в розмірі максимум 10 мільйонів євро або 2% від їх загального світового річного обороту». ***(Anita Vereb. New Hungarian Cybersecurity Laws Introduce Important Obligations – The Countdown Begins // CEE Legal Matters (https://ceelegalmatters.com/hungary/24901-new-hungarian-cybersecurity-laws-introduce-important-obligations-the-countdown-begins). 22.11.2023).***

***

## ***Австралія та Нова Зеландія***

***«Австралійська комісія з цінних паперів та інвестицій (ASIC) випустила суворе попередження для організацій по всій країні, закликаючи їх надати пріоритет заходам кібербезпеки.*** Цей заклик до дії слідує за показовим звітом, заснованим на нещодавньому дослідженні кібер-імпульсу ASIC, який підкреслює критичні прогалини в кібер-можливостях корпоративної Австралії.

Згідно з опитуванням, значна кількість організацій демонструє реактивну, а не проактивну позицію щодо управління кіберризиками.

*44% учасників не керують ризиками третіх сторін або ланцюга постачання*

Голова ASIC Джо Лонго висловив стурбованість, заявивши: «Для всіх організацій кібербезпека та кіберстійкість мають бути головним пріоритетом. ASIC очікує, що це включатиме нагляд за ризиками кібербезпеки в усьому ланцюжку постачання організації – тривогу викликало те, що 44% учасників не керують ризиками третіх сторін або ланцюга постачання. Відносини із третіми сторонами надають суб'єктам загрози легкий доступ до систем і мереж організації».

Хоча опитування виявило недоліки, воно також виявило сфери, де організації-учасники розвинули надійні можливості, зокрема в управлінні ідентифікацією та доступом, управлінні та управлінні ризиками, а також управлінні інформаційними активами. Більші організації постійно повідомляли про більш зрілі кібер-можливості порівняно з меншими організаціями. Ця розбіжність значною мірою пояснюється обмеженими людськими та фінансовими ресурсами невеликих організацій, що впливає на їх здатність керувати ризиками третіх сторін, безпекою даних і ефективно приймати галузеві стандарти.

Джо Лонго наголосив на необхідності комплексної готовності, заявивши: «Необхідно вийти за рамки лише безпеки та створити стійкість, тобто здатність реагувати на інцидент і відновлюватися після нього. Недостатньо мати плани. Їх необхідно регулярно тестувати – разом із постійною переоцінкою ризиків кібербезпеки».

Національний координатор з кібербезпеки маршал авіації Даррен Голді AM CSC привітав висновки звіту та відзначив зусилля ASIC у виявленні ключових прогалин у корпоративній кіберстійкості Австралії. Він зауважив: «Кібербезпека має бути пріоритетом для всіх нас, у тому числі для окремих людей і великих і малих компаній. Підтримка доступна – Національне управління кібербезпеки тісно співпрацює з галуззю, щоб сприяти обізнаності та найкращим практикам, а також підтримувати прийняття рішень у відповідь на кіберінциденти. Австралійська стратегія кібербезпеки на 2023-2030 роки дозволить Австралії побудувати та зміцнити свої кіберщити та розвинути нашу стійкість, щоб швидко відновити ситуацію».

Дев'яносто п'ять відсотків учасників опитування вимагали індивідуальних звітів, що вказує на рішучу прихильність підвищити кіберстійкість їхньої організації та дізнатися, як вони порівнюються з аналогами.

На тлі оцінки Австралійського центру кібербезпеки щодо кіберзлочинності, яка обійдеться Австралії в 42 мільярди доларів у 2021 році, перше дослідження ASIC Cyber Pulse є одним із найбільших заходів для оцінки кіберстійкості Австралії. Опитування оцінювало здібності учасників керувати та управляти кіберризиками, захищати інформаційні активи та реагувати на інциденти кібербезпеки…» ***(ASIC survey reveals significant cybersecurity gaps in Australia // FFEEDS DMCC (https://financefeeds.com/asic-survey-reveals-significant-cybersecurity-gaps-in-australia/). 13.11.2023).***

***

**«Два масштабних інциденти, що мали національний вплив, і два викривальні звіти за стільки ж днів, кожен з яких розповідає різні історії, але посилає те саме повідомлення.**

Опитування Cyber Pulse, проведене Австралійською комісією з цінних паперів та інвестицій (ASIC), свідчить про те, що бізнес погано готовий до кіберінцидентів. У звіті 697 добровільним учасникам приписується середньозважений бал кіберзрілості 1,66 з 4,00, і робиться висновок, що «організації швидше реагують, ніж проактивні, коли справа доходить до управління кібербезпекою». Зокрема, опитування показало, що:

44% не керують ризиками третіх сторін або ланцюга постачання,

58% мають обмежені або не мають можливості належним чином захистити конфіденційну інформацію,

33% не мають плану реагування на кіберінциденти

20% не прийняли стандарт кібербезпеки.

Щорічний звіт Австралійського управління сигналів (ASD) про кіберзагрози за 2022-23 роки охоплює ширшу сферу діяльності як компаній, так і окремих осіб,

підкреслюючи підвищену кіберзагрозу для обох. У ньому детально описано зростання за минулий рік:

кількість дзвінків на її Австралійську гарячу лінію кібербезпеки зросла на 32 відсотки (загалом 33 000)

кількість повідомлень про кіберзлочини до Австралійського центру кібербезпеки ASD зросла на 23 відсотки (загалом 94 000), з одним повідомленням кожні 6 хвилин.

середня вартість кіберзлочинності за звіт зросла на 14 відсотків до 71 600 доларів США для великого бізнесу, 97 200 доларів США для середнього бізнесу та 46 000 доларів США для малого бізнесу.

Отже, що австралійський бізнес повинен взяти із загальної ваги цих звітів? Для нас, як для кіберпрофесіоналів, у KordaMentha є три важливі речі.

По-перше, у звіті ASD повідомляється, що кожна п’ята опублікована вразливість IT використовується протягом 48 годин після публікації, при цьому половина всіх уразливостей використовується протягом двох тижнів. Це говорить нам про те, наскільки важливо, щоб підприємства якнайшвидше реагували на ці вразливості. Однак це може бути нелегко, оскільки для виправлення, оновлення або виправлення може знадобитися перевести системи в автономний режим. Крім того, IT-оновлення можуть мати ненавмисний потік впливів, які можуть порушити роботу бізнесу. Це підкреслює важливість управління ризиками для вашої мережі та заздалегідь відомості про альтернативи, доступні для вашого бізнесу, якщо це станеться.

По-друге, звіт ASIC ясно показує, що підприємства недостатньо добре захищаються від кібератак. У той час як компаніям потрібна стратегія обслуговування своїх IT-систем, яка включає виправлення та оновлення, не менш важливою є стратегія глибокого захисту, спрямована на запобігання кіберзломам, управління та пом’якшення кіберінцидентів. Звичайно, один розмір не підходить для всіх, і компаніям слід звертатися за порадою експертів, щоб переконатися, що вони розробляють і впроваджують стратегію кіберризиків, яка є актуальною та прийнятною для них.

По-третє, це питання коли, а не якщо, коли мова йде про кіберзлом. Компанії повинні знати, які дані важливі для них, і переконатися, що вони захищені. Керуйте ризиком, пов’язаним із найважливішими даними, за допомогою засобів контролю доступу та інших засобів. Наприклад, зашифруйте конфіденційні дані та обмежте доступ до них і як.

Ваша стратегія кібербезпеки визначатиметься вашим розміром і типом бізнесу, конфіденційністю даних, які ви зберігаєте, і складністю того, що ви робите. Не кожен інцидент викликає порушення даних, про яке потрібно повідомити, або спонукає до колективного позову, але кожен інцидент коштує компанії втраченого часу, втрати бізнесу та потенційної втрати репутації.

Ці два звіти підтверджують зростаючу частоту, витонченість і серйозність кіберзагроз для окремих осіб і компаній. Вони посилають те саме повідомлення, що критично важливо бути готовим». ***(Brendan Read. What two important cyber reports are telling us // KM Holdings Pty Ltd (https://kordamentha.com/insights/what-two-important-cyber-reports-are-telling-us). 17.11.2023).***

***

**«Федеральний уряд Австралії опублікував довгоочікувану стратегію кібербезпеки.**

Він супроводжувався повідомленням про виділення додаткових 587 мільйонів доларів на витрати та 20 обіцяних дій.

Ці дії утворюють шість «щитів», які уряд має намір побудувати до 2030 року, щоб зробити Австралію світовим лідером у сфері кібербезпеки.

Це: сильний бізнес і громадяни; Безпечна техніка; Обмін загрозами та блокування світового рівня; Захищена критична інфраструктура; Суверенні можливості; і Стійкий регіон і глобальне лідерство.

У цьому довгому та амбітному списку завдань, що є найбільш важливим для середнього та великого бізнесу? Як експерти з кібербезпеки, ось наш погляд на найважливіші дії в стратегії.

*Розширте охоплення та доступність програм кіберобізнаності*

З реагування на кіберінциденти ми знаємо, що переважна більшість цих інцидентів відбувається в результаті людських дій через помилку, незнання, необережність або навіть злий умисел. Освіта з питань кібербезпеки має важливе значення для зменшення цих ризиків і сприяння безпеці кожного бізнесу.

*Покращте видимість та вказівки щодо загроз програм-вимагачів*

Окремі особи та підприємства стикаються зі зростаючими та постійно змінюваними загрозами. Важливо розуміти та пом'якшувати ці загрози. Хоча це має наслідки для боротьби з відмиванням грошей і фінансуванням тероризму для бізнесу в Австралії, зосередження на підвищенні видимості та наданні вказівок з боку уряду є хорошою річчю.

*Прояснити очікування бізнесу щодо кіберуправління*

Очікування керівництва щодо бізнесу з точки зору кібербезпеки зростають. Це важливо для захисту бізнесу, а отже, і національної економіки. Однак багатьом підприємствам важко зрозуміти, з якими ризиками вони стикаються, що від них вимагається з точки зору управління та як дотримуватися вимог. Нерідкі випадки, коли компанії нічого не роблять, тому що не знають, з чого почати, а не шукають допомоги.

*Сприяти доступу до надійної підтримки після інциденту*

Це може бути критично важливим для компаній, у яких стався кіберінцидент. Ми так часто бачимо, що служба підтримки реагування на інциденти, залучена компанією для відновлення своїх систем, не може належним чином розслідувати інцидент і з'ясувати, хто відповідальний і які дані було викрадено. У процесі вони часто ненавмисно знищують докази, які можуть бути необхідними для регулятивних, страхових або судових цілей. На етапі реагування на інцидент і криміналістичної експертизи життєво важливо зберегти цілісність даних і обробляти їх з особливою ретельністю від збору до аналізу. Якщо справа опиниться в суді, звіти, які можна легко виправдати, які окреслюють ланцюжок контролю та аналітичну методологію, мають вирішальне значення.

*Захистіть наші набори даних національного значення*

Це має вирішальне значення з точки зору національної стійкості та ведення бізнесу. Критичні збої в інфраструктурі можуть призвести до зупинки значної частини країни. Таким чином, важливо визначити найважливіші дані для бізнесу та дані, які, швидше за все, стануть ціллю зловмисників, а потім переконатися, що вони безпечні за допомогою відповідних підходів до управління ризиками, таких як контроль доступу та шифрування. Також корисно переконатися, що використовуються методи мінімізації даних, щоб можна було безпечно утилізувати непотрібні дані, коли вони більше не потрібні.

*Підтримуйте безпечне та відповідальне використання ШІ*

Штучний інтелект приносить великі переваги нашій нації, як це працює на щоденній основі, і переваги, які він приносить для операційної ефективності для бізнесу. Але це також супроводжується кіберзагрозами. Загрози на основі штучного інтелекту включають використання штучного інтелекту для створення ще більш переконливих фішингових повідомлень, які тепер можуть виглядати та звучати ще більше так, ніби вони надходять від реальних людей, що збільшує ймовірність успіху шахрайства. Зосередження уваги Уряду на цьому є розумним і вітається.

Хоча ми вітаємо мету стратегії та описані дії, ми стурбовані тим, що повідомленого фінансування буде недостатньо для досягнення цих амбітних цілей і фінансування такої кількості програм протягом років до 2030 року…» ***(Brendan Read. Australian Government 2023-30 Cyber Security Strategy // KM Holdings Pty Ltd (https://kordamentha.com/insights/australian-government-cyber-security-strategy). 23.11.2023).***

***

## ***Китай***

**«Міністерство фінансів Китаю запропонувало, щоб аудитори проходили або проводили додаткові перевірки кібербезпеки, якщо їхня робота стосується національної безпеки.**

Проект нових заходів, оприлюднений у п'ятницю, також визначає, як бухгалтерські компанії повинні керувати даними, що стосуються китайських фірм.

Протягом останніх двох років орган кібербезпеки Китаю встановив політику, яка визначає, як усі підприємства повинні обробляти та впроваджувати оцінки та перевірки безпеки.

Нові заходи стосуються саме аудиторів, які були найняті вітчизняними фірмами або здійснюють транскордонну роботу. Головний партнер аудиторської фірми є особою, відповідальною за безпеку даних, йдеться в проекті правил.

Проект відкритий для громадського обговорення до 11 грудня.

Pricewaterhouse Coopers, Deloitte, KPMG і EY - четвірка найбільших світових аудиторських фірм - не відразу відповіли на запити про коментарі.

Занепокоєння щодо безпеки даних спонукало китайську владу посилити перевірку аудиторів в останні роки.

Правила, опубліковані в травні, вже передбачають, що державні компанії та підприємства, зареєстровані на біржі, повинні посилити перевірку здатності бухгалтерів керувати інформаційною безпекою.

Пекін попросив деякі державні фірми припинити використовувати чотири великі глобальні бухгалтерські фірми, оскільки він прагне приборкати вплив західних аудиторів, повідомляє Bloomberg News у лютому.

Минулого року Сполучені Штати та Китай уклали угоду щодо врегулювання тривалої суперечки щодо відповідності аудиту китайських фірм, зареєстрованих у США, погодившись проводити аудиторські перевірки в Гонконзі, оскільки Китай не надає повного доступу регуляторним органам США». ***(China proposes cybersecurity check for auditors if national security involved // yahoo! finance (https://finance.yahoo.com/news/china-drafts-measures-accounting-firms-074548941.html?fr=sycsrp_catchall). 12.11.2023).***

***

**«Звіт Управління безпеки інформаційних мереж (INSA) за допомогою «Національного опитування про кібербезпеку» показує, що обізнаність ефіопів щодо технологій і кібербезпеки дуже низька.**

Відповідно до наукового процесу було опитано 6156 користувачів, і результати, які були оголошені 30 жовтня 2023 року, показали, що лише 35% громадян мали достатні знання, але не в тому ступені, який можна було б вважати достатнім.

За простим визначенням, кібератака – це навмисне використання шкідливого програмного забезпечення проти неавторизованих комп'ютерних систем, інфраструктури та мереж з метою використання даних і порушення служб.

Як свідчить звіт, в Ефіопії з липня 2023 року по вересень 2023 року, за три місяці, було здійснено 2556 кібератак.

За словами Соломона Соки, директора INSA, «веб-сайт, на який припадає найбільша частка атак у кварталі, здійснив 764 спроби атак. Це показало зростання на 33 відсотки порівняно з попереднім кварталом».

Друге місце займають хакерські атаки з 669 спробами. Адміністрація заявила про 590 кібератак, спрямованих на порушення інфраструктури. Тим не менш, INSA оголосила, що 97,7 відсотка атак, кількість яких збільшилася, були заблоковані.

Передбачувана атака, пов'язана з мобільним банкінгом, була 1110, і, як показало INSA, проводяться дослідження для оцінки завданої шкоди.

Kaspersky Global Research, який вивчає кампанії кібершпигунства, основні тенденції зловмисного програмного забезпечення, програм-вимагачів і підпільних кіберзлочинів у всьому світі, показав, що тільки в 2023 році в Ефіопії було зафіксовано близько 18 000 атак і 30 000 програм-вимагачів. Повідомляється, що ці атаки можуть знищити онлайн-сервіси організацій, блокуючи доступ до них для користувачів і клієнтів, іноді протягом годин, аж до днів або тижнів.

За даними компаній з кібербезпеки, у 2023 році кіберзлочинність коштувала світу 8 трильйонів доларів США щорічно, 667 мільярдів доларів на місяць і 154 мільярди доларів на тиждень». ***(Eyasu Zekarias. More than 65% of Ethiopians in the***

***blind with regards to cyber security // CAPITAL (https://www.capitalethiopia.com/2023/11/05/more-than-65-of-ethiopians-in-the-blind-with-regards-to-cyber-security/). 05.11.2023).***

***

**«Навіть ChatGPT використовується для атак програм-вимагачів, тому ОАЕ не залишають каменя на камені в забезпеченні кібербезпеки в авіаційному секторі, заявив голова відділу кібербезпеки країни на конференції Aviation Mobility Conference в день відкриття 18-го Дубайського авіашоу в понеділок.**

Доктор Мохамед Аль Кувейті, голова відділу кібербезпеки уряду ОАЕ, сказав у своїй програмній промові, що ChatGPT використовується не «лише для написання електронних листів, спаму чи навіть фішингових листів, але навіть для написання деяких сценаріїв і декодування деяких речей. які ми бачили та досліджували на рівні програми-вимагача».

«І саме тут дуже важливо взяти це до уваги», — сказав він.

Він пояснив, що стратегія кібербезпеки країни побудована на п’яти стовпах: управління, покриття, захист і захист, інновації та партнерство. Країна запровадила стандарти забезпечення інформації, численні політики кібербезпеки та сприяла співпраці через державно-приватне партнерство.

*Фокус стратегії*

Стратегія зосереджена на розвитку технологій, навичок і потенціалу, визнаючи людський фактор як вирішальний елемент. «Безпека — наш пріоритет номер один», — сказав доктор Аль Кувейті.

Він сказав, що країна запровадила сертифікацію, стандарти, законодавчу політику та процедури для забезпечення кібербезпеки в усіх секторах.

«У нас є екосистема, яка дозволяє академічним колам, уряду та промисловості працювати разом, щоб придумати рішення, які відповідають багатьом аспектам наших вимог щодо кібербезпеки», — сказав він.

Доктор Аль Кувейті також закликав до міжнародної співпраці та обміну інформацією, особливо перед лицем кіберзагроз, таких як програми-вимагачі та зловживання такими технологіями, як ChatGPT». ***(Sajila Saseendran. Dubai Airshow 2023: UAE equipped to tackle cybersecurity attacks in the aviation sector // Al Nisr Publishing LLC (https://gulfnews.com/business/aviation/dubai-airshow-2023-uae-equipped-to-tackle-cybersecurity-attacks-in-the-aviation-sector-1.99366589). 13.11.2023).***

***

**«Управління з кібербезпеки (CSA) Гани подовжило кінцевий термін для ліцензування та акредитації постачальників послуг кібербезпеки (CSP), фахівців з кібербезпеки (CP) і установ кібербезпеки (CE).**

Спочатку цей термін мав закінчитися 30 вересня 2023 року, але його подовжено до 31 грудня 2023 року, щоб дозволити гравцям галузі, які ще не розпочали процес, зробити це відповідно до Закону про кібербезпеку 2020 року (Закон 1038).

У заяві про розширення CSA пояснило, що розширення також відповідає його адаптації спільного підходу до регулювання галузі та необхідності створення сприятливої та динамічної екосистеми, яка сприяла б розвитку галузі.

Тому він закликав заявників, які зареєструвалися на порталі ліцензування та акредитації CSA, але ще не подали заповнені заявки, скористатися новим графіком і зробити це протягом цього періоду продовження.

*Ліцензування*

Гана є першою країною в Африці та другою у світі після Сінгапуру, яка запровадила нормативну базу для ліцензування сектору кібербезпеки.

Мета полягає в тому, щоб забезпечити спрощений механізм для забезпечення того, щоб CSP, CE та CP пропонували свої послуги відповідно до затверджених стандартів і процедур відповідно до національних вимог і передової міжнародної практики.

Це також забезпечить більшу гарантію кібербезпеки та безпеки для споживачів, одночасно вирішуючи проблеми національної безпеки.

*Сенсибілізація*

Перед запровадженням CSA провело низку інформаційних заходів, включаючи організацію публічних консультацій, щоб отримати інформацію щодо режиму від ключових зацікавлених сторін, включаючи наукові кола, промисловість, громадянське суспільство та уряд.

Крім того, регуляторний орган співпрацює з іншими зацікавленими сторонами, щоб забезпечити відповідність.

Наприклад, на нещодавній спільній прес-конференції між CSA та Управлінням державних закупівель (PPA) обидві установи об'єднали зусилля, щоб гарантувати, що суб'єкти, які закуповують послуги з кібербезпеки, робили це відповідно до інструкцій, розроблених відповідно до Закону 1038.

Положення також поширюється на охоплені суб'єкти для залучення постачальників послуг кібербезпеки, установ кібербезпеки та спеціалістів з кібербезпеки, які мають ліцензію CSA на виконання функцій, пов'язаних з кібербезпекою.

Нормативна база узгоджується з Розділом 2 Закону про державні закупівлі, щоб гарантувати, що державні закупівлі здійснюються чесно, прозоро та недискримінаційно, як того вимагає закон». ***(Cyber Security Authority extends deadline for licensing, accreditation // Graphic Communications Group Ltd. (https://www.graphic.com.gh/news/general-news/ghana-news-cyber-security-authority-extends-deadline-for-licensing-accreditation.html). 16.11.2023).***

***

**«Запровадження малайзійського кіберзакону має стати пріоритетом для усунення законодавчих прогалин і недоліків у боротьбі з кіберзлочинами, такими як шахрайство, вважають експерти.**

Директор Глобального центру кібербезпеки Датук Хусін Джазрі сказав Malay Mail, що програми штучного інтелекту (ШІ) можна використовувати для протидії

поганим програмам ШІ, що вимагає створення комісії з кібербезпеки разом із будь-яким конкретним законом.

«Запровадження малайзійського кіберзакону має бути прийнято швидко, щоб усунути поточні прогалини та недоліки.

«І багато інших ініціатив можна запровадити на всіх рівнях, щоб покращити існуючу ситуацію», — сказав він, додавши, що такі ініціативи мають бути сплановані та реалізовані в терміновому порядку лідерами з хорошим баченням.

Правоохоронні органи також повинні охоплювати як проактивні, так і реактивні заходи шляхом ефективної координації та консолідації, сказав професор кібербезпеки Малайзійського університету Тейлора.

Незважаючи на те, що ці агентства роблять усе можливе, він сказав, що такі фактори, як відсутність транскордонної підтримки, а також застарілі закони та прогалини в законодавстві ускладнюють їхню роботу.

У той же час громадськість недостатньо обізнана щодо шахрайства, і це питання, над яким повинні діяти правозахисні агентства, такі як CyberSecurity Malaysia, за допомогою відповідних міністерств і відомств, додав він.

Тим часом головний виконавчий директор CyberSecurity Malaysia Датук Амірудін Абдул Вахаб також закликав до перегляду та оновлення існуючого законодавства та політики в рамках заходів щодо адаптації до нових тактик і технологій шахрайства.

Окрім цього, ще потрібна підтримка жертв, партнерство з індустрією технологій, а також співпраця та обмін інформацією.

Він пояснив, що прогрес у сфері штучного інтелекту та технології deepfake робить онлайн-шахрайство більш витонченим.

«Щоб вирішити ці проблеми, нам потрібні розумніші інструменти безпеки, які також використовують штучний інтелект, а також більше інформації про ці нові шахрайства.

«Йдеться про адаптацію наших засобів захисту, щоб випереджати шахраїв, які використовують ці передові трюки, щоб обдурити нас в Інтернеті», — сказав він.

Подібним чином професор Тамхіді Центру Тамхіді Університету Саїнс Ісламу Малайзії Мохамед Рідза Вахіддін погодився з необхідністю спеціального закону для боротьби з цією проблемою.

Незважаючи на те, що на початку 2024 року до Закону про комунікацію та мультимедіа 1998 року будуть внесені зміни, він сказав, що наразі розділ 233 Закону прийнятний для переслідування кіберзлочинів.

Розділ 233 передбачає кримінальну відповідальність за непристойний, непристойний, неправдивий, погрозливий або образливий онлайн-контент з наміром дратувати, образити, погрожувати чи переслідувати іншу особу, що особливо актуально у боротьбі з кіберзлочинами.

Засудження призведе до штрафу в розмірі не більше 50 000 рингітів або позбавлення волі на строк до одного року, або обох.

Однак активісти за свободу слова розкритикували розділ 233 Закону як проблематичний через неоднозначну формулювання та нечітке визначення «дратувати, образити, погрожувати або переслідувати іншу особу».

Дослідження Мохамеда Рідзи присвячено людським цифровим близнюкам: створеним комп'ютером близнюкам реальних людей через те, що технологія deepfake потребує реальної людини, щоб імітувати цільову жертву.

«Незважаючи на очевидну помилку вчинення фішингу, крадіжки особистих даних або шахрайства, в Малайзії немає жодного конкретного положення проти таких злочинів.

«Однак стаття 416 Кримінального кодексу, яка забороняє «шахрайство шляхом видавання себе за іншу особу», точніше, прикидання кимось іншим з наміром обману, служить протидією таким злочинам», – додав він.

За словами головного виконавчого директора Novem CS Муругасона Р. Тангаратнама, ще однією проблемою, з якою стикаються команди з кібербезпеки, є швидкий розвиток технологій.

«Голоса, створені комп'ютером, настільки реалістичні, що вони вводять друзів і родину в оману. Маски, створені за допомогою фотографій із соціальних мереж, можуть проникати в систему, захищену ідентифікатором обличчя.

«Звучить дуже драматично і як щось із науково-фантастичного фільму. Що ж, це реальніше, ніж ви собі уявляєте!

«Штучний інтелект і технологія глибокої підробки просто змінили правила гри, якщо вони взагалі були», — сказав він Malay Mail.

Він пояснив, що технологія deepfake є потужним інструментом для шахрайства з ідентифікаційною інформацією, оскільки вона маніпулює медіафайлами, створеними за допомогою алгоритмів ШІ, щоб дозволити шахраям переконливо змінювати або фабрикувати медіа.

Крім того, до тих, хто займається збором даних, будь то в приватному чи державному секторі, необхідно дотримуватися вищих стандартів, додав він.

У вівторок головний міністр Пенанга Чоу Кон Йоу заявив законодавчим зборам штату, що кількість випадків онлайн-шахрайства в Пенангу зросла на 45 відсотків порівняно з минулим роком.

Минулого року Selangor Mentri Besar Datuk Seri Amirudin Shari оголосив про створення групи реагування на кібернетичні ситуації Selangor (CERT Selangor) під час презентації державного бюджету на 2023 рік, сподіваючись, що це підвищить довіру до цифрової економіки». ***(Zarrah Morden. Cybersecurity experts call for better legislation to tackle evolving scam tactics // Microsoft (https://www.msn.com/en-my/news/national/cybersecurity-experts-call-for-better-legislation-to-tackle-evolving-scam-tactics/ar-AA1kummC). 25.11.2023).***

***

## Кіберстрахування

**«Індія з її стрімкою цифровою трансформацією стала свідком значного зростання кіберзагроз і атак за останні роки.** Зі зростанням оцифровки різних секторів і розширенням використання технологій окремі особи та корпорації стають більш схильними до ризиків кіберзлочинності.

У цьому контексті кіберстрахування стало важливим інструментом для захисту від фінансової та репутаційної шкоди, спричиненої кібератаками.

«Коли справа доходить до ризику, є лише три варіанти: прийняти ризик, зменшити ризик за допомогою технологій і передати ризик страховій компанії. Якщо ризики не зменшено або не передано, ви погодилися з ними та їхніми витратами. Для фізичних осіб він зосереджений насамперед на захисті від крадіжки коштів, здирництва та шахрайства в онлайн-магазинах, – говорить Сартак Дабі, співзасновник Mitigata.

Давайте заглибимося у важливість кіберстрахування та надамо уявлення про те, як ви можете захистити себе.

*Розуміння ландшафту загроз*

Розвиток ландшафту загроз в Індії вимагає проактивного підходу до захисту цифрових активів. Кібератаки, такі як програми-вимагачі, витоки даних і фішингові атаки, стали більш витонченими та цілеспрямованими.

Ці атаки можуть призвести до фінансових втрат, витоку даних клієнтів, регуляторних санкцій і шкоди репутації, що робить вкрай важливим для окремих осіб і корпорацій вжити заходів для свого захисту.

*Роль кіберстрахування*

Кіберстрахування діє як мережа безпеки, що дозволяє перекласти частину ризиків, пов’язаних з кібератаками, на страхову компанію. Це страхове покриття захищає від ряду кіберризиків і надає фінансову допомогу в разі злому або атаки.

Він охоплює різні аспекти, такі як судові витрати, витрати на сповіщення, судові дослідження, відновлення даних і переривання бізнесу. Забезпечуючи фінансовий захист, кіберстрахування допомагає окремим особам і корпораціям зменшити потенційні втрати, спричинені кіберінцидентами.

*Переваги кіберстрахування*

Переваги кіберстрахування численні. По-перше, це забезпечує фінансовий захист від витрат, пов’язаних із розслідуванням кібератаки та керуванням нею. По-друге, він покриває судові витрати, включно з потенційними регуляторними штрафами та пені.

По-третє, кіберстрахування може надати допомогу в сповіщенні клієнтів і послугах кредитного моніторингу в разі порушення даних. Нарешті, він допомагає

підприємствам відновитися після кібератаки, покриваючи витрати, пов’язані з припиненням роботи та репутаційною шкодою.

*Впровадження кіберстрахування*

Щоб ефективно захистити себе, окремим особам і корпораціям необхідно ретельно розглянути свої поліси кіберстрахування. Ось кілька ключових міркувань:

1. Оцініть свої ризики: зрозумійте свої конкретні кіберризики та визначте потенційні вразливі місця. Це допоможе визначити необхідне покриття у вашому полісі.

2. Виберіть відповідного постачальника страхових послуг: шукайте страхові компанії, які мають досвід роботи з кіберризиками та мають досвід ефективного розгляду кіберпретензій. Вивчіть їх репутацію, фінансову стабільність і відгуки клієнтів.

3. Налаштуйте свій поліс: адаптуйте свій поліс кіберстрахування відповідно до ваших конкретних потреб. Розгляньте можливість покриття витоків даних, перерви в роботі, кібервимагання, судових витрат і послуг зі зв’язків з громадськістю.

4. Регулярно переглядайте та оновлюйте: ландшафт кіберзагроз постійно розвивається, що вимагає регулярного перегляду та оновлення вашого полісу кіберстрахування. Будьте в курсі нових загроз і переконайтеся, що ваша політика залишається актуальною та ефективною.

5. Впроваджуйте надійні заходи кібербезпеки: хоча кіберстрахування забезпечує мережу безпеки, не слід покладатися на нього як на єдиний метод захисту. Застосуйте надійні заходи кібербезпеки, такі як брандмауери, шифрування, багатофакторна автентифікація та навчання співробітників, щоб мінімізувати ризик кіберінцидентів». ***(Deepika Chelani. Shielding your digital assets: How cyber insurance can provide a safety net in the face of growing cyber threats // HT Digital Streams Ltd (https://www.livemint.com/money/personal-finance/shielding-your-digital-assets-how-cyber-insurance-can-provide-a-safety-net-in-the-face-of-growing-cyber-threats-***

***11700198988302.html?utm_source=flipboard&utm_content=LiveMint%2Fmagazine%2FMoney). 17.11.2023).***

***

## Кібервійни та протидія зовнішній кібернетичній агресії

**«Російські хакери проникли в Пентагон і Міністерство юстиції, зламавши 632 000 облікових записів електронної пошти.** Хоча Міністерство США класифікувало порушення в травні як серйозний інцидент, воно вважає розкриті дані несекретними і загалом мають низький рівень чутливості.

*Зіткнення з великим порушенням*

Російські хакери успішно зламали облікові записи електронної пошти приблизно 632 000 співробітників міністерства юстиції та оборони США. Цікава техніка повідомила, що це є серйозним порушенням безпеки.

Хакери скористалися вразливістю в державному програмному забезпеченні для передачі файлів MOVEit у рамках ширшої серії атак, націлених на базу користувачів. Ця масштабна кібератака сталася на початку цього року.

*dverto Player*

Щоб усунути це порушення, представники служби кібербезпеки США співпрацювали з ФБР та іншими федеральними агентствами, щоб оцінити ступінь порушення в різних державних органах.

Як повідомляється, порушення було пов’язане з опитуваннями державних службовців і внутрішніми системами відстеження, якими керує Управління управління персоналом (OPM), що викликає занепокоєння щодо безпеки конфіденційної інформації.

MOVEit має контракти з приблизно десятком урядових установ США. Порушення безпеки вплинули не лише на державні департаменти США, але й на приватні корпорації, такі як Shell, BBC, British Airways, Університет Джона Хопкінса, Університет Джорджії та Міністерство енергетики.

Російськомовна група програм-вимагачів, відома як CLoP, взяла на себе відповідальність за атаки, як і в попередніх зламах, пов'язаних з MOVEit. За оцінками організації, її жертви обчислюються сотнями.

Джон Істерлі, директор Агентства з кібербезпеки та безпеки інфраструктури, заявив у червні, що ці хакерські атаки не становлять системного ризику для нашої національної безпеки чи мереж нашої країни. У червні через витік даних Управління транспорту штату Орегон було скомпрометовано особисту інформацію 3,5 мільйонів жителів Орегону.

Associated Press повідомило, що зламані дані включали номери соціального страхування, дати народження, фізичні адреси та іншу інформацію з водійських прав. У звіті постраждалим особам запевнено, що буде вжито заходів для надання їм необхідної інформації для захисту їх особистої інформації.

*Інші випадки*

Після витоку даних, який стався в травні, TechCrunch повідомив, що компанія, що стоїть за популярною програмою оптимізації CCleaner, розкрила, що хакери отримали значну кількість особистої інформації про її клієнтів, які платять.

Gen Digital, багатонаціональна компанія-розробник програмного забезпечення, яка володіє такими брендами, як CCleaner, Avast, Norton LifeLock і Avira, повідомила клієнтів електронною поштою, що злом стався через уразливість у широко використовуваному інструменті передачі файлів MOVEit.

MOVEit використовується багатьма організаціями, включаючи CCleaner, для передачі великих обсягів конфіденційних даних онлайн. Клієнти отримали сповіщення електронною поштою про те, що хакери отримали доступ до їх особистої інформації, включаючи імена, контактні дані та специфіку продукту.

Злам електронних адрес Міністерства юстиції та Пентагону є яскравим нагадуванням про те, що навіть найбільш укріплені організації можуть стати жертвами кібератак». ***(Inno Flores. US Defense, Justice Department Faces Major Breach, Exposing 632,000 Employees' Email Accounts // Tech Times LLC. (https://www.techtimes.com/articles/298183/20231101/us-defense-justice-department-faces-major-breach-exposing-632000-employees-email-***

***accounts.htm?utm_source=flipboard&utm_content=tradeit%2Fmagazine%2FPrivacy+and+Security). 01.11.2023).***

***

**«Спонсоровані державою кібергрупи та хакери посилили напади на критично важливу інфраструктуру, підприємства та будинки Австралії, йдеться в звіті уряду, додаючи, що його нова оборонна угода з Великою Британією та США, ймовірно, зробила її ще більшою ціллю.**

Повідомлення про кіберзлочинність зросли на 23% до понад 94 000 у фінансовому році, що закінчився червнем, повідомляє Австралійський центр кібербезпеки у своєму щорічному звіті про загрози в середу.

За його оцінками, злом австралійських активів відбувався кожні шість хвилин.

«Кібернетична загроза продовжує зростати», — заявив міністр оборони Річард Марлз радіо ABC. «Ми також бачимо більший інтерес державних суб'єктів до критичної інфраструктури Австралії».

У звіті говориться, що це сталося через нове оборонне партнерство AUKUS, «з його упором на атомні підводні човни та інші передові військові можливості».

У травні розвідувальний альянс Five Eyes і Microsoft (MSFT.O) заявили, що фінансована державою китайська хакерська група шпигує за організаціями критичної інфраструктури США. США, Канада, Нова Зеландія, Австралія та Великобританія складають мережу обміну розвідданими Five Eyes.

Методи, які використовує китайська хакерська група, можуть бути використані проти критичної інфраструктури Австралії, включаючи телекомунікації, енергетику та транспорт, йдеться у звіті.

Марлз сказав, що відносини Австралії з Китаєм, її найбільшим торговим партнером, були «складними», і уряд ніколи не вдавав, що відносини будуть легкими. Дипломатичні та торговельні зв'язки між двома країнами нещодавно стабілізувалися після кількох суперечок з 2020 року.

«Зрозуміло, ми цінуємо продуктивні відносини з Китаєм... але Китай був джерелом занепокоєння щодо безпеки для нашої країни, і ми також готуємося до цього», - сказав Марлз.

Сплеск кібервторгнень спонукав уряд у лютому створити агентство, яке б допомагало координувати реагування на хакерські атаки. Він також переглядає федеральні кіберзакони, деталі яких мають бути оприлюднені наступного тижня, і уряд заявив, що зробить для компаній обов'язковим звіт про випадки програм-вимагачів.

Середня вартість кіберзлочину для його жертви зросла на 14%, йдеться у звіті.

«Ці докази дають уряду вимогу мати набагато тісніші відносини між промисловістю та урядом», — сказав Метью Уоррен, директор Центру досліджень та інновацій у сфері кібербезпеки при університеті RMIT.

*«Деякі статистичні дані досить лякають».*

Австралійська комісія з цінних паперів та інвестицій також заявила цього тижня, що опитування 700 компаній виявило, що 44% не керують ризиками, пов'язаними з доступом третіх сторін, таких як партнери по ланцюгу постачання, до конфіденційних даних. Було також виявлено, що 58% мали обмежені заходи для захисту конфіденційних даних або взагалі не мали їх, а 33% не мали плану реагування на кіберінциденти.

Кібератаки на Австралію продовжуватимуть зростати, доки організації не почнуть докладати більше зусиль для безпеки та управління ризиками своїх інформаційних активів, сказав Найджел Фейр, професор кібербезпеки в Університеті Монаша.

Цього місяця кіберінцидент в DP World Australia, одному з найбільших портових операторів країни, змусив його призупинити роботу на три дні.

Потрясіння правил кібербезпеки в країні було спровоковано крадіжкою даних телекомунікаційного провайдера Optus у 2022 році, в результаті якої була розкрита особиста інформація 10 мільйонів австралійців». ***(Renju Jose, Byron Kaye. Australia says hacks surging, state-sponsored groups targeting critical infrastructure // Reuters***

***(https://www.reuters.com/technology/cybersecurity/australia-says-state-sponsored-cyber-groups-targeting-critical-infrastructure-2023-11-15/). 15.11.2023).***

***

**«Згідно з новим звітом, хакери, потенційно пов'язані з Головним розвідувальним управлінням російського ГРУ, здійснили серію добре скоординованих кібератак, націлених на критично важливу інфраструктуру Данії.**

SektorCERT, некомерційний центр кібербезпеки для критичних секторів Данії, повідомив, що в травні зловмисники отримали доступ до систем 22 компаній, які контролюють різні компоненти енергетичної інфраструктури Данії. У звіті, опублікованому в неділю, говориться, що хакери скористалися вразливістю нульового дня в брандмауерах Zyxel, які багато датських операторів критичної інфраструктури використовують для захисту своїх мереж.

Більшість атак були можливі через те, що компанії не оновили свої брандмауери, повідомляє SektorCERT. У ньому сказано, що кілька компаній відмовилися від оновлення програмного забезпечення через плату за встановлення. Деякі компанії помилково припускали, що відносно нові брандмауери Zyxel уже містять останні оновлення, а інші помилково вважали, що за впровадження оновлень відповідає постачальник.

Уразливості брандмауера, про які вперше було повідомлено в квітні та відстежуються як CVE-2023-28771, дозволяють зловмисникам отримувати віддалений доступ до промислових систем управління без автентифікації. SektorCERT описав кібератаку як «чудову» завдяки ретельному плануванню та координації, заявивши, що суб'єкти загрози продемонстрували здатність ідентифікувати компанії з уразливими пристроями та організовувати одночасну кампанію проти цільових фірм.

«На сьогоднішній день немає чіткого пояснення того, як зловмисники отримали необхідну інформацію, але ми можемо констатувати, що серед 300 учасників вони не промахнулися», - йдеться в повідомленні.

Згідно зі звітом, одинадцять компаній були «миттєво» скомпрометовані, що дозволило зловмисникам отримати контроль над брандмауером і отримати доступ до критичної інфраструктури за ним. У SektorCERT заявили, що одночасна атака не дозволила енергетичним компаніям попередити інших заздалегідь, «оскільки всі атакуються одночасно».

У звіті мета кібератаки описується як збір розвідувальної інформації, і сказано, що зловмисники виконали код на брандмауері, який змусив його надіслати імена користувачів і деталі конфігурації. У SektorCERT повідомили, що «зловмисники використовували цю команду як розвідку, щоб побачити, як налаштовані відповідні брандмауери, а потім вибрати, як продовжувати атаку».

Атаки почалися 11 травня, після чого 10 днів бездіяльності. Друга хвиля атак почалася 22 травня, коли SektorCERT отримав сповіщення про те, що один із його учасників завантажив нове програмне забезпечення брандмауера через незахищене з'єднання. Залишається незрозумілим, які суб'єкти національної держави чи конкретні кіберзлочинні організації стоять за атаками, а також чи були залучені кілька груп до серії кіберінцидентів, націлених на критичну інфраструктуру Данії.

Аналіз SektorCERT показав, що трафік у зламаних мережах надходив із серверів, пов'язаних із підрозділом російських військових хакерів, відомих як Sandworm. Sandworm, також відомий як Seashell Blizzard і Voodoo Bear, як відомо, атакував критичні інфраструктурні операції в Україні, коли Росія веде свою загарбницьку війну. У звіті, опублікованому на початку цього місяця, говориться, що хакерська група використала нові методи для цілеспрямованої атаки на українську електропідстанцію.

Кілька зламаних компаній уникли будь-якого значного впливу на енергетичну систему Данії, від'єднавшись від місцевих або національних енергетичних мереж і перейшовши в острівний режим роботи, що ізолювало їхні системи та запобігло потенційному поширенню атаки на ширшу енергетичну систему Данії.

SektorCERT закликав компанії створювати сегментовані мережі, щоб уникнути порушень на рівні підприємства та забезпечити відображення всіх

мережевих вхідних даних для оперативних технологічних систем». ***(Chris Riotta. Denmark Hit With Largest Cyberattack on Record // Information Security Media Group, Corp. (https://www.databreachtoday.com/denmark-hit-largest-cyberattack-on-record-a-23584?utm_source=flipboard&utm_content=PaulSmith6bpg%2Fmagazine%2FStuff+I+Think+Is+Technology+). 13.11.2023).***

***

**«Національні центри кібербезпеки Великобританії та Південної Кореї попереджають про зростання кількості та складності атак на ланцюжки поставок ПЗ з боку Північної Кореї.** Національна розвідувальна служба Південної Кореї (National Intelligence Service, NIS) та Національний центр кібербезпеки Великобританії (National Cyber Security Centre, NCSC) поширили спільне попередження для підвищення поінформованості про загрозу, спрямовану на уряди, фінансові інститути та компанії оборонної промисловості.

За даними відомств, північнокорейські хакери використовують уразливості нульового дня (Zero Day, 0day-уразливість), відомі недоліки, а також безліч експлойтів для досягнення цілей, що відповідають державним інтересам Північної Кореї. Інтереси країни включають збір коштів, шпигунство та крадіжку інтелектуальної власності та передових технологій з різних галузей, включаючи оборонну.

У попередженні підкреслюється, що в умовах цифрового та взаємопов'язаного світу атаки на ланцюжки поставок програмного забезпечення можуть мати глибокі та далекосяжні наслідки для порушених організацій. Поради щодо запобігання таким атакам включають включення двофакторної аутентифікації, оновлення систем безпеки та моніторинг мереж на предмет аномального трафіку.

NCSC і NIS перерахували приклади атак, що приписуються угрупованню Lazarus, яке вважають спонсорованим Північної Кореї підрозділом кіберармії країни. Найяскравішим прикладом є атака на ланцюжок поставок програми 3CX, в

ході якої хакери впровадили шкідливий код в інсталятор програми, використовуваний користувачами через легітимні канали.

В результаті атаки було викрадено інформацію про користувачів 3CX, включаючи дані про облікові записи. У Windows також були встановлені програми для крадіжки даних із браузерів, включаючи історію відвідувань.

Атаки Північної Кореї є частиною зусиль країни, що продовжуються, з порушення глобальної кібербезпеки і підкреслюють необхідність пильності та співробітництва в галузі кібербезпеки на міжнародному рівні». ***(Спецслужби Британії та Кореї попередили про загрозу шпигунства Північної Кореї // Internetua (https://internetua.com/specslujbi-britaniyi-ta-koreyi-poperedili-pro-zagrozu-shpigunstva-pivnicsnoyi-koreyi). 23.11.2023).***

***

## ***Кібервійна проти держави Ізраїль***

**«OpenAI припустив, що значні збої 8 листопада, які зазнали користувачі ChatGPT та інтерфейсу програмування додатків, були спричинені ймовірною атакою Distributed Denial of Service.** Група під назвою Anonymous Sudan взяла на себе відповідальність за DDoS-атаку на ChatGPT. У дописі на каналі Telegram хакери стверджують, що атака була спричинена тим, що ChatGPT має «загальне упередження щодо Ізраїлю та проти Палестини».

Після того як користувачі почали скаржитися на несправність ChatGPT, о 12:03 за тихоокеанським стандартним часом 8 листопада було опубліковано звіт про інцидент OpenAI, у якому говорилося, що проблема розслідується.

Протягом 40 хвилин до цього звіту про інцидент було додано додаткове повідомлення про те, що виправлення реалізовано та що OpenAI стежить за результатами.

На жаль, результати не були такими позитивними, оскільки подальше оновлення з міткою часу 17.23 за тихоокеанським стандартним часом зазначало, що «періодичні збої» все ще відбуваються.

О 19:49 за тихоокеанським стандартним часом OpenAI підтвердив: «Ми маємо справу з періодичними збоями через аномальну структуру трафіку, що відображає DDoS-атаку. Ми продовжуємо працювати над пом'якшенням цього»…

«Кіберзлочинці атакують з усіх боків і неймовірно безстрашні у своїх спробах. DDoS-атаки — це розумний спосіб націлити на компанію без необхідності злому мейнфрейму, але зловмисники можуть залишатися здебільшого анонімними», — каже Джейк Мур, глобальний радник з кібербезпеки постачальника безпеки ESET. «Це значно ускладнює захист, коли ландшафт абсолютно невідомий, окрім наявності найпотужнішого доступного захисту від DDoS, — продовжує Мур. — Проте, навіть із таким захистом, з кожним роком суб'єкти загроз стають краще оснащеними та використовують більше IP-адрес. наприклад, домашні пристрої IoT, можуть затопити системи, що ускладнить захист і може зробити системи повністю непридатними». Враховуючи, що OpenAI залишається однією з найбільш обговорюваних технологічних компаній, а ChatGPT — це технологія, яка постійно в новинах, кіберприціл і надалі зосереджуватиметься на ній. «Усе, що можна зробити, щоб забезпечити надійність їхніх мереж у майбутньому, — це продовжувати очікувати несподіваного», — підсумовує Мур». ***(Davey Winder. ChatGPT Down As Anonymous Sudan Hackers Claim Responsibility // Forbes (https://www.forbes.com/sites/daveywinder/2023/11/09/chatgpt-down-as-suspected-cyber-attackers-strike/?utm_source=flipboard&utm_content=forbes%2Fmagazine%2FInnovation&sh=5d1b0e69ab70). 09.11.2023).***

***

**«Іранські хакери намагалися зламати ключові ізраїльські компанії протягом останніх кількох тижнів, заявили експерти з безпеки в четвер, що свідчить про те, що Тегеран залишається зосередженим на своїй кібервійні низького рівня з Єрусалимом навіть на тлі руйнівної війни Ізраїлю з ХАМАС.**

Хакери, пов'язані з Корпусом вартових Ісламської революції Ірану — частиною групи, яку CrowdStrike назвав «Імператорським кошеням» — у жовтні

атакували ізраїльські компанії в транспортному, логістичному та технологічному секторах, повідомили дослідники фірми з кібербезпеки CrowdStrike у своєму новому звіті.

Протягом місяця після того, як Ізраїль вторгся в сектор Газа після смертоносної терористичної атаки ХАМАС 7 жовтня, пропалестинські хакери у відповідь намагалися перешкодити ізраїльському уряду та бізнесу. Ці атаки здебільшого обмежувалися тимчасовими збоями веб-сайтів і не завдали серйозної шкоди. Але співробітники розвідки США уважно стежать за Іраном, давнім ворогом Ізраїлю, на предмет ознак того, що він планує застосувати свої руйнівні кіберпотенціали в конфлікті. Тегеран вже намагався стерти комп'ютери, що належать ізраїльським технічним і освітнім організаціям.

Новий звіт CrowdStrike підсилює масштаби подвійних амбіцій Ірану: знищити критично важливу інфраструктуру в Ізраїлі, одночасно шпигуючи за його близькосхідним сусідом.

За словами охоронної фірми, групі, яка стояла за нещодавніми атаками, було доручено виконати «вимоги стратегічної розвідки, пов'язані з операціями [Корпусу вартових Ісламської революції]».

Команда хакерів Charming Kitten в основному використовує фішингові атаки, які видають за повідомлення про вербування, щоб спонукати жертв натискати шкідливі посилання або завантажувати зловмисне програмне забезпечення. Але під час триваючих атак, які CrowdStrike спостерігав з початку 2022 року, хакери також вставляли шкідливий код на веб-сайти, які їхні цілі, ймовірно, відвідували, причому код залишався бездіяльним, доки комп'ютер жертви ненавмисно не отримає до нього доступ.

За даними CrowdStrike, іранські оперативники перейшли від використання комерційного програмного забезпечення для збору інформації про людей, які відвідують їхні скомпрометовані веб-сайти, до використання спеціального коду для збору такої інформації, що свідчить про те, що їхня тактика дозріла з моменту появи їхньої групи в 2017 році.

Незрозуміло, наскільки успішною була остання кампанія іранських хакерів. Звіт CrowdStrike підтверджує, що група успішно скомпрометувала кілька веб-сайтів, переважно ті, що базуються в Ізраїлі, але в ньому не описуються результати подальших спроб групи зламати людей, які відвідували ці сайти. Компанія відмовилася надавати таку інформацію або ділитися даними про кількість і види організацій, на які націлені хакери». ***(Eric Geller. As Israel Fights Hamas, Iranian Hackers Lurk Nearby // JAF Communications Inc. (https://themessenger.com/tech/iran-israel-hacking-espionage-companies?utm_source=flipboard&utm_content=TheMessenger%2Fmagazine%2FThe+Messenger+Latest). 09.11.2023).***

***

**«Після того, як підозрювані іранські хакери заявили про низку недавніх атак на ізраїльські камери безпеки, глава кіберзахисту Ізраїлю сказав CNN, що він «дуже стурбований», що Іран може посилити свою тривалу таємну битву з Ізраїлем у кіберпросторі більш серйозними атаками на інфраструктуру в міру війни між Ізраїлем і ХАМАС.**

«Вони [Іран] знають, що можуть діяти там більш вільно [у кіберпросторі], ніж у фізичному просторі», — сказала Габі Портной, голова Національного кіберуправління Ізраїлю. «Ми готові до цього настільки, наскільки це можливо».

Портной сказав, що будь-яка іранська ескалація в кіберпросторі матиме «ціну», маючи на увазі, що ізраїльські хакери можуть помститися Ірану своїми власними операціями. Але Портной, який відповідає за кіберзахист, а не за наступ, сказав, що його мета полягає в тому, щоб кіберпростір не став «ще одним фронтом» у війні між Ізраїлем і ХАМАС.

Іранські хакерські групи виявилися вправними у руйнуванні комп'ютерних систем компаній в Ізраїлі, Саудівській Аравії та інших країнах Близького Сходу. Ізраїль має власних елітних кібероператорів, яких, поряд із США, багато підозрюють у здійсненні кібератаки на іранський ядерний об'єкт у 2009 році. Останніми роками ізраїльські таємні кібероперації проти Ірану тривали.

Згідно з інтерв’ю, протягом чотирьох тижнів після терористичних атак ХАМАС на Ізраїль підозрювані іранські хакери заявили про злом низки камер безпеки в Ізраїлі та опублікували навчальне відео про те, як зробити коктейлі Молотова, щоб «напасти на ізраїльське та американське посольства». з приватними експертами з кібербезпеки, які відстежують хакерів, і CNN перевірив дописи в соціальних мережах.

Аналітики кажуть, що цифрове бряцання зброєю є ще одним способом для Ірану продемонструвати свою владу під час війни, окрім ракетних та безпілотних атак на ізраїльські сили, які здійснюються ліванським ополченням Хезболла, та подібних ударів інших іранських проксі проти військ США в Сирії та Іраку.

Портной також стверджував, що хакери, пов'язані з Хезболлою, зламали приватні камери безпеки в Ізраїлі, щоб спробувати відстежити пересування ізраїльських солдатів протягом останніх тижнів.

Поки що підозрювані іранські хакери, схоже, мали мінімальний вплив на їхні публічно заявлені цілі в Ізраїлі за останній місяць. Їхньою метою, схоже, є поширення в ЗМІ наративів про вразливість Ізраїлю та США до кібератак.

Але низка нещодавніх кіберактивностей Ірану викликала занепокоєння серед офіційних осіб США та Ізраїлю, що Тегеран може використати свої значні хакерські можливості, щоб завдати шкоди інтересам Ізраїлю та США, уникаючи при цьому прямої кінетичної конфронтації з ізраїльтянами. Розвідувальне співтовариство США наразі вважає, що Іран та його проксі-сервери планують свою відповідь на війну Ізраїлю та ХАМАС, щоб уникнути прямого конфлікту з Ізраїлем або США, водночас стягуючи витрати на своїх супротивників, повідомляє CNN.

*Атаки зі знищенням даних заблоковано*

Нове нагадування про потенціал ескалації в кіберпросторі з’явилося в понеділок, коли американська фірма з кібербезпеки Palo Alto Networks заявила, що заблокувала спроби іранських хакерів здійснити атаки зі знищенням даних на більше десятка ізраїльських наукових організацій і постачальників технологій.

ХАМАС має власні кіберпотенціали, які в минулі роки використовувалися для шпигування за Ізраїлем і арабськими урядами, вважають експерти з безпеки.

Але Портной сказав, що ці хакери були відносно тихими під час останньої війни Ізраїлю та ХАМАС (ізраїльські авіаудари знищили інтернет-інфраструктуру в Газі).

Офіційні особи США кажуть, що після нападу ХАМАС вони зміцнили тісні відносини з Ізраїлем у кіберпросторі, обмінюючись розвідданими щодо будь-яких кіберзагроз, щойно вони з'являються. Директор ФБР Крістофер Рей стурбований можливою ескалацією у кіберпросторі.

«Кібернацілювання на американські інтереси та критичну інфраструктуру, яке ми вже бачимо як Іраном, так і недержавними акторами, ми можемо очікувати, що воно погіршиться, якщо конфлікт розшириться, як і загроза кінетичних атак», — сказав Рей на колегії Сенату у вівторок.

Ерік Голдштейн, старший чиновник Агентства кібербезпеки та безпеки інфраструктури США, заявив у заяві для CNN, що офіційні особи США «не виявили зміни в середовищі загроз, з якими стикаються американські організації», але «ми залишаємось у стані підвищеної готовності».

Стурбованість офіційних осіб США частково викликана тим, що вони вважають безрозсудним і непередбачуваним характером іранських кібероперацій порівняно з іншими цифровими супротивниками. ФБР звинуватило підтримуваних урядом Ірану хакерів у спробі злому Бостонської дитячої лікарні у 2021 році, яка не загрожувала пацієнтам, але, тим не менш, насторожила офіційних осіб США. Тегеран відкинув звинувачення.

Останніми тижнями офіційні особи США готувалися до подібного сценарію, за яким іранські хакери здійснять руйнівну атаку на критично важливу інфраструктуру США, сказав CNN високопоставлений чиновник США на умовах анонімності, оскільки вони не мають права спілкуватися з пресою.

«Існує розрив між їхніми [кібер] можливостями та їхньою риторикою», — сказав чиновник CNN, маючи на увазі хакерів, яких підтримує Іран. «Але ми знаємо, що вони досить безрозсудні і не мають розуму, щоб робити щось індивідуально».

CNN кілька разів намагався зв'язатися з постійним представництвом Ірану при ООН для цієї статті, але не отримав відповіді.

*Дозрівання кіберпрограми Ірану*

Експерти американських компаній з кібербезпеки Mandiant і CrowdStrike розповіли CNN про багато нещодавніх спроб хакерських атаок проти ізраїльських і американських організацій, що підтримують ХАМАС, були заявлені групами, які себе назвали «хактивістськими» групами, які насправді є іранськими прикриттями.

«Навіть успішні справжні кібератаки, ймовірно, не стосуватимуться фактичної атаки», — сказав CNN Джон Халтквіст, головний аналітик Mandiant. «Справа не в практичних ефектах. Йдеться про психологічний ефект».

20 жовтня хтось, який стверджував про причетність до однієї з таких груп під назвою «Воїни Соломона», надіслав електронного листа цьому репортеру CNN, щоб повідомити про ймовірний злом камер відеоспостереження в місті на півдні Ізраїлю.

Передбачуваний хакер також попросив надати контактну інформацію інших репортерів, тому що «це надзвичайна ситуація, щоб повідомити їм, що ми стаємо вірусними».

Портной сказав CNN, що Ізраїль вважає, що Солдатів Соломона підтримує Корпус вартових Ісламської революції Ірану, багато дослідників з кібербезпеки сказали, що вони погоджуються з цим твердженням, але не коментують його публічно через страх покарання.

В інформаційній війні, яка супроводжує вторгнення Ізраїлю в Газу, онлайн-персони дозволяють Ірану змішатися з купою інших пропалестинських хакерів, сказав Адам Мейерс, старший віце-президент CrowdStrike з розвідки.

Іранці можуть «просто створити нову особу з новою» тактикою, технікою та процедурами, і «таким чином вони не спалять жодну з [інших кібероперацій], які вони вже проводили», — сказав Мейєрс CNN.

У той час як Китай і Росія часто привертають більше уваги в кіберполітичних колах США, за останнє десятиліття Іран стабільно створив стайню хакерів, які часто працюють як підрядники для Корпусу вартових ісламської революції та міністерства розвідки Ірану, за словами офіційних осіб США та зовнішніх експертів.

Минулого тижня ізраїльська фірма з кібербезпеки Check Point викрила ймовірну тривалу іранську кампанію кібершпигунства, яка скомпрометувала уряди, IT та фінансові компанії на Близькому Сході, включно з Ізраїлем.

Хоча хакерські дії передували останній війні в Газі, вони могли потенційно надати Тегерану розвідувальні дані про те, як регіональні уряди реагують на війну.

«Ця кампанія є, мабуть, найскладнішою з усіх, які ми бачили в Ірані на технологічному рівні», — сказав CNN Сергій Шикевич, менеджер групи розвідки про загрози в Check Point». ***(Sean Lyngaas. Israel's cyber defense chief tells CNN he's concerned Iran could increase severity of its cyberattacks // Cable News Network (https://edition.cnn.com/2023/11/06/politics/israel-cyber-defense-iran-concerns/?utm_source=flipboard&utm_content=waral01%2Fmagazine%2FRumors+Of+War). 06.11.2023).***

***

**«З моменту початку війни між Ізраїлем і ХАМАС 7 жовтня хакери з обох сторін конфлікту здійснювали відносно незначні кібератаки, намагаючись спричинити цифрові збої в Ізраїлі, Газі та прилеглих територіях.** Зараз є ознаки того, що атаки можуть наростати.

Сьогодні у бійку вступила нова група під назвою «Cyber Toufan», націлена на ізраїльські компанії та організації. Він виклав в Інтернет величезну кількість даних, які, як стверджує, вкрав. За даними ізраїльської фірми з кібербезпеки Check Point Software Technologies Ltd, група має ознаки хакерської операції, спонсорованої державою Ірану.

«Ми вважаємо, що це показує, як Іран та його філії посилюють свої кібератаки», — сказав Гіл Мессінг, керівник апарату компанії. «Атаки зараз зростають і завдають реальної шкоди». Стиль і можливості групи подібні до інших хакерських груп, пов'язаних з Іраном, додав він.

Міністерство закордонних справ Ірану не відповіло на запити про коментарі.

Назва угруповання Cyber Toufan, схоже, натхненна нападами 7 жовтня, які ХАМАС назвав Toufan Al-Aqsa або Потоп Аль-Акса.

У заяві, опублікованій у службі обміну повідомленнями Telegram, хакери стверджували, що у відповідь на атаки Ізраїлю в секторі Газа вони знищили понад 1000 серверів під час атак і зламали 150 ізраїльських «цілей», включаючи десятки урядових установ і компаній. Нерідко самозвані хактивісти перебільшують або брешуть про свої успіхи. Але Мессінг вважає, що цю групу варто сприймати серйозно.

«Кожен день вони розкривають великі бази даних, взяті з веб-сайтів принаймні однієї організації», — каже він. За словами Мессінга, група оприлюднила дані про мільйони людей, включаючи електронні адреси, номери телефонів, імена та ділові взаємодії.

Однією з жертв угруповання стала тель-авівська компанія безпеки та управління ризиками MAX Security. Хакери Cyber Toufan опублікували файл, що містить близько 600 мегабайт даних, які, за їх словами, вони вкрали у фірми.

У MAX Security підтвердили мені, що вони зазнали злому 21 листопада. «Окрім адрес електронної пошти користувачів, жодних інших конфіденційних особистих даних не було використано», — сказав головний виконавчий директор Дрор Беккер у заяві, надісланій електронною поштою.

Раніше я писав про деякі інші групи хакерів, які діяли під час війни. У жовтні кілька груп, пов’язаних з Росією, здійснили серію розподілених атак на ізраїльські компанії та державні установи, через що деякі веб-сайти були вимкнені на короткий проміжок часу. Хакери також викрали дані ізраїльського академічного коледжу Оно та скомпрометували програму для мобільного телефону, яка використовується для попередження ізраїльтян про ракети під час конфлікту.

Але банда Cyber Toufan виглядає більш сильною загрозою. У середу, коли з'явилися новини про тимчасову паузу в боях, угруповання оголосило, що приєднається до перемир'я. Але було зазначено, що «з нетерпінням чекають припинення вогню, оскільки у нас є деякі витоки інформації». ***(Іранська хакерська група «Cyber Toufan» напала на Ізраїль // Internetua (https://internetua.com/iranska-hakerska-grupa-cyber-toufan-napala-na-izrayil). 23.11.2023).***

***

**«Численні останні кібератаки на космічні системи підкреслюють необхідність їх покращення безпеки, заявив 6 листопада представник Космічних сил США.**

«США та наші союзні сили тепер повинні протистояти зростаючим загрозам з боку перехоплення супутникового зв'язку», — сказав учасникам конференції CyberSatGov у Рестоні полковник Річард Найслі, старший начальник матеріального відділу комерційного космічного офісу Космічних сил на авіабазі Лос-Анджелеса, Каліфорнія. «Це є результатом передових методів глушіння та незаконних супутникових зв'язків. Нашій діяльності заважає порушення цілісності зв'язку та можливі витоки даних».

За його словами, Китай використовує штучний інтелект/машинне навчання для «складного» фішингу та кібератак на ділову електронну пошту, які є відносно недорогими.

Посилаючись на інформацію, надану Ерін Міллер, виконавчим директором Центру обміну та аналізу космічної інформації (Space ISAC) у Колорадо-Спрінгс, Найслі сказав, що між 9 та 13 жовтня «39 суб'єктів кіберзагрози здійснили 101 важливу кіберакцію, зосереджуючись на своїх атаки на охорону здоров'я, виробництво, уряд, освіту, юридичний і технологічний сектори».

«Пом'якшення цих кібератак на космічні мережі має вирішальне значення для забезпечення безпеки та надійності супутникового зв'язку та інших космічних систем», – сказав він.

У березні Space ISAC відкрив Центр оперативного спостереження поряд з Національним центром кібербезпеки в Колорадо-Спрінгс для моніторингу, аналізу та швидкого реагування на кіберзагрози космічним системам. Operational Watch Center має хмарну архітектуру Microsoft Azure, що дозволяє учасникам отримувати віддалений доступ до центру.

Space ISAC, заснований у 2019 році, заявив, що ділиться безкоштовними сповіщеннями та порадами від членів і партнерів щодо поточної ворожої активності. За словами Space ISAC, його члени щодня отримують повідомлення про кіберзагрози, інциденти та вразливості критичних систем.

Найслі сказав, що командування космічних систем хоче укласти угоду з Space ISAC, «якщо ми будуємо нашу систему комерційного розширеного космічного резерву [CASRF]», створену за моделлю цивільного резервного повітряного флоту.

«Обмін загрозами стане основоположним елементом CASRF», — сказав він. «Для промисловості важливо розуміти, що відбувається в зоні відповідальності, щоб приймати ділові рішення, захищати системи та краще реагувати на потреби бойовиків і союзників».

Комерційні інновації в розробці до терміну від трьох років або менше, на думку помічника міністра ВПС США з питань космічної інтеграції Френка Калвеллі, «можуть принести вирішальну перевагу» збройним силам, сказав Найслі. «Це все є частиною більшого культурного зрушення. Щоб бути успішними, ми не можемо продовжувати нарощувати можливості вдома». ***(Frank Wolfe. Cyber Security of Space Systems 'Crucial,' As US Space Force Official Notes Recent Attacks // Access Intelligence (https://www.satellitetoday.com/cybersecurity/2023/11/07/cyber-security-of-space-systems-crucial-as-us-space-force-official-notes-recent-attacks/). 07.11.2023).***

***

**«Уряд Австралії розпочав скоординовану відповідь на серйозний інцидент із кібербезпекою, який змусив DP World Australia, великого портового оператора, призупинити роботу в портах кількох штатів.**

Операції в постраждалих портах, включаючи порти в Мельбурні, Сіднеї, Брісбені та Фрімантлі в Західній Австралії, залишаються призупиненими, оскільки порушення було виявлено ввечері в п'ятницю.

Представник DP World Australia підтвердив Reuters у суботу, що тривають зусилля для відновлення нормальної роботи, підкресливши прагнення компанії безпечно вирішити ситуацію. Порушення, характер якого все ще розслідується, спонукало DP World Australia провести оцінку можливих порушень даних, одночасно тестуючи критично важливі системи, необхідні для відновлення регулярних операцій і руху вантажів.

Міністр внутрішніх справ Клер О'Ніл оголосила на платформі соціальних мереж X (раніше Twitter), що уряд Австралії активно координує реакцію на інцидент. За словами О'Ніла, Національний координатор з кібербезпеки, призначений на початку цього року у відповідь на різні серйозні витоки даних, очолює офіційну відповідь на кіберінцидент.

DP World Australia, дочірня компанія дубайського державного портового гіганта DP World, відіграє вирішальну роль в управлінні майже половиною товарів, що надходять до та з Австралії. Компанія керує чотирма контейнерними терміналами та налічує понад 7000 співробітників у 18 місцях Азіатсько-Тихоокеанського регіону.

Федеральна поліція Австралії почала розслідування кіберінциденту, хоча конкретні подробиці залишаються нерозкритими. Влада описує наслідки порушення як «серйозні та триваючі», причому перерва, ймовірно, триватиме кілька днів, суттєво вплинувши на переміщення товарів у країну та з неї, як підкреслив національний координатор з кібербезпеки Даррен Голді. DP World Australia ще не надала приблизний графік відновлення нормальної роботи.

У ході розслідування інцидент підкреслює зростаючу загрозу кібератак на критичну інфраструктуру, що спонукає до підвищеної пильності та спільних зусиль для посилення заходів кібербезпеки в ключових секторах». ***(Cybersecurity Incident Halts Operations at DP World Australia Ports // Kizhakedath Media Services (https://infotechlead.com/security/cybersecurity-incident-halts-operations-at-dp-world-australia-ports-81603). 12.11.2023).***

***

**«Okta Inc. сьогодні оприлюднила інформацію про те, що хакери вкрали 134 дані її клієнтів і здійснили кібератаки на п'ятьох після порушення її системи технічної підтримки.**

Okta, зареєстрована на Nasdaq, надає хмарну платформу, яку компанії використовують для обробки запитів на вхід у свої програми. Платформа також полегшує пов'язані завдання, такі як керування даними облікових записів користувачів. Минулого кварталу Okta отримала 556 мільйонів доларів доходу, що на 23% більше, ніж за аналогічний період минулого року.

Крадіжка даних, про яку компанія розповіла сьогодні вранці, сталася під час зламу, про який вперше стало відомо наприкінці вересня. Okta оприлюднила інцидент 20 жовтня, але не поділилася детальною інформацією про його причину чи масштаб. У дописі в блозі, опублікованому сьогодні вранці, керівник служби безпеки Okta Девід Бредбері поділився оглядом злому.

Компанія вперше помітила про злом, коли клієнт AgileBits Inc., розробник популярного менеджера паролів 1Password, повідомив про підозрілу активність своїй команді підтримки. Протягом наступних днів ще два клієнти подали подібні звіти. Okta розслідувала цю справу та визначила, що хакери зламали систему, на яку вона покладається для обробки запитів користувачів у службу технічної підтримки.

До блокування доступу кіберзлочинці отримали доступ до інформації 134 клієнтів. За словами Okta, викрадені дані включали низку сеансових токенів, які наразі використовувалися для здійснення кібератак проти п'яти її клієнтів.

Маркер сеансу — це файл, у якому програма зберігає інформацію про дії користувача. Якщо хакери викрадуть такі файли, вони можуть у деяких випадках використовувати їх для входу в облікові записи додатків законних користувачів. Один із клієнтів Okta, компанія з кібербезпеки BeyondTrust Inc., повідомила, що хакери створили обліковий запис адміністратора в її мережі за допомогою

вкраденого маркера сеансу, але не змогли отримати доступ до жодного внутрішнього робочого навантаження.

Okta визначила, що хакери отримали доступ до її системи підтримки через зламаний обліковий запис служби. Пов'язані ім'я користувача та пароль були збережені в особистому обліковому записі Google співробітником, що, можливо, стало основою для кібератаки. «Найвірогіднішим шляхом для розкриття цих облікових даних є компрометація особистого облікового запису Google або персонального пристрою працівника», — розповів Бредбері в сьогоднішньому дописі в блозі.

У відповідь на порушення компанія Okta запровадила політику, яка блокує співробітникам вхід на корпоративні комп'ютери за допомогою особистих облікових записів Google. Компанія також оновила механізм виявлення порушень у своїй системі запитів підтримки. Для додаткової міри Okta розгортає нову функцію для клієнтів своєї платформи, яка зробить їхні облікові записи адміністраторів більш безпечними.

Порушення, описане сьогодні, є одним із кількох інцидентів кібербезпеки, з якими компанія зіткнулася за останні два роки. Раніше цього тижня Okta розкрила, що кіберзлочинці вкрали дані майже 5000 її співробітників після злому зовнішнього постачальника. Раніше компанія оприлюднила порушення, яке вплинуло на кілька її внутрішніх сховищ GitHub». ***(Maria Deutscher. Okta reveals hackers accessed 134 customers' data in support system breach // SiliconANGLE Media Inc. (https://siliconangle.com/2023/11/03/okta-reveals-hackers-accessed-134-customers-data-support-system-breach/?utm_source=flipboard&utm_content=SiliconANGLE%2Fmagazine%2FSiliconANGLE). 03.11.2023).***

***

**«Популярний торрент-сайт став останньою жертвою гучного витоку даних цього року після того, як з'явилися повідомлення про те, що база даних, що містить конфіденційну інформацію користувачів, просочилася в Інтернет.**

Вважається, що таким чином були розкриті відомості про 100 000 користувачів World in HD (WiHD), включаючи адміністраторів сайтів, зокрема їхні електронні та IP-адреси, імена користувачів, паролі тощо.

Спеціалізований веб-сайт із кібербезпеки зробив це відкриття за допомогою механізму Elasticsearch. Ця новина буде особливо хвилювати всіх, хто використовував сайт для завантаження торрентів, враховуючи деякі неоднозначні асоціації з цією практикою.

*Дані користувачів WiHD витік помилково*

Дослідники з Cybernews виявили витік, який не був результатом вторгнення хакерів, а, очевидно, недогляд з боку безпеки бази даних WiHD, ймовірно, через звичайну неправильну конфігурацію.

Це викликає занепокоєння у користувачів сайту, оскільки, хоча торрент-файли самі по собі не є незаконними, широко відомо, що це популярний спосіб розповсюдження піратського вмісту в Інтернеті. Це тому, що торренти дозволяють легко обмінюватися великими файлами.

World in HD — приватний французький торрент-трекер, який спеціалізується на HD-фільмах і телешоу. Він пишається як ексклюзивністю своєї спільноти, так і високою якістю свого вмісту, який включає завантаження англійською та французькою мовами.

*Чому користувачі WiHD мають піклуватися?*

Той факт, що користувачі WiHD бачили витік своїх особистих даних в Інтернеті, викликає занепокоєння, але загроза посилюється сумнівною законністю того, що вони завантажували або не завантажували.

Як зазначають дослідники, туманність світу торрент-завантажень означає, що будь-які хакери, які отримали контактну інформацію користувачів трекера, мали б відносно легкий час для здійснення фішингових атак і спроб виманити гроші.

«Актори загрози можуть брати участь у різних незаконних діях, таких як відстеження та ідентифікація користувачів для правових наслідків, запуск цілеспрямованих фішингових атак або потенційне розкриття звичок користувачів

щодо завантаження, викликаючи конфіденційність і юридичні проблеми для постраждалих осіб», — прокоментувала команда, яка виявила порушення.

*Як захистити свої особисті дані в Інтернеті*

Хоча ми не виправдовуємо будь-яку незаконну онлайн-діяльність, торрент-завантаження чи інше, ми також вважаємо, що користувачі мережі загалом мають право займатися своїми справами без залякування хакерів.

З цією метою завжди доцільно використовувати VPN – будь то найбезпечніша VPN або одна з найкращих дешевих VPN – якщо ви хочете подвоїти захист своїх даних.

Це тому, що VPN, або повністю віртуальна приватна мережа, шифрує ваше з'єднання з Інтернетом і приховує вашу фактичну IP-адресу, направляючи її через сервер в іншій країні. Вони давно використовуються як компаніями, так і споживачами як додатковий рівень онлайн-безпеки, і ми не можемо рекомендувати їх досить високо». ***(James Laird. 100,000 Torrent Site Users Exposed in Massive Data Breach // Marketing VF Ltd. (https://tech.co/news/torrent-site-data-breach-exposed?utm_source=flipboard&utm_content=AWC%2Fmagazine%2FOur+Electronic+%26+Digital+Lives.). 08.11.2023).***

***

**«Наше цифрове життя переповнене великою кількістю програм і облікових записів. Ми всі це відчуваємо; більшість із нас це ненавидить.** Однак не йдеться про відмову від зручності. Йдеться про те, щоб бути безпечнішим в Інтернеті за допомогою меншої кількості, але сильніших кроків. Менша цифрова присутність означає кращий захист від кіберзагроз, ось тут і вступає цифровий мінімалізм.

Але що таке цифровий мінімалізм і як він може захистити вас в Інтернеті?

*Основні принципи цифрового мінімалізму та простої кібербезпеки*

Цифровий мінімалізм у кібербезпеці означає мудрий вибір, щоб зменшити свій онлайн-слід. Це підвищує вашу конфіденційність і безпеку. Це зміна мислення: цінність над обсягом. Вибирайте лише необхідні програми та облікові

записи. Це не тільки впорядковує ваш цифровий простір, але й скорочує шляхи проникнення кібер-зловмисників.

Першим кроком до цифрового мінімалізму є свідомий аудит ваших цифрових інструментів. Запитайте себе: якими службами та програмами я користуюся регулярно? Які з них мають доступ до моєї конфіденційної інформації? Часто ви підписуєтеся на послуги з примхи, яка може бути не важливою для вашого повсякденного життя. Усунувши ці додаткові інструменти, ви можете досягти більш безпечної та оптимізованої присутності в Інтернеті.

*Пріоритет конфіденційності*

Що стосується інструментів і послуг, які ви вважаєте важливими, наступним кроком є переконатися, що вони відповідають практикам, орієнтованим на конфіденційність. Вибирайте платформи з надійним досвідом захисту даних і прозорими щодо використання вашої інформації. Це може означати перехід на браузер, який не відстежує кожен ваш рух, або пошукову систему, яка поважає вашу конфіденційність. Йдеться про прийняття обґрунтованих рішень, які відповідають мінімалістичним принципам, де менший вплив означає більше безпеки.

Впровадження цифрового мінімалізму у ваше життя не відбувається відразу. Він вимагає регулярного обслуговування та зобов’язання зробити конфіденційність пріоритетом. Це може включати регулярні перевірки дозволів вашої програми, перегляд налаштувань конфіденційності в соціальних мережах і отримання інформації про найкращі практики цифрової безпеки. Таким чином ви не тільки захищаєте свої дані, але й сприяєте створенню безпечнішого цифрового середовища для всіх. Прийняття мінімалістичного підходу до кібербезпеки означає не просто робити менше; мова йде про те, що необхідно для безпечнішого цифрового життя.

*6 щоденних звичок і процедур для мінімалістичної кібербезпеки*

Зробивши мінімалістичні звички кібербезпеки частиною вашої рутини, ви створите надійний захист від багатьох онлайн-загроз. Йдеться про активність для

вашої цифрової безпеки, що дасть вам спокій під час навігації нашим підключеним світом.

1. Уважно перевірте дозволи програми

Візьміть за звичку щомісяця переглядати дозволи, які ви надали своїм програмам. Перевірте, чи є щось, що не має сенсу, і відкоригуйте відповідно. Перш ніж завантажувати програму, подумайте, чи вона потрібна. Менша кількість програм означає менше дозволів і меншу поверхню для атаки. Вибирайте програми, які надають пріоритет вашій конфіденційності та пропонують прозорі налаштування дозволів.

2. Оновіть пристрої та програми

Призначте щотижневий розпорядок дня для виконання оновлень на різних пристроях. Неухильно дотримуйтеся цього розкладу. Увімкніть автоматичні оновлення як для операційних систем, так і для програм, де це можливо, щоб забезпечити захист від нових вразливостей. Будьте в курсі життєвого циклу підтримки вашого програмного забезпечення та завчасно готуйтеся до переходу або оновлення до того, як настане дата завершення підтримки.

3. Підтримуйте хороші звички пароля

Інвестуйте в надійний менеджер паролів для створення та зберігання складних паролів. Завжди змінюйте паролі за умовчанням, особливо на нових пристроях або облікових записах, на щось унікальне та складне. Періодично змінюйте паролі, особливо для конфіденційних облікових записів, таких як електронна пошта та банківські послуги.

4. Розумно діліться в соціальних мережах

Знайдіть час, щоб зрозуміти та відкоригувати налаштування конфіденційності в соціальних мережах, щоб контролювати, хто бачить те, чим ви ділитеся. Завжди двічі подумайте, перш ніж ділитися особистою інформацією, яка може бути використана для заподіяння вам шкоди, як-от вашу адресу або коли ви їдете у відпустку. Заохочуйте оточуючих також пам’ятати про те, що вони розповідають про вас і себе.

5. Керуйте своїми цифровими активами

Періодично переглядайте та очищайте збережені дані, видаляючи непотрібні та впорядковуючи те, що є. Виберіть хмарну службу з надійними заходами безпеки та використовуйте її для зберігання своїх цифрових активів, а не кілька служб із різними протоколами безпеки. Вибирайте, кому надавати доступ до своїх цифрових активів. Використовуйте такі функції, як двофакторна автентифікація, щоб додати додатковий рівень безпеки.

6. Соціальні медіа та цифрові активи

Використання мінімалістичного підходу до кібербезпеки в соціальних мережах — це все одно, що прогулюватися жвавим містом непоміченим і безпечним. Це включає знання того, які фотографії, документи та інші особисті файли зберігаються на яких платформах, і забезпечення безпеки кожної платформи.

Ваші налаштування конфіденційності налаштовані на обмін фотографіями лише з близькими друзями чи з усім світом? Суворий контроль над цими налаштуваннями може запобігти тому, щоб особиста інформація стала надбанням громадськості.

Менша кількість пристроїв і облікових записів означає легше керування та менший ризик злому. Наприклад, виберіть одну безпечну хмарну службу для всіх своїх файлів замість того, щоб використовувати багато з різними рівнями безпеки.

*Спростіть свою присутність в Інтернеті, щоб значно підвищити безпеку*

Простота є ключем до ефективної кібербезпеки. Він діє як тихий охоронець вашого цифрового життя. Оптимізувавши захист онлайн, ви робите більше, ніж просто наводите порядок. Ви посилюєте свою присутність в Інтернеті. Зробіть розумний і ефективний вибір. Зосередьтеся на тому, що справді захищає вас без непотрібних додаткових речей. Цей мінімалістичний підхід – це більше, ніж тренд. Йдеться про створення спокійного цифрового простору. Тут душевний спокій є стандартним, а безпека плавно вписується у вашу щоденну онлайн-рутину». ***(Fatih Küçükkarakurt. 6 Minimalist Cybersecurity Tips You Can Implement Right Now // MUO (https://www.makeuseof.com/simple-cybersecurity-tips/?utm_source=flipboard&utm_content=PDimmick%2Fmagazine%2FSmart+House). 07.11.2023).***

***

**«В даний час питання кібербезпеки є особливо важливим для компаній, що працюють в екосистемі Fintech, які, саме, працюють на перетині фінансів, технологій і регулювання в поєднанні з експоненціальним зростанням використання технологічних і цифрових засобів для виконання фінансових операцій.**

Кібербезпека або інформаційна безпека суб'єкта чи віртуального простору спрямована на підтримку цілісності, доступності, конфіденційності, контролю та автентичності інформації, яка міститься, охороняється та керується в електронному обладнанні та навіть у хмарі. З кожним днем кібератаки стають все більш поширеними, завдаючи серйозного впливу на компанії з наслідками в приватній сфері клієнтів та їхніх особистих, фінансових і транзакційних даних, тому кібербезпека є однією зі стратегій, які використовуються для запобігання такому шахрайству.

Фінтех-компанії не звільнені від цих атак, тому важливо знати зобов'язання та обов'язки, які існують у нашій країні щодо захисту даних, не нехтуючи правилами, які стосуються конкретних послуг, таких як послуги кредитних і дебетових карток. встановити з цього приводу чи навіть із питань, що стосуються споживача. Вищезазначене стосується як фінтех-компаній, які безпосередньо обслуговують споживачів (B2C), так і тих, які надають послуги іншим компаніям, включаючи регульовані фінансові установи (B2B).

Наразі Коста-Ріка не має спеціальних правил для сектору Fintech у цій сфері. Однак існує загальне положення щодо захисту персональних даних і навіть щодо захисту даних, пов'язаних з кредитною поведінкою, що цікавить ті компанії в галузі, які надають кредитні засоби або надають послуги організаціям чи компаніям, які надають кредити.

Так, наприклад, Закон про захист особи від обробки персональних даних, Закон 8968 та його положення, гарантують будь-якій особі, національній чи іноземній, таке:

Повага до його права на інформаційне самовизначення щодо приватного життя чи діяльності.

Право особистості.

Захист їхньої свободи та рівноправності щодо автоматизованої або ручної обробки даних, що стосуються їх особи чи власності.

Вони також встановлюють мінімальні вимоги до автоматизованих і ручних баз даних, а також до осіб, які беруть участь у зборі, захисті та використанні персональних даних.

Крім того, щодо захисту прав споживачів, положення до Закону про сприяння конкуренції та ефективний захист споживача № 7472 регулює обов'язок продавця вживати ефективних заходів безпеки для захисту цілісності, достовірності та конфіденційності персональні дані, наявні в його базах даних, тоді як регулювання кредитних і дебетових карток регулює право користувачів фінансових послуг на захист персональних даних, отриманих фінансовими установами під час надання їхніх послуг, зокрема для надання кредитних і дебетових карток послуги. У тому ж розумінні регулювання системи платіжних карток стосується безпеки інформації пристрою платіжної картки.

Тепер, зокрема, для фінтех-компаній, які здійснюють будь-яку діяльність, перераховану в Законі про наркотичні засоби, психотропні речовини, лікарські засоби для несанкціонованого використання, пов'язану діяльність, відмивання грошей та фінансування тероризму, положення № 7786, пруденційні положення, зокрема за угодою SUGEF 13-19 (положення про запобігання ризику відмивання грошей, фінансування тероризму та фінансування розповсюдження зброї масового знищення), що застосовується до суб'єктів, пов'язаних статтями 15 і 15 bis закону 7786, регулює обов'язок ці компанії зберігати інформацію про своїх клієнтів і підтверджуючі документи під час комерційних відносин, гарантуючи конфіденційність інформації, отриманої від своїх клієнтів, а також інші аспекти, встановлені в Законі № 8968, згаданому вище. Нарешті, ми не забуваємо зазначити, що Кримінальний кодекс встановлює види покарання за протиправні дії, пов'язані з недотриманням захисту персональних даних.

Безсумнівно, сумнозвісне зростання фінтех-компаній за останні роки, як у сферах B2B, так і B2C, несе з собою ряд зобов'язань і відповідальності щодо безпеки даних, до яких вони мають доступ, зацікавленість, яка досягає влади та регулятори, які прагнуть забезпечити безпеку даних користувачів, постачальників та інших осіб, залучених до послуг і продуктів, що надаються компаніями в цій галузі.

У цьому сенсі для цих компаній життєво важливо чітко знати правила, яких вони повинні дотримуватися в цій сфері, і навіть ті, які застосовуються до їхніх клієнтів (у випадку B2B), наприклад, у фінансовому секторі, мати можливість запропонувати послугу, яка відповідає чинним вимогам і стандартам». ***(Mónica Arias Madrigal and Michael Villalobos. Cybersecurity and personal data in the Fintech environment in Costa Rica // Consortium Legal (https://consortiumlegal.com/en/2023/11/06/cybersecurity-and-personal-data-in-the-fintech-environment-in-costa-rica/). 06.11.2023).***

***

**«Маючи понад 1,8 мільярда активних облікових записів, Gmail є не лише однією з найбільш використовуваних онлайн-служб, але й однією з найбільш мішеней для хакерів.** Неважко зрозуміти, чому, адже Gmail припадає приблизно половина всього використання поштового клієнта на частку ринку США. Зламати обліковий запис Gmail, і зловмисник, незалежно від того, чи є його мотив злочинної вигоди чи стеження, може розраховувати на отримання великої кількості інформації, щоб допомогти своїй справі: від сповіщень про скидання пароля до деталей онлайн-транзакцій.

Ось чому виконання основних кроків для захисту вашого облікового запису Google є таким важливим.

*Не всі хакери Gmail змінять ваш пароль*

Не всі хакери Gmail змінять ваш пароль і негайно заблокують ваш обліковий запис Google. Хоча це дає їм час для вилучення цінних даних і потенційно скидання паролів для інших онлайн-облікових записів і служб, це не єдиний

варіант, доступний для загрозливих осіб. Дійсно, більш прихований довгостроковий підхід може бути набагато вигіднішим, якщо ця особа зацікавлена у стеженні. Така тактика залежить від того, чи власник облікового запису не знає, що неавторизована особа має доступ до його Gmail. На щастя, є кілька простих способів перевірити це. Ось лише три з них.

*Перевірте активність облікового запису Gmail*

Прокрутіть униз папки «Вхідні» Gmail і знайдіть функцію під назвою «Остання активність облікового запису». Це негайно повідомить вас про час попереднього доступу до Gmail і про те, чи здійснюється доступ до нього з іншого місця. Однак вам потрібно буде клацнути це, щоб відкрити повний монітор активності та отримати повне зображення доступу. Потім буде показано всі дати та час доступу, а також IP-адресу користувача та пристрій або програму, які ним використовуються. Візьміть за звичку перевіряти це щоразу, коли використовуєте Gmail, і ви зможете швидко помітити будь-який несанкціонований доступ. Важливо, що ви також можете вийти з них. Потім ви можете змінити свій пароль і активувати двофакторну автентифікацію, щоб уникнути їх. Google також надсилатиме сповіщення про будь-які незвичайні входи у ваш обліковий запис, нові пристрої, додані до вашого облікового запису, або зміни налаштувань безпеки. Вони також надходитимуть на вашу резервну електронну адресу, тому переконайтеся, що ви оновлюєте її та регулярно отримуєте до неї доступ.

*Перевірте наявність змін у переадресації Gmail*

Перейдіть до налаштувань Gmail і натисніть вкладку «Пересилання та POP/IMAP». Це покаже всі адреси, на які пересилається вхідна електронна пошта. Зловмисник може використати це, щоб отримати «тиху копію» всіх ваших вхідних електронних листів, не змінюючи ваш пароль і не повідомляючи вас про компрометацію. Більшість користувачів ніколи не заглиблюються в налаштування Gmail, оскільки це надто технічно для них, а Gmail настільки популярний, тому що ним також дуже легко користуватися. Проте, як і функція нещодавньої активності в обліковому записі, я б рекомендував вам виробити звичку регулярно перевіряти статус пересилання. Це також місце, де хтось може додати доступ до стороннього

клієнта електронної пошти за допомогою протоколу POP або IMAP, який у поєднанні з паролем вашого облікового запису також надає йому прихований доступ до вашої папки «Вхідні».

*Пройдіть перевірку безпеки облікового запису Google*

Google надає безкоштовно доступний потужний інструмент для перевірки безпеки вашого облікового запису. Перевірка безпеки облікового запису Google об'єднує багато цінних параметрів для захисту доступу до Gmail. Тут ви можете дізнатися, чи відбулися зміни у параметрах відновлення облікового запису, програмах і службах, яким було надано доступ до вашого облікового запису, чи активовано у вас 2FA, які системи ви використовуєте для його надання та конфіденційні налаштування Gmail. Останній може включати адреси для відповіді, відмінні від стандартних для вашого облікового запису, адреси для відправлення, які також відрізняються, і будь-які адреси, які були заблоковані, щоб перейти прямо до папки спаму. Блокування адрес сповіщень системи безпеки, наприклад, було б простим способом продовжити несанкціоновану діяльність, яка залишається непоміченою». ***(Davey Winder. Gmail Hackers Leave Vital Clues Behind—Check These 3 Things Now // Forbes (https://www.forbes.com/sites/daveywinder/2023/11/26/gmail-hackers-leave-vital-clues-behind-check-these-3-things-now/?utm_source=flipboard&utm_content=BezaKinfe%2Fmagazine%2FTechnology&sh=24be110911a1). 26.11.20.23).***

***

## Кібербезпека Інтернету речей. Штучний інтелект

**«Штучний інтелект (ШІ) часто хвалять за його здатність оптимізувати речі, автоматизувати чорні завдання (наприклад, заповнення календаря) і просто полегшити ваше життя.** Але тепер є повідомлення про те, що хакери використовують подібний інструмент під назвою WormGPT у своїх інтересах.

Подумайте про це як про ненадійний варіант ChatGPT, який хакери використовують спеціально для створення фішингових атак, не кажучи вже про багато інших мерзенних дій.

Ці фішингові атаки включають шахрайські електронні листи, текстові повідомлення та телефонні дзвінки, які обманом спонукають вас завантажити зловмисне програмне забезпечення, надати конфіденційну інформацію, наприклад ваш номер соціального страхування, облікові дані для входу, номер кредитної картки, а також будь-які інші дії, які можуть наразити вас на кіберзлочинців. WormGPT спеціально використовується для написання атак Business Email Compromise (BEC), які є фішинговими атаками, спрямованими на використання великих компаній.

Ці типи електронних листів часто персоналізовані для одержувачів, щоб приспати їх у помилкове відчуття безпеки та натиснути посилання, яке призводить до атаки. Тепер завдяки можливостям штучного інтелекту частота цих атак експоненціально зросла, каже Маанак Гупта, доцент кафедри інформатики Технічного університету Теннессі.

*Що таке WormGPT?*

WormGPT — це модуль штучного інтелекту на основі моделі мови GPT-J 2021 року. GPT-J — це велика мовна модель із відкритим кодом, яка здатна генерувати текст, схожий на людину, так само, як ChatGPT. Відкритий вихідний код — на відміну від OpenAI, лабораторії, яка працює з ChatGPT — означає, що будь-хто може перевіряти, ділитися та навіть змінювати вихідний код. Це в поєднанні з відсутністю будь-яких обмежень проти зловживань — запобігання ChatGPT від використання нецензурних слів, написання ненависті, написання вірусів — означає, що WormGPT може робити все, що від нього вимагають хакери.

Хоча багато хто говорить про здатність WormGPT писати цільові атаки BEC, насправді це лише верхівка айсберга. WormGPT пропонує низку інших розширених функцій, включаючи необмежену підтримку символів, збереження пам’яті чату та можливості форматування коду. Його здатність писати та форматувати код

особливо важлива, оскільки це означає, що він здатний створювати атаки зловмисного програмного забезпечення.

Важливо зазначити, що результати WormGPT не є складнішими за все, що може придумати людина. Краса цих типів програм, які використовуються назавжди, полягає в простоті використання та швидкості, а не в складності того, що вони можуть придумати. WormGPT особливо страшний, тому що він знижує бар'єри для входу, тобто фактично кожен може завантажити його на свій комп'ютер і сіяти хаос.

*Інші експлойти для хакерів*

Разом із WormGPT хакери також можуть використовувати ChatGPT для виконання частини своєї брудної роботи. Це передбачає «злам» існуючих платформ широкомовної моделі (LLM), таких як ChatGPT, щоб розблокувати нові функції; це дозволить використовувати інструменти, які можуть витягувати конфіденційну інформацію, маніпулювати самим ChatGPT для створення невідповідного вмісту, розкривати конфіденційну інформацію та навіть виконувати шкідливий код.

Що ще страшніше, ці джейлбрейки не містять жодного коду, а є просто підказками, які ви б скопіювали та вставили в ChatGPT, як зазвичай. Більшість цих підказок було опубліковано на GitHub — веб-сайті, який допомагає розробникам зберігати, керувати та іноді ділитися своїм кодом. Завдяки цьому будь-кому дуже легко зайти в Google і знайти ці підказки. Провівши власне розслідування, ми раді повідомити, що ChatGPT, схоже, застосував засоби захисту від цих атак, і багато хто з них просто відповіли: «Вибачте, але я не можу допомогти з цим запитом».

*Найкращий захист від WormGPT*

«Робочу силу потрібно навчити використовувати ці генеративні інструменти на основі ШІ LLM як для кіберзахисту, так і для нападу», — говорить Гупта. Гупта зазначив, що найкращі захисники у сфері кібербезпеки думають, як зловмисники, і це ключ до успіху, коли справа доходить до відсічі. На щастя, експерти з кібербезпеки змінили плани, використовуючи штучний інтелект для розпізнавання можливих атак і боротьби з ними до того, як вони відбудуться.

Незважаючи на здатність штучного інтелекту виконувати атаки BEC швидше, ніж будь-коли, найкращий механізм захисту від цих атак залишається незмінним: будьте уважні та не натискайте жодних сумнівних посилань. «Недостатня обізнаність серед співробітників і організацій — найкращий спосіб проникнути в систему для зловмисників», — каже Гупта.

Ці, здавалося б, нескінченні тренінги з кібербезпеки можуть викликати у вас біль у спині, але в кінцевому підсумку це може врятувати вашу компанію від катастрофічного витоку даних». ***(Matt Crisara. WormGPT: An AI Tool for Hackers // Hearst Magazine Media, Inc. (https://www.popularmechanics.com/technology/security/a45533297/what-is-wormgpt/?utm_source=flipboard&utm_content=thatsmystapler%2Fmagazine%2FSoftware). 03.11.2023).***

*******

**«У зв'язку з кількома резонансними кібератаками, які використовували різні аспекти безпеки та хмарної інфраструктури Microsoft за останні кілька років, технологічний гігант вирішив запустити нову ініціативу, яка прагне переглянути підхід компанії до безпеки програмного забезпечення.**

Одним із основних моментів нової ініціативи є плани Microsoft використовувати штучний інтелект, включаючи Microsoft Secure Copilot, щоб покращити свою рішучість, оскільки він відбиває атаки від досвідчених державних акторів.

*Microsoft запускає ініціативу безпечного майбутнього*

«Останніми місяцями ми прийшли до висновку, що зростаюча швидкість, масштаб і складність кібератак вимагають нової відповіді», — йдеться в повідомленні Microsoft у блозі, опублікованому цього тижня, анонсуючи нову ініціативу «Безпечне майбутнє».

Компанія також показала, що «нова кібердіяльність національної держави, спрямована на організації критичної інфраструктури в Сполучених Штатах» з використанням «складних, терплячих, прихованих, добре забезпечених ресурсами

та підтримуваних державою методів для зараження та підриву цілісності комп’ютерних мереж» доведена. стати каталізатором капітального оновлення безпеки.

Поряд із цими більшими державними загрозами, Microsoft зазначає, що компанія відстежує понад 120 менших за масштабом (але все ще дуже складних) афілійованих програм-вимагачів як послуг, які також мають змогу сіяти хаос у критичній інфраструктурі та ще дуже багато на волі.

Нова ініціатива складатиметься з трьох різних стовпів: кіберзахист на основі штучного інтелекту, прогресивна інженерія та розробка програмного забезпечення та пропаганда кращого захисту цивільного населення шляхом впровадження міжнародних норм кібербезпеки.

*Як Microsoft планує використовувати ШІ для боротьби із загрозами*

Ключовою частиною ініціативи Майкрософт щодо безпечного фокусування є використання можливостей штучного інтелекту, щоб зробити свої системи безпечнішими. Компанія робить «нові кроки» для використання штучного інтелекту в рамках Microsoft Threat Intelligence.

Microsoft також каже, що планує надати клієнтам деякі з цих можливостей і використовувати штучний інтелект, щоб зменшити поточні затримки, які виникають під час процесів виправлення вразливостей.

Технологічний гігант також використовує штучний інтелект, щоб допомогти аналітикам безпеки та підвищити їхню ефективність у роботі. Microsoft Security Copilot – орієнтований на безпеку інструмент штучного інтелекту, який був запущений у березні 2023 року – може давати рекомендації щодо безпеки та керування системою на основі аналізу величезних обсягів складних даних.

Microsoft зазначає, що компанія розгортає свою технологію штучного інтелекту відповідно до своїх правил відповідального штучного інтелекту, але зазначає, що її кодекс етики штучного інтелекту, можливо, повинен розвиватися та змінюватися разом із технологією, яка розвивається швидкими темпами.

*Чи продовжаться напади?*

Протягом останніх кількох років корпорація Майкрософт стала об'єктом низки гучних кібератак, остання з яких пов'язана з помилкою в хмарній платформі обміну повідомленнями Microsoft Exchange Online (OWA) та її службі електронної пошти Outlook.com.

У той час Microsoft піддалася значній критиці, а генеральний директор Tenable Аміт Йоран назвав мляву реакцію компанії «вкрай безвідповідальною, якщо не відвертою недбалістю».

Цьому передувала атака SolarWinds у 2020 році, під час якої системи Microsoft використовувалися, щоб продовжити те, що виявилося однією з найскладніших, шкідливих кібератак, які коли-небудь мали місце.

Такі загрози не просто так зникнуть. Але, можливо, найбільшою зміною в тому, як компанія підходила до безпеки та кіберзагроз за майже два десятиліття, є досить рішуча відповідь». ***(Aaron Drapkin. Microsoft Launches New Cybersecurity Strategy in Response to Latest Attacks // Marketing VF Ltd. (https://tech.co/news/microsoft-new-cybersecurity-strategy)ю 03.11.2023).***

***

**«У сучасному цифровому ландшафті, що постійно розвивається, кібербезпека є першочерговою проблемою, і роль штучного інтелекту (ШІ) стає потенційною суттєвою зміною.** З розвитком технологій захист нашого цифрового світу стає дедалі складнішим, і штучний інтелект дає невикористану перспективу. Однак, незважаючи на те, що штучний інтелект пропонує маяк надії в кібербезпеці, залишається певна невизначеність щодо його точної ролі та ефективності. Недавнє дослідження, проведене Adarma, проливає світло на уявлення та очікування щодо ШІ в кібербезпеці.

*Загадка штучного інтелекту в кібербезпеці*

Серед зростаючої кількості складних інструментів безпеки штучний інтелект часто виглядає як нова технологія з невловимою роллю в зміцненні операцій безпеки. Опитування, проведене Adarma серед 500 керівників відділів безпеки з

британських організацій із понад 2000 співробітників, показало, що 74 відсотки респондентів важко уявити, як ШІ допоможе їм у виконанні їхніх завдань. Ця невизначеність відображає постійну проблему ефективної інтеграції штучного інтелекту в стратегії кібербезпеки.

*Потенційні застосування ШІ*

Незважаючи на невизначеність, лідери безпеки бачать значний потенціал у ШІ. Відповідаючи на питання про його потенційні застосування, 61 відсоток респондентів вважають, що автоматизація може виконувати до 30 відсотків завдань безпеки, якими зазвичай керують люди. Ще 17 відсотків вважають, що ШІ візьме на себе більше половини цих обов'язків. Це підкреслює зростаюче визнання потенціалу штучного інтелекту трансформувати операції з кібербезпеки.

*Зменшення людських помилок і помилкових спрацьовувань*

Одна з головних сфер, на яку штучний інтелект може суттєво вплинути, — це зменшення людських помилок і тягаря помилкових спрацьовувань. Більшість сповіщень, надісланих командам безпеки, є помилковими спрацьовуваннями, які наразі потребують втручання людини для перевірки. ШІ міг швидко оцінити ці хибні спрацьовування, роблячи миттєві визначення на основі аналізу контексту. 53 відсотки респондентів вважають за краще скоротити час, витрачений на звітність, яка залишається в основному неавтоматизованою, а 70 відсотків визнали, що вони не використовують автоматизацію.

*Автоматизація повторюваних завдань*

Прогалина в автоматизації звітності та інших повторюваних чи буденних обов'язків відкриває значні можливості для ШІ. Автоматизуючи ці завдання, ШІ може підвищити задоволеність, ефективність і результативність команд безпеки. Крім того, 42 відсотки фахівців із безпеки вважають, що автоматизація надасть кращу контекстну інформацію, що допоможе прийняти більш обґрунтовані рішення.

*Допомога в ізоляції та стримуванні загрози*

Ще одна важлива сфера впровадження ШІ – це допомога в ізоляції та стримуванні потенційних загроз. Правильно налаштовані системи штучного

інтелекту можуть суттєво знизити ризик поширення загрози в IT-середовищі організації. Однак усвідомлення цих переваг вимагає від лідерів безпеки довіряти цій технології, що розвивається.

*Побудова довіри до ШІ*

Довіра до штучного інтелекту залишається серйозною проблемою, враховуючи відносну зародковість технології та брак досвіду штучного інтелекту в галузі кібербезпеки. Організаціям потрібен час, щоб зміцнити довіру до штучного інтелекту, а фахівцям із безпеки набути необхідних навичок для його безпечного та ефективного розгортання. У міру розвитку штучного інтелекту лідери безпеки повинні залишатися обережними та пильними у своєму підході.

*Проблеми впровадження автоматизації*

Цікаво, що респонденти, які розпочали свій шлях автоматизації, повідомили про помірний успіх у своїх проектах автоматизації. Однак вони також визнали складність і трудомісткість процесу. Зокрема, 42 відсотки вважали впровадження автоматизації складним і трудомістким, а ще 21 відсоток вказали, що це було більш вимогливим, ніж передбачалося спочатку. Тим не менш, переважна більшість (73 відсотки) засвідчили, що зусилля, вкладені в автоматизацію, варті того.

*Навігація в майбутньому ШІ в кібербезпеці*

Керівники служби безпеки все ще звикають до ШІ в кібербезпеці, діючи з виправданою обережністю. Застосування нових технологій вимагає пильного нагляду, щоб ефективно керувати еволюцією ШІ. Зміцнення впевненості та довіри до можливостей ШІ залишається пріоритетом.

Ретельні оцінки та постійний моніторинг гарантують, що штучний інтелект відповідає бажаним результатам. Вкрай важливо підходити до цього з розумінням того, що мета полягає не в придушенні інновацій, а в розумінні пов’язаних ризиків і комплексному ефективному управлінні ними. Оскільки в майбутньому організації будуть протистояти кіберзагрозам, ефективність і точність штучного інтелекту стануть стрижнею для підтримки надійного захисту. ШІ в кібербезпеці має потенціал для революції в галузі, і в міру зростання довіри його роль ставатиме лише помітнішою». ***(Editah Patrick. Unleashing the Power of Artificial Intelligence in***

***Cybersecurity // Cryptopolitan (https://www.cryptopolitan.com/unleashing-the-power-of-ai-in-cybersecurity/?utm_source=flipboard&utm_content=rubertus%2Fmagazine%2FInnovation%2C+Business+%26+Creativity+%7C+Innovaci%C3%B3n+y+Creatividad). 01.11.2023).***

***

**«Штучний інтелект трансформує кібербезпеку в корені. Деякі підозри про це виникли вже з появою ChatGpt, зокрема з першими новинами про використання генеративного ШІ злочинцями, вже в останні місяці. Однак останніми тижнями почулися інші новини, і вони позитивні: «хороші хлопці» починають наздоганяти «поганих», а на ринок з'являються перші передові рішення штучного інтелекту для кібербезпеки.** Про це, серед іншого, стало відомо 24 жовтня на заході Sole24Ore Cybersecurity 2023; але доказів, які надходять, багато.

Згідно зі звітом Marketsand Markets, розмір глобального ринку штучного інтелекту в сфері кібербезпеки зросте з 8,8 мільярда доларів США у 2020 році до 38,2 мільярда доларів США до 2026 року.

У звіті також наголошується, що через зростання кількості кіберзагроз і нестачу кваліфікованих фахівців з кібербезпеки нам буде дедалі більше потрібний ШІ в кібербезпеці. У певному сенсі використання штучного інтелекту в кібернетичному просторі зараз є необхідним як для вирішення давніх проблем, так і через те, що штучний інтелект все частіше використовується злочинцями. Обережно: задовго до пандемії великі та малі компанії з кібербезпеки демонстрували рішення штучного інтелекту на галузевих виставках, таких як щорічне зібрання Black Hat у Лас-Вегасі, штат Невада. Компанії пообіцяли, що їхнє останнє рішення зупинить зловмисних хакерів до того, як вони зможуть завдати шкоди. Однак у той час це був здебільшого чистий маркетинг. Щось змінюється завдяки останнім технологічним розробкам.

На цьогорічному Black Hat представники Агентства передових оборонних досліджень уряду США (Darpa) оголосили про запуск AI Cyber Challenge, дворічного конкурсу, спрямованого на створення передових систем кібербезпеки на базі штучного інтелекту та призначений для захисту критичної інфраструктури країни. У ньому беруть участь усі відомі представники галузі, як-от OpenAI, творці ChatGpt.

*Поточні кіберзагрози з ШІ*

Водночас у цьому Black Hat дослідники стартапу з кібербезпеки HiddenLayer продемонстрували ЗМІ та потенційним клієнтам, як штучний інтелект можна використовувати для злому систем онлайн-банкінгу. В одному випадку ШІ допоміг переконати банк схвалити шахрайську заявку на кредит. Щоразу, коли заявку відхиляли, штучний інтелект вивчав цю спробу та змінював запит, поки він не був прийнятий. Говорячи про обман: вже є численні приклади використання генеративного ШІ для написання ефективних фішингових повідомлень; здається неминучим, що використання глибоких фейків (аудіо та відео), створених за допомогою штучного інтелекту, щоб викрасти чиюсь особу з метою шахрайства, потім поширяться. Наприклад, отримати від компанії банківський переказ на вашу користь. В іншому випадку, представленому в останньому Black Hat, саме штучний інтелект створив уразливість у системах. Зловмисники обманним шляхом змусили надати конфіденційну фінансову інформацію банківського чат-бота на базі ChatGpt. «Штучний інтелект дозволяє здійснювати кібератаки одночасно, автоматично та швидко», — пояснює Росіта Галіандро, керівник обсерваторії кібербезпеки Exprivia.Ще одне відоме злочинне використання, про яке повідомляють численні охоронні компанії, — отримати допомогу ШІ для написання коду безпеки шкідливе програмне забезпечення.

*Рішення AI для кібер*

Але, на щастя, є й хороші новини. ШІ відкриває нову еру кіберзахисту. Майте на увазі, що традиційні підходи до кібербезпеки значною мірою покладаються на системи виявлення на основі сигнатур, які ефективні лише проти відомих загроз. Таким чином, нові та невідомі загрози можуть залишитися непоміченими. З іншого

боку, рішення на основі штучного інтелекту використовують алгоритми машинного навчання, які можуть виявляти відомі та невідомі загрози та реагувати на них у реальному часі. Переваги: більша швидкість і більша здатність виявлення. «Штучний інтелект скорочує середній час виявлення загрози в компанії на 112 днів», — говорить Стефано Ребаттоні, віце-президент Assolombarda, відповідальний за цифровий перехід і технологічні інновації. Тому кіберрішення з штучним інтелектом розмножуються, як також зазначив Джанлука. Галассо, адмірал, директор Оперативної служби Національного агентства з кібербезпеки. Галассо згадує два продукти VirusTotal, випущені кілька місяців тому. Crowdsourced AI, який зосереджується на файлах PowerShell, описуючи їх поведінку та надаючи прогнози щодо потенційного рівня загрози. CodeInsight дозволяє експертам із безпеки та аналітикам глибше зрозуміти призначення та функціонування аналізованого коду; тим самим покращуючи здатність виявляти та пом'якшувати загрози. Крім того, восени, як також зазначає Галассо, з'явиться Microsoft Security Copilot, чат-бот-помічник, призначений для експертів із безпеки. Тобто, щоб змусити співпрацю людини і машини працювати: між ШІ та експертами. На думку деяких з них, найбільшою допомогою штучного інтелекту буде полегшення робочого навантаження. Не вистачає кваліфікованих фахівців, щоб заповнити всі відкриті вакансії з кібербезпеки. Якщо ШІ зможе визначити потенційні загрози, це звільнить час аналітиків для оцінки та втручання. Системи штучного інтелекту також можуть виявитися важливим інструментом для навчання більшої кількості фахівців з кібербезпеки, допомагаючи їм навчитися робити такі речі, як зворотне проектування та розбиття коду. Коротше кажучи: якщо ШІ виявиться зброєю на службі добра, а не зла, це станеться не лише завдяки новим корисним кіберпродуктам; але перш за все, якщо це допоможе експертам працювати краще». ***(Alessandro Longo. L'intelligenza artificiale sta trasformando la cyber security // Il Sole 24 Ore (https://www.ilsole24ore.com/art/come-l-intelligenza-artificiale-sta-rivoluzionando-cyber-security-AFcI7VSB). 01.11.2023).***

***

**«…Хоча штучний інтелект допомагає розробникам кодувати швидше та бути більш продуктивними, деякі керівники стурбовані тим, що це може створити додаткові проблеми з безпекою та управлінням ризиками.** Але індустрія кібербезпеки не знайома з новими технологіями, і ми повинні продовжувати використовувати всі наявні в нашому розпорядженні інструменти для захисту екосистеми програмного забезпечення.

AI втілює в реальність обіцянку «зсуву вліво».

За умови ефективного використання штучний інтелект може запобігти запису вразливостей, радикально змінюючи систему безпеки. AI надає контекст для потенційних уразливостей і пропонує безпечний код із самого початку (хоча, будь ласка, все ж тестуйте створений AI код). Ці можливості дозволяють розробникам писати більш безпечний код у режимі реального часу та, нарешті, реалізувати справжню обіцянку «зсуву вліво».

Це революційно. Традиційно «зсув ліворуч» зазвичай означав отримання відгуку про безпеку після того, як ви перенесли свою ідею в код, але перед її розгортанням у виробництві. Але з ШІ безпека справді вбудована, а не прикручена. Немає іншого способу «зрушити ліворуч», ніж зробити це в тому самому місці, де ваші розробники втілюють свої ідеї в код, а їх пара програмістів ШІ допомагає їм у цьому. Це захоплююча нова ера, коли генеративний ШІ буде на передовій кіберзахисту.

Однак також важливо зазначити, що так само, як ШІ не замінить розробників, ШІ не замінить потребу в командах безпеки. Ми ще не досягли рівня 5 самостійного керування. Нам потрібно тримати руки на кермі та працювати з наявними засобами безпеки, а не відмовлятися від них.

*Зелене світло ШІ у вашій організації*

Деякі команди вже отримують значні переваги у продуктивності завдяки штучному інтелекту, але інші лідери все ще стурбовані ризиками безпеки та хочуть знати, як створити правильні стандарти для інструментів штучного інтелекту. Як ви можете забезпечити хороші результати безпеки, дозволяючи розробникам

програмного забезпечення виконувати найкращу (і найбезпечнішу) роботу на основі штучного інтелекту?

У GitHub ми багато практикувалися зі штучним інтелектом, і я хочу поділитися кількома найкращими практиками, які організації можуть використати, намагаючись застосувати генеративний інструмент ШІ. Ці стратегії відокремлять організації, які процвітають, і організації, яким не вдається захистити свої найцінніші активи. Давайте поглянемо.

*Ставтеся до інструментів AI як до всіх інших інструментів*

Хоча ШІ є новою технологією, вона має більше спільного з іншими інструментами, ніж ні. Ви можете почати з тих самих систем безпеки та ризиків для оцінки інструменту штучного інтелекту, що й для будь-якого іншого інструменту, який ви хочете включити у свій стек, і з часом налаштовувати їх. Попросіть діаграми потоку даних, зовнішні звіти про тестування та іншу інформацію про безпеку та зрілість інструменту.

У GitHub є процеси, які допомагають нам визначати та керувати ризиками, пов’язаними з будь-яким новим інструментом, наданим зовнішнім постачальником. Нові інструменти чи послуги ретельно перевіряються нашими відділами закупівель, юридичних питань, конфіденційності та безпеки, приділяючи особливу увагу тому, які дані використовуватимуться, як вони використовуватимуться та як дані будуть захищені зовнішнім постачальником.

*Розуміти використання та збереження даних*

Головне, за чим ви хочете стежити, це те, як керуються ваші дані або дані ваших клієнтів. Зрештою, ви можете собі уявити, які занепокоєння щодо безпеки виникають, коли сторонній постачальник зберігає та використовує вашу конфіденційну інформацію про компанію чи клієнта. Отже, вам потрібно знати, як інструмент штучного інтелекту керує вашими даними, куди дані йдуть, як ними ділиться та чи зберігаються. Зверніть увагу на те, чи використовує постачальник дані клієнтів для навчання своїх моделей штучного інтелекту, і зрозумійте, які варіанти доступні, щоб увімкнути або відмовитися від використання цих даних залежно від ваших потреб.

*Перегляньте положення про інтелектуальну власність*

Інструменти штучного інтелекту відкривають цілий новий світ питань інтелектуальної власності (ІВ), а правовий ландшафт все ще розвивається. Розгляньте положення про інтелектуальну власність нового інструменту та перегляньте умови ліцензійної угоди, щоб зрозуміти, які засоби захисту можуть бути запропоновані. Наприклад, і Microsoft, і Google пропонують клієнтам компенсацію за інтелектуальну власність при використанні своїх генеративних інструментів ШІ.

Крім того, майте на увазі, що кожен раз, коли розробник використовує код, який він не створював, він стикається з цим ризиком, наприклад, коли він копіює код з онлайн-джерела або повторно використовує код з бібліотеки. Ось чому відповідальні організації та розробники використовують політику сканування коду та інші методи перевірки.

*Слідкуйте за послужним списком інструменту*

Розуміння послужного списку інструменту є важливим. Це гарантує, що продукт ШІ є надійним, ефективним і відповідає цілям вашої компанії. Яка минула продуктивність і точність інструменту? Шукайте випадки успішного використання, які демонструють його ефективність. Який тип набору даних використовується для його навчання? Переконайтеся, що набір даних відповідає вашим проектам. Інші речі, на які варто звернути увагу, включають пом’якшення упередженості, відгуки користувачів і можливість налаштування.

*Перевірте перевірки інструменту*

Ми всі знаємо, що сторонні тестування та перевірки є неоціненними для оцінки ефективності та безпеки технології. Тут та сама історія. Запитайте, чи інструмент штучного інтелекту пройшов тестування третьої сторони. Інструмент штучного інтелекту може не відповідати вимогам через те, наскільки він новий, але чи сумісні інші продукти компанії? Чи є план досягнення відповідності продукту ШІ? Вибір інструменту, який пройшов ретельні випробування та аудит, зміцнить безпеку вашої організації.

Коли справа доходить до штучного інтелекту, вам не потрібно бути «департаментом ні». Дотримуючись наведених вище найкращих практик, ви можете встановити огородження та правила взаємодії, які призведуть до безпечних результатів.

Так само, як штучний інтелект не замінить розробників, він не замінить вашу потребу в командах безпеки, але значно покращить їхню роботу. Немає кращого способу «зрушити вліво», ніж мати програміста зі штучним інтелектом у парі прямо в IDE з вашими розробниками, допомагаючи їм писати безпечніший і надійніший код у реальному часі. Це допоможе вам швидше досягти кращих результатів безпеки — і, насмілюся сказати, радикально змінить наступне десятиліття безпеки». ***(Mike Hanley. AI is the future of cybersecurity. This is how to adopt it securely // Mansueto Ventures, LLC (https://www.fastcompany.com/90979519/ai-future-of-cybersecurity-adopt-securely?utm_source=flipboard&utm_content=AlexanderFin%2Fmagazine%2FAI%2C+CHAT+GPT+%26+AI+ART). 09.11.2023).***

***

**«Виробники електроніки Siemens, Ericsson і Schneider Electric разом з галузевою групою DigitalEurope попередили в понеділок, що обтяжливі запропоновані правила ЄС, спрямовані на ризики кібербезпеки розумних пристроїв, можуть порушити ланцюги поставок у масштабах, подібних до тих, що були під час пандемії.**

Запропонований Європейською комісією минулого року Закон про кібер-стійкість вимагає від виробників оцінювати ризики кібербезпеки своїх продуктів і вживати заходів для вирішення проблем протягом п’яти років або протягом очікуваного терміну експлуатації продуктів.

Запропоновані правила також стосуватимуться імпортерів і розповсюджувачів пристроїв, підключених до Інтернету. Занепокоєння щодо кібербезпеки різко зросло після серії гучних інцидентів, коли хакери завдавали шкоди бізнесу та вимагали величезні викупи.

«Закон у його нинішньому вигляді ризикує створити вузькі місця, які порушать єдиний ринок», — написали керівники компаній у спільному листі голові індустрії Європейського Союзу Тьєррі Бретону та керівнику цифрового відділу ЄС Вірі Юровій.

Вони сказали, що збої можуть вразити мільйони продуктів, починаючи від пральних машин і закінчуючи іграшками, продуктами кібербезпеки, а також життєво важливими компонентами для теплових насосів, охолоджуючих машин і високотехнологічного виробництва. Затримки можуть бути пов'язані з браком незалежних експертів для проведення оцінок і бюрократією, кажуть компанії.

«Ми ризикуємо створити блокування в європейських ланцюгах поставок у стилі COVID, порушивши єдиний ринок і завдавши шкоди нашій конкурентоспроможності», — заявили компанії.

Серед інших підписантів листа – генеральні директори Nokia, Robert Bosch GmbH і словацької компанії-виробника програмного забезпечення ESET.

Компанії заявили, що список продуктів з підвищеним ризиком, на які поширюється це правило, слід значно скоротити, а виробникам слід дозволити виправляти відомі ризики вразливості, а не проводити спочатку оцінку.

Вони також хочуть більше гнучкості для самостійної оцінки ризиків кібербезпеки.

Лист надійшов напередодні переговорів 8 листопада між країнами ЄС і законодавцями ЄС, щоб обговорити деталі законопроекту, перш ніж його можна буде ухвалити». ***(Foo Yun Chee. Siemens, Ericsson Warn EU Cybersecurity Rules May Disrupt Supply Chains // U.S. News & World Report L.P. (https://www.usnews.com/news/technology/articles/2023-11-06/siemens-ericsson-warn-eu-cybersecurity-rules-may-disrupt-supply-chains?utm_source=flipboard&utm_content=rubertus%2Fmagazine%2FInnovation%2C+Business+%26+Creativity+%7C+Innovaci%C3%B3n+y+Creatividad). 06.11.2023).***

***

**«Штучний інтелект, застосований до кібербезпеки, відкриває нові перспективи щодо все більш важливої та делікатної теми для бізнесу (і не тільки); сектор, у якому в найближчі роки будуть зосереджені значні інвестиції.** Щоб глибше заглибитися в тему, давайте подивимося на дослідження Іва Крамера, старшого інвестиційного менеджера Pictet asset management.

*Ідентифікатор кіберзлочинця і як захистити себе*

Жовтень повернув увагу до теми кібербезпеки. Європейський місяць кібербезпеки (ECSM), організований Агентством Європейського Союзу з кібербезпеки (Enisa), розмістив феномен соціальної інженерії, набір методів, які використовують кіберзлочинці, спрямовані на те, щоб переконати ціль розкрити певну інформацію або виконати дії з неправомірних причин. Як пише Європейський інститут, позиція кіберзлочинців добре відома: він використовує такі важелі, як емпатія та самовдоволення, щоб залицятися до своєї жертви, використовуючи терміновість запиту та здатність вирішувати проблеми (часто створені самим злочинцем), щоб отримати інформацію або гроші та замести сліди.

*Забезпечте безпеку даних*

Цифрова безпека та безпека даних є надзвичайно делікатними питаннями. У контексті, де все ще мало обізнаності, великі компанії мобілізують величезні суми інвестицій, щоб забезпечити безпеку своїх користувачів. Очікується, що між 2021 і 2025 роками загальні щорічні витрати на кібербезпеку досягнуть 1,75 трильйона доларів. У той же час очікується, що до 2025 року глобальні витрати від кіберзлочинності зростуть до 10,5 трильйонів доларів на рік. Таким чином, нездатність запобігти цьому може дорого коштувати.

До цих даних додається сфера застосування штучного інтелекту, яка матиме подвійний ефект: з одного боку, інтеграція штучного інтелекту зробить системи захисту ефективнішими, оптимізуючи час, витрачений на виявлення загроз, прискорить пропозицію рішень і покращить ідентифікацію. і захист потоку даних; з іншого боку, однак, це зробить вчинені атаки все більш витонченими, ускладнить вплив на інфраструктуру та розширить ціль.

Впровадження нових технологій для використання переваг і захисту від наслідків штучного інтелекту (ключовий елемент ефективності ринку з початку 2023 року, особливо для стратегій, пов'язаних із цифровою технікою та робототехнікою) стане фундаментальним у найближчі місяці та роки. Кібератаки вже сьогодні є величезною проблемою: кожні 39 секунд хакеру вдається проникнути в систему, і щодня через злами викрадається близько 3,8 мільйона записів. Не дивно, що галузь кібербезпеки цього року зросте на 14%, згідно з Gartner. Також виходячи з оцінок, дві третини американських компаній збільшать свої інвестиції в кібербезпеку цього року порівняно з 2022 роком, головним чином побоюючись фінансових втрат.

*Нові потреби в безпеці*

Саме виходячи з усвідомлення теми, ми можемо зрозуміти потенціал, який все ще існує в цій сфері. Нові технології відкривають нові потреби в безпеці: розумні міста все більше використовуватимуть революційні технології для вирішення демографічних, економічних, екологічних, інфраструктурних і соціальних проблем і вимагатимуть інвестицій у розумну інфраструктуру, мобільність і будівлі.

Завданням для охоронних компаній буде розробка нового покоління інструментів кібербезпеки, які включають такі технології, як генеративний штучний інтелект, щоб забезпечити швидке та масштабне розпізнавання шкідливих програм. Технологічний розвиток може призвести до створення нових підсекторів кібербезпеки, наприклад, створення нового ринку для контролю інформації, створеної системами ШІ.

У більш загальному плані, враховуючи постійну економічну невизначеність, ми вважаємо, що пріоритетом компаній і урядів буде захист критично важливих інфраструктур країн, захист цілісності громадян і забезпечення здатності бізнесу досягати своїх цілей. Російсько-український конфлікт і ескалація ізраїльсько-палестинської напруженості, ключові структурні проблеми, переосмислять такі питання, як кібербезпека, решорінг і безпека ланцюга постачання. Кіберпростір виявився новим кордоном війни: міжнародні дипломатичні труднощі ще більше

підкреслили зростаючу важливість кібербезпеки для захисту від скоординованих кібератак. У зв'язку з цим ми очікуємо, що європейський попит на продукти кібербезпеки прискориться в коротко- та середньостроковій перспективі, щоб наздогнати Сполучені Штати та Азію». ***(Cyber security sempre più strategica per le imprese. L'analisi di Pictet Am // RIPRODUZIONE RISERVATA (https://www.bluerating.com/mercati/798952/cyber-security-sempre-piu-strategica-per-le-imprese-lanalisi-di-pictet-am). 09.11.2023)***.

***

**«Дослідження RiverSafe показало, що 95% компаній терміново виступають за кіберрегулювання штучного інтелекту напередодні листопадового саміту з безпеки штучного інтелекту.**

У звіті під назвою «AI Unleashed: Navigating Cyber Risks Report», проведеному Censuswide, виявлено ставлення 250 керівників кібербезпеки до впливу ШІ на кібербезпеку.

Три з чотирьох підприємств (76% опитаних підприємств) виявили, що впровадження штучного інтелекту в їх діяльності було припинено через значні кіберризики, пов'язані з цією технологією.

Занепокоєння безпекою також спонукали 22% організацій заборонити своєму персоналу використовувати чат-боти ШІ, підкреслюючи глибоко вкорінене побоювання щодо потенційної вразливості ШІ.

Щоб управляти ризиками, дві третини (64%) респондентів збільшили свої кібербюджети цього року, демонструючи прихильність зміцненню захисту своєї кібербезпеки.

Суїд Адеянджу, генеральний директор RiverSafe, каже: «Хоча штучний інтелект має багато переваг для бізнесу, очевидно, що лідери в сфері кібербезпеки стикаються з основними ризиками. Атаки з підтримкою штучного інтелекту можуть збільшити складність порушень безпеки, наражаючи організації на інциденти з даними, і ми досі не вивчили повний ступінь ризиків, які може становити штучний інтелект. Поспішати з впровадженням штучного інтелекту без

першорядної уваги до безпеки – це небезпечний шлях, тому досягнення тонкого балансу між технологічним прогресом і надійною кібербезпекою є першорядним».

Дві третини компаній (63%) очікують зростання кількості інцидентів із втратою даних, тоді як кожен п'ятий (18%) респондент визнав, що цього року їхній бізнес зазнав серйозного кіберзлому, наголошуючи на необхідності вжиття надійних заходів кібербезпеки…» ***(Isha Jain. Research reveals that 95% of security leaders are calling for AI cyber regulations // Media Ltd. (https://dcnnmagazine.com/security/research-reveals-95-of-security-leaders-are-calling-for-ai-cyber-regulations/). 07.11.2023).***

***

**«Змагання за використання потенціалу цифрової трансформації для генеративного штучного інтелекту (ШІ) досягли найвищого рівня, яке почалося в листопаді минулого року з випуском ChatGPT.** Швидкий розвиток нових технологій часто призводить до «повільного розвитку» правових зобов'язань і зобов'язань щодо відповідності, які іноді вітаються, а іноді зневажаються.

У понеділок Білий дім опублікував свій виконавчий наказ про безпечну, захищену та надійну розробку та використання штучного інтелекту (ЕО). ЕО та його шістдесят чотири сторінки будуть розбиратися тижнями та місяцями, враховуючи численні терміни. Отже, що вам потрібно знати прямо зараз?

Зараз нічого нового не впливає на бізнес. ЕО сам по собі не встановлює жодних нових правил, положень або вимог до звітності для підприємств.

Але нові вимоги з'являються… Зрештою ЕО встановлює зобов'язання для багатьох агенцій, починаючи від наказів найняти та навчати більше спеціалістів зі штучного інтелекту до термінів подання звітів та оцінки впливу. Декілька включають директиви щодо розробки протягом наступних трьох-дванадцяти місяців вимог до звітності, правил, політики та галузевих стандартів. Багатьом із цих пропозицій доведеться подолати довгий і звивистий шлях нормотворчого процесу.

Відповідність не є кібербезпекою. ЕО, зрозуміло, реакційний. Він реагує на занепокоєння навколо штучного інтелекту, які багато компаній уже повинні активно вирішувати, наприклад, безпеки, конфіденційності та, можливо, найважливіше, кібербезпеки. Реактивний характер ЕО підкреслює терміновість вирішення проблем ШІ зараз. Зверніться до надійного юриста.

Відповідно до минулорічної заяви начальника відділу безпеки Microsoft про те, що «кібербезпека — це мати всіх проблем. Якщо ви не розв'яжете це, усі інші технологічні речі просто не відбудуться», – ЕО робить великий акцент на кібербезпеці, заявляючи в супровідному інформаційному листі, що стандарти, інструменти та тести повинні бути розроблені для вирішення проблеми кібербезпеки систем ШІ. ризики.

З поважної причини. Організації вже стикалися з кібератаками з підтримкою штучного інтелекту, які включали викрадання конфіденційної бізнес-інформації, службової інформації та вихідного коду. Ці ризики разом із зростанням «змагальності» штучного інтелекту – практики модифікації систем штучного інтелекту для навмисного маніпулювання чи нападу – є лише верхівкою айсберга.

Щоб протистояти цим новим загрозам кібербезпеки, ЕО вимагає створення розширеної програми кібербезпеки для розробки інструментів штучного інтелекту для пошуку та усунення вразливостей у критичному програмному забезпеченні. ЕО встановлює кінцеві терміни, до яких мають бути встановлені певні стандарти для обміну інформацією. Наприклад:

Звітування про кібербезпеку – протягом 90 днів (~28 січня 2024 р.) – Міністр торгівлі має опублікувати вимоги до звітності для компаній, які розробляють «базові моделі подвійного призначення», щоб повідомити про те, коли відбудеться тестування цих моделей, захист фізичної та кібербезпеки в місце проведення цих тестів і результати цих тестів. Див. § 4.2(a)-(b).

Облік кібербезпеки — протягом 90 днів (~28 січня 2024 р.) — Міністр торгівлі має запропонувати правила для іноземних громадян, які навчають штучному інтелекту з можливостями, які будуть використовуватися в зловмисних діях у кібернетичному просторі, для реєстрації та підтримки певних функцій

ведення записів. до отримання доступу до інфраструктури як послуги США («IaaS»). Див. § 4.2(c).

Рекомендації щодо критичної інфраструктури – протягом 180 днів (~28 березня 2024 р.) – міністр внутрішньої безпеки включить ризики штучного інтелекту до відповідних інструкцій щодо безпеки та безпеки для використання власниками та операторами критичної інфраструктури. Див. § 4.3(a).

Хоча ЕО насамперед спрямований на федеральні агентства та розробників штучного інтелекту, ризики штучного інтелекту підкреслюють необхідність для всіх організацій переглянути свою позицію щодо кібербезпеки, особливо свої плани реагування на інциденти, проводити оцінку ризиків і підтримувати програми безпеки. Усе це вже загальноприйнято як юридичні, регулятивні чи галузеві стандарти». ***(Romaine C. Marshall, Catherine (Cat) Kozlowski, Jonathan E. Schmalfeld. Unpacking the Executive Order on AI (for Cybersecurity) // Polsinelli PC (https://www.polsinelli.com/publications/unpacking-the-executive-order-on-ai-for-cybersecurity). 03.11.2023).***

***

**«…Глобальний прогноз кібербезпеки Google Cloud виявив, що генеративний штучний інтелект може допомогти зловмисникам і захисникам, і закликав персонал служби безпеки остерігатися атак, які підтримуються національними державами, тощо…**

*Як генеративний ШІ може вплинути на кібербезпеку в 2024 році*

Зловмисники використовуватимуть генеративний штучний інтелект і великі мовні моделі для фішингу та інших шахрайств із соціальною інженерією, прогнозує Google Cloud. Оскільки генеративний штучний інтелект може створювати контент із природним звучанням, співробітникам може бути важко розпізнавати шахрайські електронні листи через погану граматику або спам-дзвінки через роботизоване звучання голосів. Google Cloud попереджає, що зловмисники можуть використовувати генеративний штучний інтелект для створення фейкових новин або фейкового контенту.

LLM і генеративний штучний інтелект «будуть все частіше пропонуватися на підпільних форумах як платні послуги та використовуватимуться для різних цілей, таких як фішингові кампанії та поширення дезінформації», – пише Google Cloud.

З іншого боку, захисники можуть використовувати генеративний ШІ для розвідки загроз та аналізу даних. Генеративний штучний інтелект може дозволити захисникам діяти з більшою швидкістю та в масштабах, навіть якщо перетравлюються дуже великі обсяги даних.

«Штучний інтелект вже надає величезну перевагу нашим кіберзахисникам, дозволяючи їм покращувати можливості, зменшувати трудомісткість і краще захищати від загроз», — сказав Філ Венейблс, керівник відділу інформаційної безпеки Google Cloud, в електронному листі до TechRepublic.

*Національні держави можуть використовувати зловмисне програмне забезпечення для фішингу або стирання*

У звіті зазначається, що національні державні суб’єкти можуть здійснити кібератаки проти уряду США з наближенням президентських виборів у США 2024 року. Зокрема, фішинг може використовуватися для нападу на виборчі системи, кандидатів або виборців.

Хактивізм або політично вмотивовані загрози, не пов’язані з певною національною державою, відроджуються, повідомляє Google Cloud.

Зловмисне програмне забезпечення Wiper, призначене для стирання пам’яті комп’ютера, може стати більш поширеним. Google Cloud повідомила, що його розгорнули російські групи загроз, які атакували Україну. Війна в Україні показала, що спонсоровані державою зловмисники можуть атакувати космічні технології, щоб завадити противникам або здійснити шпигунство.

Шпигунські групи у 2024 році можуть створити «сплячі бот-мережі», тобто бот-мережі, розміщені в Інтернеті речей, офісних пристроях або пристроях, що вийшли з ладу, для тимчасового масштабування атак. Тимчасовий характер цих ботнетів може ускладнити їх відстеження.

*Старі типи кібератак все ще є загрозою*

Деякі з тенденцій, виділених Google Cloud, показують, що добре відомі типи кібератак все ще повинні бути на радарі команд безпеки.

Уразливості нульового дня можуть продовжувати зростати. Зловмисники з національних держав і групи дійових осіб можуть застосувати нульові дні, оскільки ці вразливості дають зловмисникам постійний доступ до середовища. Фішингові електронні листи та зловмисне програмне забезпечення зараз відносно легко виявити для команд безпеки та автоматизованих рішень, але вразливості нульового дня залишаються відносно ефективними, йдеться у звіті.

Здирництво, ще одна добре відома техніка кібератак, у 2022 році зупинилася, але можна очікувати, що воно знову зросте у 2024 році. Зловмисники рекламують викрадені дані та повідомляють про доходи від вимагань, що свідчить про зростання.

Деякі застарілі методи загроз стають достатньо популярними, щоб потрапити на радари Google Cloud. Наприклад, нещодавно знову з'явилася техніка антивіртуальної машини 2012 року. І атака, вперше задокументована в 2013 році, яка використовує недокументовані функції SystemFunctionXXX замість криптографічних функцій у задокументованому Windows API, знову стала популярною.

*Інші тенденції та прогнози кібербезпеки в хмарі, мобільних і SecOps*

Віце-президент і генеральний директор Google Cloud Суніл Потті сказав в електронному листі TechRepublic: «Наразі ми бачимо, що організації обслуговують свої дані в поєднанні багатохмарного, локального та гібридного середовища, і хоча нереалістично очікувати, що ці організації розмістять свої активи лише в одному місці, це робить уніфіковані, комплексні операції безпеки та загальне управління ризиками особливо складним».

У гібридних і багатохмарних середовищах підприємствам, можливо, доведеться стежити за неправильними конфігураціями та проблемами ідентифікації, які дозволяють суб'єктам загрози переміщатися в різних хмарних середовищах, повідомляє Google Cloud.

У 2024 році багато суб’єктів загрози, включно з національними державами, можуть використовувати безсерверні послуги. Безсерверні послуги забезпечують їм більшу масштабованість, гнучкість і автоматизацію.

Google Cloud спостерігає зростання інтересу зловмисників до атак на ланцюги поставок, розміщених на таких менеджерах пакетів, як NPM (Node.js), PyPI (Python) і crates.io (Rust). Цей тип кібератак, ймовірно, збільшиться, оскільки його розгортання коштує мало, але може мати серйозний вплив.

Мобільна кіберзлочинність, ймовірно, зросте у 2024 році, оскільки шахраї використовують нові та перевірені тактики соціальної інженерії, щоб отримати доступ до телефонів цілей, йдеться у звіті.

Нарешті, Google Cloud передбачив, що SecOps стане все більш консолідованим у 2024 році. Цю дорожню карту можна використовувати, щоб керувати стратегіями кібербезпеки та здійснювати закупівлі, намагаючись випередити будь -які події, які можуть відбутися у 2024 році». ***(Megan Crouse. Google Cloud’s Cybersecurity Trends to Watch in 2024 Include Generative AI-Based Attacks // TechnologyAdvice (https://www.techrepublic.com/article/state-of-cybersecurity-2024/). 09.11.2023).***

***

**«Україна підписала декларацію Блетчлі — документ, у якому уряди різних країн домовились об’єднати зусилля щодо безпеки штучного інтелекту.**

Про це повідомили у прес-службі Міністерства цифрової трансформації.

Зокрема, співпраця країн буде зосереджена на виявленні ризиків штучного інтелекту й розробці політики безпеки, що ґрунтується на цих ризиках.

«З огляду на швидкі й невизначені темпи змін штучного інтелекту, а також контекст прискорення інвестицій у технології, ми стверджуємо, що поглиблення нашого розуміння цих потенційних ризиків і заходів щодо їхнього усунення є особливо актуальним», — ідеться в декларації.

Крім того, у документі зазначили особливі ризики ШІ в таких сферах як кібербезпека та біотехнології. Там також відзначили, що штучний інтелект створює загрозу «серйозної шкоди» у вигляді дезінформації.

Декларацію підписали під час міжнародного заходу з безпеки штучного інтелекту AI Safety Summit, який відбувся 1-2 листопада у Великій Британії. У ньому взяли участь представники урядів 29 країн…» ***(Аліна Квітко. Україна приєдналась до міжнародної декларації щодо безпеки використання штучного інтелекту // Онлайн-медіа «НикВести» (https://nikvesti.com/ua/news/business/278877). 03.11.2023).***

***

**«Британське агентство з кібербезпеки заявило у вівторок, що штучний інтелект становить загрозу для наступних національних виборів у країні, а кібератаки з боку ворожих країн та їхніх проксі поширюються, і їх стає все важче відстежувати.**

Національний центр кібербезпеки заявив, що «цього року спостерігалася поява державних акторів як нової кіберзагрози для критично важливої національної інфраструктури», такої як електромережі, водопостачання та інтернет-мережі.

Центр — частина британського агентства кібершпигунства GCHQ — зазначив у своєму щорічному огляді, що минулого року також спостерігалася «поява нового класу кіберсупротивників у формі державних акторів, які часто симпатизують подальшому вторгненню Росії». України та мають ідеологічну, а не фінансову мотивацію».

У ньому сказано, що держави та державні групи становлять «постійну та значну загрозу»: від російськомовних злочинців, які атакують британські фірми за допомогою програм-вимагачів, до «афілійованих державою Китаю кібератакторів», які використовують свої навички для досягнення «стратегічних цілей, які загрожують безпеці». і стабільність інтересів Великобританії».

Повторюючи попередження британських розвідувальних агентств MI5 і MI6, центр назвав зростання Китаю як технологічної наддержави «визначальним викликом для безпеки Великобританії».

«Ми ризикуємо Китаю стати домінуючою силою в кіберпросторі, якщо наші зусилля з підвищення стійкості та розвитку наших можливостей не встигнуть за темпом», — йдеться в повідомленні.

У звіті також наголошується на загрозі виборам, включаючи національні вибори у Великій Британії, які мають відбутися до січня 2025 року, технологія ШІ, що швидко розвивається.

У той час як старомодний британський метод голосування за допомогою олівця та паперу ускладнює хакерам зірвати саме голосування, у центрі заявили, що підроблені відео та «гіперреалістичні боти» полегшать поширення дезінформації під час кампанії». ***(UK cybersecurity center says 'deepfakes' and other AI tools pose a threat to the next election // Associated Press (https://apnews.com/article/uk-cyber-threats-ai-elections-b6482d3127ae524551e15887b3fdb01b). 14.11.2023).***

***

**«Штучний інтелект та кібербезпека окремо є двома темами, які заслуговують на увагу в новинах цього року, враховуючи швидку популяризацію генеративного штучного інтелекту, з одного боку, та зростання кількості кібератак і витоків даних, з іншого. Поодинці вони всюдисущі, але рідко можна побачити їх у групі.**

Спільний звіт Центру безпеки та нових технологій Джорджтаунського університету та Інституту Алана Тюрінга робить саме це, оцінюючи підвищений інтерес до застосування ШІ для посилення кіберзахисту.

*Що таке автономна кіберздатність?*

Автономний кіберзахист використовує штучний інтелект для захисту мережі та систем завдяки здатності виявляти зловмисну активність і реагувати зі швидкістю цифрових атак.

Автономний кіберзахист може включати захисні контрзаходи, засновані на ідентифікації та виявленні порушень, але він також може виходити за межі виявлення загроз і реалізувати такі кроки, як посилення системи та використання приманок для відповіді на атаку.

Що робить кіберзахист автономним, так це здатність штучного інтелекту приймати важливі рішення, не вимагаючи явного попереднього схвалення або дозволу людини. Як тільки потрібне схвалення людини («людина в циклі»), кіберзахист втрачає свою перевагу в швидкості над кібератаками. Дослідницька лабораторія військово-морських сил США описує зростаючу невідповідність між кібератаками та кіберзахистом так:

«Зловмисники можуть здійснювати динамічні, швидкі та масштабні кібератаки, тоді як кібератаки відповідають швидкості людини. У нинішніх системах кіберзахисту більшість процесів адаптації та відновлення систем є одноразовими, ручними та повільними. Не відставати від існуючих і нових загроз кібербезпеці є складним завданням, особливо якщо не покладатися на людський досвід системних адміністраторів і кібервоїнів».

Але, як ми зазначаємо нижче, усунення людського нагляду може спричинити юридичні ризики.

В Австралії є власне змодельоване навчальне середовище (так званий «тренажерний зал») для кібербезпеки під назвою CybORG, і в усьому світі його використовували в серії змагань із кіберзахисту та викликів, починаючи з 2021 року. У спільному звіті порівняння глобальних тренажерних залів виявляється, що австралійська CybORG гідна «Особлива увага», оскільки це відкритий вихідний код, його дизайн орієнтований на оборону (що важливо, як ми пояснюємо нижче), і він дозволяє відносно складне моделювання.

*Технічні проблеми автономного кіберзахисту*

У спільному звіті відверто визнається, що поточна технологія штучного інтелекту недостатньо зріла, і для роботи автономних агентів кіберзахисту необхідні подальше масштабування, тестування та навчання. Спільний звіт рекомендує тренувати цих агентів за допомогою навчання з підкріпленням (RL),

добре відомої парадигми машинного навчання, за допомогою якої винагорода керує бажаною поведінкою (використовується, наприклад, OpenAI для створення chatGPT).

Але в спільному звіті визнається наявність значних проблем.

Основним завданням є «вибір завдань і створення навчальних середовищ, які є досить складними, щоб бути корисними, і водночас достатньо малими з точки зору кількості дій і спостережень, щоб ними можна було керувати». У спільному звіті суть цього виклику описується наступним чином:

«Кожен настроюваний параметр на кожному комп'ютері, маршрутизаторі та пристрої — це потенційна дія. Крім того, кожен біт даних, що надходить у мережу або знаходиться на комп'ютері, є потенційно важливим для спостереження. Наприклад, десять комп'ютерів, кожен з яких має десять програмних засобів, кожен з яких має десять можливих налаштувань безпеки для налаштування, призводить до тисячі можливих дій… Кількість дій і спостережень зростає експоненціально і швидко стає некерованим».

У спільному звіті стверджується, що створення та навчання єдиної системи, ймовірно, буде неможливо. Замість цього пропонується підхід, який використовує низку окремих взаємодіючих агентів, навчених індивідуально для більш вузького набору завдань:

«Наприклад, один агент може розглядати комп'ютери лише як чорні ящики, які можна заразити або очистити, і він може виконати лише кілька дій, щоб ізолювати або виправити їх. Інший агент може працювати на цих комп'ютерах, спостерігаючи за всіма запущеними процесами та поведінкою користувачів. Він міг вирішити, чи зупинити деякі з цих процесів або заблокувати користувачів, і він міг би повідомити першому агенту, чи заражений комп'ютер чи ні».

По-друге, здатність запам'ятовувати характер і ознаки попередніх атак має вирішальне значення для ефективного кіберзахисту:

«З захисної точки зору виявлення сигнатур зловмисного програмного забезпечення або тактик зловмисників корисно, лише якщо їх можна запам'ятати. Здатний автономний агент кіберзахисту не може бути хворим на амнезію».

Однак агенти кіберзахисту, які розгортаються в мережах, які вони захищають, мають бути достатньо малими, щоб вони не виснажували обчислювальні ресурси цих мереж і пристроїв. Як наслідок, сучасний кіберзахист має порівняно обмежену здатність зберігати параметри.

У спільному звіті пропонується підхід, згідно з яким інформація зберігається за межами нейронної мережі та отримує доступ до неї агентів кіберзахисту, коли це необхідно. Це метод, прийнятий канадським тренажерним залом CyGil.

По-третє, за будь-якого підходу RL важливо ретельно та чітко визначати цілі, що часто вимагатиме визначення пріоритетів цілей, які суперечать одна одній. Це може бути особливим викликом при управлінні кібератаками через нескінченну різноманітність потенційних сценаріїв атак і складність для агента в оцінці ступеня серйозності кожного разу, вирішуючи, коли і як подолати обмеження втрати даних і максимізацію часу безвідмовної роботи.. Алгоритми також можуть бути дуже «буквальними» у своїх реакціях, якщо цілі визначені надто широко: наприклад, якщо метою агента є просто «не допустити зловмисне програмне забезпечення в усіх системах», він може досягти цієї мети, різко вимкнувши всі системи..

*Фактор Франкенштейна*

Багато сучасних кіберзалів призначені в першу чергу для створення наступальних агентів, оскільки вони потрібні для тестування та нарощування можливостей захисних агентів. Фактично, у спільному звіті сказано, що «[на даному етапі] незрозуміло, чи можливо взагалі створювати захисні агенти, не будуючи також їхніх наступальних аналогів».

Очевидно, що агресивні агенти можуть завдати значної шкоди, якщо їх витік або викрадення. Зловісно, але в спільному звіті зазначається, що наразі незрозуміло, хто переможе в змаганні між розумними автономними кібер-зловмисниками, які використовувалися для «породження» автономних кібер-захисників, і тими аналогами-захисниками.

У міру того, як розробляються складніші агенти нападу, спільний звіт підкреслює потребу в суворих захисних заходах, щоб запобігти їх викраденню або

розголошенню без дозволу, а також подальшому розгортанню або зворотній інженерії.

*Розпакування юридичного виклику*

Створення автономних агентів кіберзахисту створює низку політичних проблем на етапі створення, а також для довгострокового використання та управління після того, як агенти виведені на поле.

Однією з головних проблем є те, що агенти навчання з підкріпленням, які використовуються для навчання цих інструментів, потребують «детальних даних про те, як мережі, комп'ютери та пристрої налаштовуються, керуються та атакуються» для розробки реалістичних захистів. Обмін даними є серйозною політичною проблемою, оскільки більшість даних зберігається приватними компаніями, які вважають дані конфіденційним матеріалом (і, ймовірно, становлять ризик для безпеки в разі їх розголошення), зберігаючи їх у таємниці та захищаючи їх конфіденційність. Крім того, у сфері національної безпеки дані про загрози, інциденти, відповіді та слабкі місця є конфіденційними та контрольованими, а їх використання суворо обмежено щодо захисту даних.

У спільному документі пропонується, щоб розвинути цей простір, необхідно розробити нові правила або встановити нові норми, але очевидно, що існують проблеми, які необхідно подолати, оскільки обмін даними без відповідних гарантій може створити підвищені ризики для безпеки, навіть якщо це має намір зробити з точністю до навпаки.

Що відбувається, коли ці агенти не можуть виявити або запобігти атаці? Можливості невдач дуже різноманітні, і включають як надмірну реакцію на уявні загрози, так і неспроможність ідентифікувати або відповісти на атаки, до яких вони повинні бути готові. Агенти також можуть завдати шкоди, працюючи без авторизації за межами мереж, які вони захищають.

Для регульованих організацій існує очевидний ризик покладатися на автономний кіберзахист для виконання або допомоги у виконанні нормативних зобов'язань, таких як ті, що покладаються на певні фінансові установи відповідно

до пруденційних стандартів, таких як CPS 234, 231 і 230, виданих Австралійським пруденційним регуляторним органом.

Якщо клієнти, які закуповують цих агентів захисту, забезпечать надійні режими договірної відповідальності, це може сприяти певному захисту від більш чітких проблем розподілу ризиків. Однак шкоду, спричинену збоями в системі кібербезпеки, важко належним чином пом'якшити за допомогою договірних засобів, враховуючи не лише регулятивні штрафні санкції та претензії клієнтів, але й найсуттєвішу можливість завдати суттєвої шкоди репутації

Захоплення високого рівня: чи може ШІ забезпечити тактичну перевагу проти кібератак?

У міру того, як швидкість, частота та масштаб кібератак перевищують швидкість, частоту та масштаб, які люди можуть впоратися, кібербезпека все більше ставатиме «битвою машин».

У спільному звіті зазначається, що, хоча було проведено багато лабораторних тестів і змагань, автори не знають про автономну систему кіберзахисту, яка ще розгортається в реальному світі. Однак, хоча немає гарантії, що автономний кіберзахист буде успішним, у спільному звіті стверджується, що автономний простір кіберзахисту, здається, знаходиться на етапі, коли потрібна підтримка, і що він є достатньо перспективним, щоб бути гідним цієї підтримки.

Але в спільному звіті є останнє застереження для апарату національної безпеки, який був озброєний значними, якщо не надзвичайними, повноваженнями нагляду, контролю та управління IT-системами та ланцюгами постачання технологій. Спільна доповідь попереджає політиків «уникати втручання в обмін знаннями чи даними таким чином, що може призвести до стагнації прогресу чи задушення нової галузі, водночас захищаючи національні інтереси, перешкоджаючи просуванню ворожих організацій і зберігаючи переваги національної безпеки». Це, безсумнівно, важко досягти балансування, але потенційно принесе великі переваги, якщо вдасться». ***(Stephanie Essey. AI to the rescue: can it stem the tide of cyber-attacks? // Gilbert + Tobin***

***(https://www.gtlaw.com.au/knowledge/ai-rescue-can-it-stem-tide-cyber-attacks). 20.11.2023).***

***

## Кіберзлочинність та кібертероризм

**«Галузь кібербезпеки переживає шокуючу новину про те, що SEC висунула звинувачення SolarWinds та її колишнього керівника CISO у шахрайстві, пов'язаному з горезвісною атакою SUNBURST.**

У 68-сторінковій скарзі, поданій 30 жовтня, стверджується, що принаймні з жовтня 2018 року до 12 січня 2021 року компанія SolarWinds і її тодішній керівник служби безпеки Тімоті Г. Браун обманювали інвесторів і клієнтів шляхом «викривлень, упущень і схем, які приховували як погані практики кібербезпеки компанії та її підвищені — і зростаючі — ризики кібербезпеки».

SUNBURST — синонімом якого тепер є назва SolarWinds — була однією з найзначніших кібератак в історії, оскільки вона проникла в ланцюжок постачання програмного забезпечення та завдала хаосу підприємствам будь-якого розміру по всьому світу. Уряд США навіть постраждав, що спонукало до суворіших інструкцій і вимог щодо захисту федерального ланцюга постачання програмного забезпечення.

Повні наслідки атаки поки що невідомі та, ймовірно, будуть відчутні в осяжному майбутньому.

Звинувачення в шахрайстві висунуті в той момент, коли SEC посилює підзвітність у сфері кібербезпеки — особливо це стосується нової чотириденної вимоги щодо розкриття інформації для публічних компаній — і це може мати драматичні наслідки далеко за межами сфери кібербезпеки.

«Ці звинувачення служать нагадуванням для CISO про важливість етичної та професійної поведінки», — сказав Джордж Герчоу, викладач дослідницької та консультативної фірми з кібербезпеки IANS Research. «Для CISO вкрай важливо

підтримувати високий рівень чесності, дотримуватись етичних стандартів і надавати пріоритет безпеці та конфіденційності даних своєї організації».

*Внутрішній документ каже, що компанія «не дуже безпечна»*

SolarWinds, що базується в Оклахомі, пропонує інструменти керування мережевими та інфраструктурними системами для сотень тисяч організацій у всьому світі.

Імовірно, ще у 2018 році хакери отримали доступ до мережі компанії та розгорнули шкідливий код у системі моніторингу IT Orion. За даними SEC, Orion вважається «коронним» активом, на частку якого у 2020 році припадало 45% доходу компанії.

Агентство стверджує, що під час наступної дворічної атаки SolarWinds і Браун зробили «суттєво неправдиві та оманливі заяви та упущення» щодо ризиків і практик кібербезпеки в кількох публічних розкриттях, включаючи «заяву про безпеку» на своєму веб-сайті та звітах, поданих до SEC.

Наприклад, у жовтні 2018 року — у тому самому місяці, коли SolarWinds провело первинне публічне розміщення акцій (IPO), Браун написав у внутрішній презентації, що «поточний стан безпеки SolarWinds робить нас дуже вразливими для наших критично важливих активів».

В інших презентаціях того періоду налаштування віддаленого доступу SolarWinds називали «не дуже безпечними» і що експлуататор міг «загалом робити все, що завгодно, не виявляючи цього, поки не стане надто пізно», що може призвести до «великої репутації та фінансових втрат».

Крім того, у внутрішньому документі від вересня 2020 року, наданому Брауну та іншим, зазначено, що «кількість проблем із безпекою, виявлених за останній місяць, перевищила здатність команд інженерів вирішити».

«Публічні заяви SolarWinds про її методи кібербезпеки та ризики намалювали картину, яка кардинально відрізняється від внутрішніх дискусій та оцінок», — йдеться у скарзі.

SEC також повідомляє, що компанія неповно розкрила інформацію про атаку у формі 8-K від 14 грудня 2020 року, після чого ціна її акцій впала приблизно на 25% протягом наступних двох днів і на 35% до кінця місяця.

З тих пір компанія намагалася відновити свою репутацію, а лідери нещодавно працювали над ребрендингом і висунули ідею повернутися до приватної моделі.

У дописі в блозі генеральний директор Судхакар Рамакрішна сказав, що SolarWinds «рішуче виступає проти» дій SEC.

«Те, як ми відреагували на SUNBURST, — це саме те, що уряд США прагне заохотити», — сказав він.

Отже, «тривожно» те, що SEC подала заяву про те, що, на думку компанії, є «помилковим і неналежним правозастосуванням», яке представляє «регресивний набір поглядів і дій, несумісних із прогресом, якого має досягти галузь і який заохочує уряд».

*SUNBURST лише підкреслив гострі проблеми безпеки*

Експерти наголошують, що SEC не націлена на SolarWinds через SUNBURST: у скарзі йдеться, що неправдиві заяви про безпеку порушували б законодавство про цінні папери, навіть якби SolarWinds не було зламано.

«Те, що вони були ціллю, лише підкреслило проблеми», — сказав Вільямс.

Майкл Ісбіцкі, директор із стратегії кібербезпеки в Sysdig, вказав на численні прогалини в безпеці: віддалений доступ для некерованих пристроїв, помилки моделювання загроз, неадекватне тестування веб-додатків, неналежні політики керування паролями та слабкі засоби контролю доступу.

Незважаючи на те, що SolarWinds засвідчила дотримання загальних найкращих практик безпеки, таких як NIST Cybersecurity Framework, NIST Security and Privacy Controls for Information Systems and Organizations і Secure Development Lifecycle (SDL), докази, здається, показують, що вони мали значні прогалини у відповідності всім критеріям для всіх програм. і системи, сказав Ісбіцкі. Це створило суттєві проблеми, які не були розкриті належним чином, і ввело інвесторів в оману.

«Ключовий висновок тут — вибрати стандарт і переконатися, що ви дотримуєтеся його повсюдно», — сказав він.

*Тривалі наслідки SUNBURST*

Це не означає, що SUNBURST кардинально не змінив індустрію кібербезпеки.

«Атака SUNBURST змінила нашу галузь багатьма способами, — сказав Герхов.

Зокрема, це привернуло увагу до важливості безпеки ланцюга постачання. «Організації тепер краще усвідомлюють потенційні ризики, пов'язані зі стороннім програмним забезпеченням, і вживають заходів для підвищення рівня безпеки», — сказав він.

Атака також підкреслила необхідність постійного моніторингу та виявлення загроз, що спонукало організації інвестувати в передові інструменти та технології. Нарешті, і, мабуть, найбільш помітно, це привернуло увагу регуляторів.

«Це може призвести до більш суворих вимог до організацій щодо забезпечення безпеки своїх ланцюгів постачання», — сказав Герхов.

*SEC встановлює новий стандарт*

Цей випадок підкреслює критичність чесності щодо стану та зрілості програм кібербезпеки, особливо для публічних компаній, відзначають експерти.

Відповідна експертиза, процеси кібербезпеки та історія інцидентів безпеки повинні бути розкриті згідно з правилами розкриття інформації про кібербезпеку SEC, сказав Ісбіцкі. Вони існували в різних формах більше десяти років, а остання версія набула повної чинності в грудні 2023 року.

Крім того, бути відкритим і чесним – це просто хороша практика ведення бізнесу. «Прозорість має вирішальне значення для збереження довіри клієнтів, партнерів і зацікавлених сторін», — сказав Герхов.

Коли відбувається порушення, важливо повідомити тих, хто може постраждати, щоб вони могли вжити необхідних запобіжних заходів і захистити себе, підкреслив він. Відкрито кажучи про порушення, компанії демонструють відданість безпеці своїх клієнтів і демонструють відповідальність.

Колега Герчоу Джейк Вільямс, колишній хакер Агентства національної безпеки США (NSA) і співробітник дослідницького факультету IANC, прокоментував, що «цим позовом SEC встановлює новий стандарт для розкриття інформації про безпеку».

Він попередив: «Не дивуйтеся, побачивши, що цей стандарт використовується в судовому процесі, якщо ви робите неправдиві, неповні або оманливі заяви про безпеку для клієнтів або ділових партнерів».

Крім того, повідомлення Wells — наміри стягнути плату — зазвичай видаються генеральним і фінансовим директорам, сказав Сіван Техіла, генеральний директор платформи кібербезпеки Onyxia. Але в цьому випадку явно включено CISO Brown.

«Це може означати нові зобов'язання для керівників відділів кібербезпеки», — сказав Техіла.

*Слідкуйте за корпусом SolarWinds, поки він розгортається*

Експерти з кібербезпеки радять CISO уважно стежити за цією справою.

Для початку він служить нагадуванням про потенційні правові та нормативні наслідки, які можуть виникнути внаслідок інцидентів кібербезпеки, сказав Герхов. Розуміння цих звинувачень і остаточного результату справи може допомогти керівникам служби безпеки оцінити потенційні ризики, з якими вони можуть зіткнутися в подібних ситуаціях, і вжити профілактичних заходів.

«KICO повинні проаналізувати конкретні звинувачення, висунуті SEC, і оцінити, чи має їхня власна організація подібні вразливості або недоліки», — сказав Герхов. «Це може допомогти їм визначити сфери для вдосконалення та зміцнити свою позицію в галузі кібербезпеки».

Він порадив CISO вивчити дії SolarWinds щодо реагування на інциденти, щоб оцінити їхню ефективність. Вивчення цього як прикладу використання може допомогти їм покращити власні плани реагування на інциденти, включаючи стратегії зв'язку, заходи стримування та процеси відновлення. Не менш важливо, щоб керівники служби безпеки зміцнювали етичну поведінку в своїх організаціях.

Ісбіцкі погодився, сказавши, що компанії та їхнє керівництво повинні слідкувати за позовом, оскільки він розгортається, «оскільки це одне з перших бойових випробувань остаточних правил кібербезпеки». ***(Taryn Plumb. Cybersecurity industry responds to SEC charges against SolarWinds and former CISO // VentureBea (https://venturebeat.com/security/cybersecurity-industry-responds-to-sec-charges-against-solarwinds-and-former-ciso/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 01.11.2023).***

***

**«Британська бібліотека в Лондоні … постраждала від того, що вона називає «кіберінцидентом». Відтоді його веб-сайт не працює, і вчені не можуть отримати доступ до його онлайн-каталогу.** У бібліотеці також перестав працювати Wi-Fi, а співробітникам не дозволяли вмикати комп'ютери. Його сувенірний магазин відкритий для бізнесу, але лише для тих, хто має готівку, щоб купити дрібнички, такі як олівці від Британської бібліотеки.

Користувачі бібліотек, багато з яких включають письменників зі стислими дедлайнами, починають страждати.

В інтерв'ю цього тижня семеро постійних користувачів бібліотеки — включно з автором майбутньої книги про класичну музику, викладачем Кембриджського університету, двома аспірантами та шекспірознавцем — сказали, що бібліотека фактично повернулася до доцифрової епохи.

Зараз, за словами співробітника бібліотечного читального залу «рідкісних книг і музики», замовлення книги передбачає пошук її каталожного номера в одній із кількох сотень книг у твердій палітурці або на зовнішньому веб-сайті, запис цього номера на аркуші паперу, а потім передаючи її бібліотекарю, який, у свою чергу, перевіряв їхні записи, щоб побачити, чи доступна книга. Книги доступні, лише якщо вони зберігаються в головній бібліотеці.

Будь-який інцидент у Британській бібліотеці, як правило, стає резонансною новиною у Британії. Його колекція включає такі артефакти, як дві копії Великої

хартії вольностей, одна з особистих Біблій короля Генріха VIII, п’ять копій Першого фоліо Шекспіра та деякі рукописні тексти пісень Бітлз.

Проте Британська бібліотека опублікувала лише короткі коментарі щодо епізоду на X, соціальній медіа-платформі, раніше відомій як Twitter. У вівторок він опублікував заяву, в якій говориться, що бібліотека «переживає серйозний технологічний збій в результаті кіберінциденту. Це впливає на наш веб-сайт, онлайн-системи та сервіси, а також деякі локальні сервіси, включаючи публічний Wi-Fi».

У заяві додається, що співробітники бібліотеки розслідують інцидент разом з Британським національним центром кібербезпеки.

У п’ятницю речниця бібліотеки повідомила в електронному листі, що не може надати подальших коментарів. Вона не відповіла на запитання, чи справді стався напад.

29-річна Джессіка Боялл, яка була в бібліотеці в четвер, щоб дослідити докторське дослідження, сказала, що вона міркувала з іншими користувачами про те, що могло спричинити закриття. «Нічого подібного тут ніколи не відбувається», — сказала вона, додавши. «У всіх ходять чутки».

Тим часом вона змінила план роботи на тиждень. «Я намагаюся робити ті моменти, для яких не потрібні книжки», — сказала вона.

Незважаючи на дефіцит інформації, інші бібліотеки в Європі припускали, що Британська бібліотека стала жертвою навмисного нападу. Речниця Національної бібліотеки Шотландії заявила в електронному листі, що «після нападу на Британську бібліотеку» вона посилила «постійний моніторинг і захист наших послуг і колекцій».

Це не перший раз, коли бібліотека стикається з кіберінцидентом. Цього року кіберзлочинці націлилися на Національну бібліотеку Німеччини, хоча її генеральний директор Франк Шольце заявив у п’ятницю в телефонному інтерв’ю, що його співробітники змогли «відбити це».

«Раніше бібліотеки насправді не були цілями — ми трохи поза увагою», — сказав Шольце. «Але це, здається, змінюється».

Тасміна Іслам, викладач освіти з кібербезпеки в Королівському коледжі Лондона, сказала в електронному листі, що мотивація атаки на бібліотеку може бути фінансовою.

«Кіберзлочинці можуть отримати доступ до великої кількості інформації з бібліотеки, включаючи особисті дані користувачів», — сказала вона. Бібліотеки також «зберігають електронні книги, дослідницькі статті та різну інтелектуальну власність, яку кіберзлочинці можуть використовувати для незаконного розповсюдження», додав Іслам.

За її словами, інцидент у Британській бібліотеці «послужив попередженням для інших бібліотек і установ щодо ретельної оцінки власних заходів безпеки».

Цього тижня в бібліотеці один із співробітників описав подію як «кошмар» і сказав, що працівники були збентежені тим, що сталося і чому…». ***(Alex Marshall. An Apparent Cyberattack Hushes the British Library // The New York Times Company (https://www.nytimes.com/2023/11/03/arts/british-library-cyber-attack.html?utm_source=flipboard&utm_content=user%2Fnewyorktimes). 03.11.2023)***.

***

**«За даними Statista, збитки, завдані кіберзлочинністю цього року, становитимуть 11,5 трильйонів доларів, але до 2027 року хмарна міграція та поширення підключених пристроїв можуть збільшити цю цифру до 23 трильйонів доларів.** Не дивно, що підприємства подвоюють свої зусилля щодо захисту конфіденційних даних.

Згідно з опитуванням Morgan Stanley, у третьому кварталі витрати на програмне забезпечення для кібербезпеки зросли найбільше з усіх категорій IT-продуктів. Це особливо цікаво, оскільки штучний інтелект домінував у заголовках газет цього року, але насправді компанії більше зосереджені на покращенні своєї безпеки.

Інвестори можуть скористатися цією можливістю, створивши кошик акцій кібербезпеки у своїх портфелях. Ось чому CrowdStrike Holdings (CRWD 2,98%) і Zscaler (ZS 3,25%) належать до цього кошика.

1. CrowdStrike Holdings

CrowdStrike є визнаним лідером на багатьох кінцевих ринках кібербезпеки, включаючи безпеку кінцевих точок (пристроїв), безпеку в хмарі та кероване виявлення та реагування. Його платформа об'єднує більше двох десятків програмних модулів, які стосуються кількох категорій кібербезпеки. Ця широта особливо важлива, оскільки більшість підприємств покладаються на десятки точкових продуктів, що робить безпеку більш обтяжливою. Але CrowdStrike може зменшити цей операційний тягар, дозволяючи підприємствам стандартизуватись на одній платформі.

Консолідація продуктів є привабливим пунктом продажу, але не менш важливими є власні дані, які CrowdStrike зібрав як лідер у сфері кібербезпеки. Цитуючи Forrester Research, «розширений погляд CrowdStrike на ландшафт загроз і служби реагування на інциденти дає йому перевагу, коли йдеться про аналіз загроз». Це натякає на чудовий штучний інтелект (ШІ) — дані є основою машинного навчання, а наслідком цієї переваги даних є безпрецедентний захист від загроз.

CrowdStrike повідомила про солідні фінансові результати у другому кварталі. Продажі підскочили на 37% до 732 мільйонів доларів, а чистий прибуток за стандартами бухгалтерського обліку більш ніж подвоївся до 180 мільйонів доларів. Але компанія навряд чи охопила свій адресний ринок у 76 мільярдів доларів, і генеральний директор Джордж Курц звучав оптимістично під час звіту про прибутки: «У нас є технології, інновації, команда, яка керується місією, і значний масштаб, щоб очолити консолідацію платформи кібербезпеки».

Аналітики Уолл-стріт також загалом оптимістично налаштовані. CrowdStrike має консенсус-рейтинг «купити» та середню 12-місячну цільову ціну в 198 доларів США за акцію, що означає 15% зростання від поточної ціни. Morgan Stanley також вважає CrowdStrike одним із постачальників програмного забезпечення, який має

найкращі позиції для монетизації генеративного штучного інтелекту, маючи на увазі нещодавно оголошений інтерфейс природної мови Charlotte AI, а Морнінгстар очікує, що дохід компанії зростатиме на 31% щорічно протягом наступних п’яти років.

У цьому контексті його поточна оцінка в 15,5 разів перевищує обсяг продажів виглядає розумною. Тож інвестори повинні відчувати себе комфортно, додаючи невелику позицію в CrowdStrike до свого кошика акцій кібербезпеки сьогодні.

2. Zscaler

Zscaler спеціалізується на доступі до мережі без довіри (ZTNA) і захисті робочого навантаження в хмарі. Платформа Security Service edge (SSE) модернізує корпоративні мережі, керуючи застосуванням політики та виявленням загроз у хмарі, а не в приватних центрах обробки даних. Ця стратегія усуває потребу у дорогих локальних засобах безпеки, а також забезпечує клієнтам набагато кращий захист.

Якщо говорити детальніше, то Zscaler керує найбільшою хмарою мережевої безпеки у світі. За словами керівництва, цей масштаб є основою потужного мережевого ефекту, який, зрештою, забезпечує чудовий захист від загроз. Платформа Zscaler щодня обробляє сотні мільярдів запитів, збираючи в процесі сотні трильйонів сигналів безпеки, і кожен сигнал покращує механізм ШІ у виявленні кібератак.

Zscaler є визнаним лідером серед платформ ZTNA та SSE, і обидва ринки мають швидко розвиватися, оскільки компанії вкладають більше грошей у хмарну міграцію та інші проекти цифрової трансформації. Дійсно, консалтингова компанія Gartner оцінює, що до 2025 року 80% підприємств впровадять платформи SSE для уніфікації безпеки в приватних програмах, публічних хмарних службах і відкритому Інтернеті, порівняно з 20% у 2021 році.

Zscaler повідомив про обнадійливі результати в останньому кварталі. Його кількість клієнтів зросла на 14% до 7700, а середній клієнт витрачав на 20% більше. У свою чергу, дохід зріс на 43% до 455 мільйонів доларів, а чистий прибуток за стандартами бухгалтерського обліку зріс на 177% до 101 мільйона доларів. Але

керівництво дивиться в майбутнє з оптимізмом, посилаючись на доступний ринок у 72 мільярди доларів США та лідерські позиції на ринку.

Уолл-стріт також загалом оптимізує. Zscaler має консенсус-курс «покупки» та середню 12-місячну цільову ціну в 185 доларів США за акцію, що передбачає 20% зростання від поточної ціни. Morgan Stanley очікує, що дохід Zscaler зростатиме на 25% щорічно протягом наступних п’яти років. У цьому контексті її поточна оцінка в 13,8 разів перевищує продажі, і поточний мультиплікатор, безумовно, є більш привабливим, ніж трирічне середнє значення в 32,3 рази на продажі. Довгострокові інвестори повинні додати невелику позицію в цьому зростаючому запасі до свого кошика кібербезпеки сьогодні…» ***(Trevor Jennewine. Cybercrime Costs Are Soaring Toward $20 Trillion: 2 Magnificent Growth Stocks to Buy Now and Hold Forever // The Motley Fool (https://www.fool.com/investing/2023/11/04/cybercrime-costs-soaring-2-growth-stocks-to-buy/?utm_source=flipboard&utm_content=alannishihara%2Fmagazine%2FTHE+FLIPBOARD+MAGAZINE+OF+ALAN+NISHIHARA). 04.11.2023).***

***

**«Підпільна мережа кіберзлочинців SWAT USA Drop Service, розташована в Росії, наразі налічує понад 1200 американських співробітників, багато з яких випадково залучені до пересилання розкішних споживчих товарів, куплених за допомогою вкрадених кредитних карток.**

Ця служба вилучення — це потужна мережа кіберзлочинців, відома відмиванням незаконно отриманих товарів. Нещодавно його зламали, розкривши великі подробиці про його внутрішню роботу, фінанси та організаційну ієрархію. Ця масова підпільна операція розслідувалася протягом тривалого часу, але нещодавнє порушення надало правоохоронним органам золоту жилу інформації для потенційного знищення мережі. Мимовільні учасники, яких часто набирають за допомогою стриманих оголошень про роботу, зараз ризикують отримати

потенційні юридичні наслідки, що викликає занепокоєння щодо етичних наслідків найму осіб без їхнього знання про незаконний характер їхньої роботи.

*Поява схем скидання речей і пересилання з експлуатацією невинних осіб*

Коли онлайн-продавці почали відмовляти в доставці в місця, відомі шахрайством з кредитними картками, виникли підпільні схеми повторного відправлення, залучаючи людей у США та Європі для прийому та пересилання вкрадених речей у зони обмеженого доступу. Такі служби, як фейковий SWAT, у колах кіберзлочинців називають «Drops for stuff». Ці незаконні послуги вербують осіб, часто несвідомо, для того, щоб діяти як «підсадники», які отримують вкрадені товари та згодом надсилають їх шахраям у обмежені місця. Анонімність, яку забезпечують мережі пересилання, дозволяє кіберзлочинцям обійти традиційні заходи боротьби з шахрайством і продовжувати використовувати інформацію про викрадену кредитну картку.

Люди, які виступають у ролі «дропів», зазвичай знаходять роботу вдома з пересилання пакетів на таких веб-сайтах, як Craigslist та інших платформах пошуку роботи. Шахраї обіцяють щомісячну заробітну плату та премії, але зв’язок зазвичай припиняється до настання першої зарплати. Потім ці нічого не підозрюють особи стають несвідомими партнерами в злочинних діях, пов’язаних з переміщенням крадених товарів. Нічого не підозрюють «краплі» можуть зіткнутися з юридичними наслідками, і вони залишаться без обіцяної зарплати, що ставить їх у скрутне фінансове становище.

Значна частина фальшивого доходу SWAT надходить від отримання до 50% прибутку від «наповнювачів», злочинців, які використовують викрадені кредитні картки, щоб купувати дорогоцінні речі та відправляти їх до місця «здачі». Ці «розбивачі» можуть отримати товари, не будучи безпосередньо пов’язаними зі злочином, що ускладнює органам влади пошук викрадених товарів. Крім того, їхня співпраця з командою SWAT дозволяє створювати розгалужену мережу, що призводить до отримання значних прибутків, необхідних для кримінальних операцій обох сторін.

*Як SWAT адаптується та розвивається, щоб залишатися в бізнесі*

Після отримання дропу та пересилання посилки наповнювач може продати товар на місцевому чорному ринку. Phony SWAT працював майже десять років під різними іменами та керівними конфігураціями. Протягом багатьох років організації вдалося адаптуватися та еволюціонувати у відповідь на репресії з боку правоохоронних органів, через що її демонтаж стає дедалі складнішим.

З розвитком технологій як фейковий SWAT, так і інші подібні операції використовували нові методи для оптимізації своїх операцій і залишалися поза увагою, створюючи серйозну проблему для влади». ***(Deanna Ritchie. Unraveling cybercrime network's underground operations // ReadWrite, INC (https://readwrite.com/unraveling-cybercrime-networks-underground-operations/?utm_source=flipboard&utm_content=ReadWrite%2Fmagazine%2FAll+Stories). 03.11.2023).***

***

**«В епоху цифрового зв'язку кіберзагрози стають масштабними, перетинаючи кордони з нерівномірним впливом.** Це дослідження заглиблюється в кіберзагрози, розкриваючи їхні різноманітні наслідки для окремих осіб, компаній та установ, а також підкреслюючи глибокі суспільні наслідки в нашому взаємопов'язаному світі. Ласкаво просимо до «Кіберзагрози: вплив і наслідки.

*Типи кіберзагроз*

Зловмисне програмне забезпечення, скорочення від шкідливого програмного забезпечення, — це широка категорія, що охоплює віруси, хробаки, трояни та шпигунське програмне забезпечення. Це як цифровий хамелеон, який пристосовується до навколишнього середовища. Зловмисне програмне забезпечення часто націлюється на людей через оманливі завантаження, вкладення електронної пошти або скомпрометовані веб-сайти. Для компаній він може проникати в мережі через фішингові електронні листи, створюючи значний ризик для конфіденційних даних.

Фішинг - це мистецтво обману. Кіберзлочинці видають себе за довірених осіб за допомогою електронних листів, повідомлень або веб-сайтів, спонукаючи користувачів розкрити конфіденційну інформацію, як-от паролі чи дані кредитної картки. Окремі особи є головними цілями, але кіберзлочинці також націлюються на співробітників організацій, щоб отримати доступ до корпоративних мереж.

Програмне забезпечення-вимагач блокує користувачам їхні власні дані, доки не буде сплачено викуп. Окремі особи можуть виявитися заблокованими для доступу до особистих файлів, у той час як компанії часто стикаються з далекосяжними перебоями в роботі. Кіберзлочинці полюють на бізнес, знаючи, що вони можуть вимагати більш значні викупи за критично важливі системи та конфіденційні дані.

Не всі загрози надходять ззовні. Інсайдерські загрози стосуються окремих осіб в організації, які зловживають своїми правами доступу. Це може варіюватися від випадкового витоку даних до навмисного саботажу. Незважаючи на те, що внутрішні загрози в першу чергу викликають занепокоєння для компаній, вони також можуть впливати на державні установи та навчальні заклади.

DDoS-атаки заповнюють цільовий сервер або мережу величезним обсягом трафіку, що призводить до збою служб. Як правило, ці атаки спрямовані на зрив бізнес-операцій, унеможливлення доступу до веб-сайтів і часто мають фінансову мотивацію. Мішенями часто стають як підприємства, так і державні установи.

Експлойти Zero-day спрямовані на невиправлені вразливості в програмному забезпеченні, апаратному забезпеченні або програмах. Ці загрози дуже затребувані кіберзлочинцями та спонсорованими державою хакерами. Вони можуть зосереджуватися на будь-кому, хто використовує вразливі системи, від окремих осіб до великих корпорацій і державних установ.

*Хто найбільше постраждав від кіберзагроз?*

Люди опиняються на передовій, коли йдеться про кіберзагрози, стикаючись із такими небезпеками, як фішингові електронні листи, зловмисне програмне забезпечення та крадіжка особистих даних, що є частиною їхнього щоденного цифрового існування. Тривожна статистика підкреслює масштаби проблеми: лише

за першу половину 2022 року було зафіксовано приголомшливі 236,1 мільйона атак програм-вимагачів у всьому світі. Наслідки цих атак проявляються як фінансові втрати, порушення конфіденційності та кошмарний досвід крадіжки особистих даних.

Малі та середні підприємства (SMBs), часто джерело життя багатьох економік, є привабливими цілями через їх цінні активи даних і часто обмежені ресурси кібербезпеки. Дослідження показують, що 43% усіх кібератак спрямовані на малий бізнес. Наслідки для цих підприємств можуть бути жахливими: від фінансових труднощів до репутаційної шкоди, яку важко виправити.

Великі корпорації, враховуючи їх експансивну цифрову присутність, борються з кіберзагрозами в промислових масштабах. Не дивно, що ці корпоративні гіганти вкладають значні кошти в заходи кібербезпеки. Однак у 2020 році витік даних навіть для цих гігантів становив у середньому 3,86 мільйона доларів США за інцидент. Великі корпорації повинні захистити себе не лише від фінансових втрат, але й від потенційної довгострокової шкоди своєму бренду та ерозії довіри клієнтів.

Державні органи несуть відповідальність за захист критично важливих даних, у тому числі конфіденційної інформації громадян і секретів національної безпеки. Кіберзагрози, націлені на ці організації, становлять значний ризик. Відповідно до висновків фірми з кібербезпеки Emsisoft, у 2019 році в Сполучених Штатах спостерігався надзвичайний і невпинний сплеск атак програм-вимагачів, які торкнулися не менше ніж 966 державних установ, навчальних закладів і постачальників медичних послуг. Потенційні витрати, спричинені цими атаками, перевищують приголомшливі 7,5 мільярда доларів. Наслідки поширюються глибоко, охоплюючи проблеми національної безпеки та спектр витоків даних із далекосяжними наслідками.

*Вразливі місця та виклики*

Люди: залежність від технологій наражає багатьох на ризик. Необізнаність, слабкі паролі та ризиковані кліки роблять їх основними цілями. Соціальна інженерія використовує довіру, ризикуючи особистою інформацією та фінансами.

Малий і середній бізнес (SMBs): Обмежені ресурси перешкоджають надійній безпеці. Обмежений бюджет, неадекватна підготовка та сприйняття менш привабливих цілей роблять їх уразливими. Обробка конфіденційних даних збільшує ризик.

Корпорації: величезні цифрові екосистеми несуть унікальні загрози. Атаки на ланцюг постачання, шпигунство та внутрішні ризики викликають постійне занепокоєння. Керування великою кількістю даних вимагає суворих заходів.

Уряди: обробка масивних конфіденційних даних робить їх основними кібер-мішенями. Складні системи та проблеми з прозорістю перешкоджають міцному захисту.

*У сфері кібербезпеки:*

Індивідуальні особи: важко розповісти про загрози та передову практику. Ненадійні паролі, нехтування оновленнями та стають жертвами фішингу. Баланс між зручністю та безпекою є важкою задачею.

Малий і середній бізнес: обмежені ресурси створюють проблеми. Ключовим є пошук доступних, але ефективних рішень. Недооцінка загроз може призвести до самовдоволення.

Корпорації: захист величезних мереж, різноманітних кінцевих точок і хмари є складною справою. Щоб не відставати від загроз, що розвиваються, потрібні значні інвестиції.

Уряди: уряди повинні вирішити подвійну проблему захисту національних інтересів і поваги до приватного життя громадян. Встановлення правильного балансу між ефективними методами кібербезпеки та прозорістю є постійним викликом. Крім того, державні установи часто стикаються з бюджетними обмеженнями та бюрократичними перепонами під час впровадження заходів безпеки.

*Наслідки кіберзагроз*

Кібернетичні загрози, часто недооцінені, мають глибокі наслідки по всьому спектру. Давайте зануримося в наслідки, які вони завдають фізичним особам,

малим і середнім підприємствам (SMB), корпораціям і навіть державним установам.

*Вплив на окремих осіб*

Фінансові втрати: кібератаки можуть призвести до значних фінансових втрат для окремих осіб. Атаки програм-вимагачів можуть блокувати особисті дані, доки не буде сплачено чималий викуп, залишаючи жертв у фінансовій кризі.

Порушення конфіденційності: особиста інформація, якщо її зламано, може призвести до непоправної шкоди. Порушення конфіденційності може розкрити інтимні подробиці, спричинивши глибоке емоційне страждання.

Крадіжка особистих даних: кошмар крадіжки особистих даних є суворою реальністю цифрової епохи. Викрадені дані можуть бути зловживані в різних злочинних діях, залишаючи людей з розбитими життями.

*Вплив на малий і середній бізнес*

Економічні наслідки: малий і середній бізнес, джерело життя багатьох економік, може розвалитися під вагою кібератак. Вартість відновлення в поєднанні з потенційними втратами доходу може завдати шкоди.

Пошкодження репутації: втрачену довіру важко відновити. Малому та середньому бізнесу може бути важко відновити свою репутацію після порушення безпеки, що призведе до втрати клієнтів.

Втрата даних. Серцем багатьох малих і середніх підприємств є їхні дані. Втрата важливих даних не тільки порушує роботу, але й ставить під загрозу життєздатність бізнесу.

*Вплив на корпорації*

Фінансові збитки: для корпорацій фінансові збитки можуть досягати мільйонів або навіть мільярдів доларів. Кібератаки можуть порушити роботу, призвести до юридичних санкцій і призвести до різкого падіння цін на акції.

Репутаційна шкода: корпорації сильно покладаються на свій імідж. Порушення даних може заплямувати їхню репутацію, підірвати довіру клієнтів і акціонерів.

Юридичні наслідки: правові наслідки кіберзагроз можуть бути складними та дорогими. Недотримання правил захисту даних може призвести до суворих покарань.

*Вплив на державні органи*

Занепокоєння національною безпекою: державні установи зберігають конфіденційну інформацію, яка є важливою для національної безпеки. Порушення можуть мати серйозні наслідки, включаючи шпигунство та компрометацію військових чи розвідувальних даних.

Витоки даних із далекосяжними наслідками. Витоки державних даних можуть мати далекосяжні наслідки, впливаючи не лише на національну безпеку, але й на життя громадян, чиї дані розкрито.

*Пом'якшення та запобігання*

Люди можуть посилити свій кіберзахист за допомогою:

Зміцнення паролів: використовуйте складні, єдині у своєму роді паролі для облікових записів в Інтернеті.

Багатофакторна автентифікація (MFA): активуйте MFA, коли це можливо, для додаткового рівня безпеки.

Будьте в курсі: переконайтеся, що пристрої та програмне забезпечення залишаються актуальними для виправлення вразливостей.

Будьте пильними: будьте обережні щодо фішингових електронних листів і підозрілих посилань.

Захист даних: регулярно створюйте резервні копії важливих даних, щоб запобігти втраті під час потенційних атак.

Малий і середній бізнес може захистити себе:

Брандмауер і антивірусний захист: розгортайте надійні брандмауери та антивірусні рішення.

Навчання співробітників: навчіть персонал виявляти потенційні загрози та реагувати на них.

Контроль доступу: обмежте доступ до конфіденційних даних на основі ролей.

Шифрування даних: Шифруйте дані під час передачі та зберігання.

План реагування на інциденти: розробіть комплексну стратегію для вирішення кіберінцидентів.

Корпорації можуть захистити свою діяльність за допомогою:

Комплексні політики безпеки: створіть і суворо дотримуйтесь політики кібербезпеки.

Постійне інформування співробітників: інформуйте співробітників про найкращі практики кібербезпеки.

Регулярні перевірки безпеки: проводите часті перевірки та оцінки безпеки.

Інвестуйте в аналіз загроз: розподіляйте ресурси, щоб випереджати нові загрози.

Сприяти співробітництву IT-безпеки: сприяти співпраці між IT-командами та відділами безпеки.

Уряди можуть забезпечити захист критичної інфраструктури та даних за допомогою:

Національні стратегії кібербезпеки: Сформулюйте та реалізуйте національні стратегії кібербезпеки.

Регуляторний нагляд: забезпечте дотримання правил, які зобов'язують організації відповідати за безпеку.

Глобальне співробітництво в галузі кібербезпеки: співпрацюйте з іншими країнами над ініціативами з кібербезпеки.

Інвестиції в дослідження: виділіть кошти на передові дослідження кібербезпеки.

Ініціативи з підвищення обізнаності громадськості: інформуйте громадян про кіберзагрози та безпеку.

У всіх секторах постійна освіта та обізнаність щодо кібербезпеки є ключовими для боротьби з кіберзагрозами. Це охоплює:

Поінформованість про фішинг: навчання окремих осіб і співробітників щодо виявлення спроб фішингу.

Практики безпеки в Інтернеті: інформування користувачів про відповідальну поведінку в Інтернеті та обробку даних.

Кібергігієна: виховання хороших звичок кібергігієни, включаючи регулярні оновлення та надійне керування паролями.

Реагування на кризові ситуації: забезпечення того, щоб кожен знав, як реагувати у разі порушення, таким чином мінімізуючи потенційну шкоду.

*Висновок*

Кіберзагрози є невибірковими, перетинаючи кордони, впливаючи на окремих осіб, компанії та уряди. Ці загрози мають різноманітні наслідки, включаючи фінансові втрати, шкоду репутації та ризики національній безпеці.

Розуміння найбільш постраждалих сторін є життєво важливим для ефективного запобігання та пом'якшення наслідків. Незалежно від того, чи є ви фізичною особою, яка захищає особисті дані, малим підприємством, яке забезпечує собі засоби до існування, корпорацією, яка захищає свою репутацію, чи урядом, який захищає національні інтереси, кібербезпека є спільним імперативом.

У цю цифрову еру боротьба з кіберзагрозами є колективною роботою. Це нагадує нам, що ми повинні об'єднатися, залишаючись пильними, інформованими та активними, щоб захистити наше цифрове майбутнє». ***(Emmanuel Ohaba. Cyber Threats: Who Is Most Affected and Its Implications? // ReadWrite, INC (https://readwrite.com/cyber-threats-who-is-most-affected-and-its-implications/?utm_source=flipboard&utm_content=ReadWrite%2Fmagazine%2FAll+Stories). 02.11.2023).***

***

**«Індія є найбільш цільовою країною, з 13,7 відсотками всіх кібератак, за нею йдуть США з 9,6 відсотками, Індонезія та Китай з 9,3 відсотками та 4,5 відсотками відповідно, повідомляє новий звіт у понеділок.** За даними фірми з кібербезпеки Cyfirma, Індія була найбільшою цільовою країною у 2022 році, оскільки атаки на державні установи зросли більш ніж удвічі.

У другій половині 2022 року було на 95 відсотків більше кібератак на державні установи, ніж за той самий період у 2021 році. Кількість фінансованих державою кібератак в Індії зросла більш ніж на 100 відсотків у 2022 році порівняно

з 2021 роком. Охорона здоров'я є Згідно зі звітом, це найбільш цільовий сектор з боку хакерів, за яким йдуть освіта, дослідження, державний і військовий сектори.

«Зростаюча популярність Індії на світовій арені та підштовхування західних економік віддавати перевагу Індії перед іншими великими країнами, молоде та технічно підковане населення з низьким рівнем зрілості в кіберсекунді зіграло ключову роль у нападах хакерів на критично важливі активи, урядові установи з наміром порушувати їх і завдавати шкоди стратегічним інтересам Індії», — сказав Кумар Рітеш, генеральний директор і засновник Cyfirma.

Крім того, звіт показав, що в 2022 році організація в Індії зазнавала в середньому 1866 атак на тиждень. Найпоширенішими типами кібератак є фішингові атаки, атаки зловмисного програмного забезпечення та атаки програм-вимагачів. Близько 78 відсотків індійських організацій зазнали атаки програм-вимагачів у 2021 році, причому 80 відсотків цих атак призвели до шифрування даних, йдеться у звіті.

У період із січня по липень 2023 року у звіті спостерігалося 39 кампаній, націлених на різні галузі Індії. За цими кампаніями підозрювали такі відомі групи, як FancyBear, TA505, Mission 2025, Stone Panda та Lazarus Group. З цих 39 кампаній 14 були керовані групами, спонсорованими державою Китаю, з метою шпигунства.

Близько 11 із цих кампаній були заплановані хакерами, які підтримувалися Північною Кореєю, у рамках HaaS. Тоді як 10 атак були здійснені російськими загрозливими акторами, з яких лише чотири були спонсоровані державою, йдеться у звіті». ***(Shubham Verma. This is world's most targeted country for cyberattacks // TECHLUSIVE.IN. (https://www.techlusive.in/news/this-is-worlds-most-targeted-country-for-cyberattacks-1428838/?utm_source=flipboard&utm_content=techlusiveOFCL%2Fmagazine%2FTechlusive). 07.11.2023).***

***

**«Комплексне дослідження, проведене світовим лідером у сфері кібербезпеки McAfee, виявило зростаючу загрозу шахрайських повідомлень в**

**Індії. У дослідженні під назвою «Дослідження шахрайських повідомлень McAfee 2023» було опитано понад 7000 дорослих у семи країнах, проливаючи світло на вплив шахрайських повідомлень, розширених за допомогою штучного інтелекту (AI), на споживачів у всьому світі.**

Індія, країна з 900 мільйонами користувачів Інтернету, особливо сильно постраждала від розповсюдження шахрайських повідомлень. Дослідження показує, що щодня індійці отримують в середньому 12 фальшивих повідомлень або шахрайства через електронну пошту, текстові повідомлення або соціальні мережі. Ще більше занепокоєння те, що 82% індійських споживачів зізналися, що натискали або потрапляли на фальшиві повідомлення.

Ці шахрайські повідомлення стають все більш витонченими завдяки використанню кіберзлочинцями технології ШІ. Такий прогрес ускладнив для одержувачів розрізнення справжніх повідомлень від шахрайських. В результаті індійці витрачають в середньому 1,8 години на тиждень на перевірку автентичності повідомлень. Це додає до двох повних робочих тижнів щороку, присвячених виявленню шахрайства.

Шахраї покращили свою гру, що ускладнює виявлення шахрайських повідомлень. Згідно з дослідженням, 60% респондентів в Індії вважають, що виявлення шахрайських повідомлень стало складнішим завдяки тому, що хакери використовують ШІ для створення переконливіших обманів. Крім того, 49% опитаних відзначили, що шахрайські повідомлення тепер мають покращену граматику та позбавлені помилок, що робить їх дуже правдоподібними.

*Різні типи шахрайських повідомлень*

Ви виграли приз – обдурили 72% одержувачів

Фальшиві сповіщення або пропозиції про роботу – обдурюють 64% осіб

Банківські сповіщення – переконують 52% одержувачів

Інформація про несанкціоновану покупку – обман 37% цільових

Оновлення підписки Netflix (або подібне) – введення в оману 35% одержувачів

Фальшиві сповіщення про пропущену доставку або проблему з доставкою – вводить в оману 29% людей

Сповіщення безпеки Amazon або сповіщення про оновлення облікового запису – вводять в оману 27% цільової аудиторії

Наплив шахрайських повідомлень викликав у людей почуття приголомшення: середній індієць витрачає 105 хвилин щотижня на розшифровку повідомлень. Дослідження показало, що споживачі щодня отримують фальшиві повідомлення або шахрайство, причому 90% респондентів стикаються з цими загрозами електронною поштою та текстовими повідомленнями, а 84% – через соціальні мережі.

Зростання обсягу та складності шахрайських повідомлень також призвело до високого показника кліків: 82% індійців зізналися, що клацали фальшиві повідомлення або потрапляли на них.

Щоб боротися з цією тривожною тенденцією, дослідження припускає, що потрібні інструменти та ресурси на основі ШІ для боротьби з шахраями. Вражаючі 88% респондентів в Індії висловили свою довіру до рішення або функції, які використовують штучний інтелект для виявлення онлайн-шахрайства, а 59% вважають, що штучний інтелект є важливим для протидії шахрайству за допомогою ШІ». ***(Rahul Verma. India's Cyber Crisis: McAfee Study Reveals 82% People Are Falling Prey To Daily Scam Onslaught // Mashable India (https://in.mashable.com/tech/63560/indias-cyber-crisis-mcafee-study-reveals-82-people-are-falling-prey-to-daily-scam-onslaught?utm_source=flipboard&utm_content=MashableIndia%2Fmagazine%2FTECHNOLOGY). 09.11.2023).***

***

***«Кіберзлочинність є загрозою, яка постійно розвивається в епоху цифрових технологій, і Туреччина не є винятком із цієї глобальної проблеми.*** Від фішингових атак до хакерства та крадіжки особистих даних, окремі особи та компанії в Туреччині стикаються з низкою кіберзагроз. У цій статті ми дослідимо

вирішальну роль адвоката з кіберзлочинності в Туреччині, який відіграє важливу роль у захисті від кіберзлочинців і забезпеченні правосуддя для жертв.

*Розуміння зростаючої загрози кіберзлочинності в Туреччині*

*Кіберзлочинність: сучасна загроза*

Світ став свідком експоненціального зростання кількості кіберзлочинів, і Туреччині не чужа ця тривожна тенденція. В епоху, коли технології пронизують усі аспекти нашого життя, кіберзлочинці знайшли нові способи використовувати вразливі місця в комп'ютерних системах, викрадати конфіденційну інформацію та сіяти хаос. Для боротьби з цією загрозою роль адвоката з кіберзлочинності в Туреччині стає незамінною.

*Зміна обличчя кіберзлочинності*

Кіберзлочинність – це хамелеон, який постійно адаптується, щоб використовувати нові технології та слабкі місця в онлайн-безпеці. Фішинг, зловмисне програмне забезпечення та крадіжка особистих даних стали поширеними термінами, і це лише верхівка айсберга. Оскільки хакери стають все більш досвідченими, потреба в правових знаннях у цій сфері ніколи не була такою великою.

*Роль адвоката з кіберзлочинності в Туреччині*

*Багатогранний захист*

Юристи з питань кіберзлочинності в Туреччині є першою лінією захисту від цих загроз, що постійно розвиваються. Вони озброєні багатогранним арсеналом, що включає юридичні знання, технічну експертизу та глибоке розуміння середовища кіберзлочинців.

*Експертиза в галузі кібербезпеки та криміналістичного аналізу*

Однією з ключових ролей юриста з кіберзлочинності є розплутування заплутаної мережі доказів, залишених кіберзлочинцями. Ці юристи працюють рука об руку з експертами з кібербезпеки та судово-медичними аналітиками, щоб відстежити цифрові сліди та побудувати справу проти хакерів, шахраїв і крадіжок особистих даних.

*Адвокати жертв*

Жертви кіберзлочинів часто стикаються з важким і складним судовим процесом. Юристи з питань кіберзлочинності в Туреччині діють як адвокати, направляючи жертв через правову систему, пояснюючи їхні права та домагаючись справедливості від їхнього імені. Вони відіграють ключову роль у забезпеченні відповідальності винних за свої дії.

*Захист від кіберзлочинців*

*Правові дії проти винних*

Коли відбувається кіберзлочин, першочерговим завданням юриста з кіберзлочинності є виявлення та притягнення до суду проти винних. Вони співпрацюють з правоохоронними органами, надаючи їм необхідну правову підтримку для затримання та притягнення до відповідальності кіберзлочинців.

*Штрафи та переслідування*

Юристи з кіберзлочинності невпинно працюють, щоб забезпечити притягнення винних осіб до відповідальності за всією суворістю закону. Вони добре знаються на системі кримінального правосуддя, розуміючи покарання та наслідки, з якими стикаються кіберзлочинці.

*Захист підприємств і фізичних осіб*

*Підприємства на передовій*

Підприємства в Туреччині часто стають об’єктами кібератак. Юрист з питань кіберзлочинності є важливим активом для компаній, він допомагає їм розробляти надійну політику кібербезпеки, реагувати на витоки даних і орієнтуватися в складних правових питаннях, пов’язаних з кіберінцидентами.

*Права особи та конфіденційність*

Окремі особи також можуть скористатися досвідом юриста з кіберзлочинності. Ці професіонали в галузі права гарантують захист конфіденційності та прав людей, пропонуючи судовий захист, якщо особисту інформацію викрадено або використовується зловмисно.

*Правові виклики в епоху цифрових технологій*

*Розвиток законів і юрисдикції*

Ландшафт законодавства про кіберзлочинність постійно змінюється, і юристи з кіберзлочинності повинні бути в курсі останніх правових розробок. Вони орієнтуються в складності юрисдикції у справах, які охоплюють міжнародні кордони, і працюють над усуненням юридичних лазівок, якими можуть скористатися кіберзлочинці.

*Роль адвокатів з кіберзлочинності в резонансних справах*

У резонансних справах про кіберзлочини адвокати з кіберзлочинності часто займають центральне місце. Вони рішуче захищають своїх клієнтів, дотримуючись принципів справедливості, справедливості та підзвітності.

*У пошуках справедливості для жертв кіберзлочинів*

*Компенсація та реституція*

Юристи з питань кіберзлочинності в Туреччині також допомагають жертвам отримати компенсацію та відшкодування. Вони працюють над тим, щоб гарантувати, що жертви не лише виправдані, але й отримають відшкодування своїх втрат, фінансових чи емоційних.

*Запобігання кіберзлочинності та поінформованість про безпеку*

Крім своєї ролі в залі суду, адвокати з кіберзлочинності виступають за запобігання. Вони активно сприяють підвищенню обізнаності про безпеку, наголошуючи на важливості ефективних заходів кібербезпеки для компаній і окремих осіб…» ***(Zeynep Atım Kurucuk. Navigating the Digital Battlefield: The Role of a Cybercrime Lawyer in Turkey // Kurucuk & Associates (https://www.kurucuk.com.tr/post/cybercrime-lawyer-in-turkey). 04.11.2023).***

***

**«KnowBe4, найбільший у світі постачальник тренінгів з питань безпеки та симуляції фішингової платформи, оголосив про свої прогнози щодо кібербезпеки на 2024 рік від своєї команди глобальних експертів галузі.**

Кіберзагрози є більш витонченими та складними, ніж будь-коли, і швидко розвиваються завдяки новим технологіям, таким як штучний інтелект, які з кожним днем стають все більш прогресивними. Культивування міцної культури безпеки має першочергове значення для зміцнення людського брандмауера організації.

П’ять найбільш прогнозованих тенденцій кібербезпеки на 2024 рік включають:

1. Розвиток кіберзлочинності та методів захисту, пов’язаних зі штучним інтелектом

Зловмисники покращать свою здатність використовувати штучний інтелект для посилення поширення кіберзлочинності завдяки автоматизованій генерації атак соціальної інженерії та покращенню масштабованості кампаній. Інструменти штучного інтелекту та машинного навчання використовуватимуться для аналізу величезних обсягів даних, доступних у відкритому доступі та за допомогою дампів зломів, доступних на ринках темної мережі, дозволяючи створювати детальні профілі осіб, забезпечуючи набагато більш цілеспрямовані атаки на співробітників і окремих осіб.

Позитивним моментом є те, що захисні інструменти з використанням ШІ допоможуть покращити захист кібербезпеки. Протягом останніх 10 років багато компаній з кібербезпеки використовують і вдосконалюють своє використання ШІ. Штучний інтелект, який використовують хороші актори, покращить інструменти кібербезпеки та реагування.

2. Атаки програм-вимагачів, спрямовані на послуги ланцюга поставок

Групи кіберзлочинців, які займаються програмами-вимагачами, продовжуватимуть посилювати свої атаки, але будуть більш цілеспрямованими та працюватимуть над атаками на служби ланцюга поставок, щоб порушити та завдати шкоди організаціям у всьому світі.

3. Охолодження економіки, що вплине на програми безпеки та плани безперервності бізнесу

Потенційні втрати через кіберзлочинність у поєднанні з потенційним охолодженням глобальної економіки загрожуватимуть прибуткам і змусять

компанії переглядати та переглядати свої програми безпеки та плани безперервності бізнесу. Ці перевірки виконуватимуться, щоб переконатися, що кіберзлочин не загрожує банкрутством їх компанії.

4. Посилення уваги до співпраці для боротьби з кіберзлочинністю

У зв'язку з глобальним характером кіберзагроз, особливо як інструменту допомоги у війні, буде приділено підвищену увагу співпраці та обміну інформацією між національними та міжнародними агентствами з кібербезпеки. Це також просочуватиметься у більш широке державно-приватне партнерство та використовуватиметься для боротьби з кіберзлочинністю, усунення загроз національних держав, а також проактивного виявлення та реагування на нові кіберзагрози.

5. Кампанії з дезінформації, які призводять до схем здирництва

Кампанії з дезінформації будуть використовуватися для здійснення атак або відволікання від поточних атак. Ми можемо очікувати, що побачимо відповідні пропозиції послуг у темній мережі, що призведе до дезінформації як послуги. Це вплине на політику та приватний сектор. Дезінформація стає інструментом у наборі інструментів кіберзлочинців, які прагнуть отримати гроші від законного приватного бізнесу за допомогою схем вимагання. Зловмисники посилять використання глибоких фейків, зокрема відео та голосу.

«Кібератаки, такі як фішинг, стає все важче виявити», — сказав Стю Сьюверман, генеральний директор KnowBe4. «Вкрай важливо, щоб співробітники пам'ятали про загрозу фішингових атак і не впадали в самовдоволення. Це стало можливим лише завдяки періодичному навчанню з питань безпеки та імітації фішингу, щоб кінцеві користувачі мали знання, щоб ідентифікувати фішингові атаки, повідомляти про них і краще захищати свої організації. Це зводиться до створення міцної культури безпеки, і ми побачимо, як організації продовжуватимуть зосереджуватися на цьому та розвиватися на цьому у 2024 році»…» ***(Top Five 2024 Cybersecurity Predictions by KnowBe4 Cybersecurity Experts // Microsoft (https://www.msn.com/en-za/news/other/top-five-2024-cybersecurity-predictions-by-knowbe4-cybersecurity-experts/ar-AA1jQOZT). 13.11.2023).***

***

**«За даними американської хмарної компанії Cloudflare Inc, більше половини тайських організацій, опитаних в опитуванні, повідомили про понад 10 інцидентів кібербезпеки за минулий рік, а також про багатомільйонні збитки.**

Звіт про порушення даних, створений на замовлення IBM, показав, що у 2023 році середня глобальна вартість порушення досягла історичного максимуму в 4,45 мільйона доларів США.

«Протягом останнього року ми стали свідками зростання кількості інцидентів у сфері кібербезпеки в Азіатсько-Тихоокеанському регіоні, причому величезна частина випадків була спрямована на бізнес у Таїланді — більше, ніж будь-де в регіоні», — сказав Джонатон Діксон, віце-президент і керуючий директор. для Азіатсько-Тихоокеанського регіону, Японії та Китаю в Cloudflare.

Підприємствам Таїланду необхідно зміцнити свою інфраструктуру кібербезпеки, щоб справлятися зі зростаючою складністю розподіленої робочої сили.

Компанія випустила звіт під назвою «Забезпечення майбутнього: опитування готовності кібербезпеки в Азіатсько-Тихоокеанському регіоні», який було проведено Sandpiper Communications від імені Cloudflare. Було опитано 4009 осіб, які приймають рішення з кібербезпеки, і керівників від малих до великих компаній із широкого спектру галузей промисловості, які працюють на 14 ринках Азіатсько-Тихоокеанського регіону, включаючи Таїланд. Кількість респондентів, які брали участь, різна від країни до країни, коливаючись від 203 до 426.

Дослідження показало, що 57% тайських респондентів повідомили про понад 10 інцидентів кібербезпеки за останній рік. Респонденти також вказали, що основною метою кіберзлочинців є розповсюдження шпигунського програмного забезпечення, а потім фінансова вигода та програми-вимагачі.

Незважаючи на частоту інцидентів з кібербезпекою в Таїланді, 48% респондентів зазначили, що готові їм запобігти. Відсутність поінформованості про

підвищення ризику серед працівників (52%) була найбільшою проблемою, з якою зіткнулися респонденти з Таїланду щодо готовності до кібербезпеки.

Інциденти кібербезпеки виявилися дорогими для організацій у Таїланді: приголомшливі дві третини, або 65% респондентів, зазнали фінансових наслідків щонайменше в 1 мільйон доларів за останні 12 місяців.

Організації середнього розміру постраждали сильніше: 76% респондентів вказали, що вони зазнали фінансових наслідків у розмірі щонайменше 2 мільйонів доларів США за той самий проміжок часу. Окрім фінансових втрат, респонденти також називали репутаційну шкоду разом із втратою клієнтів найбільшим впливом на їхній бізнес.

Наслідки інцидентів кібербезпеки також поширюються на організаційні операції: 38% респондентів сказали, що їхні організації скоротили або обмежили гібридну роботу, звільнили персонал і призупинили плани розвитку. Лише 33% респондентів сказали, що їхня організація повідомляла про порушення у відповідні органи.

Підготовленість є ключовою — бізнес-лідери повинні розглядати кібербезпеку як стратегічний імператив на всіх рівнях організації. Відповідно до звіту, освіта співробітників для підвищення обізнаності про наявні ризики також є важливою для забезпечення надійного захисту компанії від майбутніх загроз.

Відповідно до іншого звіту під назвою «Cost of Data Beach report 2023», проведеного незалежно Інститутом Ponemon і спонсорованого, проаналізованого та опублікованого IBM Security, середня глобальна вартість витоку даних досягла історичного максимуму в 2023 році в 4,45 мільйона доларів США, тобто на 2,3% більше від вартості, повідомленої в 2022 році.

У довгостроковій перспективі середня вартість зросла на 15,3% з 3,86 млн доларів США у звіті за 2020 рік.

У звіті вивчено 553 організації, які постраждали від витоку даних, який стався з березня 2022 року по березень 2023 року. Дослідження проводилося в 16 різних країнах і регіонах, включаючи АСЕАН.

Щонайменше 51% організацій планують збільшити інвестиції в безпеку в результаті злому.

Хоча витрати на порушення безпеки даних продовжують зростати, учасники опитування майже однаково розділилися щодо того, чи планують вони збільшити інвестиції в безпеку через порушення даних.

Основні сфери, визначені для додаткових інвестицій, включали планування та тестування реагування на інциденти (IR), навчання співробітників і технології виявлення загроз і реагування.

Було показано, що штучний інтелект безпеки та автоматизація є важливими інвестиціями для зниження витрат і мінімізації часу, необхідного для виявлення та локалізації порушень. Організаціям, які широко використовували ці можливості в рамках свого підходу, у середньому знадобилося на 108 днів менше, щоб виявити та локалізувати порушення.

Вони також повідомили, що пов'язані витрати були на 1,76 мільйона доларів менше, ніж витрати, про які повідомили організації, які не використовували ШІ безпеки та можливості автоматизації.

З точки зору цільових галузей, охорона здоров'я продовжує відчувати найвищий рівень витрат на витік даних серед усіх галузей, які зросли з 10,1 мільйона доларів у 2022 році до 10,9 мільйона доларів цього року». ***(Report reveals extent of cybersecurity threat // Microsoft (https://www.msn.com/en-xl/news/other/report-reveals-extent-of-cybersecurity-threat/ar-AA1jKd77). 11.11.2023).***

***

**«Кібератаки стають все більш витонченими та поширеними, і під загрозу потрапляють компанії та особи будь-якого розміру.** Розуміючи останню статистику загроз, ми можемо краще захистити себе від цих атак.

Ось деякі ключові статистичні дані щодо загроз за 2023 рік:

Середня вартість витоку даних зараз становить 4,35 мільйона доларів проти 3,92 мільйона доларів у 2022 році.

Атаки програм-вимагачів зростають, середня сума викупу зросла зі 116 000 доларів США у 2021 році до 210 000 доларів США у 2022 році.

Фішингові електронні листи все ще залишаються найпоширенішим вектором атак, понад 90% успішних атак починаються з фішингового електронного листа.

Кількість уразливостей, про які повідомляється щороку, продовжує зростати, у 2022 році було зареєстровано понад 20 000 уразливостей.

Поверхня атаки швидко розширюється разом із розвитком Інтернету речей (IoT) і хмарних обчислень.

Ці статистичні дані показують, що ландшафт загроз постійно змінюється, і що компанії та окремі особи повинні бути пильними у своїх зусиллях щодо кібербезпеки.

*Знищення сучасної кіберзлочинності*

Для прикладу організації, яка стикається з постійними загрозами, давайте розглянемо захист Cisco Umbrella Cloud Architecture, яка є глобальною хмарною системою захисту, яка щодня обробляє мільярди онлайн-транзакцій. Аналіз їх використання в листопаді 2021 року дає миттєвий знімок типу злочину, який зараз здійснюється. Нижче ви знайдете діаграму з розподілом типів атак за один місяць.

Ви помітите, що основним типом атаки, виділеним на цій діаграмі, є рекламне програмне забезпечення, яке є типом програмного забезпечення, яке часто показує рекламу користувачеві та зазвичай встановлюється шляхом обману або без згоди. Інша категорія складається з різноманітних, менш поширених атак, таких як викрадач браузера. Це програмне забезпечення, яке змінює веб-браузер користувача без дозволу, як правило, щоб спрямувати користувача на певний веб-сайт. Однак у цій статті ми зосередимося на трьох найпоширеніших типах атак, які можуть завдати значної шкоди комп’ютеру або системі користувача; це атаки троянів, програм-вимагачів і ботнетів.

*Троянські атаки*

Найпоширеніша атака, зазначена на діаграмі, – це атака трояна. Назва є історичною згадкою про битву під Троєю, коли греки, як кажуть, обійти оборону троянців, обманом змусивши їх загнати дерев’яного коня, повного ворожих

солдатів, у своє місто. Це загальний термін, який охоплює кілька типів атак, зокрема:

Експлойт троянів

Трояни-завантажувачі

Трояни-викупники

Бекдорні трояни

Хоча трояни поводяться по-різному залежно від типу, спільною рисою цього підходу є те, що користувач ненавмисно вводить шкідливий код в організацію та запускає його за захисними стінами. Найкращий захист від атак троянів – це пильне використання Інтернету. Деякі рекомендації полягають у тому, щоб ніколи не натискати небажаний електронний лист із неочікуваними вкладеннями та завжди перевіряти доменні імена та посилання, перш ніж натискати їх. Будьте особливо пильні з орфографічними помилками, як-от нулі, замінені літерами «О» — трюк, який використовується, щоб спонукати необережного користувача завести коня за ворота. Нижче ви знайдете приклад потенційно зловмисного електронного листа разом зі списком загальних попереджувальних знаків, про які слід знати.

*Атаки програм-вимагачів*

Другим за поширеністю типом атаки з попередніх даних є програми-вимагачі. Нагадаємо, програмне забезпечення-вимагач – це підхід до кіберзлочинності, який призначений для порушення роботи сервісів. Цей підхід часто згадується в новинах через масштаби впливу. Нерідкі випадки, коли ці атаки відбуваються в національному масштабі, ціллю яких є інфраструктура та життєво важливі служби. Серед останніх прикладів:

Керівник служби охорони здоров’я Ірландії (HSE) у 2021 році.

Критична інфраструктура України у 2022 році.

Коста-Ріка, яка оголосила надзвичайний стан, коли 30 державних установ були затримані під викуп.

Методологія цих типів атак полягає в тому, щоб отримати доступ до системи та заблокувати законного власника, доки не буде виконано запит. Один із підходів до найкращого пом’якшення цього типу атак полягає в тому, щоб жодні сторонні

особи не отримали доступу до вашої системи. Передові практики для досягнення цієї мети включають наступне:

Використовуйте надійні паролі. Надійний пароль важко вгадати, і зазвичай він містить комбінацію символів, цифр і символів.

Підтримуйте свою систему в актуальному стані за допомогою останніх виправлень безпеки.

Переконайтеся, що тільки люди, які мають повноваження для системи, можуть використовувати її систему.

*Ботнет-атаки*

Далі йдуть ботнет-атаки, які становлять 13% задокументованих атак на діаграмі вище. Бот можна визначити як онлайн-програмне забезпечення, яке виконує автоматизовані та повторювані завдання. Вони є засобом створення відмови в обслуговуванні організації. Якщо атака трояна є тонкою спробою обійти захист програми, атаку бота можна описати як повне масштабування стін, як показано нижче.

Ці атаки організовані таким чином, що система заражена незліченною кількістю запитів на інформацію та послуги. Ці запити можуть надходити з будь-якого сумісного пристрою в Інтернеті речей (IoT), який має IP-адресу. Інтернет речей стосується пристроїв онлайн і буде розглянуто більш детально пізніше.

Цей тип атаки можна поєднати з атакою троянів, коли частина коду, зловмисно вбудованого в систему, використовується для запиту іншої системи. Таким чином зловмисник використовує чужі цифрові ресурси, щоб знищити ресурси цільової жертви. Одним із захисних підходів для пом’якшення цих типів атак є моніторинг мережевого трафіку на наявність підозрілої активності. Якщо визначено, що певне джерело здійснює повторювані виклики, що впливають на роботу системи, цю адресу можна заблокувати. Однак у разі використання різноманітних скомпрометованих систем необхідно застосовувати більш складні підходи.

*Висновок*

Як ви вже могли зробити висновок, кіберзлочинність – це широке поле, яке охоплює різноманітні засоби вимагання грошей від організації. Це варіюється від зупинки комерційної діяльності до видалення цінних предметів, таких як інформація користувача…» ***(Threat stats: What they tell us about the state of cybersecurity // HackerNet.in (https://hackernet.in/threat-stats-what-they-tell-us-about-the-state-of-cybersecurity/). 12.11.2023).***

***

**«ФБР і Агентство з кібербезпеки та безпеки інфраструктури США закликають організації критичної інфраструктури застосувати методи пом'якшення, щоб перешкодити групі кіберзлочинців, відомій як Scattered Spider, яка націлена на великі компанії та їхні служби підтримки IT.**

У спільній консультації хакерська група, також відома як Octo Tempest і UNC3944, описує групу хакерів, яка має досвід у соціальній інженерії, яка використовує фішинг, бомбардування та інші методи для отримання несанкціонованого доступу до мереж комерційних об'єктів, які надають послуги роздрібної торгівлі, розваг і розміщення. громадськість.

Хакери Scattered Spider є унікальними серед кіберзлочинних організацій, оскільки група складається з носіїв англійської мови та не має чіткої публічної присутності в Інтернеті, на відміну від багатьох російських і колишніх радянських колег.

Під час телефонної розмови з журналістами у четвер високопоставлені представники CISA та ФБР пов'язали хакерську групу з масштабною кібератакою у вересні, яка була спрямована на MGM Resorts International і зруйнувала роботу кількох популярних казино та готелів Лас-Вегаса.

У повідомленні йдеться, що хакери Scattered Spider видавали себе за співробітників IT-служби компанії та використовували телефонні дзвінки або текстові повідомлення, щоб отримати облікові дані співробітників і отримати

несанкціонований доступ до їхніх мереж. Група монетизує доступ до мереж жертв за допомогою здирництва, програм-вимагачів та інших операцій з крадіжки даних.

ФБР і CISA рекомендують організаціям запроваджувати розширені засоби контролю додатків і проводити перевірки своїх інструментів віддаленого доступу, на додаток до перегляду журналів для виконання програмного забезпечення віддаленого доступу для виявлення аномалій. Рекомендації також включають вимогу щодо використання авторизованих рішень віддаленого доступу лише в мережах над схваленими рішеннями, такими як віртуальні приватні мережі, а також використання програмного забезпечення безпеки для виявлення додаткових аномалій і можливого зловживання.

Високопоставлений чиновник ФБР підтвердив, що з моменту кібератаки в Лас-Вегасі на комерційних об'єктах і підсекторах – одному з 16 визначених секторів критичної інфраструктури в США – стали додаткові жертви Scattered Spider. Вони відмовилися надати додаткову інформацію про цих жертв, пославшись на триваюче розслідування». ***(Chris Riotta. CISA, FBI Issue New Warning Following Las Vegas Cyberattack // Information Security Media Group, Corp. (https://www.databreachtoday.com/cisa-fbi-issue-new-warning-following-las-vegas-cyberattack-a-23616?utm_source=flipboard&utm_content=other). 16.11.2023).***

***

**«Минулого літа уряди п'яти країн Європи, Африки та Азії зробили помилку, знайому практично всім, хто має комп'ютер: вони не оновили своє програмне забезпечення, проігнорувавши попередження розробника програми про те, що це вкрай необхідно зробити.** Результат? Відповідно до нового дослідження, зібраного Google, вони залишили відкритим бекдор для банди опортуністичних хакерів.

Чотири окремі хакерські кампанії були націлені на державні установи в Греції, Молдові, Тунісі, В'єтнамі та Пакистані, використовуючи вразливість у широко використовуваній платформі електронної пошти Zimbra від Баффало, штат Нью-Йорк, повідомляє Google у блозі. Три атаки відбулися після того, як Zimbra

опублікувала рішення проблеми, пропонуючи нові докази того, що багато жертв регулярно не встановлюють важливі оновлення безпеки, які могли б захистити їх від кібератак.

Zimbra — це альтернатива з відкритим кодом дорогим корпоративним платформам електронної пошти, які продають Microsoft і Google. Його нижча вартість може зробити його популярним серед урядів із низьким і середнім доходом, які не можуть дозволити або не хочуть платити за більш відомі продукти технічних гігантів США.

Грецька атака сталася 29 червня, за шість днів до того, як Zimbra опублікувала екстрене виправлення. Але атаки на Молдову, Туніс, В'єтнам і Пакистан відбулися протягом наступних двох місяців, причому пакистанське вторгнення відбулося навіть після того, як Zimbra опублікувала більш офіційний патч 25 липня.

Хронологія атак «демонструє важливість того, щоб організації якнайшвидше застосовували виправлення на своїх поштових серверах», пишуть дослідники Google. Також було підкреслено, як хакери відстежують веб-сайти з розміщенням коду, такі як Github, де Zimbra опублікувала своє екстрене виправлення, «щоб випадково використовувати вразливості» у вікні між екстреним виправленням і офіційним патчем.

Google не ідентифікувала хакерів у грецьких, в'єтнамських чи пакистанських інцидентах, але приписала атаки на Молдову та Туніс групі хакерів, тісно пов'язаній з урядами Росії та Білорусі. Ця група раніше використовувала недоліки Zimbra.

Під час атаки на урядову установу Греції хакери змогли не лише викрасти дані з поштових скриньок своїх цілей, але й налаштувати автоматичне пересилання для перехоплення повідомлень, які ці цілі отримували в майбутньому.

Атаки в Молдові та Тунісі почалися 11 липня, за два тижні до того, як Zimbra випустила офіційний патч для уразливості, і були ретельно сплановані, щоб обдурити цільові дії. За словами Google, кожне посилання, яке хакери

використовували для запуску вад Zimbra, «містило унікальну офіційну адресу електронної пошти для певних організацій у цих урядах».

У третій кампанії, націленою на В'єтнам, хакери скеровували свої цілі на сторінки входу в електронну пошту, які виглядали легітимними, але насправді передавали хакерам паролі жертв. Цікаво, що паролі були доставлені на веб-сайт, «розміщений на офіційному державному домені», що свідчить про те, що хакери раніше контролювали цю систему». ***(Eric Geller. Hackers Pounced on World Governments That Made a Very Relatable Blunder // JAF Communications Inc. (https://themessenger.com/tech/hackers-zimbra-collaboration-email-software-greece-vietnam-tunisia-pakistan-moldova?utm_source=flipboard&utm_content=TheMessenger%2Fmagazine%2Fwhat%27s+new). 16.11.2023).***

***

**«…Останнє десятиліття з його стрімкою цифровізацією всієї людської діяльності сприяло подальшому прискоренню кіберзагроз; Тепер ціллю може стати кожен і все – від вашого банку до кабінету лікаря, пристроїв Інтернету речей і електромобіля.** Однак ми не залишилися самі в цій боротьбі: безліч компаній намагаються захистити нас від цифрових загроз і намагаються заробити на цьому гроші. Але хоча захист від кіберзлочинності може бути майже таким же прибутковим, як і сам злочин, не кожна компанія з кібербезпеки впорається з цим завданням.

*Невинні хакери*

Офіційна історія кіберзлочинності почалася в 1981 році, коли першого в історії хакера було засуджено за вторгнення у внутрішні комп'ютерні системи AT&T. Однак цей випадок був сприйнятий як курйоз і маловідомий. Вперше влада та широка громадськість зрозуміли, що в проводах таїться небезпека, було в 1988 році, коли комп'ютерний хробак скалічив десяту частину того, що тоді було Інтернетом, і завдав шкоди на 15 мільйонів доларів. Потім, у 1995 році, відбувся арешт Кевіна Мітніка, першого знаменитого хакера всіх часів, злочинця, який став

реформатором, який став першим у світі експертом з комп'ютерної безпеки, заклавши основу індустрії кібербезпеки.

Часи невинності, коли кіберзлочинність була кустарним виробництвом або навіть трюком однієї людини, давно минули. Сьогодні це величезний бізнес, який охоплює континенти та посилає свої щупальця в усі можливі цифрові місця. Звісно, це не «супермафія» з науково-фантастичних фільмів, але все ж таки екосистема безлічі людей та організацій, яка нині є небезпечнішою для людства, ніж збройні конфлікти та пандемії.

*Дорогі викупи*

Минулого року глобальні збитки від кіберзлочинності оцінювалися в 8,5 трильйонів доларів; Фахівці галузі очікують, що до 2027 року ці витрати зростуть втричі. Втрати, пов'язані з кібератаками, включають пошкодження або втрату даних; втрата продуктивності; шахрайство, шахрайство, вимагання та інші види крадіжки грошей; викрадення персональних або фінансових даних; зрив бізнесу; вандалізм тощо.

У 2021 році хакери-вимагачі вразили системи компанії Colonial Pipeline, змусивши її припинити роботу та залишивши дві третини АЗС у Південній Каролініі порожніми, що викликало паніку. Ці хакери, яких так і не знайшли, отримали щонайменше 90 мільйонів доларів у вигляді викупу – і це лише один випадок конкретного виду злочину.

Того ж року хакери-вимагачі навіть наважилися атакувати Департамент столичної поліції Вашингтона, округ Колумбія, погрожуючи розповсюдити особи інформаторів злочинцям, якщо вони не сплатять викуп у розмірі 50 мільйонів доларів.

*Небезпечні для життя одиниці та нулі*

Але фінансові витрати, якими б великими вони не були, не є найактуальнішою проблемою щодо кіберзлочинності. Останніми роками ми стали свідками стрімкого зростання кількості кібератак із жахливими фізичними наслідками, а також злиття кіберзлочинності з насильницькою та/або

організованою злочинністю, як-от торгівля людьми, наркотиками, зброєю, тероризмом тощо.

Тоді як атака на комп'ютерні системи банку може призвести до значної втрати капіталу, атака на лікарню може призвести до значної втрати життя. Насправді ці атаки є не віддаленою загрозою, а реальністю: у 2021 році десятки європейських і американських медичних закладів були заблоковані в критично важливих системах через атаки програм-вимагачів. Крім того, злочинці можуть заволодіти електрикою чи іншими важливими інфраструктурними системами з тяжкими наслідками. Зламана автономна система керування автопарком, командний центр аеропорту чи навіть металургійний завод (приклад із реального життя) може призвести до великомасштабної втрати життя.

Крім комерційних хакерів, існує цілком реальна загроза кібервійн, коли фінансовані іноземними державами кібератаки спрямовані на енергетичну інфраструктуру, зривають військові операції або впливають на політику, що призводить до соціальних заворушень.

*Зростаючий попит на «Хороших хлопців»*

Враховуючи тривожне розширення масштабів і охоплення кібератак, не дивно, що ринок кібербезпеки, який захищає нас від цих загроз, також швидко розширюється і, за прогнозами, зростатиме на 14%-16% до 2030 року.

Однак, враховуючи поточний масштаб і поширення кіберзагроз, а також постійне розширення «бізнес-можливостей» для кіберзлочинців на фоні стрімкого технологічного прогресу та постійно зростаючої цифрової залежності уряду, бізнесу та приватної діяльності, ці цифри можуть добре бути заниженням. McKinsey припускає, що глобальний ринок адресної кібербезпеки може становити від 1,5 трлн до 2,0 трлн доларів, оскільки поточне проникнення продуктів і послуг кібербезпеки далеке від очевидної потреби ринку в цифровому захисті. Таким чином, ринок кібербезпеки пропонує майже необмежений довгостроковий потенціал для компаній, які працюють у цьому просторі, а також для їхніх інвесторів.

*Не всі цінні папери безпечні*

Таким чином, ми встановили, що швидка глобальна цифровізація та пов’язана з цим необхідність кіберзахисту представляють величезні можливості для бізнесу для компаній, що спеціалізуються на продуктах і рішеннях для кібербезпеки. Однак інвестори, які бажають заробити на цьому постійному зростанні, стикаються з ринком, який характеризується високою волатильністю окремих акцій, а також великими відмінностями у фінансових показниках і показниках прибутковості компаній, що діють у цій сфері.

Слід зазначити, що перші позиції в списку компаній з кібербезпеки займають різноманітні технологічні гіганти з великими кіберпідрозділами та майже необмеженими коштами на розробку своїх продуктів, такі як Microsoft (MSFT), IBM (IBM) і Cisco Systems (CSCO).).

Найвідоміші компанії з кібербезпеки, які домінують на ринку, це Palo Alto Networks, Inc. (PANW), Fortinet, Inc. (FTNT), CrowdStrike Holdings, Inc. (CRWD), Cloudflare, Inc. (NET) і Check Point. ТОВ «Програмні технології» (ЧКП). Однак не всі з цих відомих лідерів ринку можуть продемонструвати навіть позитивний чистий прибуток: і CrowdStrike, і Cloudflare все ще мають «мінуси» у своїх прибутках, незважаючи на те, що вони працюють на ринку більше десяти років. Хоча CRWD знаходиться на межі беззбитковості, очікується, що NET не досягне прибутковості в найближчі кілька років, що підкреслює жорстку конкуренцію на цьому фрагментованому ринку. PANW, один із беззаперечних лідерів ринку, отримав чистий прибуток лише минулого року.

Іншими важливими гравцями на ринку кібербезпеки є Zscaler, Inc. (ZS), Akamai Technologies, Inc. (AKAM), Leidos Holdings, Inc. (LDOS), Gen Digital Inc. (GEN), Okta, Inc. (OKTA), Qualys, Inc. (QLYS) і SentinelOne, Inc. (S). З цих учасників лише AKAM, LDOS, GEN і QLYS вже приносять позитивний чистий прибуток. Окрім відмінностей у місцях ведення бізнесу та прибутковості, ці компанії значно відрізняються показниками якості та оцінки, а також потенціалом зростання прибутку.

*Дослідження, щоб захистити ваш капітал*

Ці значні відмінності в фундаментальних принципах і перспективах розвитку компаній підкреслюють важливість досліджень для початківців інвесторів у кібербезпеку. Незважаючи на те, що ринок кіберзахисту надає прибуткове ігрове поле з величезними можливостями, не кожна компанія на цьому ринку може скористатися цими можливостями. Таким чином, дуже важливо копатися в даних, аналізуючи фінанси компаній, конкурентоспроможність галузі, перспективи зростання та ризики тощо.

Крім того, інвестори можуть скористатися наявним аналізом, використовуючи дослідження, проведене провідними аналітиками Уолл-стріт. TipRanks має кілька інструментів, які можуть допомогти інвесторам використовувати величезні обсяги даних і досліджень, що зберігаються в його базі даних, на свою користь. Перегляньте таблицю TipRanks нижче, щоб отримати огляд ефективності кількох відомих із кібербезпеки. компаній

Як інший варіант, інвестори можуть придбати один із ETF кібербезпеки, використовуючи один із багатьох інструментів TipRanks ETF, щоб вибрати виграшний фонд.

Підсумовуючи, акції кібербезпеки надають інвесторам можливість отримати прибуток від прискорення глобального попиту на захист від цифрових загроз, а також дозволяють більшу диверсифікацію портфеля, оскільки багато з цих компаній демонструють помірну кореляцію з широкими ринковими рухами. Зважаючи на це, важливо брати до уваги фінанси та перспективи компаній, щоб вибрати переможців, які можуть створити довгострокову цінність для своїх акціонерів». ***(Yulia Vaiman. Cybersecurity Stocks: Investing in "The Good Guys" // Microsoft (https://www.msn.com/en-us/money/other/cybersecurity-stocks-investing-in-the-good-guys/ar-AA1kuOlm). 24.11.2023).***

***

**«Згідно з даними Arkose Labs, боти та ферми шахрайства були відповідальними за мільярди атак у першій половині 2023 року та в третьому**

**кварталі.** Ці атаки склали 73% усього виміряного трафіку веб-сайтів і додатків. Іншими словами, майже три чверті трафіку до цифрових ресурсів є шкідливим.

Дослідники оцінили атаки за трьома основними векторами атак: базові боти, інтелектуальні боти та ферми шахрайства. Шахраї використовують ці вектори для здійснення таких типів атак, як шахрайство з використанням SMS-повідомлень, сканування веб-сторінок, тестування карток, введення облікових даних тощо.

Аналіз показує, що кількість атак ботів загалом зросла на 167% у першому півріччі 2023 року, значною мірою враховуючи збільшення кількості інтелектуальних ботів на 291%. Ці розумні боти здатні до складної взаємодії з урахуванням контексту.

У другому кварталі 2023 року кількість ботів, які намагалися заволодіти фінансовими рахунками споживачів, зросла на 202%, а кількість ботів, які намагалися відкрити підроблені нові банківські рахунки, – на 164%. Ця тенденція збереглася і в третьому кварталі, коли кількість нових фальшивих банківських рахунків зросла на 30% порівняно з другим кварталом.

Зловмисники намагалися вивести баланси з рахунків через атаки ATO, тоді як фальшиві онлайн-акаунти, швидше за все, були кращими методами відмивання незаконних доходів, отриманих від реальних злочинів, таких як торгівля людьми, торгівля наркотиками чи продаж зброї.

*Ферми шахрайства людей*

Однак атаки не обмежувалися ботами. Дослідження показало, що коли боти шахраїв блокуються, вони спрямовують атаки на ферми шахрайства, кількість яких зросла на 49% з 1 по 2 квартал 2023 року.

«Атаки ботів за допомогою ферм шахрайства людей стосуються не тільки квитків на концерти та дорогих кросівок. Вони можуть вказувати на набагато темнішу діяльність», — сказав Кевін Гошалк, генеральний директор Arkose Labs.

«Ми бачимо більше атак, використовуємо більше інтелектуальних ботів, проводимо більш складні типи атак. Підроблена реєстрація облікового запису, підміна облікових даних, сканування, шахрайство з SMS-повідомленнями – це типи атак, які шахраї використовують як перші кроки до більш шкідливих злочинів.

Вони призводять до романтичних шахрайств, які ведуть до торгівлі людьми, відмивання грошей від угод з наркотиками або крадіжки для фінансування незаконної зброї», – продовжив Гошалк.

Виділено дві тенденції, що сприяють збільшенню рівня атак: генеративний штучний інтелект (GenAI) і кіберзлочинність як послуга (CaaS).

Протягом останніх шести місяців дослідники загроз Arkose Labs спостерігали значне зростання використання GenAI для створення вмісту зловмисниками, які тепер можуть писати чисті фішингові електронні листи для атак Man-in-the-Middle або ідеально сформульовані відповіді на додатки для знайомств у своїх романтичних шахрайствах. Крім того, дослідники виявили, що зловмисники використовують ботів для збирання даних із веб-сайтів, а потім використовують ці дані для налаштування своїх моделей GenAI.

GenAI знизив бар'єр для проникнення зловмисників, що, у свою чергу, швидко зробило це обов'язковим, а не вибором для CISO та їхніх команд.

Не менш вражаюча тенденція – Cybercrime-as-a-Service (CaaS) знижує бар'єр для проникнення зловмисників, які хочуть вчинити кіберзлочин. Постачальники CaaS відкрито рекламують свої сумнівно-легальні послуги.

Кожен може зв'язатися з цими постачальниками, щоб купити ботів, щоб обійти заходи безпеки або здійснити атаку. Шахраї з обмеженими до нуля технічними навичками можуть використовувати повністю автоматизованих ботів у великих масштабах, які завдають великої шкоди підприємствам і споживачам.

Шахраям більше не потрібно знати, як кодувати, щоб розгорнути складну об'ємну атаку ботів. Вони можуть просто придбати ботів в Інтернеті разом із необхідним навчанням і навіть скористатися «клієнтською» підтримкою продавців.

Гошальк додав: «Велике зростання CaaS повністю змінило економіку противників. Набагато дешевше атакувати компанії, і атаки просто кращі, тому що атаки здійснює магазин розробників, а не окремі кіберзлочинці».

*Галузі промисловості під ударом*

З огляду на таку велику кількість трафіку на цифрові властивості, створеного зловмисними атаками, дослідники Arkose Labs глибше заглибились у конкретні галузі, які зазнали атаки. Майже кожна галузь зазнала збільшення кількості атак.

У звіті перераховуються наступні галузі, у яких понад 50% трафіку надходять від поганих ботів, і детально описуються типові атаки зловмисних ботів.

Подорожі та гостинність – 76% поганих ботів

Технологія – 71% поганих ботів

Роздрібна торгівля – 65% поганих ботів

Потокове передавання – 61% поганих ботів

Подарункові картки – 57% поганих ботів». ***(Cybercriminals turn to ready-made bots for quick attacks // Help Net Security (https://www.helpnetsecurity.com/2023/11/23/bot-attacks-h1-2023/). 23.11.2023).***

***

## ***Діяльність хакерів та хакерські угруповування***

---

**«Група кіберзлочинців під назвою Lockbit, яка в п'ятницю заявила, що зламала Індустріально-комерційний банк Китаю (ICBC), за останні місяці зламала деякі з найбільших організацій світу, викравши та передавши їх конфіденційні дані, якщо вони не заплатили викуп.** Ось деякі подробиці про групу:

ЗВІДКИ LOCKBIT?

Lockbit було виявлено в 2020 році, коли його однойменне шкідливе програмне забезпечення було виявлено на російськомовних форумах про кіберзлочинність, що змусило деяких аналітиків безпеки припустити, що банда базується в Росії. Проте банда не заявляла про підтримку будь-якого уряду, і жоден уряд офіційно не відносив її до національної держави.

«Ми знаходимося в Нідерландах, абсолютно аполітичні і цікавимося лише грошима», — повідомляє банда у своєму темному веб-блозі.

За словами офіційних осіб США, лише за три роки воно стало найбільшою загрозою програм-вимагачів у світі. Ніде він не був таким руйнівним, як у Сполучених Штатах, вразивши понад 1700 американських організацій майже в усіх галузях – від фінансових послуг і продуктів харчування до шкіл, транспорту та державних відомств.

Серед її останніх жертв – оборонний та аерокосмічний гігант Boeing (BA.N). У п'ятницю Lockbit злив кеш внутрішніх даних, отриманих під час зламу систем Boeing. Раніше цього року зловмисники групи ION, яка надає послуги фінансової торгівлі, порушили роботу клієнтів, серед яких були деякі з найбільших у світі банків, брокерських компаній і хедж-фондів.

ЯК LOCKBIT НАЦІЛЮЄТЬСЯ НА ОРГАНІЗАЦІЇ?

Угруповання кіберзлочинців заражає систему організації-жертви програмами-вимагачами – шкідливим програмним забезпеченням, яке шифрує дані, – а потім змушує цілі платити викуп за їх розшифровку або розблокування. Такий викуп зазвичай вимагається у формі криптовалюти, яку важче відстежити та забезпечує анонімність одержувача.

США та інші офіційні особи в альянсі з 40 країн намагаються зупинити глобальне лихо програм-вимагачів, обмінюючись між країнами розвідувальною інформацією про адреси криптовалютних гаманців таких злочинців.

У темній мережі блог Lockbit демонструє постійно зростаючу галерею організацій-жертв, яка оновлюється майже щодня. Поруч із їхніми іменами є цифрові годинники, які показують кількість днів, що залишилися до кінцевого терміну, наданого кожній організації для виплати викупу. Якщо цього не зробити, банда публікує конфіденційні дані, які вона зібрала.

Часто організації-жертви звертаються за допомогою до компаній з кібербезпеки, щоб визначити, які дані витік, і домовитися з хакерами про суму викупу. За словами аналітиків безпеки, такі закулісні переговори зазвичай залишаються приватними і іноді можуть тривати кілька днів або тижнів.

Зазвичай імена деяких жертв не відображаються в блозі Lockbit, якщо загроза була зроблена приватно. Американський підрозділ ICBC, який заявив, що працює над усуненням злому, не був зазначений у блозі Lockbit у п’ятницю.

ЯК ПРАЦЮЄ LOCKBIT?

Частково успіх Lockbit залежить від його так званих «філій» — злочинних груп однодумців, яких залучають для здійснення атак за допомогою інструментів цифрового вимагання Lockbit.

На своєму веб-сайті банда хвалиться своїми успіхами у зломі різних організацій і викладає детальний набір правил для кіберзлочинців, які можуть подати «форму заявки» на співпрацю з ними. «Попросіть своїх друзів або знайомих, які вже працюють з нами, поручитися за вас», — говорить одне з цих правил.

Ця мережа альянсів між групами кіберзлочинців ускладнює відстеження такої хакерської діяльності та спроб викупу за жертв, оскільки їх тактика та методи можуть змінюватися з кожною атакою». ***(Zeba Siddiqui, James Pearson. Explainer: What is Lockbit? The digital extortion gang on a cybercrime spree // Reuters (https://www.reuters.com/technology/cybersecurity/what-is-lockbit-digital-extortion-gang-cybercrime-spree-2023-11-10/). 11.11.2023).***

***

## ***Вірусне та інше шкідливе програмне забезпечення***

---

**«Дослідники з кібербезпеки виявили новий шкідливий «шпигунський мод WhatsApp», який атакував користувачів платформи обміну повідомленнями Telegram більше 340 000 разів тільки в жовтні, йдеться в новому звіті.** За даними фірми з кібербезпеки Kaspersky, це зловмисне програмне забезпечення в основному націлене на користувачів, які спілкуються арабською та азербайджанською мовами, а жертв ідентифікують у всьому світі.

Оскільки користувачі звертаються до сторонніх модів для популярних програм обміну повідомленнями, щоб додати додаткові функції, дослідники

пояснили, що деякі з цих модів, покращуючи функціональність, також містять приховане шкідливе програмне забезпечення.

За їх словами, новий мод WhatsApp пропонує не тільки доповнення, такі як заплановані повідомлення та настроювані параметри, але також містить модуль шкідливого шпигунського ПЗ.

Змінений файл маніфесту клієнта WhatsApp містить підозрілі компоненти (сервіс і приймач трансляції), яких немає в оригінальній версії.

Приймач ініціює службу, запускаючи шпигунський модуль, коли телефон увімкнено або заряджається.

Після активації шкідливий імплант надсилає запит із інформацією про пристрій на сервер зловмисника.

Ці дані охоплюють IMEI, номер телефону, код країни та мережі тощо.

Він також передає контакти жертви та деталі облікового запису кожні п’ять хвилин, а також може налаштовувати записи з мікрофона та вилучати файли із зовнішньої пам’яті, йдеться у звіті.

Найбільше нападів було зафіксовано в Азербайджані, Саудівській Аравії, Ємені, Туреччині та Єгипті. Хоча перевага надається арабськомовним та азербайджанськомовним користувачам, вона також стосується людей із США, Росії, Великобританії, Німеччини та інших країн.

Щоб бути в безпеці, експерти рекомендують використовувати офіційні торговельні майданчики, завантажувати програми та програмне забезпечення з надійних та офіційних джерел і уникати сторонніх магазинів додатків, оскільки там вищий ризик розміщення шкідливих або скомпрометованих програм.

«Поширення шкідливих модів через популярні сторонні платформи підкреслює важливість використання офіційних клієнтів миттєвих повідомлень. Однак, якщо вам потрібні деякі додаткові функції, яких немає в оригінальному клієнті, вам слід розглянути можливість використання надійного рішення безпеки перед встановленням стороннього програмного забезпечення., оскільки це захистить ваші дані від зламу», – сказав Дмитро Калінін, експерт з безпеки Kaspersky». ***(New WhatsApp spy mod attacks Telegram users over 340K times in***

***October: Report // India Dot Com Private Limited (https://www.zeebiz.com/technology/news-new-whatsapp-spy-mod-attacks-telegram-users-over-340k-times-in-october-report-262869?utm_source=flipboard&utm_content=ZeeBusiness%2Fmagazine%2FZee+Business). 04.11.2023).***

***

**«Дослідники з кібербезпеки з Jamf виявили нову шкідливу програму для macOS, розроблену та розповсюджену північнокорейським загрозливим актором BlueNoroff.**

ObjCShellz намагається виконувати команди оболонки, надіслані з сервера зловмисника, на скомпрометованих кінцевих точках.

Незважаючи на те, що Jamf не зміг з'ясувати, як поширювалося зловмисне програмне забезпечення, він каже, що кампанія «дуже узгоджується» з попередньою кампанією під назвою Rustbucket.

«У цій кампанії актор звертається до цілі, стверджуючи, що зацікавлений у партнерстві з ним або пропонує їм щось вигідне під виглядом інвестора чи мисливця за головами», — пояснили дослідники. «BlueNoroff часто створює домен, який виглядає так, ніби він належить до законної криптокомпанії, щоб злитися з мережевою діяльністю».

Джамф описує BlueNoroff як «фінансово вмотивовану хакерську групу», відому тим, що нападає на криптобіржі, фінансові організації та банки по всьому світу.

Попередні звіти також описували групу як відділ Lazarus Group, спонсорованого державою Північної Кореї загрозливого актора, якого звинувачують у деяких з найбільших криптографічних крадіжок в історії.

Нібито Лазарус є частиною Головного розвідувального бюро (RGB), головного розвідувального агентства Північної Кореї.

Дослідники описали ObjCShellz як «досить просте», але дуже функціональне шкідливе програмне забезпечення, яке справляється зі своєю роботою. «Схоже, це

тема з останнім шкідливим програмним забезпеченням, яке ми бачили від цієї групи APT», — сказав Джамф.

«Грунтуючись на попередніх атаках, здійснених BlueNoroff, ми підозрюємо, що це зловмисне програмне забезпечення було пізньою стадією багатоетапного шкідливого програмного забезпечення, доставленого за допомогою соціальної інженерії».

Востаннє ми чули про BlueNoroff на початку липня цього року, коли дослідники кібербезпеки з Elastic Security Labs знайшли нову версію Rustbucket, націлену на кінцеві точки macOS.

Кажуть, що нова версія є більш стійкою та її важче виявити». ***(Sead Fadilpašić. North Korean hackers are targeting Apple users with new macOS malware // Future US, Inc. (https://www.techradar.com/pro/security/north-korean-hackers-are-targeting-apple-users-with-new-macos-malware?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 08.11.2023).***

***

***Програми-вимагачі***

---

**«Високопоставлений чиновник Білого дому оголосив у вівторок, що 50 країн планують підписати зобов'язання ніколи не платити викупи кіберзлочинцям, намагаючись стиснути їхні ресурси.**

Міжнародна ініціатива боротьби з програмами-вимагачами була створена в той час, коли кількість атак програм-вимагачів досягла глобального максимуму, майже половина з яких (46%) відбувається в Сполучених Штатах.

*Як працюватиме Альянс?*

Під час атак програм-вимагачів хакери шифрують системи організації та вимагають викуп в обмін на їх розблокування. Часто вони також викрадають конфіденційні дані та використовують їх для вимагання жертв і витоку в Інтернеті, якщо платежі не здійснені.

Вони часто використовують цю викрадену інформацію для здійснення атак на компанії в інших країнах, тому так важливо, щоб країни співпрацювали, якщо вони хочуть мати шанс зупинити цих хакерів.

До 50 країн альянсу входять Албанія, Австралія, Австрія, Бельгія, Бразилія, Болгарія, Канада, Колумбія, Коста-Ріка, Хорватія, Чехія, Домініканська Республіка, Єгипет, Естонія, Європейський Союз, Франція, Німеччина, Греція, Індія, Інтерпол, Ірландія, Ізраїль, Італія, Японія, Йорданія, Кенія, Литва, Мексика, Нідерланди, Нова Зеландія, Нігерія, Норвегія, Папуа-Нова Гвінея, Польща, Португалія, Республіка Корея, Румунія, Руанда, Сьєрра-Леоне, Сінгапур, Словаччина, Південна Африка, Іспанія, Швеція, Швейцарія, Україна, Об’єднані Арабські Емірати, Великобританія, Сполучені Штати та Уругвай. до них також приєдналися Інтерпол і Європейський Союз

Керівний принцип альянсу полягає в тому, що без викупу ці кіберзлочинці не зможуть діяти настільки ефективно. Буде створено дві платформи для обміну інформацією: одну Литвою, а іншу спільно Ізраїлем та ОАЕ.

*Наскільки велика проблема?*

За останні роки було багато прикладів гучних зломів. За даними платформи даних Statista, минулого року організаціями було виявлено 493 мільйони спроб атак програм-вимагачів, що в першій половині 2023 року склало 449,1 мільйона доларів у вигляді криптовалютних платежів зловмисникам-вимагачам. Згідно з даними, ця цифра на 175,8 мільйона доларів більше, ніж за аналогічний період минулого року. для Chainalysis, американської компанії з аналізу блокчейнів.

Аналітики додають, що якщо так триватиме й надалі, зловмисники-вимагачі матимуть другий найкращий рік в історії.

Згідно зі статистикою кіберзлочинності, зібраною Tech.co, середньостатистичний зловмисник вимагає 1,5 мільйона доларів у 2023 році. Однак понад 80% тих, хто заплатить викуп, будуть перенацілені під час іншої атаки.

*Як компанії можуть захистити себе*

Атаки програм-вимагачів починаються з простих електронних листів у 69% випадків і найчастіше націлені на компанії, які є легкою мішенню та недостатньо зміцнили свою безпеку.

Атаки програм-вимагачів можуть мати руйнівний вплив на бізнес. У 40% випадків компанії, які постраждали від атаки програм-вимагачів, звільняють співробітників.

Хоча загрози зростають і захиститися від них стає набагато важче, найгірше, що ви можете зробити, — це нічого не зробити. Ось кілька порад щодо захисту вашої компанії:

Інвестуйте в кібербезпеку, як і в інший бізнес.

Захищене обладнання.

Шифрувати дані.

Навчіть співробітників передовим практикам кібербезпеки.

Використовуйте засоби захисту від зловмисного програмного забезпечення та ефективні брандмауери.

Оновлюйте операційні системи та програмне забезпечення.

Регулярно тестуйте системи резервного копіювання та безпеки.

Використовуйте сторонніх постачальників з високими стандартами безпеки.

Розгляньте страхування кібербезпеки.

Не ігноруйте перші ознаки злому». ***(Abby Ward. 50 Countries Set to Ruin Every Ransomware Hacker's Day // Marketing VF Ltd. (https://tech.co/news/us-anti-cybercrime-alliance?utm_source=flipboard&utm_content=other). 02.11.2023).***

***

**«Компанія Shimano, провідний виробник компонентів для велосипедів, стала мішенню атаки програм-вимагачів, яка вразила 4,5 терабайта конфіденційних даних компанії.**

Як повідомляється, японський виробник, став мішенню групи програм-вимагачів LockBit, яка погрожує оприлюднити дані 5 листопада 2023 року о 18:34:13 UTC.

Вперше про це повідомив Escape Collective, про атаку також зазначено в Live Ransomware Updates на веб-сайті Ransom-db, де Shimano.com показано як жертву LockBit 3.0, а датою атаки є 2 листопада 2023 року.

Його також зазначено на сайті Ransomlook.io, який описується як проект із відкритим вихідним кодом, спрямований на допомогу користувачам у відстеженні публікацій і дій, пов'язаних із програмами-вимагачами, на різних сайтах, форумах і в каналах Telegram, де можна побачити повне повідомлення про викуп.

У повідомленні стверджується, що група зламала дуже конфіденційні дані, зокрема:

Інформація про співробітника, включаючи ідентифікаційні номери, номери соціального страхування, адреси та скани паспортів

Фінансові документи, включаючи баланси, звіти про прибутки та збитки, банківські виписки, різні податкові форми та звіти

Дані клієнта, включаючи адреси, внутрішні документи, поштову кореспонденцію, конфіденційні звіти, юридичні документи та результати інспекції фабрики

Інші документи, включаючи угоди про нерозголошення, контракти, конфіденційні схеми та креслення, матеріали розробки та лабораторні випробування

Зловмисник, LockBit, є кіберзлочинною групою, яка використовує зловмисне програмне забезпечення для зламу конфіденційних даних компанії, а потім намагається вимагати гроші в обмін на те, щоб уникнути його публічного оприлюднення.

Компанія Flashpoint, яка займається захистом кіберзлочинності , описує її як «найактивнішу» групу програм-вимагачів у світі, кажучи, що вона несе відповідальність за 27,93% усіх відомих атак програм-вимагачів за 12 місяців до

червня 2023 року. Загальна кількість жертв 1036 осіб більш ніж удвічі перевищує показник група BlackCat на другому місці.

Shimano — лише остання в низці відомих жертв групи LockBit. За даними Trendmicro, британська поштова служба Royal Mail зазнала атаки в січні, що фактично призупинило її міжнародні експортні послуги. У лютому дублінська компанія-виробник програмного забезпечення Ion Group постраждала, а в червні тайванський виробник мікросхем TSMC зіткнувся з викупом у 70 мільйонів доларів США.

Гігант з виробництва літаків Boeing також в даний час вимагається групою.

Коли представник Cyclingnews зв'язався з представником Shimano, він сказав: «Це внутрішня справа Shimano, яка розслідується, однак наразі ми не можемо нічого коментувати».

Наразі незрозуміло, який викуп (якщо такий вимагав) вимагала група, але ясно, що ця новина стане ще одним серйозним ударом у важкий період для японського бренду.

Лише минулого місяця компанія оголосила про відкликання 2,8 мільйона дорожніх шатунів у всьому світі через давню проблему роз'єднання. Через кілька тижнів колективний позов у Північній Америці було подано. В останньому квартальному звіті повідомляється, що загальні продажі велосипедних компонентів впали на 24,8%, а операційний прибуток впав майже вдвічі». ***(Josh Croxton. Shimano hit by ransomware attack // Future Publishing Limited Quay House (https://www.cyclingnews.com/news/shimano-hit-by-ransomware-attack/?utm_source=flipboard&utm_content=Cyclingnews%2Fmagazine%2FCycling+Gear+and+Tech+-+Cyclingnews). 03.11.2023).***

***

**«Спільнота кібербезпеки багато говорить про атаки програм-вимагачів: хто є останніми групами програм-вимагачів, типові вектори атак, скільки компанії виплачують викуп і які протоколи реагування на інциденти мають команди безпеки.**

Це все має значення, звичайно. Однак загалом служби безпеки вже знають про загрозу програм-вимагачів завдяки особистому досвіду. У 2023 році 81% компаній постраждали від програм-вимагачів за попередні 12 місяців. Наслідки, про які повідомляється, дуже різні: від необхідності придбати рішення для боротьби з атаками програм-вимагачів до активного нападу та фактичної сплати викупу. Незважаючи на це, кількість компаній, уражених програмами-вимагачами, залишається стабільно високою з 2021 року.

Далекосяжні наслідки програм-вимагачів у поєднанні з тим фактом, що ми наближаємося до другого найдорожчого року для програм-вимагачів в історії, означають, що настав час ще раз поглянути на проблему програм-вимагачів і подумати про вирішення її під новим кутом зору. Придивившись уважніше до того, як взагалі відбуваються атаки програм-вимагачів – за допомогою засобів, які, можливо, ще не знаходяться на радарах команд безпеки, – ми можемо швидше помітити попереджувальні знаки та діяти на них, щоб повністю захиститися від атак.

*Як зазвичай запускається програма-вимагач*

Почнемо з однієї з найпоширеніших точок входу для атаки програм-вимагачів: скомпрометовані облікові дані.

Злочинці люблять облікові дані автентифікації, тому що вони є надійним важелем для отримання доступу до систем та інформації, які дозволяють їм вчиняти злочини. Зловмисники часто отримують облікові дані за допомогою зловмисного програмного забезпечення infostealer, яке зазвичай розгортається через шкідливі веб-сайти, ботнети або фішингові електронні листи.

Одним клацанням миші користувач може заразитися, дозволяючи шкідливому програмному забезпеченню викрасти широкий спектр інформації, що зберігається на комп’ютері користувача – від особистих даних, таких як номери кредитних карток, до імен користувачів і паролів і навіть файлів cookie веб-сеансу, які відкривають двері до корпоративних ресурси.

І коли одні двері відчиняються, часто відкриваються й інші. Дослідження SpyCloud показує, що 72% користувачів, чиї дані були розкриті в результаті двох

або більше зломів у 2022 році, повторно використовували свої паролі в різних програмах. Це означає, що майже троє з чотирьох людей активно використовували зламаний пароль, завдяки чому зловмисникам було досить легко отримати одну розкриту пару облікових даних і отримати доступ до їх інформації та файлів у кількох облікових записах, включаючи робочі програми.

*Що говорять нові дослідження про зловмисне програмне забезпечення infostealer*

Ось тут стає цікаво. Завдяки обліковим даним доступу, отриманим за допомогою зловмисного програмного забезпечення infostealer, зловмисники можуть з'єднати точки, щоб потім викрасти, зашифрувати та отримати викуп конфіденційних або пропрієтарних даних у системі підприємства, запускаючи повномасштабну атаку програм-вимагачів. Вперше передові дослідження підтверджують, що це роблять (принаймні деякі) суб'єкти загрози. Наявність зараження infostealer справді є раннім попереджувальним сигналом про потенціал програм-вимагачів.

У вибірці північноамериканських і європейських компаній, які зазнали атаки програм-вимагачів у 2023 році, майже кожна третя була інфікована зловмисним програмним забезпеченням infostealer за кілька місяців до атаки (Звіт про захист від програм-вимагачів SpyCloud 2023).

*Що це означає для команд безпеки?*

Як сигнал ризику, наявність зловмисного програмного забезпечення інфокрадію має викликати радар компаній-вимагачів і спонукати до комплексної реакції на усунення зловмисного програмного забезпечення.

Ми не можемо з упевненістю сказати, що атака програми-вимагача щоразу слідує за зараженням шкідливим програмним забезпеченням infostealer. Лише самі суб'єкти загроз знають, як вони збираються використовувати інформацію, яку вони викрадають. Але присутність зловмисного програмного забезпечення infostealer є хорошою відправною точкою для кращого захисту та запобігання.

Ми можемо використати цю відправну точку, щоб побудувати ширшу картину та зрозуміти роль, яку грають викрадачі інформації в атаці програм-

вимагачів. Це покращить обізнаність про потенційні загрози та краще інформує про пріоритети та тактику захисту безпеки.

Отже, як ми можемо використати роль інфокрадіючих інфекцій у ланцюжку знищення програм-вимагачів?

По-перше, ми розширюємо нашу перспективу. Ми оцінюємо обставини, які передували зараженню. Виправлення пріоритетів, які зосереджені на вразливостях, які можна використати, наприклад, можуть ускладнити входження суб'єкта загрози. Навчання з питань безпеки, яке відповідає сучасним методам зловмисників, може мати подібний пом'якшувальний вплив на ризик зловмисного програмного забезпечення-викрадача інформації.

Ми також розглядаємо кроки, які зловмисник, ймовірно, зробить після зараження, і дані, до яких вони мають доступ. Можливо, цільовою метою актора є облікові дані єдиного входу та додатковий доступ до програм. Або, можливо, зловмисники шукають криптогаманці.

Збір і оцінка сигналів навколо зловмисного програмного забезпечення infostealer може пролити світло на статус і обставини компанії та допомогти належним чином знайти шкідливе програмне забезпечення infostealer у ланцюжку знищення програм-вимагачів. Ці додаткові сигнали додадуть контексту та нюансів у наше розуміння зловмисного ПЗ infostealer і можуть навіть самі послужити додатковими сигналами раннього попередження.

По-друге, ми діємо на основі того, що знаємо, і продовжуємо спостерігати. Ми приступаємо до моніторингу та усунення заражень шкідливим програмним забезпеченням infostealer і вживаємо заходів для обмеження потенційної шкоди, яка може виникнути внаслідок викрадання даних.

Потім ми продовжуємо збирати та оцінювати дані та сигнали, оскільки компанії або стають жертвами зловмисників-вимагачів, або уникають їх. З часом ці сигнали виявлятимуть шаблони, які ще більше контекстуалізують зв'язок інфокрадії та програм-вимагачів. Вони дозволять дослідникам використовувати широкомасштабну аналітику та алгоритми машинного навчання, щоб зрозуміти це, вчитися на цьому та використовувати для підтримки оборонної тактики.

У боротьбі з програмами-вимагачами найкращий захист — це той, який базується на даних і відповідає загрозам, з якими стикається компанія. Вразливість організації до атак програм-вимагачів частково залежатиме від її унікального середовища, характеристик і потреб. Проте наше дослідження в SpyCloud показує, що зв'язок між зараженням інфо-викрадачами та атаками програм-вимагачів зберігається незалежно від форми чи розміру компанії.

Якщо це так, план запобігання програм-вимагачів можна вважати комплексним, лише якщо він включає моніторинг та усунення впливу зловмисного програмного забезпечення інфокрадії». ***(Wallis Romzek. The ransomware warning sign we should all have on our radar // World Economic Forum (https://www.weforum.org/agenda/2023/11/the-ransomware-warning-sign-we-should-all-have-on-our-radar/?utm_source=flipboard&utm_content=justiz2015%2Fmagazine%2FSOFTWARE+%2F+DATA+%2FSECURITY+%2FPRIVACY). 08.11.2023).***

***

**«Повільно, але впевнено роздрібні продавці програють битву з операторами програм-вимагачів, стверджує тривожний новий звіт.**

Опитавши 3000 лідерів у сфері інформаційних технологій та кібербезпеки в малих і середніх компаніях і на підприємствах по всьому світу (включаючи 355 представників галузі роздрібної торгівлі), Sophos виявила, що лише 26% роздрібних торговців змогли запобігти атаці програм-вимагачів до того, як їх дані були зашифровані. Минулого року було 28%, а позаминулого – 34%.

Опитування має стати тривожним дзвіночком для організацій у секторі роздрібної торгівлі, стверджує Честер Вишневскі, директор глобального технічного директора Sophos, кажучи, що роздрібні торговці мають посилити заходи безпеки вже зараз.

*Більш тривале відновлення*

Не кожна жертва платить вимогу викупу. Але серед тих, хто це зробив, середня вартість відновлення (без урахування викупу) у чотири рази перевищувала

вартість відновлення тих, у кого була робоча резервна копія (3 мільйони доларів США та 750 000 доларів США відповідно).

Звіт Sophos показав, що понад два з п’яти (43%) сплатили вимогу викупу. «У таких ситуаціях немає ярликів, і майже завжди потрібна перебудова систем. Краще позбавити злочинців їхньої здобичі та відбудувати краще», – сказав Вишневський.

Хороша новина для роздрібних торговців (але не для всіх інших) полягає в тому, що відсоток роздрібних фірм, які стали мішенню програм-вимагачів, знизився з 77% минулого року до 69% цього року. Проте відсоток компаній, які одужали менш ніж за добу, знизився з 15% до 9%. Водночас відсоток тих, кому знадобилося на це більше місяця, зріс з 17% до 21%.

Програми-вимагачі зазвичай починаються з того, що необачний працівник завантажує зловмисне програмне забезпечення або якимось чином надає зловмисникам доступ до своїх кінцевих точок. Отже, найкращий захист від програм-вимагачів починається з навчання співробітників небезпеці кібератак.

Також допомагає резервне копіювання ключових систем і даних, а також встановлення служб захисту кінцевих точок». ***(Sead Fadilpašić. Many retailers are struggling to deal with ransomware attacks // Future US, Inc. (https://www.techradar.com/pro/security/many-retailers-are-struggling-to-deal-with-ransomware-attacks?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 08.11.2023).***

***

**«Цього тижня Сполучені Штати приєдналися до 39 інших країн у Міжнародній ініціативі протидії вимагачам, намагаючись зупинити потік платежів викупу кіберзлочинцям.** Ініціатива спрямована на усунення фінансування злочинців шляхом кращого обміну інформацією про рахунки для сплати викупу. Держави-члени розроблять дві платформи для обміну інформацією: одну створить Литва, а іншу спільно Ізраїль та Об’єднані Арабські Емірати. Учасники ініціативи будуть ділитися «чорним списком» через Міністерство

фінансів США, включаючи інформацію про цифрові гаманці, які використовуються для переміщення платежів програм-вимагачів. Нарешті (у цікавому об'єднанні двох останніх надто великих елементів квитка в технології), ініціатива використовуватиме штучний інтелект для аналізу блокчейнів криптовалюти для виявлення злочинних транзакцій.

У той час як урядовці майже одноголосно радять не платити викупи, організації, які потрапили під атаку програм-вимагачів, часто платять, щоб уникнути збентеження та знизити витрати на реагування на інциденти та пом'якшення наслідків. Однак у макросі сплата викупу призводить до зростання вимог щодо викупу та ескалації активності програм-вимагачів. Ця ініціатива може вирішити ці довгострокові тенденції». ***(Blair Robinson. 40 Countries Including US Vow Not to Pay Ransomware // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2023/11/40-countries-including-us-vow-not-to-pay-ransomware/). 03.11.2023).***

***

**«Toyota Financial Services (TFS) підтвердила, що виявила несанкціонований доступ до деяких своїх систем у Європі та Африці після того, як програма-вимагач Medusa атакувала компанію.**

Toyota Financial Services, дочірня компанія Toyota Motor Corporation, є глобальною організацією, яка представлена на 90% ринків, на яких Toyota продає свої автомобілі, надаючи автофінансування своїм клієнтам.

Раніше сьогодні банда програм-вимагачів Medusa включила TFS до свого сайту витоку даних у темній мережі, вимагаючи виплати 8 000 000 доларів США за видалення даних, імовірно вкрадених у японської компанії.

Зловмисники дали Toyota 10 днів на відповідь з можливістю продовження терміну за 10 000 доларів на день.

Хоча Toyota Finance не підтвердила, чи дані були вкрадені під час атаки, зловмисники стверджують, що викрали файли, і погрожують витоком даних, якщо викуп не буде сплачено.

Щоб підтвердити вторгнення, хакери опублікували зразки даних, які включають фінансові документи, електронні таблиці, рахунки-фактури, хешовані паролі облікових записів, ідентифікатори та паролі користувачів у відкритому тексті, угоди, скани паспортів, внутрішні організаційні діаграми, звіти про фінансову діяльність, електронні адреси співробітників тощо.

Medusa також надає файл.TXT з файловою структурою дерева всіх даних, які вони, як стверджують, вкрали з систем Toyota.

Більшість документів написано німецькою мовою, що свідчить про те, що хакерам вдалося отримати доступ до систем, які обслуговують діяльність Toyota у Центральній Європі.

BleepingComputer звернувся до японського автовиробника, щоб прокоментувати витік даних, і представник компанії зробив наступну заяву:

«Toyota Financial Services Europe & Africa нещодавно виявила несанкціоновану діяльність у системах в обмеженій кількості своїх місць».

«Ми відключили певні системи, щоб розслідувати цю діяльність і зменшити ризик, а також почали співпрацювати з правоохоронними органами».

«На даний момент цей інцидент обмежений Toyota Financial Services Europe & Africa».

Що стосується статусу постраждалих систем і їх очікуваного повернення до нормального функціонування, речник повідомив нам, що процес відновлення роботи систем уже триває в більшості країн.

*Ще одне порушення Citrix Bleed?*

Раніше сьогодні, після того, як Medusa розкрила TFS як свою жертву, аналітик безпеки Кевін Бомонт підкреслив, що в німецькому офісі фірми була доступна в Інтернеті кінцева точка Citrix Gateway, яка не оновлювалася з серпня 2023 року, що вказує на те, що вона була вразлива до критичної Citrix Bleed (CVE-2023-4966) проблема безпеки.

Кілька днів тому було підтверджено, що оперативники програм-вимагачів Lockbit використовували загальнодоступні експлойти для Citrix Bleed, щоб досягти

зломів проти Industrial and Commercial Bank of China (ICBC), DP World, Allen & Overy і Boeing.

Цілком можливо, що інші групи програм-вимагачів почали використовувати Citrix Bleed, користуючись перевагами масивної поверхні атаки, яка нараховує кілька тисяч кінцевих точок». ***(Bill Toulas. Toyota confirms breach after Medusa ransomware threatens to leak data // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/toyota-confirms-breach-after-medusa-ransomware-threatens-to-leak-data/?utm_source=flipboard&utm_content=KevinCarrol78tk%2Fmagazine%2Fsysadmin). 16.11.2023).***

***

**«Одна з найактивніших у світі груп програм-вимагачів застосувала незвичайну — якщо не безпрецедентну — тактику, щоб змусити одну зі своїх жертв заплатити: повідомила про жертву Комісію з цінних паперів і бірж США.**

Про тактику тиску стало відомо в публікації, опублікованій у середу на темному веб-сайті AlphV, злочинного синдикату програм-вимагачів, який діє вже два роки. Після того, як вперше заявили, що зламали мережу публічної цифрової кредитної компанії MeridianLink, представники AlphV опублікували скріншот скарги, надісланої до SEC через веб-сайт агентства. Згідно з нещодавно прийнятим правилом, яке набуде чинності наступного місяця, публічні компанії повинні подати звіт про розкриття SEC протягом чотирьох днів після того, як дізнаються про інцидент безпеки, який мав «істотний» вплив на їхній бізнес.

«Ми хочемо привернути вашу увагу до питання щодо відповідності MeridianLink нещодавно прийнятим правилам розкриття інцидентів кібербезпеки», — написали представники AlphV у скарзі. «Нашій увазі стало відомо, що MeridianLink у світлі значного порушення даних клієнта та оперативної інформації не подав необхідне розкриття інформації згідно з пунктом 1.05 форми 8-K протягом чотирьох робочих днів, передбачених новою правила SEC».

Категорія порушення, вибрана в онлайн-звіті, була «Істотне викривлення або упущення в документах або фінансових звітах компанії або їх ненадання».

Повідомлення в темній мережі в середу також включало те, що, здавалося, було автоматичною відповіддю, отриманою від SEC, що підтверджує отримання скарги.

Як зазначалося, правило ще не набуло чинності, тому навіть якщо порушення відповідає юридичному визначенню суттєвої події, навряд чи MeridianLink буде порушувати. Тим не менш, AlphV, ймовірно, використовує занепокоєння в галузі, викликане нещодавнім рішенням SEC подати до суду на головного спеціаліста з інформаційної безпеки SolarWinds. SEC стверджувала, що керівник SolarWinds ввів інвесторів в оману щодо практики кібербезпеки компанії перед кібератакою російських хакерів у 2020 році, які потім заразили 18 000 клієнтів SolarWinds шкідливим програмним забезпеченням.

Офіційні особи MeridianLink відхилили запит на інтерв'ю чи відповіді на запитання про те, чи дані клієнта були зламані під час вторгнення в мережу, чи відбулася атака на безпеку, яку можна вважати істотною. Натомість компанія опублікувала заяву, в якій підтвердила, що офіційні особи виявили «інцидент кібербезпеки», і продовжила:

Виявивши загрозу, ми негайно вжили заходів, щоб стримати загрозу, і залучили групу сторонніх експертів для розслідування інциденту. На основі нашого розслідування на сьогоднішній день ми не виявили доказів несанкціонованого доступу до наших виробничих платформ, і інцидент спричинив мінімальні перерви в роботі. Якщо ми визначимо, що будь-яка особиста інформація споживача була залучена до цього інциденту, ми надамо сповіщення, як того вимагає закон.

Бретт Каллоу, аналітик безпеки з Emsisoft, зазначив, що група програм-вимагачів, відома як Maze, раніше попереджала жертв, що вона «підтримує зв'язок з основними органами регулювання цінних паперів і фінансів і визнає їх про всі витоки даних і порушення, якщо угода не буде досягнута».

«Я не впевнений, чи вони це робили насправді», — сказав Келлоу Ars. «Банди також погрожували скаргами щодо GDPR, і IIRC, можливо, хтось дійсно

виконав це». Він сказав, що йому невідомо, щоб якась група подала скаргу до SEC. GDPR є скороченням від Загального регламенту захисту даних, закону Європейського Союзу, який надає особам широкий захист конфіденційності.

AlphV вперше з'явився в листопаді 2021 року та відомий тим, що використовує програмне забезпечення-вимагач під назвою BlackCat, розроблене на мові сценаріїв Rust. Група націлена як на середовища Windows, так і на Linux.

«Станом на квітень 2023 року ALPHV перетворилася на одну з найпотужніших груп програм-вимагачів у поточному ландшафті загроз, поступаючись лише групі програм-вимагачів Lockbit у спостережуваній активності», — писав у травні аналітик із геополітики та кібербезпеки Кріс Лукас. «Будучи групою, що базується в основному в Росії, ALPHV навряд чи буде орієнтуватися на організації, що базуються в Російській Федерації або в інших країнах Співдружності Незалежних Держав (СНД), які складають колишній Радянський Союз».

Група вже була відома незвичайною практикою погроз запустити розподілені атаки на відмову в обслуговуванні на цілі, які вона вже скомпрометувала, намагаючись застосувати додатковий тиск для оплати.

Під час торгів у четвер акції MeridianLink впали на 0,2 відсотка, або 4 центи, до 18,51 долара». ***(Dan Goodin. Ransomware group reports victim it breached to SEC regulators // Condé Nast (https://arstechnica.com/security/2023/11/ransomware-group-reports-victim-it-breached-to-sec-regulators/?utm_source=flipboard&utm_content=user%2FArsTechnica). 17.11.2023).***

***

**«Малі та великі компанії, схоже, не думають, що стануть жертвами атак програм-вимагачів, але в той же час обидва дуже стурбовані впливом і розвитком таких атак.**

В опитуванні, проведеному OpenText, більшість малих і середніх підприємств і підприємств (які мають понад 1000 співробітників) не вважали або не були впевнені, що вони є цілями програм-вимагачів. Проте, дещо навпаки, 90% малих і

середніх підприємств і 87% підприємств також дуже або певною мірою стурбовані атаками програм-вимагачів.

Більше половини (54%) малих і середніх компаній і підприємств також сказали, що відчувають більший ризик атак програм-вимагачів завдяки використанню ШІ зловмисниками для підвищення їх ефективності. У відповідь 57% малих і середніх підприємств і 53% підприємств планують збільшити свої бюджети на кібербезпеку наступного року.

*Збільшення витрат і персоналу*

З малих і середніх підприємств, які планують збільшити бюджети, 40% мають на меті збільшити свої витрати на 5-10%, тоді як 33% мають на меті збільшення на 10-20%. Подібні цифри стосувалися і підприємств.

44% малих і середніх підприємств також планують мати більше працівників із кібербезпеки, а 50% хочуть збільшити кількість працівників на 5-10%. 43% підприємств також хотіли б збільшити кількість співробітників у сфері кібербезпеки, а 46% хотіли б збільшити штат на 5-10%.

Наразі 52% малих і середніх підприємств передають свою кібербезпеку MSP або постачальникам каналів, тоді як 42% підприємств роблять те саме, за винятком того, що для цих фірм ця кількість зростає.

Коментуючи результати опитування, виконавчий віце-президент OpenText Cybersecurity Прентіс Донох'ю сказав: «Переконання «зі мною цього не трапиться» є ризикованим мисленням. Кібератаки стають все більш поширеними і можуть мати серйозні наслідки; жоден бізнес не застрахований від них. напад».

Він додав: «хоч багато компаній вживають правильних захисних заходів, таких як використання контролю доступу, розгортання резервного копіювання та моніторингу загроз, багаторівневий підхід до безпеки, який включає освіту, залишається найкращим захистом від програм-вимагачів».

Судячи зі збільшення кількості та складності атак програм-вимагачів цього року, частково завдяки штучному інтелекту, здається, що компанії мають рацію, щоб хвилюватися». ***(Lewis Maddison. Businesses are more worried about ransomware attacks than ever - but they still don't think it'll happen to them // Future US, Inc.***

***(https://www.techradar.com/pro/security/businesses-are-more-worried-about-ransomware-attacks-than-ever-but-they-still-dont-think-itll-happen-to-them?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 16.11.2023).***

***

**Міжнародна ініціатива з боротьби з програмами-вимагачами (CRI) — це міжнародна ініціатива, до якої входять 48 країн, Європейський Союз та Інтерпол.** Сполучені Штати є визначним членом цієї групи не лише через проведення цієї щорічної зустрічі, але й через виконання функцій Секретаріату CRI. CRI має на меті «підірвати життєздатність програм-вимагачів, переслідувати суб'єктів загрози, боротися з незаконним фінансуванням, що лежить в основі екосистеми програм-вимагачів, співпрацювати з приватним сектором для захисту від атак програм-вимагачів і співпрацювати на міжнародному рівні для вирішення всіх елементів загроз програм-вимагачів». CRI зосереджується на партнерстві та обміні інформацією для зміцнення колективної безпеки від загроз програм-вимагачів.

CRI було створено, щоб протистояти зростанню загроз і активності програм-вимагачів. Атака програм-вимагачів відрізняється від інших кібератак тим, що хакери шифрують дані організації, а потім вимагають оплату в обмін на передачу їм даних у незашифрованому вигляді. У деяких сценаріях зловмисники також погрожуватимуть не лише зберегти зашифровані дані, але й оприлюднити конфіденційні дані, якщо викуп не буде сплачено.

У Сполучених Штатах жертви програм-вимагачів заплатили 1,5 мільярда доларів у вигляді викупу з травня 2022 року по червень 2023 року. Американські організації також залишаються головною ціллю; За словами Енн Нойбергер, заступника радника з національної безпеки США, американці піддаються 46% глобальних кібератак.

*Застава*

1 листопада всі члени CRI схвалили зобов’язання не сплачувати державні викупи за атаки програм-вимагачів. Однак застава не забороняє прямих платежів; натомість обіцянка дозволяє урядам приймати індивідуальні рішення щодо виплати викупу та як можуть застосовуватися винятки для надзвичайних ситуацій. Надзвичайні ситуації можуть включати атаки програм-вимагачів на певні об’єкти, як-от лікарні, де здоров’я пацієнтів знаходиться під безпосереднім ризиком. Щоб досягти цілей спільної політичної заяви, CRI збирається створити, через зобов’язання Міністерства фінансів США обмінюватися даними про незаконні гаманці, чорний список цифрових гаманців, які використовуються для здійснення діяльності програм-вимагачів.

Застава також обмежена державними установами; у Сполучених Штатах застава поширюється лише на діяльність федеральних агенцій і звільняє державні та місцеві юрисдикції. Підприємства можуть продовжувати приймати рішення щодо платежів на основі власного аналізу витрат і вигод під час програми-вимагача. Однак, навіть без прямої заборони платежів, заява, підтримана 48 країнами, надсилає чітке повідомлення зловмисникам про те, що вони не повинні очікувати від урядів мовчазної згоди на їхні вимоги.

Ініціативи CRI

На додаток до обіцянки, CRI вживає кількох заходів для розширення співпраці між членами. Як було оголошено під час третьої щорічної зустрічі, найближчим часом буде запущено дві нові платформи для обміну інформацією. Перша — платформа обміну інформацією про зловмисне програмне забезпечення, розроблена Литвою. Другий — Crystal Ball, платформа обміну інформацією з базами даних, платформами віртуальної координації та списками контактів, створена як спільний проект Ізраїлю та ОАЕ. Ці платформи дозволять членам ділитися деталями про атаки програм-вимагачів, підозрюваних зловмисників, поточні розслідування тощо, щоб допомогти в колективних зусиллях зупинити атаку до того, як жертву вимагають. CRI сподівається, що учасники ділитимуться в середньому однією інформацією щотижня на платформах, щоб забезпечити потік інформації.

Інші результати третього щорічного саміту включали запуск проекту, який використовуватиме штучний інтелект для аналізу даних ланцюга блоків і протидії програмному забезпеченню-вимагачу. На додаток до зобов'язань щодо виплат, кілька членів також зобов'язалися «допомагати будь-якому члену CRI у реагуванні на інциденти, якщо їхні урядові сектори або сектори рятувальних служб постраждали від атаки програм-вимагачів». Нарешті, новим членам CRI буде запропоновано наставництво та можливості програми тактичного навчання для розвитку свого кіберпотенціалу.

Протягом наступного року CRI планує продовжувати залучати нових членів, краще розуміти фінансову модель атак програм-вимагачів і ділитися інформацією для нарощування національного потенціалу боротьби з програмами-вимагачами.

Робота CRI спиратиметься на інші види діяльності, спрямовані на програмне забезпечення-вимагач, у Сполучених Штатах і доповнюватиме їх. Наприклад, Joint Ransomware Task Force — це міжвідомчий орган, який координує федеральні інструменти для протидії атакам програм-вимагачів шляхом розробки найкращих практик, проведення розслідувань, надання вказівок і обміну інформацією. Цільову групу спільно очолюють Агентство з кібербезпеки та безпеки інфраструктури та Федеральне бюро розслідувань. Цільова група створила та оновила «єдиний ресурс», щоб допомогти організаціям захистити свої приміщення, персонал і клієнтів від загроз програм-вимагачів за допомогою посібника #StopRansomware. Ми очікуємо, що цільова група продовжуватиме оновлювати вказівки, які вона надає компаніям США, і що вона може включати уроки, отримані з CRI». ***(Brian E. Finch, Aimee P. Ghosh, Amaris Trozzo. Initiative Pledges to Halt Government Ransom Payments, but with Exceptions // Pillsbury Winthrop Shaw Pittman LLP (https://www.pillsburylaw.com/en/news-and-insights/international-counter-ransomware-initiative-government-ransom-payments.html). 21.11.2023).***

***

**«Словенська енергетична компанія Holding Slovenske Elektrarne (HSE) зазнала атаки програм-вимагачів, яка скомпрометувала її системи та**

**зашифровані файли, але компанія заявляє, що інцидент не порушив виробництво електроенергії.**

HSE є найбільшою генеруючою компанією Словенії, на яку припадає приблизно 60% внутрішнього виробництва, і вона вважається критичною інфраструктурою в країні.

Заснована в 2001 році урядом Словенії та належить державі, компанія керує кількома гідроелектростанціями, тепловими та сонячними електростанціями, а також вугільними шахтами по всій країні, а також володіє дочірніми компаніями в Італії, Сербії та Угорщині.

Як вперше повідомило місцеве інформаційне видання 24ur.com у суботу, минулої середи HSE зазнала атаки програм-вимагачів, і компанія нарешті стримала її в п'ятницю, 24 листопада.

Директор Управління інформаційної безпеки Урош Свете повідомив ЗМІ, що масштабна кібератака не вплинула на роботу з виробництва електроенергії. І все ж IT-системи та файли були «заблоковані» «криптовірусом».

Організація негайно повідомила Національне управління з кіберінцидентів Si-CERT і поліцейську адміністрацію Любляни та залучила зовнішніх експертів, щоб пом'якшити атаку та запобігти поширенню вірусу на інші системи по всій Словенії.

Наразі організація не отримала вимоги про викуп, але заявила, що, можливо, ще занадто рано для цього, тому вони залишаються у стані підвищеної готовності, оскільки очищення системи все ще триває.

Сьогодні Урош Свете видав спільну заяву з генеральним директором HSE Томажем Щокелем, запевнивши громадськість, що ситуація під контролем і що через цей інцидент не очікується жодних збоїв у роботі чи значних економічних збитків.

За словами речників, порушення обмежується веб-сайтами ТЕС Шоштань і вугільної шахти Веленьє.

*Палець вказав на Рисіду*

Неофіційна інформація, надана місцевим ЗМІ, приписує атаку банді програм-вимагачів Rhysida, яка була активна останнім часом, що спонукало ФБР і CISA випустити попередження, у якому висвітлюються TTP (техніки, тактика та процедури) групи.

Якщо Rhysida стоїть за атакою, це також пояснює, чому HSE заявляє, що вони не отримували вимоги про викуп, оскільки нотатки Rhysida про викуп містять лише адресу електронної пошти для зв'язку зі загрозливими суб'єктами без вказівки будь-яких грошових вимог.

Як повідомляється, оператори програм-вимагачів зламали HSE, викравши паролі для систем HSE із незахищеного хмарного сховища.

BleepingComputer не зміг перевірити цю інформацію та зв'язався з HSE, щоб отримати заяву щодо звинувачень, і ми все ще чекаємо на відповідь.

Rhysida вперше була запущена в травні 2023 року, швидко атакуючи організації під час резонансних атак, зокрема на чилійську армію, Prospect Medical і Британську бібліотеку.

Атаки зловмисників на охорону здоров'я спонукали Міністерство охорони здоров'я та соціальних служб США (HHS) випустити попередження про банду програм-вимагачів.

Нещодавно Rhysida розмістила на своєму сайті витоку даних китайський державний електроенергетичний конгломерат, продаючи нібито вкрадені дані за 50 BTC (1 840 000 доларів США)». ***(Bill Toulas. Slovenia's largest power provider HSE hit by ransomware attack // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/?utm_source=flipboard&utm_content=other). 27.11.2023).***

***

## *Виявлені вразливості технічних засобів та програмного забезпечення*

**«Хакери використовують уразливість Citrix Bleed у дикій природі, щоб переслідувати кінцеві точки в державних установах, юридичних організаціях та інших фірмах по всьому світу.**

Про це стверджує дослідник кібербезпеки Mandiant, який нещодавно опублікував звіт, у якому описано принаймні чотири активні кампанії. Акції нібито стартували наприкінці серпня цього року.

Зловмисники використовують Citrix Bleed, відстежуваний як CVE-2023-4966, для націлювання на пристрої NetScaler ADC і NetScaler Gateway. Уразливість має оцінку вразливості 9,4 і використовується для захоплення особистої інформації, такої як облікові дані для входу, і для забезпечення бокового переміщення через скомпрометовану мережу.

*Десятки інструментів*

Очевидно, хакери також залишають дуже мало доказів, перетворюючи криміналістику на кошмар. Однак у своєму аналізі Mandiant заявив, що виявив спроби експлуатації та викрадення сесії за допомогою аналізу запитів WAF, кореляції реєстру Windows і перевірки дампа пам’яті.

Наприкінці жовтня Citrix випустила патч для недоліку та закликала користувачів застосувати його, стверджуючи, що вразливість зловживає в дикій природі.

До реакції Citrix і Mandiant, і CISA попереджали про недолік. Mandiant сказав, що хакери, ймовірно, використовували його для викрадення сеансів автентифікації та викрадення корпоративних даних із серпня. CISA, з іншого боку, не була настільки конкретною, заявивши, що вразливість «невідома», але «використовується в кампаніях програм-вимагачів».

Тим часом хтось опублікував на GitHub доказ концепції під назвою Citrix Bleed.

У Mandiant кажуть, що хакери використовують кілька інструментів у своїх атаках, зокрема net.exe для розвідки Active Directory, netscan.exe для перерахування внутрішньої мережі, 7-zip для стиснення та шифрування даних розвідки, FREEFIRE як бекдор.NET і AnyDesk для керування віддаленим робочим столом - це лише деякі з них.

Не всі інструменти є зловмисними за своєю думкою, але в невірних руках вони можуть завдати значної шкоди». ***(Sead Fadilpašić. Governments around the world are being hacked thanks to Citrix flaws // Future US, Inc. (https://www.techradar.com/pro/security/governments-around-the-world-are-being-hacked-thanks-to-citrix-flaws?utm_source=flipboard&utm_content=TechRadar%2Fmagazine%2FTechRadar%3A+The+Full+Screen). 02.11.2023).***

***

**«Форум груп реагування на інциденти та безпеки (FIRST) офіційно випустив CVSS v4.0, наступне покоління стандарту загальної системи оцінки вразливостей, через вісім років після CVSS v3.0, попередньої основної версії.**

CVSS — це стандартизована структура для оцінки серйозності вразливостей безпеки програмного забезпечення, яка використовується для призначення числових балів або якісного представлення (таких як низький, середній, високий і критичний) на основі можливості використання, впливу на конфіденційність, цілісність, доступність і необхідні привілеї з вищими бали, що позначають більш серйозні вразливості.

Він допомагає визначати пріоритетність реакцій на загрози безпеці, оскільки забезпечує послідовний спосіб оцінки впливу вразливостей і порівняння ризиків у різних системах і програмному забезпеченні.

«Переглянутий стандарт пропонує більш дрібну деталізацію базових показників для споживачів, усуває неоднозначність оцінки в нижній частині,

спрощує показники загроз і підвищує ефективність оцінювання вимог безпеки до середовища, а також компенсаційних засобів контролю», — сказав FIRST.

«Крім того, було додано кілька додаткових показників для оцінки вразливості, включно з автоматичним (можливим черв'яками), відновленням (стійкість), щільністю цінності, зусиллями реагування на вразливість і терміновістю постачальника.

«Ключовим удосконаленням CVSS версії 4.0 також є додаткова застосовність до OT/ICS/IoT із показниками безпеки та значеннями, доданими до груп показників Supplemental та Environmental».

Ця остання версія також додає нову номенклатуру з базовим (CVSS-B), базовим + загрозою (CVSS-BT), базовим + екологічним (CVSS-BE) і базовим + загрозою + екологічним (CVSS-BTE) рейтингами серйозності.

Повний перелік усіх змін, які постачаються зі стандартом CVSS v4.0, включаючи більш детальну деталізацію за допомогою нових базових показників/значень і кращих показників впливу, доступний тут.

FIRST оприлюднив CVSS 4.0 у червні під час своєї 35-ї щорічної конференції в Монреалі, Канада, як «кардинальний фактор, що змінив кіберсектор», через 18 років після випуску CVSS версії 1 у лютому 2005 року.

«Система CVSS швидко розвивалася протягом останніх 18 років, причому кожна версія базувалася на наших можливостях захисту від кіберзлочинності. Я надзвичайно пишаюся CVSS-SIG за наполегливу роботу та самовідданість, які знадобилися для створення версії 4.0. І це своєчасно, оскільки ми продовжуємо спостерігати значне зростання загроз у всьому світі», – сказав Кріс Гібсон, генеральний директор FIRST.

«Як членська організація, наша мета полягає в тому, щоб розширити можливості наших членів і сектор, демонструючи лідерство та гарантуючи, що ми постійно вдосконалюємо те, як ми працюємо разом, щоб захистити людей по всьому світу від кібератак».

Минулого року FIRST також опублікував TLP 2.0, останню версію свого стандарту протоколу світлофора (TLP), який використовується в спільноті групи

реагування на інциденти комп'ютерної безпеки (CSIRT) під час обміну конфіденційною інформацією». ***(Sergiu Gatlan. New CVSS 4.0 vulnerability severity rating standard released // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/new-cvss-40-vulnerability-severity-rating-standard-released/?utm_source=flipboard&utm_content=ray_stahl%2Fmagazine%2FCybersecurity+Today). 01.11.2023).***

***

**«Хакери програм-вимагачів схопилися за використання нещодавно виявленої вразливості нульового дня в екземплярах Atlassian Confluence через кілька днів після того, як компанія закликала своїх клієнтів негайно виправити.**

Компанії безпеки Rapid7 і GreyNoise повідомили, що в неділю вони почали виявляти сплеск хакерів, які використовують помилку, яку Atlassian описує як уразливість неналежної авторизації.

У понеділок австралійський розробник робочої області для співпраці та керування вмістом підвищив критичність помилки до 10, максимально можливого за шкалою CVSS.

Дослідники спочатку описали небезпеку від недоліку, відстежуваного як CVE-2023-22518, як знищення даних. Кілька з кібербезпеки фірм заявили, що хакери використовують його для розгортання програм-вимагачів Cerber.

Волонтери служби безпеки з The DFIR Report заявили, що група, яка використовує ім'я «C3RB3R» у записці про викуп, скористалася помилкою Atlassian.

Proofpoint, Cerber увійшов до трійки найкращих варіантів програм-вимагачів 2021 року разом із Ryuk і SamSam За даними. Того року компанія нарахувала 52,5 мільйона атак Cerber, поступившись лише Рюку (93,9 мільйона). Невідомо, чи були ці атаки з боку тієї самої злочинної групи, відповідальної за попередній плідний

запуск Cerber, особливо враховуючи тенденцію повторного використання хакерами програм-вимагачів украдених або розповсюджених штамів програм-вимагачів.

Тривога про програму-вимагач прозвучала після того, як дослідники виявили хакерів, які використовують спеціально створений.zipархівний файл для завантаження веб-оболонки, яка «може дозволити довільне віддалене виконання коду в системі на додаток до видалення даних з екземпляра Confluence», — написала компанія з кібербезпеки Red Canary.

У фірмі заявили, що хакери отримали початковий доступ до вразливих екземплярів Confluence та використовували команди PowerShell для завантаження виконуваного файлу програми-вимагача Cerber з двох адрес інтернет-протоколу. Виконуваний файл зберігається в папці temp і запускається без відображення вікна. VirusTotal зафіксував надсилання двійкового файлу програми-вимагача 1 листопада, припускаючи, що атаки почалися протягом 24 годин після розкриття вразливості – до того, як Atlassian 3 листопада попередив про загальнодоступний експлойт.

Аналіз програми-вимагача Cerber, проведений Red Canary, виявив зв’язки з неіснуючою групою програм-вимагачів Conti. У ньому сказано, що зразок програм-вимагачів Cerber «імовірно був отриманий з матеріалів, виявлених у витоках програм-вимагачів Conti».

Двійковий файл програми-вимагача використовує чіппер потоку ChaCha для шифрування файлів, що узгоджується з останньою відомою збіркою Conti, яка використовує той самий алгоритм шифрування. Двійковий файл містить можливість використовувати AES і RC4 для різних операцій шифрування, подібно до можливостей Conti. Він також підтримує шифрування кількох типів файлів на локальних дисках, а також віддалених спільних файлах. Код Конті просочився в Інтернет у 2022 році, коли група розвалилася на тлі внутрішніх розбіжностей через свою прихильність до Кремля після того, як Росія розпочала загарбницьку війну проти України.

Під час виконання двійковий файл шифрує файли на локальних дисках і в мережевих ресурсах, додає .LOCK3D розширення файлу, створює м’ютекс у

пам’яті, видаляє тіньові копії томів, видаляє нотатки про викуп, а потім видаляє себе, додає він.

Двійковий файл програми-вимагача створює м’ютекс hsfjuukjzloqu28oajh727190об’єкт, щоб гарантувати, що одночасно працює лише один екземпляр шкідливого програмного забезпечення. Дослідники раніше виявили, що цей конкретний м’ютекс використовується для зразків Conti та додаткових сімейств програм-вимагачів. Він нібито походить від витоку коду Conti». ***(Mihir Bagwe. Cerber Ransomware Operators Exploit Latest Atlassian Bug // Information Security Media Group, Corp. (https://www.databreachtoday.com/cerber-ransomware-operators-exploit-latest-atlassian-bug-a-23552?utm_source=flipboard&utm_content=LeBui2014%2Fmagazine%2FSecuCybe). 08.11.2023).***

***

**«У світі кібербезпеки спалахує новий скандал. Група аналізу загроз Google виявила серйозну вразливість у сервері електронної пошти Zimbra, яка призвела до крадіжки даних в урядах Греції, Молдови, Тунісу, В'єтнаму та Пакистану.**

Цей експлойт, відомий як CVE-2023-37580, націлений на поштовий сервер Zimbra Collaboration з метою крадіжки даних електронної пошти, облікових даних користувачів і токенів автентифікації.

Перший випадок використання експлойту стався у Греції наприкінці червня. Зловмисники, які виявили вразливість, відправили електронні листи з експлойтом до однієї з урядових організацій.

Користувачі, які перейшли за посиланням під час входу до свого облікового запису Zimbra, стали жертвами атаки хакерів, їх дані електронної пошти були скомпрометовані, а кіберзлочинці отримали контроль над їхніми акаунтами.

Zimbra опублікувала виправлення для вразливості на Github вже 5 липня, але масове поширення експлойту почалося пізніше, оскільки багато користувачів не оновили програмне забезпечення вчасно.

У середині липня група кіберзлочинців Winter Vivern за допомогою цього експлойту атакувала урядові організації у Молдові та Тунісі. Пізніше невідомий зловмисник використав уразливість для отримання облікових даних урядовців В'єтнаму.

Останній випадок використання експлойту, описаний групою аналізу загроз Google - крадіжка токенів автентифікації з поштового сервера Пакистану. Ці токени використовуються для доступу до заблокованої або захищеної інформації». ***(Уряди одразу п'яти країн стали жертвами хакерів // Internetua (https://internetua.com/uryadi-odrazu-p-yati-krayin-stali-jertvami-hakeriv). 16.11.2023).***

***

**«Дослідники з мережевої фірми Akamai повідомили в четвер, що зловмисники активно використовують дві нові вразливості нульового дня, щоб об'єднати маршрутизатори та відеореєстратори у ворожий ботнет, який використовується для розподілених атак типу «відмова в обслуговуванні».**

Згідно з повідомленням Akamai, обидві уразливості, про які раніше не було відомо їх виробникам і дослідницькому співтовариству безпеки в цілому, дозволяють віддалено виконувати шкідливий код, коли уражені пристрої використовують адміністративні облікові дані за замовчуванням. Невідомі зловмисники використовували zero-days, щоб зламати пристрої, щоб їх можна було заразити Mirai, потужним програмним забезпеченням з відкритим кодом, яке робить маршрутизатори, камери та інші типи пристроїв Інтернету речей частиною ботнету, здатного вести DDoS раніше немислимих розмірів.

Дослідники Akamai повідомили, що один із атакуваних нульових днів знаходиться в одній або кількох моделях мережевих відеореєстраторів. Інший нульовий день знаходиться в «маршрутизаторі бездротової локальної мережі на основі розетки, створеному для готелів і житлових приміщень». Маршрутизатор продається японським виробником, який «виробляє кілька комутаторів і маршрутизаторів». Функція маршрутизатора, яка використовується, є «дуже

поширеною», і дослідники не можуть виключити можливість, що вона використовується в кількох моделях маршрутизаторів, які продаються виробником.

Akamai заявила, що повідомила про вразливості обом виробникам, і що один із них надав гарантії, що виправлення безпеки будуть випущені наступного місяця. Akamai повідомила, що не ідентифікує конкретні пристрої чи виробників, доки не будуть внесені виправлення, щоб запобігти більш широкому використанню нульових днів.

«Хоча ця інформація обмежена, ми вважали своїм обов'язком попередити спільноту про триваючу експлуатацію цих CVE в дикій природі. Існує тонка межа між відповідальним розголошенням інформації, щоб допомогти захисникам, і надмірним поширенням інформації, що може сприяти подальшим зловживанням з боку натовпів загрозливих акторів».

Повідомлення Akamai надає безліч хешів файлів та IP-адрес і доменних адрес, які використовуються в атаках. Власники мережевих відеокамер і маршрутизаторів можуть використовувати цю інформацію, щоб перевірити, чи пристрої в їхніх мережах були ціллю.

Віддалене виконання коду використовує техніку, відому як ін'єкція команди, яка спочатку вимагає від зловмисника автентифікації за допомогою облікових даних, налаштованих на вразливому пристрої. Аутентифікація та ін'єкція здійснюється за допомогою стандартного запиту POST.

В електронному листі дослідник Akamai Ларрі Кешдоллар написав:

«Пристрої зазвичай не дозволяють виконувати код через інтерфейс керування. Ось чому потрібне отримання RCE через ін'єкцію команди.

Оскільки зловмиснику потрібно спочатку пройти автентифікацію, він повинен знати деякі облікові дані для входу, які будуть працювати. Якщо пристрої використовують легко вгадані логіни, такі як admin:password або admin:password1, вони також можуть опинитися під загрозою, якщо хтось спробує розширити список облікових даних».

Він сказав, що обидва виробники були повідомлені, але поки що лише один з них зобов’язався випустити патч, який очікується наступного місяця. Статус виправлення від другого виробника наразі невідомий.

У Cashdollar заявили, що неповне сканування Інтернету показало щонайменше 7000 вразливих пристроїв. Фактична кількість постраждалих пристроїв може бути більшою.

Mirai вперше привернув широку увагу громадськості в 2016 році, коли ботнет — тобто мережа скомпрометованих пристроїв під контролем ворожої загрози — зламав сайт новин безпеки KrebsOnSecurity з рекордною на той час швидкістю 620 гігабіт на секунду. DDoS.

Окрім величезної вогневої потужності, Mirai виділявся й іншими причинами. По-перше, пристрої, якими він керує, являли собою набір маршрутизаторів, камер безпеки та інших типів пристроїв IoT, чого до цього майже не бачили. З іншого боку, основний вихідний код швидко став вільно доступним. Незабаром Mirai використовувався в ще більших DDoS, націлених на ігрові платформи та провайдерів, які їх обслуговували. Відтоді Mirai та інші ботнети Інтернету речей стали фактом життя Інтернету.

Штам Mirai, який використовувався в атаках, виявлених Akamai, є переважно старішим, відомим як JenX. Однак його було змінено, щоб використовувати набагато менше доменних імен, ніж зазвичай, для підключення до командно-контрольних серверів. Деякі зразки зловмисного програмного забезпечення також показують зв’язки з окремим варіантом Mirai, відомим як hailBot.

Код, який використовувався в атаках нульового дня, спостережуваних Akamail, включно з образливими расистськими образами, майже ідентичний тому, який використовувався в DDoS-атаках, які китайська охоронна фірма спостерігала проти російського сайту новин у травні. На зображенні нижче показано паралельне порівняння…

Люди чи організації, стурбовані можливістю того, що ці експлойти можуть стати їх ціллю, можуть використовувати правила Snort і індикатори компрометації, опубліковані Akamail, для виявлення та відбиття атак. На даний момент неможливо

визначити конкретні вразливі пристрої або виробників цих пристроїв». ***(Dan Goodin. Thousands of routers and cameras vulnerable to new 0-day attacks by hostile botnet // Condé Nast (https://arstechnica.com/security/2023/11/thousands-of-routers-and-cameras-vulnerable-to-new-0-day-attacks-by-hostile-botnet/?utm_source=flipboard&utm_content=ArsTechnica%2Fmagazine%2FArs+Technica). 22.11.2023).***

***

## ***Технічні та програмні рішення для протидії кібернетичним загрозам***

---

**«До кінця року Discord перейде на тимчасові посилання на файли для всіх користувачів, щоб заблокувати зловмисникам використання CDN (мережі доставки вмісту) для розміщення та просування шкідливого програмного забезпечення.**

«Discord розвиває свій підхід до URL-адрес CDN вкладених файлів, щоб створити більш безпечний і захищений досвід для користувачів. Зокрема, це допоможе нашій групі безпеки обмежити доступ до позначеного вмісту та загалом зменшить кількість шкідливих програм, що поширюються через нашу CDN», сказав BleepingComputer.

«Немає жодного впливу на користувачів Discord, які діляться вмістом у клієнті Discord. Будь-які посилання в клієнті оновлюватимуться автоматично. Якщо користувачі використовують Discord для розміщення файлів, ми рекомендуємо їм знайти більш відповідний сервіс.

«Розробники Discord можуть відчути мінімальний вплив, і ми тісно співпрацюємо з спільнотою над переходом. Ці зміни запровадять пізніше цього року, і ми поділимося додатковою інформацією з розробниками в найближчі тижні».

Після того, як зміна хостингу файлів (описана Discord як примусова автентифікація) стане доступною пізніше цього року, усі посилання на файли, завантажені на сервери Discord, втратять чинність через 24 години.

URL-адреси CDN постачатимуться з трьома новими параметрами, які додадуть мітки часу закінчення терміну дії та унікальні підписи, які залишатимуться дійсними до закінчення терміну дії посилань, запобігаючи використанню CDN Discord для постійного розміщення файлів.

Незважаючи на те, що ці параметри вже додаються до посилань Discord, вони все ще потребують примусового виконання, а посилання, які надаються за межами серверів Discord, втратять чинність лише після того, як компанія запровадить зміни в застосуванні автентифікації.

«Щоб покращити безпеку CDN Discord, URL-адреси CDN вкладених файлів мають 3 нові параметри URL-адреси: ex, is і hm. Щойно цього року почнеться примусова автентифікація, посилання з певним підписом (hm) залишатимуться дійсними до мітки часу закінчення (ex)», - пояснила команда розробників Discord у публікації, опублікованій на сервері Discord Developers.

«Щоб отримати доступ до посилання CDN вкладення після закінчення терміну дії посилання, вашій програмі потрібно буде отримати нову URL-адресу CDN. API автоматично повертатиме дійсні URL-адреси без терміну дії, коли ви отримуєте доступ до ресурсів, які містять URL-адресу CDN вкладення, наприклад, під час отримання повідомлення.»

*Величезний стрибок у боротьбі зі шкідливими програмами*

Це довгоочікуваний крок до поточних проблем, з якими стикається Discord у стримуванні кіберзлочинності на своїй платформі, оскільки її сервери вже давно служать розсадником зловмисної діяльності, пов’язаної з фінансово мотивованими та підтримуваними державою хакерськими групами.

Можливості постійного розміщення файлів Discord часто зловживали для розповсюдження зловмисного програмного забезпечення та викрадання даних, зібраних із скомпрометованих систем за допомогою веб-хуків.

Незважаючи на ескалацію цієї проблеми в останні роки, Discord наразі намагався запровадити ефективні заходи для запобігання зловживанню платформою з боку кіберзлочинців і рішуче вирішити проблему або, принаймні, обмежити її вплив.

Відповідно до нещодавнього звіту компанії з кібербезпеки Trellix, URL-адреси Discord CDN використовувалися принаймні 10 000 операцій зловмисного програмного забезпечення для скидання зловмисного навантаження другого етапу на заражені системи.

Ці корисні навантаження в основному складаються із завантажувачів шкідливих програм і сценаріїв, які встановлюють шкідливі програми, наприклад RedLine stealer, Vidar, AgentTesla, zgRAT і Raccoon stealer.

Згідно з даними Trellix, різні сімейства шкідливих програм, включаючи Agent Tesla, UmbralStealer, Stealerium і zgRAT, також використовували веб-хуки Discord протягом останніх кількох років, щоб викрасти конфіденційну інформацію, як-от облікові дані, файли cookie браузера та криптовалютні гаманці зі зламаних пристроїв». ***(Sergiu Gatlan. Discord will switch to temporary file links to block malware delivery // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/discord-will-switch-to-temporary-file-links-to-block-malware-delivery/). 04.11.2023).***

***

**«Кібербезпека є необхідною в сучасному цифровому ландшафті. У міру того, як компанії та окремі особи здійснюють більше діяльності в Інтернеті, розширюється коло потенційних вразливостей. Ось найцікавіше — на сцену виходить обробка природної мови (NLP).**

Ця інноваційна технологія вдосконалює традиційні методи кібербезпеки, пропонуючи інтелектуальний аналіз даних і ідентифікацію загроз. Оскільки цифрова взаємодія розвивається, NLP є незамінним інструментом у зміцненні заходів кібербезпеки.

*Що таке NLP?*

NLP – це гілка машинного навчання (ML), яка дозволяє комп'ютерам розуміти, інтерпретувати та реагувати на людську мову. Він застосовує алгоритми для аналізу тексту та мовлення, перетворюючи ці неструктуровані дані у формат, зрозумілий машинам.

*Чому NLP має значення для кібербезпеки*

Збіг між NLP і кібербезпекою полягає в аналізі та автоматизації. Обидва поля вимагають просіювання незліченних вхідних даних для виявлення шаблонів або загроз. Він може швидко обробляти безформні дані до форми, з якою може працювати алгоритм — те, що традиційні методи можуть важко зробити.

Отже, чому НЛП стає великою проблемою цифрової безпеки? Мова йде про ефективність і точність. Він може автоматично оцінювати текстові дані, як-от електронні листи чи публікації в соціальних мережах, на наявність спроб фішингу чи підозрілих дій. Він виконує це завдання швидше та точніше, ніж ручні методи.

Алгоритми забезпечують перевагу в аналізі даних і виявленні загроз, перетворюючи розпливчасті показники в практичну інформацію. НЛП може просіювати шум, щоб точно визначити реальні загрози, покращуючи час реакції та зменшуючи ймовірність помилкових спрацьовувань.

*Приклади НЛП в кібербезпеці*

Нижче наведено переконливі реальні програми, які демонструють, як НЛП революціонізує індустрію кібербезпеки. Від виявлення фішингових електронних листів до збору доказової інформації з балаканини в соціальних мережах, це виявляється прогресивним.

*Виявлення фішингової електронної пошти*

Одним із найбільш практичних прикладів NLP у кібербезпеці є виявлення фішингових електронних листів. Ці шахрайства часто націлені на компанії з низьким профілем цифрової безпеки. понад 10 мільярдів доларів. було втрачено Дані Звіту ФБР про злочини в Інтернеті показали, що у 2022 році через кіберзлочини

Кіберзлочинці створюють фішингові повідомлення, щоб виглядати легітимними, часто імітуючи надійні організації або відтворюючи поточні події;

наприклад, у 2021 році щодня надсилалося понад 18 мільйонів шахрайських електронних листів, пов'язаних із COVID-19. Аналізуючи мову, структуру та контекст електронних листів, алгоритми NLP можуть виявити тонкі ознаки фішингу, такі як непослідовна мова, терміновість у тоні або невідповідні посилання, які здаються недоречними. Він пропонує динамічний і проактивний підхід замість того, щоб покладатися на відомі фішингові сигнатури.

*Розвідка про загрози в соціальних мережах*

Соціальні мережі — це більше, ніж просто для обміну мемами та фотографіями з відпустки — це також осередок потенційних загроз кібербезпеці. Зловмисники часто обговорюють тактику, діляться шкідливим програмним забезпеченням або беруть на себе відповідальність за атаки на ці платформи. Саме тут НЛП стає неймовірно корисним у зборі інформації про загрози.

Алгоритми НЛП можуть сканувати величезну кількість даних соціальних мереж, позначаючи відповідні розмови чи дописи. Це можуть бути кодована мова, погрози або обговорення методів злому. Швидко сортуючи шум, NLP надає цілеспрямовану інформацію, на яку можуть діяти фахівці з кібербезпеки.

*Автоматизація звітів про інциденти*

Подання звітів про інциденти є необхідним, але часто займає багато часу. У сфері, де час має важливе значення, автоматизація цього процесу може стати порятунком. NLP може автоматично генерувати підсумки інцидентів безпеки на основі зібраних даних, оптимізуючи весь процес звітування.

Аналізуючи журнали, повідомлення та сповіщення, NLP може ідентифікувати цінну інформацію та звести її у послідовний звіт про інцидент. Він фіксує такі важливі деталі, як характер загрози, уражені системи та рекомендовані дії, заощаджуючи дорогоцінний час для команд з кібербезпеки.

*Переваги використання НЛП у кібербезпеці*

Це незаперечні переваги НЛП. Від прискорення аналізу даних до підвищення точності виявлення загроз, це змінює те, як працюють фахівці з кібербезпеки.

*Швидший аналіз даних*

Час часто є критичним фактором кібербезпеки, і саме тут НЛП може прискорити аналіз. Традиційні методи можуть бути повільними, особливо при роботі з великими неструктурованими наборами даних. Однак алгоритми можуть швидко просіювати інформацію, виявляючи відповідні шаблони та загрози за частку часу.

Ця швидкість дозволяє швидше приймати рішення та швидше розгортати контрзаходи. Простіше кажучи, NLP скорочує час між виявленням загрози та відповіддю, надаючи організаціям явну перевагу в сфері, де кожна секунда на рахунку.

*Покращена точність виявлення загроз*

Точність є наріжним каменем ефективної кібербезпеки, і НЛП значно підвищує планку в цій сфері. Традиційні системи можуть видавати помилкові спрацьовування або пропускати нюанси загроз, але складні алгоритми точно аналізують текст і контекст з високою точністю. Це призводить до меншої кількості помилок і більш надійного виявлення загроз.

Розуміючи тонкощі мови та шаблонів, НЛП може ідентифікувати підозрілі дії, які можуть бути зловмисними, які інакше могли б проскочити. Результатом є більш надійна система безпеки, яка фіксує загрози, про існування яких можуть не знати команди з кібербезпеки.

*Покращуйте роботу користувачів завдяки автоматизації*

Підвищення досвіду користувачів є ще однією переконливою перевагою впровадження НЛП. Автоматизація таких завдань, як звітування про інциденти або запити в службу підтримки, усуває тертя та робить процеси плавнішими для всіх учасників.

Автоматизація за допомогою NLP оптимізує операції та зменшує людські помилки. Користувачі отримують швидші та точніші відповіді, незалежно від того, запитують статус безпеки чи повідомляють про інцидент. Це створює зручне для користувача середовище, сприяючи довірі та задоволенню.

*Поради щодо впровадження НЛП у кібербезпеку*

Наступний крок — з’ясувати, як ефективно впровадити НЛП. Ці практичні поради можуть стати в нагоді організаціям, коли вони включатимуть технологію у свої практики кібербезпеки.

*Почніть з малого*

Розпочати з малого — це розумна стратегія, коли ви занурюєтеся в сферу НЛП. Замість того, щоб іти ва-банк, спробуйте поекспериментувати з одним додатком, який відповідає певним потребам у структурі кібербезпеки організації. Можливо, це виявлення фішингової електронної пошти або автоматизація базових звітів про інциденти — виберіть один і зосередьтеся на ньому.

Цей цілеспрямований підхід дозволяє людям вимірювати ефективність, збирати відгуки та точно налаштовувати програму. Це простий спосіб освоїти правила, не перевантажуючи команду чи систему з кібербезпеки.

*Надайте пріоритет якості даних*

Якість даних є фундаментальною для успішного впровадження NLP у кібербезпеку. Навіть найдосконаліші алгоритми можуть давати неточні або оманливі результати, якщо інформація невірна. Таким чином, забезпечення чистоти, послідовності та надійності вхідних даних має вирішальне значення.

Почніть із регулярного аудиту поточних джерел даних. Перевірте їх достовірність і оцініть, наскільки актуальна інформація. Щоб підвищити точність, видаліть усі застарілі або нерелевантні дані.

*Розгляньте командне навчання*

НЛП є потужним інструментом, але команда розкриває свій потенціал лише тоді, коли використовує його правильно. Навчання стає необхідним для повної інтеграції в практику кібербезпеки.

Почніть із вступних сесій, які охоплюють основи НЛП та її застосування в кібербезпеці. Поступово переходьте до практичного навчання, де члени команди можуть взаємодіяти з інструментами НЛП і бачити їх.

*Майбутнє кібербезпеки, розширеної за допомогою NLP*

НЛП пропонує багато переваг, які можуть революціонізувати зусилля з кібербезпеки. Настав час зробити стрибок і інтегрувати технологію в набір інструментів цифрової безпеки організації.

Скористайтеся цією можливістю, щоб побачити його трансформаційний вплив на заходи безпеки. Майбутнє кібербезпеки світле, і НЛП лідирує». ***(Zac Amos, ReHack. How to apply natural language processing to cybersecurity // VentureBeat (https://venturebeat.com/ai/how-to-apply-natural-language-processing-to-cybersecurity/). 23.11.2023).***

***

## Питання криптографії

**«За словами видатного дослідника, для зламу шифрування RSA-2048 можна використовувати комерційний смартфон або комп'ютер з ОС Linux.** Доктор Ед Герк готує дослідницьку статтю з деталями, але не міг утриматися від того, щоб похвалитися своїми неймовірними досягненнями в області квантових обчислень (якщо це правда) у своєму профілі на LinkedIn. Давайте прояснимо: заяви здаються фальшивими, але слід визнати, що світ не готовий до готової системи, яка може зламати RSA-2048, оскільки великі фірми, організації та уряди ще не перейшли до технологій шифрування, які захищені для постквантової ери.

У своєму дописі в соціальних мережах Герк стверджує, що такий скромний пристрій, як смартфон, може зламати найнадійніші ключі шифрування RSA, які використовуються сьогодні, завдяки математичній техніці, яка «була прихована приблизно 2500 років — з часів Піфагора». Далі він уточнив, що під час злому ключів RSA-2048 не використовувалися кріогенні чи спеціальні матеріали.

BankInfoSecurity зв'язався з Герком у пошуках більш детальної інформації про його заявлений прорив RSA-2048 і в надії на якісь докази того, що те, що заявлено, можливо і практично. Герк поділився анотацією своєї майбутньої статті. Схоже, це показує, що замість використання алгоритму Шора для злому ключів

була використана система, заснована на квантовій механіці, і вона може працювати на смартфоні або ПК.

У певному сенсі це добре, що заявлений прорив не претендує на використання алгоритму Шора. Алан Вудворд, професор інформатики в Університеті Суррея, сказав BankInfoSecurity, що жоден існуючий квантовий комп'ютер не має достатньо воріт, щоб реалізувати алгоритм Шора та зламати RSA-2048. Тож принаймні ця частина пояснення Герка відповідає дійсності. Однак анотація до статті Герка виглядає так, ніби це «вся теорія, яка доводить різні припущення — і ці докази безумовно під питанням», за словами Вудворда.

У звіті BankInfoSecurity про статтю Герка «Алгоритми контролю якості: швидше обчислення простих чисел» цитуються інші скептики, більшість з яких чекають додаткової інформації та доказів, перш ніж влаштувати овації Герку стоячи.

Якщо ви перейдете до публікації доктора Герка на LinkedIn, ви побачите, що вчений був зайнятий відповідями на запити спільноти перед повною публікацією. Він також не боїться розпалювати суперечки, кажучи, що такі компанії, як IBM і Google, «просто помиляються» у своїх інтерпретаціях суперпозиції та заплутаності в квантових обчисленнях.

Герк є розробником постквантового, сумісного з HIPAA, наскрізного, безпатентного, безпечного онлайн-рішення без експорту» для криптографії, яке, за його словами, можна використовувати для заміни RSA. Це було б зручно, якщо його заяви щодо зламу RSA-2048 правильні. Природно, це також викликає питання, чи цей «злом» є просто рекламним трюком для його продукту.

Ми з цікавістю спостерігатимемо, як розвиватиметься історія злому RSA-2048. Це виглядає майже як новий момент LK-99, але може мати ще більший вплив на наше життя, якщо заголовок витримає перевірку». ***(Mark Tyson. Scientist Claims Quantum RSA-2048 Encryption Cracking Breakthrough // Future US, Inc. (https://www.tomshardware.com/software/security-software/quantum-rsa-2048-encryption-cracking-breakthrough-claim-met-with-***

***scepticism?utm_source=flipboard&utm_content=AWC%2Fmagazine%2FOur+Electronic+%26+Digital+Lives.). 03.11.2023).***

***

**«Rust був визнаний найулюбленішою мовою програмування протягом восьми років за короткий термін його існування – 14 років.** Популярність мови зумовлена її безпекою, однією з основних причин її створення. Rust був розроблений як безпечніший варіант, який забезпечує безпеку на першому місці, щоб програмісти писали стабільний і розширюваний асинхронний код.

Rust структуровано таким чином, що за своєю суттю запобігає розробникам від ненавмисного впровадження найпоширеніших видів недоліків безпеки, які можна використовувати. Ця характеристика мови може значно вплинути на звичайний процес виправлення вразливостей і покращення кібербезпеки.

На початку цього року Microsoft почала переписувати свої основні бібліотеки Windows у Rust. «Насправді Windows завантажуватиметься з ядром Rust протягом наступних кількох тижнів або місяців, і це дуже круто», — сказав Девід Вестон, віце-президент із безпеки ОС для Windows. Крім того, він сказав, що «основна мета полягала в тому, щоб перетворити деякі з цих внутрішніх типів даних C++ на їхні еквіваленти Rust»…

*Кілька функцій безпеки*

Однією з головних функцій безпеки Rust є наголос на безпеці пам’яті. Це досягається за допомогою моделі суворого володіння, яка визначає, як розподіляється пам'ять і як їй керувати.

Кожна частина даних у Rust має унікального власника, і мова забезпечує виконання правил щодо того, як і коли можна отримати доступ до даних або змінити їх. Ця система ефективно запобігає поширеним помилкам пам’яті, таким як переповнення буфера та розіменування нульового вказівника, які є частими векторами атак в інших мовах.

Крім основної функції безпеки під час розподілу пам’яті, Rust виділяється своїм підходом до паралелізму, який є ключовим аспектом його дизайну, що забезпечує безпеку та захист у багатопоточних програмах.

Унікальні правила власності мови застосовуються до її моделі паралелізму, що робить доступ до даних потоково безпечним і вільним від перегонів даних. Таке ретельне поводження з паралелізмом не тільки підвищує продуктивність, але й значно зменшує низку вразливостей безпеки, які зазвичай пов’язані з багатопоточними середовищами.

Доповнюючи свою модель паралелізму, Rust може похвалитися мінімальним часом виконання. Це є значною перевагою безпеки. На відміну від мов, які залежать від більших середовищ виконання або віртуальних машин, економна архітектура середовища виконання Rust мінімізує потенційну поверхню атаки. Це означає, що є менше компонентів, які можуть стати ціллю або використати хакери, підвищуючи загальну безпеку програм, розроблених у Rust.

Обробка помилок у Rust є ще одним наріжним каменем системи безпеки. Мова зобов’язує програмістів чітко обробляти потенційні помилки, таким чином запобігаючи неочікуваним збоям або поведінці. Цей чіткий і передбачуваний підхід до обробки помилок інтегровано в мову на рівні компіляції, що значно знижує ймовірність помилок під час виконання, які можуть бути використані під час кібератак.

Rust також отримує велику користь від свого менеджера пакунків Cargo. Cargo має ключове значення для підтримки безпечного коду, оскільки він ефективно керує залежностями, відстежує версії бібліотеки та гарантує, що всі компоненти проекту є актуальними. Ця функція має вирішальне значення для безпеки; це дозволяє розробникам оперативно впроваджувати виправлення та оновлення, особливо для бібліотек, які можуть мати вразливі місця.

Активна участь спільноти Rust відіграє життєво важливу роль у забезпеченні безпеки мови. Регулярні оновлення та перегляди спільнотою допомагають усунути відомі вразливості та постійно вдосконалювати функції безпеки мови. Цей

проактивний підхід, керований спільнотою, є невід'ємною частиною підтримки стійкості Rust проти загроз безпеці.

Підсумовуючи, хоча жодна мова програмування не може запропонувати абсолютний захист від злому, продуманий дизайн Rust, що включає безпечний паралелізм, мінімальний час виконання, явну обробку помилок, ефективне керування пакетами та залучену спільноту, позиціонує його як більш безпечну альтернативу порівняно з мовами, такими як C і C++. Ці атрибути разом сприяють здатності Rust ефективно пом'якшувати широкий спектр поширених уразливостей.

*Швидка міграція*

Розробників, які переходять з інших мов, приваблює переконливий набір функцій Rust. Його ефективне керування паралельним програмуванням забезпечує паралельне виконання коду, а його легкий і швидкий характер, з тестами, що конкурують із C/C++, є значною перевагою. Цей перехід відповідає рекомендації NSA щодо переходу від C/C++ до безпечних для пам'яті мов, таких як Rust.

Розробка Rust була орієнтована на користувача, зосереджена на основних, але часто забутих функціях. Сюди входять генерики, алгебраїчні типи, сумісність зовнішнього функціонального інтерфейсу (FFI), надійний інструмент керування залежностями та процедурні макроси, які сприяють більш приємному досвіду програмування в Rust.

У технологічній індустрії основні гравці використовують Rust через його переваги. Mozilla, наприклад, оновлює Firefox за допомогою Rust, щоб підвищити його безпеку, надійність і продуктивність. Подібним чином Amazon використовує Rust для AWS і Kindle і навіть розробляє компілятор Rust для Java, віддаючи пріоритет продуктивності та масштабованості.

Google і Dropbox також використовують Rust. Google використовує Rust у Chrome і Android і створює компілятор Rust для Go, щоб підвищити безпеку та надійність. Dropbox, тим часом, переводить свою серверну частину на Rust, прагнучи покращити продуктивність і масштабованість.

Facebook також використовує потенціал Rust. Компанія використовує Rust для розробки блокчейну Libra та Oculus VR, а також працює над компілятором Rust

для C++, зосереджуючись на створенні більш безпечного та надійного програмного забезпечення». ***(Rust Provides the Ultimate Security Against Hackers // Analytics India Magazine Pvt Ltd & AIM Media House LLC (https://analyticsindiamag.com/rust-provides-the-ultimate-security-against-hackers/?utm_source=flipboard&utm_content=NagsMags%2Fmagazine%2FTech+World). 15.11.2023).***

***