УДК 004.056.56:342(042.2)

Ковальов Кирило Олексійович
(Національний Авіаційний Університет, Україна)

Види порушень кібербезпеки

Розглянуто тенденцію збільшення випадків порушеня кібербезпеки. На цьому фоні проаналізовано проблематику питання кіберзахисту та проведений аналіз різних видів порушень безпеки. Перечислено та описано найрозповсюджені типи загроз.

Кібератаки стали звичайним явищем у міру розвитку мереж, тому для боротьби з кібератаками потрібні різні рішення. Але тільки якщо ви знаєте типи порушень кібербезпеки, вам буде легше вжити необхідних запобіжних заходів для захисту даних і мережі вашої організації. Усі знають, наскільки небезпечними можуть бути кібератаки, якщо їх не лікувати. Кібербезпека охоплює всі аспекти захисту та забезпечення безпеки цінних даних та інформації організації. Правильне використання кібербезпеки також може призвести до створення більш безпечного середовища для працівників, захищеного від кіберзагроз.

У третьому кварталі 2022 року в результаті витоків даних у всьому світі було розкрито 15 мільйонів записів. Якщо порівнювати цей показник із попереднім кварталом, то він збільшився на 37%. З першого кварталу 2020 року у четвертому кварталі 2020 року було зафіксовано найбільшу кількість оприлюднених записів даних або майже 125 мільйонів наборів даних.

Загальне визначення витоку даних - це порушення безпеки, при якому хакери копіюють або крадуть захищені, чутливі та конфіденційні дані організації. Весь процес здійснює окрема людина чи група хакерів. Хакери чи злочинці спланували все для здійснення цієї дії. Витік даних, витік інформації та витік даних - це інші терміни, що позначають ненавмисне розкриття інформації. Кібератаки небезпечні тим, що можуть погіршити стан організації та вкрасти приховані дані. Ваш бренд – і ваші доходи – можуть бути знищені внаслідок витоку даних. Проте кожен хакер чи злочинець має свою тактику боротьби з кібератаками. Іноді вони надсилають текстове повідомлення зі шкідливим файлом, і багато хто з нас одразу ж натискає на нього. Від атак хакерів на університети та студентів до витоків інформації з лікарень - за останні кілька років ми стали свідками сотень витоків, що порушили конфіденційність мільйонів користувачів. Щоб зробити ситуацію простішою та зрозумілішою, я розділив типи порушень кібербезпеки на дві групи. Однак ціль обох груп однакова: обидва типи кібератак або витоків даних володіють цінними або санкціонованими даними організацій.

Ці порушення відбуваються, коли неавторизовані особи отримують доступ до комп'ютера або мережі. Це може статися, якщо хтось зловмисно зламає вашу систему або якщо ви випадково залишите пристрій незахищеним. Порушення фізичної безпеки можуть завдати великої шкоди, призвести до крадіжки особистих даних та фінансових втрат.

Порушення фізичної безпеки. Ці порушення відбуваються, коли неавторизовані особи отримують доступ до комп'ютера або мережі. Це може статися, якщо хтось зловмисно зламає вашу систему або якщо ви випадково залишите пристрій незахищеним. Порушення фізичної безпеки можуть завдати великої шкоди, призвести до крадіжки особистих даних та фінансових втрат.

Порушення цифрової безпеки. Вони відбуваються, коли хакери беруть під контроль комп'ютер або мережу, щоб вкрасти інформацію, таку як номери кредитних карток, паролі або особисті дані. Вони також можуть використовувати ваш комп'ютер як частину ботнета - групи комп'ютерів, захоплених хакерами і використовуються для розсилки спаму, атак типу "відмова в обслуговуванні" на веб-сайти або розповсюдження шкідливих програм.

Нижче наведено деякі поширені типи порушень фізичної та цифрової кібербезпеки.

Фішингові атаки – один з найпоширеніших і найефективніших способів крадіжки будь-яких даних або мережі. При фішинг злочинці або хакери отримують доступ до середовища організації. У цьому типі кібератак жертва стає легше керованою за допомогою хитрощів, коли хакери відправляють посилання, щоб відкрити вкладення. Більшість співробітників стають жертвами цього трюку, тому що іноді вони натискають на посилання, що призводить до використання даних мережі.

Вкрадені дані. Частина вкраденої інформації, коли непрофесійний співробітник залишає інформацію про продукт, який ще не випущений, та інформація про обладнання поширюється по всьому цифровому світу (інтернету). Такий необережний вчинок чи людська помилка можуть завдати великої шкоди безпеці організації. У той же час для багатьох корпорацій звичайною справою є залишення інформації у відкритому доступі та її крадіжка.

Ransomware. Замість того, щоб шифрувати файли, програми-вимагачі крадуть дані, щоб вимагати гроші у жертв та їхніх клієнтів. Деякі ransomware групи або окремі особи загрожують або використовують розподілені атаки типу «відмова в обслуговуванні» (DDoS), щоб змусити жертву заплатити викуп. Однак у багатьох випадках вимога ransomware пов'язана з грошима, і з передачею авторизованих даних хакеру.

Розподілена відмова в обслуговуванні (DDoS). Відмова в обслуговуванні Атаки запускаються одночасно з кількох джерел. Вони перешкоджають доступу користувачів до системи, коли вони перебувають на роботі. Клієнти не можуть отримати доступ до послуг компанії, якщо сайт недоступний через атаку. Це створює приголомшливий хаос для всієї організації та великі збитки. Незважаючи на необов'язковість втрати даних, порушення безпеки може змусити компанію припинити роботу, що призведе до втрати доходу.

Шкідливі програми. Еволюція шкідливих програм домінує над еволюцією кібератак. Автори шкідливих програм та кіберзахисники постійно розробляють методи подолання чи обходу заходів безпеки. Успіх цих кібератак часто провокує створення нового покоління.

У період цифрових технологій порушення безпеки стали фактом життя. Обидві проломи в системі безпеки мають достатній потенціал для створення великого безладдя та хаосу. Керівники повинні розглянути нову тактику, щоб знайти високозахищений спосіб убезпечити свої мережі від фізичних та цифрових порушень безпеки. Будь то скімінгові пристрої на банкоматах або кіберзлочинці, яким вдалося проникнути через брандмауери вашої компанії, важливо знати, що таке порушення безпеки і як їм запобігти.

Список літератури

1. Класифікація кіберзагроз та їх легітимація у нормативно-правових атак України. GOAL: вебсайт. URL: https://goal-int.org/klasifikatsiya-kiberzagroz-ta-yih-legitimatsiya-u-normativno-pravovih-aktah-ukrayini/ (дата звернення: 01.03.2023).
2. Типи загроз для кібербезпеки. *Microsoft*: вебсайт. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity (звернення: 01.03.2023).