УДК 004.773.3:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.181

НАЙПОШИРЕНІШІ ЗАГРОЗИ БЕЗПЕЦІ ЕЛЕКТРОННІЙ ПОШТІ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

Шевчук В.В.
Науковий керівник – к.т.н., доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна
e-mail: vladyslav.shevchuk@nure.ua

The most common 2023 attacks are considered and effective methods of protection against them are proposed. Phishing, social engineering, virus attacks, and other forms of cybercrime often attempt to use mail to gain unauthorized access to sensitive information or cause other harmful effects. Therefore, there is a need to effectively protect users and organizations from cyber threats that can lead to large financial losses, violate privacy, and increase malware.

Найпоширенішими атаками на електронну пошту у 2023 р. стали: фішинг, спуфінг, цільовий фішинг, програми-вимагачі, віруси/шкідливе програмне забезпечення та спам. Порівняння вдалих атак у 2023 р. і 2019 р. наведено на рисунку 1.

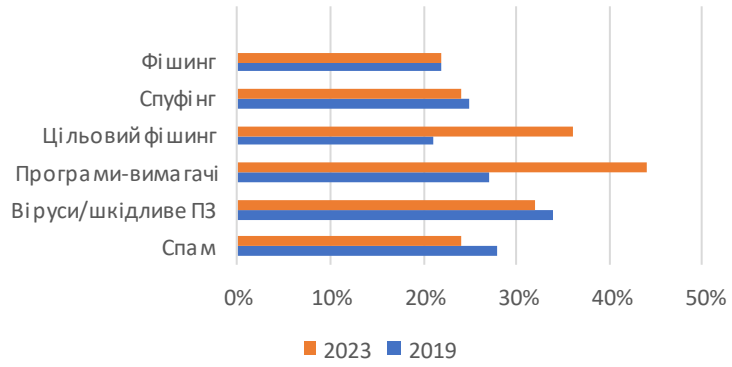

Рисунок 1 – Діаграма вдалих атак на електронну пошту

–Фішинг (Phishing) – вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних. Сценарій такої атаки заснований на незнанні користувачами основ мережевої безпеки, та перенаправлення на фішингові сайти або ураження пристрою програмою-вимагачем, або шифрувальником.

–Спуфінг (spoofing) – це атака, під час якої надають неправдиві дані, аби здаватися справжніми користувачами, наприклад, надсилання листа з акаунта, який має вигляд офіційної банківської email-адреси.

–Цільовий фішинг (Spear phishing) – вид фішингової атаки електронної пошти, спрямована на конкретну організацію чи особу з метою отримання несанкціонованого доступу до конфіденційної інформації.

–Програми-вимагачі (Ransomware) – це тип шкідливої програми, який злочинці встановлюють на комп'ютерах користувачів. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати комп'ютер. Такий тип програм поділяються на три типи: шифрування даних, блокування системи, та блокування або перешкода роботи в браузері.

–Віруси/шкідливе ПЗ (malware) – програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем, частіше проявлятися у вигляді коду, скрипту, активного контенту або іншого програмного забезпечення.

–Спам (Spam) – це небажані повідомлення у будь-якій формі, надіслані у великій кількості. Найчастіше спам надсилається у формі комерційних електронних листів на велику кількість адрес, а також через миттєві та текстові повідомлення (SMS), соціальні медіа або голосову пошту.

Аналізуючи атаки, загрози та вразливі місця в системах захисту електронної пошти, можна розробити ефективні методи захисту від цих атак. Методи використовуються на рівні користувачів послуг та на рівні постачальників послуг електронної пошти.

Головний аспект захисту починається з усвідомлення користувачами політики безпеки та використання ефективних методів її реалізації. Це застосування надійних паролів і періодична їхня зміна, заборона використання однакових паролів на різних сервісах. Застосування багатофакторної аутентифікації значно зменшує ризик несанкціонованого доступу до електронної пошти. Слід навчити співробітників розпізнавати фішингові атаки, усвідомлювати можливі ризики та додержуватися правил безпеки на їхньому рівні. Такі організаційні заходи дозволяють уникнути чисельних атак на електрону пошту.

На рівні постачальників послуг одним з ефективним методом захисту являється застосування різних методів автентифікації. Існує три типи автентифікації електронної пошти, які можна налаштувати під потреби користувача:

–Sender Policy Framework (SPF) – це технічний стандарт і метод автентифікації електронної пошти, який допомагає захистити відправників і одержувачів електронної пошти від спаму, підробки повідомлень та фішингу. SPF встановлює метод отримання поштових серверів для перевірки того, що вхідна пошта з домену була надіслана з хоста, авторизованого адміністраторами цього домену.

–DKIM (DomainKeys Identified Mail) – це протокол, який дозволяє організації взяти на себе відповідальність за передачу повідомлення, підписавши його таким чином, щоб постачальники поштових скриньок

могли перевірити. Перевірка запису DKIM стала можливою за допомогою криптографічної автентифікації.

–DMARC Domain-based Message Authentication, Reporting, and Conformance) – технологія, що дозволяє отримувачу електронної пошти перевірити справжність її відправника. Визначає масштабований механізм визначення політик та налаштувань для валідації, розташування, та журналювання електронних повідомлень на стороні відправника, якими може скористатись отримувач для поліпшення оброблення електронних листів.

Важливим методом захисту є резервне копіювання всіх даних, яке унеможливіть їхню втрату або видалення. Завжди потрібно створювати резервні копії всіх важливих листів. Для цього можна вибрати зовнішній жорсткий диск, USB-накопичувач або завантаження даних в хмарне сховище. Слід пам’ятати, що фізичний зовнішній жорсткий диск або USB-накопичувач можна загубити або пошкодити, а при зберіганні у хмарі хакери також мають можливість розкрити конфіденційні дані.

Застосування проксі-серверів забезпечує додатковий захист електронної пошти, дає змогу зберігати конфіденційність інформації про свою геолокацію, надсилати листи і проводити онлайн-дослідження, не розкриваючи власний IP-адрес.

Використання шифрування дає ефективний захист від перехоплення повідомлень. Для шифрування повідомлень використовують захищені протоколи TLS (Transport Layer Security) або SSL (Secure Sockets Layer), або метод шифрування End-to-end encryption (E2EE), який забезпечує конфіденційність повідомлень від усіх, у тому числі від служби обміну повідомленнями. При використанні E2EE, повідомлення з’являється лише в розшифрованому вигляді для особи, яка надсилає повідомлення, і для особи, яка отримує повідомлення.

Важливим аспектом безпеки є ефективний моніторинг та виявлення вразливостей в системі захисту. Для цього застосовується система виявлення вторгнень (IDS), яка дозволяє вчасно розпізнавати та реагувати на підозрілу активність, чи спроби отримати несанкціонований доступ до поштових серверів. Слід застосувати журнал для реєстрації та аналізу інцидентів , таких як невдалі спроби входу, чи надмірне споживання тих або інших ресурсів, обмежити надсилання великої кількості повідомлень.

Список використаних джерел:

1. Тенденції безпеки електронної пошти 2023 [Електронний ресурс] // Softprom. – 2023. – Режим доступу до ресурсу: https://softprom.com/ua /tendentsiyi-bezpeki-elektronnoyi-poshti-2023.

2. Zinkovska O. Надійні рішення для захисту електронної пошти: 12 найкращих практик [Електронний ресурс] / Olena Zinkovska // stripo.email. – 2023. – Режим доступу до ресурсу: https://stripo.email/ua/blog/top-email-security-practices/.