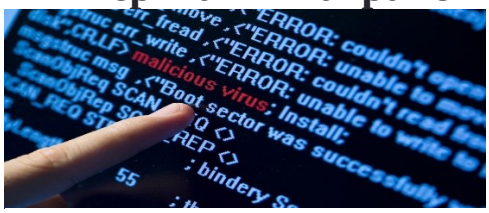
Понад 353 мільйони користувачів минулого року стали жертвами шахрайства з крадіжкою особистої інформації



Щороку атак стає більше і складність їх підвищується. Згідно з даними Verizon, кількість використаних вразливостей, пов'язаних із витоком даних, у 2024 році зросла на 180% порівняно з 2023 роком.

Кіберзлочинці використовують на свою користь дії, викликані людською помилкою, а також неправильне налаштування критичних IT-систем, таких як хмарні облікові записи, а також відсутність надійного пароля; можуть застосовувати інсайдерську інформацію та інструменти, які використовуються в компанії. Найпоширеніші загрози:

1. Фішинг та інші способи соціальної інженерії: зловмисники вивчають жертву, зокрема, напередодні переглянувши інформацію про неї в соціальних мережах, наприклад, LinkedIn.
2. Завантаження кіберзлочинцями шкідливого програмного забезпечення в компоненти з відкритим кодом; встановлення шкідливого коду в оновлення програми.
3. Злам облікових даних в результаті недостатнього захисту або управління паролем, фішингових атак, масштабного витоку даних або атак методом підбору пароля.
4. Уразливість до різних кіберзагроз особистих пристроїв: хакери можуть отримати дані для входу в корпоративні облікові записи в хмарі, доступ до робочої електронної пошти тощо.
5. Зростання використання зловмисниками інструментів на основі штучного інтелекту.

Зменшити ризик атак, кількість яких продовжує зростати через цифрову трансформацію, допоможуть такі заходи безпеки:

- використовуйте управління виправленнями на основі оцінки ризику, включаючи регулярне тестування на наявність можливих вразливостей;
- забезпечте захист усіх корпоративних пристроїв за допомогою багаторівневого рішення з безпеки;
- встановіть рішення для запобігання втрати даних (DLP);
- використовуйте продукт для захисту мобільних пристроїв, щоб поліпшити безпеку організації завдяки захисту від шкідливих програм, крадіжки даних і можливостям управління мобільними пристроями;
- подбайте про застосування надійних паролів і багатофакторної аутентифікації на всіх пристроях співробітників;
- підвищуйте обізнаність персоналу про можливі кіберзагрози, зокрема навчіть розпізнавати фішингові повідомлення;
- створіть план реагування на інциденти та періодично перевіряйте його актуальність;
- забезпечте шифрування даних під час передачі та зберігання;
- проводьте аудит сторонніх постачальників і партнерів;
- виконайте моніторинг мереж і робочих станцій, щоб отримати попереднє попередження про будь-які підозрілі дії;
- переконайтеся в правильності налаштування хмарних систем на всіх рівнях.