Кібербезпека

Відділ цифрової трансформації

Більшість “зламів” у соціальних мережах і в месенджерах - не злам, а шахрайство

- Технічного втручання в роботу системи немає
- Частота випадків, коли “ламають код” популярного сайту або сервісу - дуже низька
- Скоріше, при зламі буде йти мова про роботу над компрометацією ключів доступу користувача

Тріада CIA

- Конфіденційність
- Цілісність
- Доступність

DDoS-атаки

Метод масового завантаження певного сервісу великою кількістю запитів, який поза завершенням цієї атаки не несе жодної шкоди

Фактори автентифікації

- ключ від машини або квартири
- пароль або пін-код
- біометрія
- NFC, RFID
- номер телефону, електронна пошта

Способи зламу паролю

- bruteforce
- перебір за словником

a-z, A-Z, 0-9 =62 символи - алфавіт паролю

1000 переборів комбінацій за секунду

1 символ - 0.062 секунди
2 символи - 3.8 секунди
3 символи - 4 хвилини
4 символи - 4 години
5 символів - 10,5 діб
6 символів - 2 роки

не використовувати паролі, пов’язані виключно з персональною інформацією, бажано мати випадково згенеровані паролі

Соціальна інженерія

- складання профілю жертви і перебір за “персональним” словником за інформацією із відкритих джерел
- провокування користувача на поширення власної персональної інформації (в тому числі через пабліки в соцмережах)
- обман людини з метою отримати код підтвердження, який прийшов на телефон або e-mail
- фішинг (підміна веб-сайту)

Рекомендації

- поставте AdBlock
- бачите емоційний пост із запитом на персональну інформацію в пабліку - не реагуйте
- якщо з вами спілкуються з метою отримати якусь інформацію і представляються вашими знайомими - перевірте
- не вносіть інформацію, яка доступна про вас публічно, як частину паролів
- перевіряйте адреси сайтів на які ви заходите, щоб уникнути фішингу
- якщо вам переслали посилання або файл, який потрібно завантажити і запустити:
  1) проігноруйте
  2) перепитайте особу, яка вам це прислала (якщо ви її знаєте)
- “ламане” програмне забезпечення - це безплатний сир в мишоловці

Що зробили, якщо ваші соцмережі вже зламали?

1) Знайдіть функцію “Вийти з усіх пристроїв” та застосуйте її
2) Якщо доступ до сервісу по паролю, встановіть новий пароль
3) Повідомте друзів та знайомих, що вас зламали
4) Якщо доступ до облікового запису втрачено, напишіть у підтримку.

Якщо зламали когось із ваших знайомих

1) повідомте їх
2) якщо від облікового запису ваших знайомих йде спам-розсилка, прокоментуйте її, аби інші не переходили на посилання
3) якщо є функція “позначити як спам”, скористайтеся нею.

Кібергігієна

Найкращий спосіб захисту - не одноразові акції протидії, а стала робота над звичками

Цифровий слід

Цифровий слід людини - вся інформація яка доступна на даний момент, або була доступна у Web.

Де ви залишаєте цифровий слід?

- Власні аккаунти соцмереж
- Публічна інформація згідно закону (ЄДР, Прозорро), сайт закладу освіти
- Новини

Цифровий слід, який ви залишаєте “напівсвідомо”

- локації
- історія пошуку та історія перегляду браузера
- повідомлення, аудіоповідомлення

OSINT - розвідка з відкритих джерел

- Google Street View (geoguesser)
- Google Maps (і фото, зв’язані з ними)
- Google Earth
- відкриті реєстри
- соцмережі
- репортажі