УДК 004.056:316.42

МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У ФУНКЦІОНУВАННІ СУЧАСНОГО СУСПІЛЬСТВА

Маньковський А.Г.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків,
Україна
тел. +38(068) 755 13 21

The report provides an analysis of social engineering methods that can be used by an attacker to attack an enterprise. Weaknesses and strengths of methods of protection against attacks using social engineering are given, and mechanisms of protection against attacks using social engineering methods are analyzed in detail.

Ефективність підприємства пов'язана не лише з її технологічними можливостями, методами управління та реалізації продукції, а також можливістю протистояти тим зовнішнім впливам, які накладає конкурентна боротьба. Соціальна інженерія – метод отримання доступу до інформації, заснований на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних та інших захищених систем.

В доповіді проведений аналіз методів соціальної інженерії при реалізації загроз інформаційної безпеки. Стисло наведемо дані методи.

Претекстинг - це метод соціальної інженерії, при якому зловмисник використовує неправдиві приводи та обман, щоб отримати доступ до конфіденційної інформації чи систем. Вони вигадують привід чи цілий сценарій, щоб вивідати дані чи спонукати жертву на дії. Вони часто просять жертву підтвердити свою особистість. А для цього нібито слід відповісти на серію питань. Наприклад, назвати дівоче ім'я матері, місце народження, дату народження, пароль, номер банківського рахунку, номер зі зворотного боку банківської картки. Отримані дані використовують у своїх цілях для подальшої атаки.

Фішинг – це техніка інтернет-шахрайства, спрямовану отримання конфіденційної інформації користувачів - авторизаційних даних різних систем. Основним видом фішингових атак є підроблений лист, відправлений жертві електронною поштою, який виглядає як офіційний лист від платіжної системи або банку.

Троянський кінь – це техніка ґрунтується на цікавості, страху чи інших емоціях користувачів. Зловмисник відправляє листа жертві за допомогою електронної пошти, у вкладенні якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника.

Quid pro quo (послуга за послугу) – дана техніка передбачає звернення зловмисника до користувача електронною поштою або корпоративним телефоном. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці.

Дорожнє яблуко – цей метод є адаптацією троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій у загальнодоступних місцях на території компанії (парковки,мїдальня, робочі місця співробітників, туалети). Для того, щоб у співробітника виник інтерес до цього носія, зловмисник може нанести на носій логотип компанії та якийсь підпис. Наприклад, "дані про продаж", "зарплата співробітників", "звіт у податкову" та інше.

Зворотна соціальна інженерія - цей вид атаки спрямований на створення такої ситуації, за якої жертва змушена буде сама звернеться до зловмисника за «допомогою».

Tailgating (або piggybacking) - це метод маніпулювання людьми, який полягає в тому, щоб проникнути в обмежену зону, яка зазвичай охороняється, за рахунок використання чужих облікових записів або підробки легітимності.

Методи атаки.

1. Теорія десяти рукостискань. Головна мета зловмисника, який використовує телефон для соціальної інженерії, полягає в тому, щоб переконати свою жертву в одному з двох моментів:

а) Жертві дзвонить співробітник компанії;

б) Телефонує представник уповноваженого органу (наприклад, правоохоронець чи аудитор).

2. Вивчення корпоративної мови.

3. Запозичення музики очікування під час дзвінків.

4. Спуфінг (підміна) телефонного номера.

5. Використання новин проти вас.

6. Використання довіри до соціальних платформ.

7. Тайпсквоттінг.

В доповіді приводяться напрямки захисту підприємства від атак з використанням методів соціальної інженерії. Приводиться приклад процесів, які мають бути реалізовані при побудові систем управління інформаційною безпекою [1], надаються технічні механізми виявлення атак методами соціальної інженерії.

Список використаних джерел:

1. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks [Електронний ресурс]. – Режим доступу до ресурсу: https://www.iso.org/standard/80585.html.