ВИКОРИСТАННЯ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ ДЛЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

Орест Полотай, Ростислав Гриник

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The main methods of social engineering, attackers are using in the course of unautorized access to information. We describe the essence of socio-technical systems. The features of social engineering as a socio-technical actors attacks.

Keywords: social engineering, information, fishing, pretexting

Останнім часом, все більшої популярності набуває поняття «соціотехнічна система». Не важко зрозуміти, що соціотехнічна система є однією з підвидів систем, під якими розуміють сукупність елементів та взаємних зв'язків між ними, яким володіють конкретними властивостями, метою, цілями та функціями. Соціотехнічні системи, це сукупність соціальних та технічних систем складовою яких є людина-керуючий ЕОМ, разом з сукупністю його знань, та навичок. Дана людина (оператор) взаємодіє з технічним пристроєм, що призводить до підвищення ефективності поставлених перед нею цілей. [1].

Забезпечення безпеки на сьогоднішній момент є об'єктивною необхідністю ефективного управління в соціотехнічних системах, оскільки такі системи виступають якнайкращим плацдармом для реалізації соціоінженером/соціотехніком (зловмисником) інформаційних операцій та атак, тобто так-званих соціотехнічних атак.

Як відомо, соціоінжера за рівнем своєї підготовки до здійснення соціотехнічної атаки поділяють на новачка, аматора та професіонала і за ймовірністю отримання несанкціонованого доступу різних рівнів до інформації їм наділяють ступінь в межах від 1 до 3 (1 – найменший ступінь, 3 – найбільший).

В залежності від того, під яку категорію підпадає соціальний інженер, він використовує для здійснення несанкціонованого доступу різні методи соціального інжинірингу (соціальної інженерії). Під даними методами розуміються такі методи, які мають на меті використовувати людський чинник як джерело отримання соціоінженером необхідної йому інформації. При використання методів соціального інжинірингу, соціоінженери експлуатують в своїх цілях довірливість, лінь, люб'язність і навіть ентузіазм своїх жертв. Для цього соціоінженер намагається переконати суб'єкти атаки надати йому інформацію, що забезпечує доступ до корпоративних систем або їх ресурсів [2].

Якщо порівнювати атаку, в основі якої лежать методи соціальної інженерії, та кібернетичні атаки, то перший вид атак має на меті нанести шкоду не комп'ютерній системі, а її користувачам, використовуючи при цьому, в якості допоміжних, різноманітні технічні засоби.[3].

Основна тактика соціальної інженерії - за допомогою психологічних методів (наприклад, спілкуючись начебто від імені сервісної компанії чи банку) переконати користувача розкрити інформацію особистого характеру (паролі, номери кредитних карток тощо).

Для успішної реалізації методів соціального інжинірингу, соціоінженери можуть використовувати певні джерела даних про свої потенційні жертви, або так звані ігрові площадки, в межах яких здійснювати певні етапи атаки. Сюди можна віднести різноманітні соціальні мережі, соціальні закладки, соціальні каталоги чи соціальні бібліотеки.

Бурхливий розвиток ІТ-технологій, дає змогу соціоінженеру повний набір засобів для здійснення несанкціонованого доступу до інформації, за допомогою методів соціальної інженерії. Нескладно прогнозувати, що завдяки процесу глобальної комп'ютеризації соціоінженери на довірі не відчуватимуть дефіциту жертв.

В природі виділяють багато методів соціальної інженерії, існує їх класифікація за певними ознаками, характеристиками на особливостями проведення. Серед усіх методів соціального інжинірингу, найбільш розповсюдженими є наступні: претекстинг, фішинг, аналіз сміття, індивідуальні підходи та інші. Розглянемо коротко кожні з них.

Претекстинг – застосування заздалегідь розробленого сценарію, щоб змусити вибрану жертву до розголошення інформації чи виконання дій, які необхідні зловмиснику та які зазвичай вона б не здійснила [3].

Фішинг – метод, який полягає в тому, щоб заволодіти інформацією приватного характеру нечесним шляхом. Сюди можуть відноситись оманливі листи від банків, організацій з шкідливими веб-посиланнями. Сюди також можуть відноситись телефонні дзвінки, під час яких соціоінженер може видавати себе за будь-яку особу.

Метод аналізу сміття полягає у використанні зловмисником не знищеної інформації з корзини (у випадку електронного сміття) або паперових документів.

До індивідуальних підходів відносяться такі методи як залякування (шантаж), переконання, виклик довіри.

Також, якщо відштовхуватись від класифікації методів соціального інжинірингу, то тут можуть поділятись методи за дистанційністю здійснення, за типом атакованого джерела, за порушенням характеристик безпеки інформації.

Методам соціального інжинірингу слід приділяти серйозну увагу, оскільки, як свідчить статистика вони стають дедалі популярними, особливо на території України.

Література

1. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
2. Озерський К.Г. Соціотехнічні методи несанкціонованого доступу до інформації. Веб-сайт молодіжної електронної наукової школи-конференції «Актуальні проблеми захисту інформації та інформаційної безпеки». [Електронний ресурс]. – Режим доступу з http://stavkombez.ru/conf/category/section2/
3. Соціальна інженерія. Веб-сайт Вікіпедія. [Електронний ресурс]. – Режим доступу з https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека)