УДК 004

Т.А. Дмитренко, к.т.н., доцент
кафедри комп'ютерних та
інформаційних технологій і систем
Є. Нікітченко, студент, 102-ТН
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Соціальна інженерія є одним із основних напрямів дослідження доступу до інформації, заснований на особливостях психології людей.

Соціальна інженерія – це мистецтво маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації іншим способом, ніж як через засоби технічного руйнування баз даних.

Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних і інших захищених систем. Є декілька головних варіантів нападу, які використовуються при проведенні атак за допомогою соціальної інженерії:

- онлайн ();
- телефон;
- аналіз сміття;
- особисті підходи.

Однак крім цього, треба також знати цілі нападу, розуміти, що зловмисник сподівається отримати. Його цілі засновані на тих же потребах, які керують усіма нами: гроші, соціальний поступ і самоствердження.

Мережеві загрози. У нашому все більш і більш пов'язаному діловому світі персонал часто використовує інформацію і відповідає на запити, які отримує за допомогою електроніки з середини і ззовні компанії. Таке забезпечення зв'язку дає можливість зловмисникам підійти до вашого персоналу, використовуючи відносну анонімність мережі Internet. Також не слід забувати про комп'ютерні віруси, які також можна підхопити.

Телефон. У наші часи доступу до телефону буває достатньо, щоб, наприклад, украсти дані банківської карти, а то і зовсім відіслати кошти прямо на свій рахунок, або знайти в ньому якусь особисту інформацію і шантажувати людину.

Аналіз сміття. Незаконний аналіз сміття – цінна діяльність для зловмисника. Ділові паперові відходи можуть містити інформацію, яка має безпосередню вигоду для хакера (наприклад номера рахунків і призначених для користувача ідентифікаторів) або можуть служити основною інформацією, наприклад, телефонний довідник організації або списки співробітників.

Особисті підходи. Для хакера найпростіший і найдешевший шлях отримання інформації – це попросити про це безпосередньо. Цей підхід

може здаватися грубим і очевидним, але це основа шахрайства з незапам'ятних часів. Існує чотири різновиди такого підходу:

Залякування.

Переконання.

Фізичні методи: менш поширений, але більш ефективний для хакера підхід є прямим, особистим контактом з адресатом. Хоча ці підходи мають набагато більші ризики для злочинця. Зростання в використанні мобільних технологій, які дають можливість користувачам приєднатися до корпоративних мереж, в той час як вони знаходяться в дорозі або вдома, є іншою головною загрозою IT-ресурсі в компанії. Можливі напади включають як найпростіші нападу, так і більш складні. Хоча основна частина великих компаній розробила інфраструктури захисту сайту, однак, офіси середнього розміру можуть бути слабкіше обізнані про правила контролю відвідувачів офісу. Ситуація, в якій злочинець слід за кимось проходить в офіс, є дуже простим прикладом нападу з використанням соціальної інженерії. Правила повинні передбачати неможливість проходу в будівлю компанії без належного дозволу. Отже, захист від атак соціальної інженерії безсумнівно, одне з найскладніших в розробці справ. Даний тип захисту не можна побудувати виключно технічними методами. Крім того, хотілося б відзначити що для побудови системи протидії таким атакам, безсумнівно, варто залучати професійних консультантів, а не намагатися будувати захист своїми силами.

Література

1. Соціальна інженерія (безпека) [Електронний ресурс]/Вікіпедія: Вільна енциклопедія. — Режим доступу: https://uk.wikipedia.org/wiki/ Соціальна_інженерія _(безпека)

2. Соціальна інженерія [Електронний ресурс]/Режим доступу: http://wiki.tntu.edu.ua/Соціальна_інженерія