УДК 681.3.06

Нікітіна Є.О., студентка гр. УБіт-14-1
Науковий керівник: Тимофєєв Дмитро Сергійович, ст. викладач кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

СОЦІАЛЬНА ІНЖЕНЕРІЯ В СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У роботі розглянуто схеми та методи соціальної інженерії; види шахрайства, основою яких є соціальна інженерія; способи захисту від загроз, основою яких є соціальна інженерія.

Ключові слова – соціальна інженерія, соціальний хакер, соціоінженер, соціотехніка.

ВСТУП

В майбутньому найбільшу загрозу інформаційній безпеці як великих компаній, так і звичайних користувачів, будуть представляти методи соціальної інженерії, що застосовуються для злому існуючих засобів захисту.

Основною причиною цього є те, що застосування соціальної інженерії не вимагає значних фінансових витрат і досконалого знання інформаційних технологій.

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Соціальна інженерія – метод несанкціонованого доступу до інформації або до систем зберігання інформації без використання технічних засобів.

Метод заснований на використанні слабкостей людського фактору. [1]

Дослідження показують, що людям притаманні деякі поведінкові схильності, які можна використати для маніпулювання. Більшість зломів систем безпеки відбуваються завдяки використанню соціальної інженерії, а не електронному злому. [2]

БАЗА ДЛЯ СОЦІАЛЬНИХ ІНЖЕНЕРІВ (СОЦІАЛЬНИХ ХАКЕРІВ)

Першим етапом будь-якої атаки є дослідження. Соціоінженер повинен знати хто з працівників компанії має доступ до інформації, яка його цікавить, хто в якому підрозділі працює, де розташовані підрозділи, яке програмне забезпечення встановлено на корпоративних комп`ютерах і т.д.

Соціальний хакер повинен орієнтуватися в термінології, володіти професійним жаргоном, знати внутрішні порядки компанії-жертви.

Наступним етапом в діяльності соціоінженера є розробка плану атаки.

Найпоширенішими методами атак є:

- отримання, передача або несанкціонована зміна паролів;
- створення облікових записів (з правами користувача або адміністратора);
- запуск шкідливого ПЗ;
- отримання інформації про способи віддаленого доступу до корпоративної інформаційної мережі;
- несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи;
- передача або поширення конфіденційної інформації. [3]

СХЕМА ДІЇ ТА МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Схема дії соціальної інженерії:

- визначення мети впливу на об`єкт;
- збір інформації про об`єкт;

- виявлення найбільш зручної мішені впливу;
- створення необхідних умов для впливу;
- примус до виконання потрібної дії;
- досягнення потрібного результату. [4]

Методи соціальної інженерії

Віртуальні методи

Соціальні хакери, як правило, використовують електронну пошту або спливаючі вікна. У більшості випадків атаки спрямовані на конкретну особу і основною метою їх здійснення є отримання ідентифікаційних даних жертви.

Телефонні технології дають змогу встановити менш масові, але більш особисті контакти з жертвами.

Фізичні методи

Встановлення особистого контакту з жертвою є менш популярним, але ефективнішим способом підготовки до здійснення атаки.

Фізичні методи є більш ризикованими, але вони надають ряд переваг.

Поширення мобільних технологій, які дають змогу користувачам підключатись до корпоративних мереж вдома або в дорозі, є серйозною загрозою для компаній.

Організація безпеки систем співробітників, які працюють вдома, у більшості випадків, обмежується технічними засобами. Політика безпеки повинна вимагати, щоб домашні системи даних працівників були захищені брандмауерами (міжмережевими екранами), які блокуватимуть спроби зловмисників отримати доступ по мережі ззовні. [2]

ВИДИ ШАХРАЙСТВА, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Фішинг – процес відправки електронних або паперових листів, які начебто надходять від достовірного джерела. Мета – отримання конфіденційної інформації адресата.

Фармінг – встановлення на комп`ютери користувачів шкідливих програм, які після запуску збирають дані платіжних сайтів і надсилають їх зловмиснику.

Вішинг – процес отримання інформації за допомогою телефону. Зловмисники використовують phone spoofing, тобто підміну телефонного номеру.

Уособлення – вид шахрайства, у якому соціальний хакер виступає в ролі іншої людини. Його метою є отримання потрібної інформації. [4]

Зворотна соціальна інженерія. Мета соціоінженера – змусити жертву звернутися до нього за «допомогою». Соціальний хакер може використовувати диверсію або рекламу. [1]

ЗАХИСТ ВІД ЗАГРОЗ, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Основним способом захисту від соціальної інженерії є навчання.

Персонал підприємства повинен мати чіткі інструкції щодо спілкування зі сторонніми людьми.

Всім працівникам у день прийому на роботу необхідно повідомити, що видані їм паролі є власністю компанії і їх не можна використовувати у власних цілях.

Повинен існувати алгоритм для встановлення особи відвідувача.

Компанія може витрачати значні кошти на удосконалення технічних засобів забезпечення інформаційної безпеки, але вони будуть марними, якщо персонал буде нехтувати заходами з протидії соціальним хакерам. [1]

ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ ВІД ЗАГРОЗ, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Для створення системи захисту персоналу від загроз, основою яких є соціальна інженерія, потрібно виконати три дії.

I. Розробка стратегії управління процесом забезпечення безпеки. Потрібно визначити завдання захисту від соціотехічних загроз і призначити працівників, відповідальних за їх виконання.

II. Оцінка ризику. Необхідно проаналізувати всі соціотехнічні загрози і визначити ступінь небезпеки.

III. Інтеграція принципів захисту від соціотехнічних атак в політику безпеки. Потрібно розробити та перевірити політики і процедури, які регламентують дії персоналу в ситуаціях, які можуть бути соціотехнічними атаками. [3]

РЕАЛІЗАЦІЯ ЗАХОДІВ ЗАХИСТУ ВІД ЗАГРОЗ, ОСНОВОЮ ЯКИХ Є СОЦІАЛЬНА ІНЖЕНЕРІЯ

Для реалізації заходів захисту від загроз, основою яких є соціальна інженерія, використовують інформування та управління інцидентами.

Інформування. Потрібно ознайомити персонал з розробленою політикою безпеки. Для інформування можна обрати структуровані навчальні курси, неформальні зустрічі і т.д.

Управління інцидентами. Працівники служби підтримки повинні знати порядок дій у разі соціотехнічної атаки. Одним з принципів управління інцидентами є те, що у відповідь на атаку проводиться аудит безпеки.

При реєстрації інциденту керівний комітет із забезпечення безпеки повинен з`ясувати представляє він нову загрозу або є зміненою загрозою. Після цього необхідно створити або оновити політики і процедури.

Для управління інцидентами служба підтримки повинна використовувати затверджений протокол, який містить відомості про: жертву атаки; підрозділ жертви; дату атаки; опис атаки; результат атаки; наслідки атаки; рекомендації.

Реєстрація інцидентів дає змогу визначити шаблони атак і покращити захист від майбутніх атак. [5]

ВИСНОВОК

Навіть найбільш надійні технології безпеки малоефективні у боротьбі з хакери, які користуються методами соціальної інженерії. Робота з персоналом та навчання працівників застосуванню політики безпеки і технікам протистояння соціальним хакерам є необхідною складовою комплексної системи безпеки.

Стратегія управління процесом забезпечення безпеки повинна давати загальне уявлення про загрози, основані на соціальній інженерії, яких зазнає компанія, і визначити працівників, які будуть відповідальними за розробку політик і процедур для блокування цих загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Краткое введение в социальную инженерию [Електронний ресурс] – Режим доступу https://habrahabr.ru/post/83415/. Назва з екрана.

2. М. В. Кузнецов, И. В. Симдянов. Социальная инженерия и социальные хакеры. Учебник / М. В. Кузнецов, И. В. Симдянов. - СПб.: БХВ-Петербург, 2007. – 10 с.

3. Социальная инженерия - методы, которыми хакеры пользуются, чтобы обмануть корпоративных пользователей и обойти самые мощные системы информационной безопасности. [Електронний ресурс] – Режим доступу https://www.eos.ru/eos_delopr/eos_delopr_intesting/detail.php?ID=11199. Назва з екрана.

4. Старостина Е., Хрусталева Е. Мишень социальной инженерии – это вы сами. IT Manager, 2015, 142, 64-67.

5. Как защитить внутреннюю сеть и сотрудников компании от атак, основанных на использовании социотехники [Електронний ресурс] – Режим доступк https://technet.microsoft.com/ru-ru/library/cc875841.aspx#EBAA. Назва з екрана.