СУЧАСНИЙ МЕНЕДЖМЕНТ

Черноус В.І.
студентка,
Національний технічний університет України
«Київський політехнічний інститут»

ВИКОРИСТАННЯ СЦЕНАРІЇВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ІНСАЙДЕРСЬКИХ АТАК

Соціальною інженерією прийнято називати одну з частин соціальної психології, спрямовану на те, щоб маніпулювати людьми, тобто породжувати в їхньому розумі визначену, потрібну (у даному випадку – інсайдерові) модель поведінки. Основні засоби, що дозволяють, наприклад, отримати від необережних користувачів паролі для входу в корпоративні мережі, добре відомі злочинцям.

Але власне чому інсайдери використовують соціальну інженерію для одержання інформації? Відповідь очевидна – тому що це простіше. Навіщо намагатися обходити нові системи безпеки, шукати слабкі місця в програмних продуктах безпеки, коли можна зробити кілька дзвінків і отримати аналогічний результат. При цьому використання соціальної інженерії зводить до мінімуму імовірність виявлення зловмисника. Ретельно спланована та успішно проведена соціальна атака залишиться непоміченою в організації. Більшість співробітників можуть навіть не згадати про те, що колись вони повідомили конфіденційну інформацію людині по той бік телефону. Усе тому, що атака соціального інженера буде виглядати для жертви, як повсякденна дія. Згідно з даними досліджень у цій галузі, в середньому лише одна людина з десяти може розпізнати і відбити атаку соціального інженера [1, с. 251].

Існує ряд вже готових сценаріїв соціальної інженерії, знаючі які можна планувати ряд заходів захисту інформації від інсайдерських атак, який дозволить у подальшому розробити систему організаційних заходів захисту інформації від інсайдерських атак вже для конкретної організації.

Сценарій із новим співробітником. Наприклад, представившись начальником сусіднього відділу, злочинець може попрохати ще

погано обізнану з правилами безпеки жертву виконати на його комп'ютері якісь дії. Пояснити таке прохання він може описавши якісь проблеми, з якими він зіштовхнувся. І жертва, намагаючись бути корисною, виконає операції на потрібному комп'ютері (наприклад, додасть нового користувача для вилученого доступу або завантажить шкідливе ПО) сама не усвідомлюючи того, що вона робить.

Щоб запобігти атаці, компанія повинна заборонити слідувати проханням незнайомців крім ситуацій, офіційно дозволених менеджером. Ситуації, що дозволяються, включають: запити, що робляться добре відомою людиною, коли точно пізнається голос; коли підтверджено особистість питаючого завдяки спеціальним процедурам перевірки, описаним у рекомендаціях зі створення політики безпеки; коли дія дозволена начальником, або кимсь, хто добре знає ту людину.

Сценарій із співробітниками, що не усвідомлюють значення інформації. Незнання рівня важливості може спровокувати витік конфіденційної або важливої для підприємства інформації. До даного виду співробітників відносяться реєстратори, секретарі, телефоністи, адміністративні помічники, охоронці та інші.

Щоб запобігти атаці, інформація в організації повинна бути класифікована, співробітники повинні бути навчені розпізнавати клас інформації. Якщо класифікація не була приведена – то вся інформація повинна сприйматися співробітниками, як конфіденційна, якщо не позначено інакше.

Співробітники відділу кадрів володіють інформацією про структуру організації і про можливості контактів з іншими співробітниками організації. Дана інформація може являти цінність для інсайдера на першому етапі нападу: одержавши інформацію про співробітників, або, що ще небезпечніше, співробітників конкретного типу, зловмисник може більш точно спланувати свою атаку, підвищивши тим самим імовірність її здійснення.

Щоб запобігти атаці, необхідно розробити окремий підрозділ політики безпеки для відділу кадрів використовуючи рекомендації зі створення політики безпеки.

Часто, представившись менеджером з іншої філії, інсайдер може запитати відкриту інформацію (про наявність товару, відсутнього в його філії, або інше) і завести дружню розмову з жертвою. Після зав'язування ділової дружби, атакуючий може використовувати безліч засобів для одержання інформації, що вже являє для нього

зацікавленість. Наприклад, прикинувшись, що в їхній філії всі комп'ютери вийшли з ладу і попросити жертву подивитися якусь інформацію про клієнта або фірму. Після чого побалакати «як завжди» про інші речі з жертвою і вона, можливо, і не згадає потім про це прохання. Коли прийшов час для атаки, жертва втрачає пильність та обережність [2, с. 98].

Тому важливо пам'ятати, що техніка побудови довіри є однієї з найбільш ефективних тактик. Працівники мають завжди бути готовими до ідеї, чи добре вони знають людину, з якою нещодавно розмовляли. Адже в деяких випадках вона може бути не тою за кого себе видає.

Сценарій із використанням страху жертви перед авторитетом. Зловмисник використовує страх жертви перед начальством або главою компанії для одержання важливої інформації. Більшість службовців бояться своїх начальників і готові зробити усе, що завгодно, аби не дратувати верхівку. Цим уміло користуються й інсайдери.

Наприклад, інсайдер дзвонить жертві та намагається з'ясувати, де ж його звіт, що жертва вже давно повинна була переслати. Так само зловмисник говорить, що роботу, де використовується даний звіт, необхідно здавати вже завтра і бос буде дуже незадоволений, коли довідається, що зловмисник нічого не зробив через жертву. Під таким тиском і страхом перед «великим босом», жертва готова передати будь-як звіти, аби не випробувати на собі його гнів.

Тому варто проводити тренінги для співробітників мають містити в собі курс навчання персоналу уникати впливу авторитету в дружніх або ділових відносинах, але без нанесення шкоди спілкуванню.

Сценарій із небезпечним паролем. Зловмисник роз'ясняє політику безпеки жертві представляючись співробітником з відділу безпеки. Наприклад, інсайдер відволікає жертву тим, що пояснює загальновідомі принципи безпеки в організації. В ході розмови заводить тему пароля жертви та дізнається чи використовує вона в ньому тільки букви або ще і цифри чи додаткові символи. Жертва швидше за все не використовує тільки букви. І зловмисник може запитати її пароль і запропонувати як його змінити – додати цифри або символи наприкінці. Зловмисник так само пропонує варіант зміни пароля, і жертва його приймає.

Тому, перш, ніж новим співробітникам буде дозволено одержати доступ до комп'ютерних систем, вони повинні бути

навчені правилам безпеки, особливо правилам про нерозголошення паролів. Усі, хто мають доступ до комп'ютера, повинні розуміти, що навіть така проста процедура, як зміна пароля, може привести до серйозного розладу в безпеці системи.

Сценарій із спрямуванням об'єкта за неправильною веб-адресою. Часто люди не зауважують, що адреса сайту, за якою вони перенаправляються відрізняється від оригінальної, хоч і є схожою. Наприклад, користувач Інтернет-магазину «books.com» може подумати, що адреса «books-nauka.com» є також веб-адресою цього магазину, але з безпечним і тематично спрямованим доступом. Насправді ж ця адреса зареєстрована зловмисником спеціально для одержання особистої інформації користувача. Повністю скопійований з оригінального сайту інтерфейс також сприяє тому, що користувач нічого не помічає.

Жертва одержує листа з пропозицією одержати бонуси (гроші, або участь у розіграші подарунків) за поновлення своєї особистої інформації на сайті, яким жертва постійно користується (Інтернет-магазини, аукціони). Але посилання, що додається наприкінці листа веде не на потрібний сайт, а на сайт зі схожою адресою. Жертва йде за посиланням, бачить звичний інтерфейс (повністю скопійований з оригіналу) та заповнює особисту картку бажаючи одержати подарунок. Зловмисник у такий спосіб може одержати практично будь-яку інформацію про жертву.

У погоні за бонусами люди втрачають пильність. Але ж не так складно перевірити адресу посилання, на яку намагаються направити. Тим більше в цьому випадку, коли необхідно вводити особисту інформацію. Користувач має перевіряти, чи відповідає сайт на якому він вводить особисту інформацію всім мірам безпеки. Чи ввімкнене шифрування переданої інформації, чи не застаріли сертифікати дійсності.

Таким чином, на базі розглянутих сценаріїв соціальної інженерії керівництво певної конкретної компанії може розробити політику безпеки та впроваджувати міри захисту інформації не лише на рівні програмного забезпечення й апаратного захисту.

Адже при будь-якому, навіть найвищому рівневі технічного захисту інформації організації залишається людський фактор, не досконально керований автоматизованими системами та програмами захисту інформації. Тому такий напрям, як, наприклад, соціальна інженерія цілком здатен показати ряд інструментів-

сценаріїв роботи саме з людським фактором. У нашому випадку – для досягнення успіху завдання інсайдером в організації.

Список використаних джерел:

1. Скиба В.Ю., Курбатов В.А. Защита от внутренних угроз информационной безопасности. – СПб.: Питер 2008. – 320 с.

2. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправдання безопасность. М.: Компания АйТи; ДМК Пресс, 2004. – 348 с.