УДК 004.7

Власьєв К.Є.

ЗАГРОЗИ І ЗАХИСТ ВІД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Постановка проблеми. Сьогодні в інформаційні безпеці найважливішу роль відіграє людський чинник. Думка, що проблему інформаційної безпеки можна вирішити просто за допомогою апаратних і програмних засобів, є помилковою, тому що технології безпеки, яким довіряють, міжмережні екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережевих атак - малоефективні в протистоянні хакерам. З появою різних технік і методик злому з'явився усім відомий, але забутий прекрасний метод злому - соціальна інженерія. Як набір технік вона може бути використана для маніпулювання людьми з метою виконання ними яких-небудь дій або отримання конфіденційної інформації. Соціоінженерні атаки найуспішніше проходять коли враховуються культурні особливості нації – довірливість, відплата добром, особиста довіра, дружні відносини, прихильність до корпоративного порядку тощо. В основному соціальна інженерія застосовується для отримання комп'ютерного доступу і майже завжди жертва і шахрай не зустрічаються віч на віч. Система безпеки буде комплексною тільки тоді, коли буде вестись потужна робота зі співробітниками щодо застосування політики безпеки і техніки протистояння соціоінженерам. Дуже важливо знати усі загрози від соціальної інженерії і створити систему безпеки, яка б захистила корпоративну таємницю.

Мета статті. Розкрити принципові загрози при застосуванні методів соціальної інженерії та надати рекомендації з захисту при застосуванні методів соціальної інженерії для несанкціонованого отримання інформації в корпоративному середовищі.

Матеріали та результати досліджень. Методи соціальної інженерії достатньо різноманітні і проведені дослідження дозволяють стверджувати про їх ефективність з кожного вектору нападу.

Розрізняють наступні головні вектори нападу, які використовуються при проведенні атак за допомогою соціальної інженерії (рис.1):

- он-лайн (інтерактивно);
- телефон;
- аналіз сміття;
- фізичні підходи
- особисті підходи;
- реверсивна соціальна інженерія.

На рис.1 показана структурна схема векторів нападу при проведенні атак методами соціальної інженерії. Проте, крім цього необхідно також знати мету нападу, розуміти, що хочуть одержати. Розуміти, що мета отримання інформації заснована на все тих же потребах, які управляють всіма нами: гроші, соціальне становище і самоствердження. Розглянемо послідовно особливості кожного з векторів нападу.

Мережеві (он-лайн) погрози. У нашому все більш і більш пов'язаному діловому світі, персонал часто використовує інформацію і відповідає на запити, які одержує за допомогою електроніки зсередини і зовні компанії. Таке забезпечення зв'язку дає можливість хакерам підійти до вашого персоналу, використовуючи відносну анонімність мережі Internet (рис.2).

Використання електронної пошти як інструменту соціальної інженерії стало звичайним за минуле десятиліття. Багато співробітників одержують десятки або сотні електронних листів щодня і від ділових, і від приватних кореспондентів. Об'єм електронної пошти може заважати приділяти ретельну увагу до кожного повідомлення.

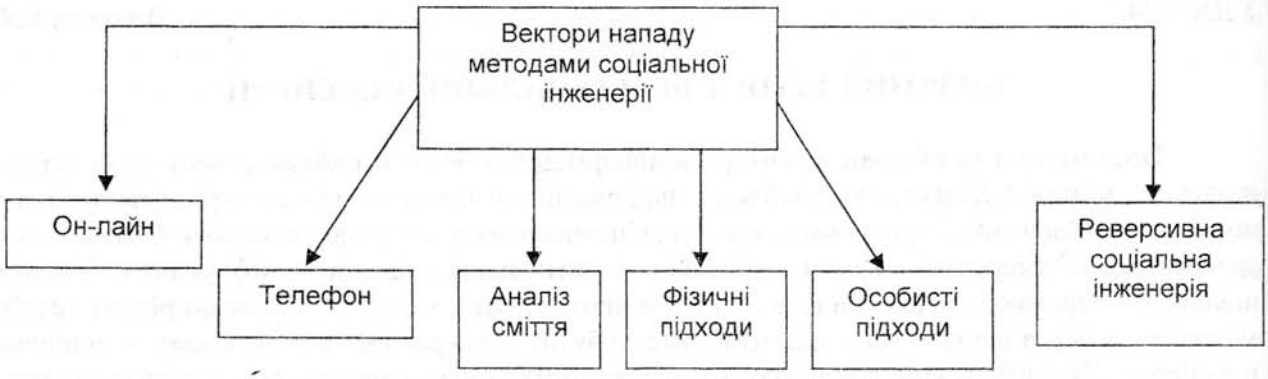

Рис1. Вектори нападу при проведенні атак методами соціальної інженерії

Рис 2. Вектори нападу методами соціальної інженерії при використанні мережі Інтернет.

Phishing - це використання електронної пошти для отримання персональної інформації від користувача. Хакери посилають поштові повідомлення, які, здається, виходять з «правильних» організацій - банків або компаній партнерів.

Кожен phishing-лист маскується під запит про призначену для користувача інформацію, який нібито повинен полегшити користувачу встановити оновлення або забезпечити додаткове обслуговування.

Новий вигляд phishing-атак - spear-phishing. Це вузьконаправлені координовані атаки на організацію або конкретного користувача з метою отримання критично важливих даних.

В даному випадку хакер здійснює правдоподібніший обман, максимально наближаючись до цільової групи і використовуючи для маскування внутрішню інформацію компанії Цей підхід набагато складніший, тому що в даному випадку хакеру необхідна внутрішня інформація компанії.

Щоб ефективніше чинити опір хакерським нападам, що використовують соціальну інженерію, треба відноситися зі скептицизмом до будь-чого несподіваного у поштовій скриньці.

На додаток до цих рекомендацій, Ви повинні включити приклади нападів phishing, при консультуванні та навчанні персоналу. Після того, як користувачі розпізнають одне обдурювання phishing, вони зрозуміють, що це набагато простіше, ніж здавалося, і почнуть звертати увагу на інші.

Спливаючі додатки і діалогові вікна. Помилково припускати, що персонал використовує доступ компанії до Internet тільки для службових потреб. Такі дії персоналу

можуть принести службовцям небезпеку контакту з хакерами, що використовують соціальну інженерію.

Найзвичайніші методи спокусити користувача натиснути кнопку в діалоговому вікні - це прислати користувачу попередження про проблему, яке виглядає як відображення реалістичної операційної системи або прикладного повідомлення про помилки, або пропозиція додаткових послуг, наприклад, безкоштовне завантаження, яке нібито примусить комп'ютер користувача працювати швидше.

Захист користувачів від спливаючих додатків, що використовують соціальну інженерію – це головним чином функція розуміння. Потрібно впевнитися в тому, що користувачі знають, що вони не повинні натискати посилання на спливаючих вікнах, не порадившись з персоналом підтримки. Тому ваш персонал повинен бути упевнений, що штат підтримки не буде поверхнево відноситися до прохань користувачів про допомогу, якщо користувач проглядає Internet. Ці довірчі відносини можна передбачити політикою безпеки щодо роботи в Internet.

Системи миттєвої передачі повідомлень. Миттєва передача повідомлень (ІМ) - відносно нове середовище зв'язку, яка вже встигла одержати широку популярність як діловий інструмент. Безпосередність і доброзичливий інтерфейс ІМ, роблять його «багатим мисливським угіддям» для різноманітних технік нападів, що використовують соціальну інженерію, тому що користувачі розцінюють дану службу як телефон і не пов'язують її з потенційними погрозами ПЗ. Дві головні атаки, які можна відтворити, використовуючи ІМ - гіперпосилання на malware в межах ІМ-повідомлення і розсилка фактичних файлів. Є безліч потенційних погроз, властивих ІМ при атаці за допомогою соціальної інженерії. Перший - невимушеність ІМ. Балакуча природа ІМ, разом з опцією надання прізвиська або помилкового імені означає, що не зрозуміло, з ким ви розмовляєте, це значно розширює можливості для атаки.

Якщо Ви прагнете використовувати зручність ІМ, ви повинні включити ІМ-безпеку у політику безпеки. Для управління ІМ в межах вашої компанії, Ви повинні встановити наступні п'ять правил використання:

- ввести стандарт на єдину ІМ платформу;
- визначити параметри настройки безпеки розгортання;
- рекомендувати, користувачам не використовувати настройки за замовчуванням.
- встановити стандарти для обирання паролей;
- розробити керівництво щодо використання.

Погрози при використанні телефонного зв'язку. Телефон пропонує унікальний спосіб нападу для хакерів. Це - знайоме середовище, проте воно також знеособлює того, хто дзвонить, тому що адресат не може бачити хакера.

Є три головних типи атак хакерів, що нападають на офісні АТС, під час яких вони:

- просять інформацію, імітуючи законного користувача, щоб або звернутися до телефонної системи безпосередньо або дістати видалений доступ до комп'ютерних систем;
- дістають доступ до "вільного" використання телефону;
- дістають доступ до системи комунікацій.

Запити про інформацію або доступ по телефону - відносно вільна від ризику форма нападу. Якщо адресат стає підозрілим або відмовляється виконувати запит, хакер може просто покласти трубку. Але такі напади складніші, ніж атака хакера, що просто дзвонить в компанію і просить призначений для користувача ідентифікатор і пароль. Хакер, звичайно, пропонує сценарій, просячи або пропонуючи довідку, перш ніж майже машинально відбувається запит про особисту або ділову інформацію.

Служба ІТ-підтримки або довідкова служба - є одним із засобів захисту проти атак хакерів, але, разом з тим, це адресат для хакерів, що використовують соціальну інженерію. Хоч штат служби підтримки повідомлено про загрозу злому, він також повинен навчатися,

щоб допомогти і підтримати користувачів, пропонуючи їм поради і вирішення їх проблем. Іноді ентузіазм, що демонструється штатом технічної підтримки в забезпеченні рішення, примушує забути їх про свої обов'язки щодо виконання процедур безпеки. Якщо службі підтримки надають строгі стандарти безпеки, вимагаючи доказів, що можуть перевірити правильність запиту користувача, то з'являються зайві перешкоди в роботі.

Служба підтримки повинна балансувати між безпекою і діловою ефективністю, а політика і процедури безпеки повинні допомагати в цьому.

Важче захистити аналітика служби підтримки проти внутрішнього злому. У внутрішнього хакера буде хороше практичне знання внутрішніх процедур щоб упевнитися, що ці знання забезпечують всю необхідну інформацію перед тим, як зробити сервісний запит. Процедури захисту повинні забезпечити подвійну роль в цій ситуації:

- аналітик служби підтримки повинен мати гарантії аудиту всіх дій;
- аналітик служби підтримки повинен мати добре структуровану процедуру дій обробки запитів користувачів.

Якщо користувачі знають про ці правила, і керівництво підтримує їх виконання, то дотримання таких правил набагато ускладнить дії хакерів, особливо в тому, щоб реалізувати атаку і залишатися невиявленим. Створення журналів (аудит всіх процедур) - найцінніший інструмент в запобіганні і розкритті інциденту.

Незаконний аналіз сміття - цінна діяльність для хакерів. Ділові паперові відходи можуть містити інформацію, яка має безпосередню вигоду для хакера (наприклад номери рахунків і призначених для користувача ідентифікаторів), або можуть стати основною інформацією, наприклад, телефонний довідник організації або списки співробітників. Цей тип інформації є безцінним для хакера, що використовує соціальну інженерію, тому що це допомагає йому здаватися вірогідним співробітником компанії під час атаки.

Ще корисніші електронні носії. Якщо в компанії немає правил управління відходами, які включають позбавлення від несправних використаних носіїв, то на викинутих жорстких дисках, компакт-дисках та інших цифрових носіях можна знайти всі види інформації. В цьому випадку політика безпеки компанії повинна включати положення про управління життєвим циклом носіїв, включаючи процедури руйнування або стирання.

Атаку на сміття не можна вважати правопорушенням, тому необхідно інформувати персонал і включити в політику безпеки компанії правила поводження з непотрібними матеріалами, різноманітним сміттям та іншими відходами.

На додаток до управління зовнішніми відходами - паперовими або електронними носіями, які можуть бути доступні поза компанією - необхідно також управляти внутрішніми відходами. Одним з найефективніших заходів при роботі зі сміттям є - специфікація класифікації даних. Визначте різні категорії інформації і як персонал повинен їх оброблювати.

Особисті підходи. Для хакера найпростіший і найдешевший шлях отримання інформації - це попросити про це безпосередньо. Цей підхід може здаватися грубим і очевидним, але це є основою шахрайства з незапам'ятних часів. Існує чотири різновиди такого підходу, які показані на рис.3.

Безперечна довіра - одна з цілей хакера. Захист проти нападу залякування – це розвиток культури "відсутності страху із-за помилки" в межах організації. Якщо нормальна поведінка - ввічливість, то успіх залякування зменшується.

Переконання завжди було важливим людським методом досягнення особистих цілей. Створена вами атмосфера порозуміння в компанії і політика паролів - ваш кращий захист.

Якщо хакер, що використовує соціальну інженерію, одержує постійну роботу в межах вашої компанії, то кращий захист – це розуміння і виконання персоналом політики безпеки.

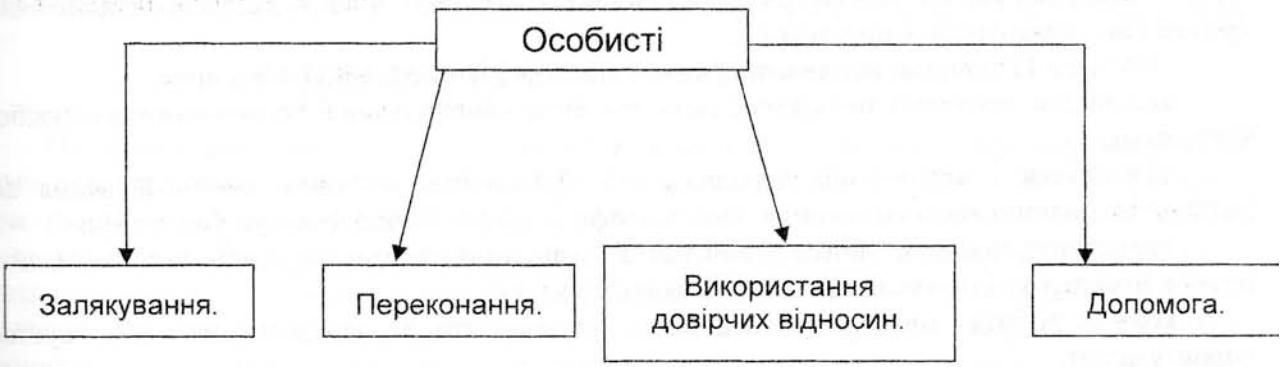

Рис 3. Різновиди особистих підходів при здобуванні інформації.

Нарешті, напади «допомоги» можуть бути скорочені, для чого необхідна ефективна сервісна підтримка. Внутрішній помічник - часто результат втрати довіри до існуючих послуг служби підтримки компанії. Необхідно передбачити, щоб штатні працівники входили в контакт з сервісною службою, а не з неправомочним внутрішнім експертом - або гірше, експертом, що не належить до компанії. Для цього необхідно:

- визначити у політиці безпеки, що служба підтримки – це єдине місце, куди користувачі повинні повідомляти про проблеми;
- гарантувати, що служба підтримки має узгоджений процес відповіді в межах встановленого рівня обслуговування;
- перевіряти виконання сервісних робіт регулярно, щоб упевнитися, що користувачі одержують відповідний рівень відповідей і рішень.

Не можна недооцінювати важливість служби підтримки в забезпеченні захисту першого рівня проти нападів соціальної інженерії.

Фізичні підходи. Менш поширений, але ефективніший для хакера підхід – це прямий, особистий контакт з адресатом. Тільки найпідозріліший службовець буде сумніватися в законності того, хто представляється і просить або пропонує допомогу в використанні комп'ютерної системи. Хоч ці підходи мають набагато більші ризики для злочинця, проте переваги очевидні.

Зростання використання мобільних технологій, які дають можливість користувачам приєднатися до корпоративних мереж, коли вони знаходяться в дорозі або вдома, є іншою головною загрозою IT-ресурсам компанії. Можливі напади включають як найпростіші напади, так і складніші.

Незважаючи на те, що основна частина великих компаній розробила інфраструктуру захисту сайту, офіси середнього рівня можуть бути менше обізнані з правилами контролю відвідувачів офісу. Ситуація, в якій неправомочна особа слідує за кимось, входячи в офіс, є дуже простим прикладом нападу з використанням соціальної інженерії.

Захищеність проти таких погроз по суті залежить від виконання користувачами дій, заснованих на ефективній політиці безпеки компанії, яка повинна враховувати наступні три складові: сайт компанії; будинок; мобільну роботу.

Правила повинні передбачати неможливість входу в будівлю компанії без належного дозволу. Декілька простих умов в межах політики безпеки компанії зроблять майже неможливим фізичний напад з використанням соціальної інженерії в межах будівлі. Ці умови можуть включити:

- ідентифікацію за допомогою фотографій на пропусках, які необхідно показувати всякий раз, коли співробітник входить або покидає будівлю;
- введення книги відвідувачів, в якій розписується відвідувач і співробітник, якого він відвідує, зазначається час прибуття і виходу з будівлі;

- введення картки відвідувача, яка повинні бути видно, поки відвідувач знаходиться в будівлі і яка повертається при відході.

Послуги ІТ повинні включати правила, що передбачають наступні умови:

- кожна дія технічної підтримки повинна бути запланована і уповноважена службою підтримки;
- підрядчики і внутрішній персонал, які здійснюють локальне обслуговування або інсталяцію повинні мати документи, що ідентифікують особу, включаючи фотографію;
- користувач повинен увійти в контакт з ІТ-відділом підтримки, щоб сповістити, коли прибув інженер з підтримки і коли він закінчив роботу;
- кожна робота має документально оформлюватися нарядом, що підписується користувачем;
- користувач ніколи не повинен звертатися до інформації або реєстрації на комп'ютері, щоб забезпечити доступ інженера.

Останній пункт є критичним. Це необхідно для групи ІТ-послуг, щоб упевнитися, що інженер, який не працює в даній організації має достатні особисті права доступу, щоб виконувати роботу. Якщо інженер не має достатніх прав доступу, щоб завершити завдання, він повинен увійти в контакт з сервісною службою. Ця вимога є основною, тому що невибагливий сервісний інженер для компанії обчислювальних центрів - одна з найвигідніших вакансій, яку може знайти передбачуваний хакер. Це робить хакера і володарем повноважень і помічником в той же самий час.

Мобільні працівники часто використовують свої комп'ютери в переповненому людьми середовищі: у транспорті, в аеропортах, ресторанах.

Якщо співробітники використовують PDA,необхідно включити в політику безпеки вимоги щодо їх використання.

Реверсивна соціальна інженерія описує ситуацію, в якій адресат або адресати пропонують хакеру інформацію, яку вони хочуть продати. Такий сценарій може здаватися маловірогідним, але користувачі, що володіють відповідними технічними або соціальними повноваженнями, часто одержують особисту інформацію інших користувачів *(ідентифікатори і паролі), тому вони можуть потрапити під підозру.*

Захист від реверсивної соціальної розробки, ймовірно, найважчий. Адресат не має ніякої причини підозрювати хакера, оскільки вважає, що вони знаходяться в одній команді. Головний захист - угода у вашій політиці захисту, що всі проблеми повинні бути вирішені через сервісну службу. Якщо співробітники служби підтримки ефективні, ввічливі, і не суб'єктивні, інші службовці довірятимуть їм і не шукатимуть допомоги у сторонніх людей.

Висновки:1. Створення політики безпеки захисту інформації від несанкціонованого доступу э необхідною складовою загальної справи підприємства; 2. Підтримка розуміння необхідності забезпечення безпеки повинна виходити від кожного працівника. 3. Технічний контроль захисту інформації від атак соціальної інженерії можливо здійснювати без знання працівників підприємства, але необхідно заручатися їх підтримкою.

Список літератури

1. *Кузнецов М.,* Симдянов И. Социальная инженерия и социальные хакеры. - БХВ-Петербург, 2007.
2. *Митник К.*, Саймон В. Искусство обмана. Киев: Компания «Ай-ти», 2004.
3. Суименко Э.И. Социальная инженерия: к вопросу в научном статусе//Социологическая наука и образование в Украине. - Выпуск №1., - Киев: МАУП., 2000.
4. *Подшивалкина В.И.,* Лукашевич М.П., Суименко Э.И., Каменская Т.Г. Макро-и микросоциальная инженерия. Социоинженерний практикум. - Одесса, 2001.

Надійшла 03.01.2009