УДК 004.056.5

СОЦІАЛЬНА ІНЖЕНЕРІЯ: ПОНЯТТЯ, ВИДИ ТА МЕТОДИ ПРОТИДІЇ

Нороха В. О., студ. гр КБ-181
Науковий керівник: **Ткач Ю. М.,** д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Соціальна інженерія – це наука, що вивчає людську поведінку та фактори, які на неї впливають.

Основною метою соціальної інженерії є:

- дослідження причин тої чи іншої поведінки людини;
- обставин та середовища, що впливають на формування системи цінностей індивіду, і як наслідок – їх поведінки.

На базі цих досліджень можна визначити, що саме спонукає людину на конкретну дію

Наприклад: вивчення середовища, в якому жив вбивця, допоможе зрозуміти його систему цінностей. Ця інформація надасть можливість розробити соціальну структуру, в якій будуть формуватись інші системи цінностей. Системи цінностей, у яких насамперед буде цінуватись людське життя та індивідуальність.

Термін «соціальна інженерія» як акт психологічної маніпуляції також пов'язують із суспільними науками, однак він широко використовується серед спеціалістів з комп'ютерної та інформаційної безпеки.

Методи несанкціонованого доступу до інформації можна умовно поділити на дві категорії: з використанням методів соціальної інженерії та без них. На відміну від другого випадку, коли зловмисник повинен володіти знаннями у галузі ІТ, у першому для отримання конфіденційних даних він спирається на знання з соціології та психології.

Психологічною передумовою застосування методів соціальної інженерії є така особливість людської психіки, як когнітивні упередження. Через це надійність комп'ютерної системи є не вищою, ніж надійність її оператора. Зловмисники проникають навіть у добре спроектовані, захищені комп'ютерні системи, скориставшись неуважністю довірених користувачів або умисно вводячи їх в оману (наприклад, відрекомендувавшись системним адміністратором або амбасадором комерційного бренду, надсилають повідомлення із запитом паролів).

Існують різні типи кібератак, наприклад, уведення шкідливого коду у код веб-сайту або застосування шкідливих програм (вірусів, троянів тощо). Атаки такого виду перешкоджають керуванню пошкодженим продуктом або його налагодженню. Що ж стосується соціальної інженерії, то цей тип атак спрямований не безпосередньо на комп'ютерну систему, а на її користувачів – «найслабшу ланку», і шляхом обходу інфраструктури, призначеної для захисту від шкідливих програм, він дозволяє досягти тих же результатів, що й інші види кібератак. Оскільки такі прийоми значно складніше виявити чи запобігти їм, цей напрям атак є набагато ефективнішим за інші.

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). Претекстинг у Великій Британії також використовується термін blagging, полягає у застосуванні заздалегідь розробленого сценарію (приводу, чи претексту), щоб спонукати вибрану жертву до розголошення інформації чи виконання дій, до яких у звичайних обставинах вона не вдалася б. Оскільки цей метод ґрунтується на спланованій схемі обману, то атакуванню передує збір інформації, необхідної шахраєві для того, аби видати себе за іншу особу (з'ясування дати народження, паспортних та інших ідентифікуючих даних, суми останнього рахунку тощо), щоб у жертви не виникло сумнівів у законності дій шахрая.

Фішинг – це метод заволодіння інформацією приватного характеру обманним шляхом. Зазвичай фішер надсилає електронний лист начебто від імені офіційної установи – банку чи

платіжної системи – із запитом про «верифікацію» інформації та попередженням про настання певних негативних наслідків у разі невиконання зазначених вимог. Такий лист, як правило, містить посилання на підробну веб-сторінку, схожу на справжню (із логотипами компанії, аналогічним контентом та ін.), де від користувача вимагається ввести у форму особисті дані, від домашньої адреси до PIN-коду банківської платіжної картки.

Телефонний фішинг – це один з найстаріших методів соціальної інженерії. Телефонний зв'язок забезпечує унікальні можливості для проведення соціотехнічних атак і є звичним і знеособленим засобом спілкування, оскільки жертва не може бачити зловмисника. Основні цілі таких атак:

– запит інформації, яка забезпечує доступ до самої телефонної системи або дозволяє отримати віддалений доступ до комп'ютерних систем;

– отримання можливості здійснювати безкоштовні дзвінки:

– отримання доступу до комунікаційної мережі.

Запит інформації чи доступу по телефону є порівняно безпечним видом атаки для зловмисника. Якщо жертва починає підозрювати щось чи відмовляється виконувати запит, зловмисник завжди може покласти трубку.

Метод атаки «Дорожнє яблуко» схожий на дію троянської програми. Зміст атаки в тому, щоб підкинути співробітнику компанії фальшивий фізичний носій інформації (флеш-накопичувач, тощо). Носій має виглядати як офіційний, мати логотип чи надпис, що зацікавить співробітника, наприклад флеш-накопичувач з надписом «заробітна плата 2017–2018». Якщо співробітник вставить такий носій до комп'ютеру, що має зв'язок з корпоративною мережею підприємства, запускається шкідливий код і зловмисник отримує доступ до одного комп'ютера чи до усієї мережі.

Пошук інформації в смітті. Варто дотримуватися правил утилізації паперового сміття та електронних носіїв інформації, особливо якщо це стосується конфіденційної та корпоративної, закритої чи відкритої інформації. Міри безпечної утилізації стосуються і електронних офісних пристроїв.

Індивідуальні підходи. До індивідуальних підходів можна віднести як негативні стратегії, так і позитивні. Є наступні підходи: залякування (зловмисники, які обрали цю стратегію, примушують жертву виконати запит за допомогою шантажу або видачі себе за іншу особу), переконання, виклик довіри.

Зворотня соціотехніка. Соціотехніка – цей термін використовується для позначення шахрайських дій, спрямованих на отримання інформації, яка дає змогу проникнути до певної системи та даних, що в ній знаходяться. Соціотехніка зазвичай є грою зловмисника на довірі людини. Захист від атак, заснованих на зворотній соціотехніці, є досить важким. У жертви немає підстав підозрювати зловмисника у чомусь, оскільки при таких атаках створюється враження, що ситуація знаходиться під її контролем.

Соціальна інженерія є багатогранним і складним способом отримання конфіденційної інформації від користувачів із застосуванням методів переконання і технологічних засобів. Будь-яка людина в сучасному світі є вразливою до соціальної інженерії, а отже, повинна залишатися постійно в курсі того, з ким вона взаємодіє як в режимі онлайн, так і віч-на-віч. Завдяки підвищенню розпізнавання недостовірної інформації та спроб обдурити користувачів у розголошенні секретної інформації компанія та її співробітники зможуть підтримувати безпечне середовище не тільки для себе, а й для клієнтів та власних активів.

Поняття соціальної інженерії було введено Кевіном Митником і досить часто згадується в ряді статей та доповідей з тематики безпеки мереж та інформації. Статистика демонструє, що велика кількість людей ставиться до використання власної конфіденційної інформації недостатньо уважно. Для прикладу можна розглянути вибір складності паролів, обставини доступу до онлайн-рахунку в банку; також яскравим прикладом є необережність при вході в соціальні мережі. Поняття паролю і таємного (секретного) запитання здається тривіальним для більшості користувачів, хоча недооцінювати їх значення не можна.

Для того, щоб захистити себе, експерти з кібербезпеки пропонують почати зі встановлення якісної антивірусної програми, яка допомагатиме, наприклад, у спробах виявлення фішингу.

Також завжди слід бути пильним щодо джерела, яке запитує конфіденційні дані. Банк, наприклад, навряд чи буде телефонувати, щоб дізнатися код на зворотному боці картки.

Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд.

Якщо людину просять ввести особисті дані – краще окремо зайти на сайт компанії, наприклад, банку. Ще краще – зателефонувати на офіційний номер установи для уточнення інформації.

Варто також критично ставитися до отриманих повідомлень: наскільки правдоподібною може бути інформація про те, що принц із Саудівської Аравії міг залишити вам спадщину?

Не слід також забувати і про сповіщення про такі небезпеки інших членів сімей. Адже часто літні люди, наприклад, можуть не знати про те, що розголошення CVV-коду банківської картки може призвести до викрадення грошей.

Наскільки б банальний вигляд не мали методи соціальної інженерії у сучасному цифровому світі, люди все ще продовжують потрапляти на її «гачок».

Список використаних джерел

1.«Соціальна інженерія: як шахраї використовують людську психологію в інтернеті» - https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html

2.«Соціальна інженерія (безпека)» - https://uk.wikipedia.org/wiki/%D0%A1%D0% BE%D1%86%D1 %96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5 % D1%80%D1%96%D1%8F_(%D0%B1%D0%B5%D0% B7%D0%BF%D0%B5%D0%BA%D0%B0)

УДК 004.056.5

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРЗАХИСТУ

Кузьмина В. І., Стародубець І. О., студ.гр. КБ-171,
Ткач Ю. М., д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Із широким впровадженням хмарних і мобільних технологій світ зробив об'єкт кібербезпеки нескінченно складним. Крім того, збільшення кількості точок доступу і удавана відсутність виснажливості сучасних хакерів означає, що потреба в створенні адекватних заходів безпеки мережі ніколи не була більш важливою. Утримати попит, як мінімум, складно. Штучний інтелект виявляється ідеальним рішенням.

В контексті інформаційної безпеки штучний інтелект (artificial intelligence, AI) - це ПЗ, здатне інтерпретувати стан середовища, розпізнавати події, які відбуваються в ньому, і самостійно вживати необхідні заходи. AI особливо добре справляється з розпізнаванням закономірностей і аномалій, тому може бути прекрасним інструментом виявлення загроз.

Одна з конкретних областей, в яких кібербезпека, заснована на AI, може збільшити людські IT-команди, - це використання аналітики передбачення. При цьому технологія використовує і старі, і нещодавно розроблені дані. По суті, це може полегшити активний, а не реактивний підхід до мережевої безпеки. Для тих неминучих випадків, коли загрозам вдається пройти, інтелектуальна автоматизація може допомогти у своєчасному та ефективному виявленні, викоріненні і усуненні порушень.

На сьогоднішній день в компаніях вже почали користуватися штучним інтелектом для розпізнавання загроз безпеки і реагування на них.

Зокрема, AI застосовують для виявлення ознак компрометації систем в локальній мережі і в хмарному середовищі. При цьому необхідна обробка гігантських обсягів даних, а в зв'язку з швидкою зміною світового ландшафту загроз, для протистояння їм необхідні найпередовіші технології та методи.