УДК 004.056

СВІТЛИЧНИЙ Віталій Анатолійович,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3381-3350

ДЕЯКІ КОНЦЕПЦІЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Інформаційні технології стрімко розвиваються, з'являється величезна кількість сервісів та додатків, у тому числі й у складі критичної інфраструктури, що особливо важливо в умовах військового стану. Натомість підвищуються різні ризики, зокрема ризики пов'язані з використанням зловмисниками соціальної інженерії. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист вид кіберзлочинців. [1]

Соціальна інженерія запозичує більшість своїх концепцій із психології, на відміну від традиційної інформаційної безпеки, яка використовує концепції з інформатики, системного адміністрування, програмування та адміністрування баз даних. З цієї причини кіберполіцейські, що розслідують кіберзлочини повинні добре розумітися у психології людській поведінці, тобто бути фахівцями в галузі соціальної інженерії.

Розглянемо деякі основні психологічні концепції, які широко застосовуються зловмисниками для соціальної інженерії.

Найбільш популярною є концепція впливу. Вплив – це нейтральний термін, що означає діяльність людини, яка спонукає інших до певного результату. Вплив може бути позитивним чи негативним. Прикладом впливу може бути лікар, який розмовляє з пацієнтом про його стан здоров'я, зміни в способі життя, які він повинен зробити, та ризики, з якими він стикається, щоб надихнути пацієнта вести здоровіший спосіб життя.

Не менш популярною концепцією є маніпуляція. За межами світу психології люди зазвичай не бачать різниці між маніпуляцією та впливом. Але серед фахівців ці терміни мають різні значення. Маніпуляція – це згубний вплив, зазвичай спрямований на заподіяння шкоди. У соціальній інженерії як зловмисники, так і благонамірені пентестери часто використовують маніпуляції замість впливу через недостатню підготовку чи з недомислу.

Наступна концепція – порозуміння, взаємна довіра. Більшість словників визначають взаєморозуміння як «дружні, гармонійні відносини» і додають, що такі відносини зазвичай «характеризуються угодою, взаємною довірою чи співпереживанням, які роблять спілкування можливим чи легким».

Американська психологічна асоціація (АПА) ґрунтується на цьому визначенні, кажучи, що «встановлення взаєморозуміння з клієнтом у психотерапії часто є важливою проміжною метою для лікаря, щоб полегшити та поглибити терапевтичний досвід та сприяти оптимальному прогресу та покращенню». Як і психотерапевти, зловмисники від соціальної інженерії намагаються встановити контакт зі своїми об'єктами для завоювання їхньої довіри. Щоб побудувати взаєморозуміння,

вони часто покладаються на загальний досвід (реальний чи вигаданий), грають на користь жертви та підкреслюють власні риси характеру. При цьому зловмисники широко використовують інструменти OSINT, щоб дізнатися про симпатії та антипатії жертви.

Далі розглянемо особливості концепції впливу. Прийнято виділяти сім основних принципів впливу на людей, а саме: авторитет; привабливість; терміновість та дефіцит; сталість та послідовність; соціальний доказ; взаємність.

Авторитет. Люди схильні робити певні дії, коли хтось, наділений владою, просить їх про це або коли їх змушують повірити (правдиво чи під хибним приводом), що таку саму дію робить авторитетна особа. Наприклад, зловмисники використовують у вишингу посилання на авторитети. Тобто вони повідомляють жертві соціальної інженерії, що діють за розпорядженням генерального директора, директора з інформаційної безпеки або відповідно до визначеного закону України. У будь–якому разі жертва переповнюється почуттям своєї значущості, і її подальша обробка стає дуже ефективною.

Привабливість. Люди, як правило, прагнуть допомогти тим, кого вважають милим та привабливим. Ви колись зустрічали продавця, який хоча б не намагався виглядати приємною людиною? Швидше за все, він буде робити вам компліменти щодо одягу, зовнішності та інтелекту, щоб завоювати вашу прихильність.

Терміновість та дефіцит. Якщо є ризик, що людина чогось не отримає, вона починає хотіти цього набагато сильніше. Наприклад, рекламні акції інтернет магазинів, сайтів і т.і. Наприклад, в у процесі реєстрації на сторінці сайту з'являється таймер, який попереджає про те, що залишилося кілька хвилин, щоб завершити процедуру, інакше людина буде виключена зі списку пільгових клієнтів. Таймер дає потенційним клієнтам штучне обмеження за часом та гостре відчуття, що вони втратять щось важливе, якщо не діятимуть швидко.

Займаючись фішингом, зловмисники заявляють, що продають чи роздають щось таке, чого є лише невелика кількість [2]. Щоб спокусити жертву діяти, будь то перехід за посиланням або введення інформації, вони пропонують щось цінне в угоді, яка надто хороша, щоб бути правдою, але із застереженням, що жертва має діяти в найкоротший термін. В інших випадках зловмисник може спробувати змусити заплатити викуп за свою програму–вимагач, виділяючи жертві лише кілька годин на оплату, перш ніж безповоротно видалити, вкрасти чи оприлюднити дані, незалежно від того, чи збирається він виконати загрозу.

У будь–якому разі зловмисник сподівається налякати жертву та змусити її діяти до того, як вона встигне все обміркувати. Як приклад можна навести ситуацію коли зловмисники обдзвонюють клієнтів під виглядом служби підтримки стільникових операторів і повідомляють нібито про злом особистого кабінету абонента або телефону. Для «запобігання» розповсюдженню особистих даних або припиненню несанкціонованого переказу коштів, зловмисники просять набрати на телефоні спеціальну USSD – команду , що складається з комбінації цифр та символів, що вводяться під час дзвінка, та номера телефону. Таким чином абонент самостійно змінює налаштування своєї SIM – картки та встановлює переадресацію SMS та дзвінків на номер зловмисника. Потім жертві знову можуть зателефонувати та повідомити про усунення проблеми зі зломом, а насправді

зловмисники отримують коди з повідомлень і можуть викрасти гроші з рахунків у банку, отримавши доступ до особистого кабінету банку.

Постійність та послідовність. Люди цінують постійність і здебільшого не люблять змін. Зловмисники від соціальної інженерії іноді залишаються послідовними, а іноді порушують постійність та послідовність, щоб впливати на жертву. Простий приклад із життя: продавець може стверджувати, що більш зацікавлений в успіху свого клієнта, ніж у комісійних, говорячи щось на кшталт: «Я завжди дбав про своїх клієнтів. Я розумію ваші потреби з першого дня співпраці. Я завжди працюю з вами за принципом "що обіцяно, те й зроблено"». Цей прийом є особливо поширеним серед продавців, успіх яких залежить від міцних довгострокових відносин.

Соціальний доказ. Суспільство вимагає від нас "не відставати від сусіда". Іншими словами, ми часто робимо щось виключно тому, що решта вважає це нормальним, статусним. Зловмисник переконує свою жертву в тому, що певна поведінка чи дія підвищує соціальний статус, що всі інші ефективні співробітники виконують певну дію. Переконання співрозмовника у бажаності чогось називається соціальним доказом.

Простий приклад із життя: продавець автомобілів може спробувати вмовити вас купити розкішну машину, сказавши, наприклад, що на ній їздять успішні люди вашого віку.

Зловмисник може вигадати соціальний доказ, використовуючи інформацію, отриману з OSINT. Наприклад, він може визначити, хто у компанії є впливовою особою. Потім надішле вам електронний лист, стверджуючи, що розмовляв з авторитетною людиною, яка захоплено відгукувалася про вас і надала контактну інформацію, щоб ви допомогли «вирішити проблему».

Взаємність. Погодьтеся, ми охоче допомагаємо людям, які допомогли нам. Часто пентестери допомагають комусь, а потім просять зробити щось натомість (і не завжди це на користь того, хто допомагає).

Симпатія чи емпатія. Відмінним способом встановити взаєморозуміння є прояв симпатії – це турбота про людину, яка відчуває себе погано або відчуває стрес, наприклад, після втрати коханої людини або домашньої тварини.

На відміну від симпатії, емпатія – це здатність відчувати ті ж почуття, що й інші люди, начебто ви опинилися на їхньому місці. Емпатія означає загальні емоції чи погляду, тоді як вона висловлює співчуття і турботу з вашого боку. Те й інше важливо задля встановлення взаєморозуміння за певних обставин. Зловмисники вміють висловлювати свої почуття і розуміють почуття жертви, мають можливість впливати і розуміють, коли заходять надто далеко (жертва може зісковзнути з гачка). Взаємодіючі з жертвою, зловмисник охоче поділитися історією (реальною або вигаданою) про схожу ситуацію, в якій опинилася його жертва. Це дозволить жертві проявити зустрічне співчуття до ситуації, розказаної зловмисником, та покращить взаєморозуміння. Як альтернатива, якщо хтось розповідає про ситуацію, до якої зловмисник не має жодного відношення, то він просто задає уточнюючі питання, а потім заявляє, що дуже шкодуєте про те, що це сталося, висловлюючи таким чином співчуття своїй жертві [3].

Резюмуючи сказане вище, відзначимо, що зловмисники постійно удосконалюють існуючі, вигадують нові концепції соціальної інженерії. Єдиний спосіб

уникнути грошових втрат при зустрічі з зловмисниками, це критично сприймати будь – які пропозиції, перевіряти ще раз інформацію і ніколи не поспішати при прийнятті фінансових рішень. Обов'язково дотримуйтесь базових правил фінансової безпеки:

1. Нікому ні в якому разі не повідомляйте повні реквізити банківської картки, включаючи тризначний код зі зворотного боку; а також ПІН–коди та паролі із СМС від банку [4].

2. Не переходьте за сумнівними посиланнями з повідомлень і не переказуйте незнайомцям гроші на першу вимогу.

3. Не зберігайте багато грошей на карті, якою розплачуєтесь в інтернеті: кладіть тільки ту суму, яку збираєтеся витратити зараз. У цьому випадку, навіть якщо шахраї спробують вкрасти гроші, їм не вдасться вивести дуже багато.

4. Отримавши раптовий дзвінок із будь–якої фінансової організації з терміновим питанням або пропозицією, покладіть слухавку і зателефонуйте туди самі, знайшовши номер на офіційному сайті [4]. Набирайте номер вручну. Якщо з вами зв'язалися з компанії, клієнтом якої ви не є, спершу перевірте її за довідником фінансових організацій.

5. Не погоджуйте відразу ні на які «привабливі пропозиції» – чи то «вигідний кредит», чи грошова допомога. Дайте собі час на роздуми, порадьтеся зі знайомими, дізнайтесь в інтернеті інформацію про подію та поцікавтеся відгуками, коментарями.

Список використаних джерел

1. Світличний В.А. Застосування методів соціального інжинірингу при розслідуванні кіберзлочинів. Збірник тез доповідей щорічної Всеукраїнської науково–практичної конференції «Актуальні питання протидії кіберзлочинності та торгівлі людьми». Харків. ХНУВС. 2017. 2017. С.159–161.

2. Світличний В.А. Деякі особливості кібератак за допомогою адресного фішингу, клон – фішингу та уейлінгу. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. наук.–практ. конф. (27 травня 2022 р., м. Харків). Харків. ХНУВС. 2022. С. 98–101.

3. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/socialna–inzhenerija–shaxrajstvo/29460139.html (дата звернення: 19.04.2023).

4. Финансовая культура. *Финансовая культура*. URL: https://fincult.info/article/sotsialnaya–inzheneriya–pochemu–lyudi–sami–otdayut–moshennikam–dengi/ (дата звернення: 19.04.2023).

Одержано 20.04.2023