Трокоз Є. М., ст. викладач,
Таргонський О. В., магістрант
Державний університет «Житомирська політехніка»

СУЧАСНІ ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Час не стоїть на місці. Глобальна всесвітня комп'ютеризація зіткнулася з глобальною кіберзлочинністю. Міжнародні експерти стверджують, що кожне третє злочинне діяння у світі відбувається у віртуальному світі. Одним із найнебезпечніших типів атак є соціальна інженерія.

Соціальна інженерія (у контексті інформаційної безпеки) – це наука, яка вивчає методи та фактори впливу на людську свідомість та її переконання. У контексті кібербезпеки – соціальна інженерія є одним з найнебезпечніших типів атак та серйозною загрозою інформаційній безпеці. Метою соціальної інженерії є спонукання людей робити певні дії, які вони за звичних умов ніколи б не вчинили. Американський консультант з комп'ютерної безпеки, письменник Кевін Митник, а в минулому один із найвідоміших у світі комп'ютерних хакерів, стверджував, що «зламати людину набагато простіше, ніж комп'ютер, оскільки комп'ютери дотримуються інструкцій, а люди піддаються емоціям» [1].

Кіберзлочинці знаходять все нові і нові способи експлуатації людського фактору. Найпоширенішими є повідомлення про терміновість порятунку рідної людини, про проблеми із банківською карткою і т.д. Маніпулювання людською свідомістю відбувається настільки професійно, що жертва стає співавтором виконання задумів злочинців (особливо зараз, коли ми знаходимося у стані війни та психіка громадян надзвичайно травмована). Тому для ефективного захисту від атак кіберзлочинців надзвичайно важливо володіти знаннями про психологічні підходи, якими вони володіють, та про сучасні інструменти та технології, які вони використовують.

Відомий психолог Роберт Чалдіні виділив шість психологічних прийомів, на яких базується весь арсенал інструментарію та технологій соціальної інженерії, а саме: взаємність (людина намагається відповісти добром на добро, послугою на послугу, щоб не бути у «боргу»); послідовність (хакер спочатку провокує жертву розкрити малий обсяг інформації та, користуючись принципом «послідовності», досягає своєї мети); конформізм (людина погоджується з тим, що робить більшість); авторитет (людині притаманно слідувати за тими, кому вона довіряє, кого знає, хто для неї є авторитетом); симпатія (людина охочіше та швидше виконує прохання тих, хто їй симпатичний, або зробить те, що їй подобається); дефіцит (людина завжди більше бажає того, що їй недоступно) [2].

В залежності від поставленої мети зловмисника, використовуються і відповідні інструменти та технології соціальної інженерії. Фішинг – найпопулярніший сучасний інструмент соціальної інженерії. Зловмисник надсилає електронний лист або інше повідомлення, яке містить посилання на підроблений веб-сайт. Жертва переходить за посиланням, вводить свої облікові дані або іншу конфіденційну інформацію, яка потім може бути використана для злому її облікового запису. Вішинг – телефонне шахрайство, метою якого є отримання реквізитів банківських карток або будь-якої іншої конфіденційної інформації. Смішинг – використовуються текстові SMS-повідомлення, які містять шкідливі посилання або вміст. Претекстинг – вид атаки, який передбачає використання голосових засобів, таких як Skype, телефон і т.п. Попередньо проводиться збір персональних даних жертви. Підманювання – зловмисники використовують привабливі пропозиції або стимули, щоб заманити жертву в пастку. Соціальна інженерія на основі штучного інтелекту – вид атаки, в якому зловмисники використовують штучний інтелект для створення більш реалістичних і ефективних атак соціальної інженерії [3].

Таким чином, соціальна інженерія є досить актуальною проблемою, яка впливає на людську свідомість. Сценарії, за якими працюють шахраї, є досить різноманітними. Атаки соціальної інженерії можуть бути спрямовані на отримання фінансової вигоди, отримання конфіденційної інформації, нанесення збитків, можуть мати політичні мотиви та ін. Важливо розуміти, що атаки соціальної інженерії можуть стати загрозою для будь-якої особи або організації, незалежно від їх статусу чи потреб.

Список використаних джерел

1. Mitnick, Kevin, and William L. Simon. The Art of Deception: Controlling the Human Element of Security. Wiley, 2002. – 368 p.

2. Cialdini R.B. Influence: The psychology of persuasion / Robert B. Cialdini. – New York: Harper Business, HarperCollins Publishers, 2007. – 322 p.

3. Social engineering attack techniques. URL: https://www.imperva.com/learn/application-security/social-engineering-attack/